НАО «Алматинский Университет Энергетики и Связи
имени Гумарбека Даукеева»

БАКИРОВ АХАТ СЕРІКҰЛЫ

Разработка теоретических основ методов противодействия современным формам информационной войны

6D071900 – Радиотехника, электроника и телекоммуникации

Диссертация на соискание степени
доктора философии PhD
в форме серии статей

Научный консультант:
доктор химических наук,
кандидат физико-математических наук,
профессор, академик И.Э. Сулейменов

Зарубежный научный консультант:
доктор философских наук,
профессор О.А. Габриелян

Республика Казахстан
Алматы 2026

АННОТАЦИЯ

диссертации на соискание степени доктора философии (PhD) по специальности «6D071900 – Радиотехника, электроника и телекоммуникации»

БАКИРОВА АХАТА СЕРІКҰЛЫ

Тема диссертационного исследования:

«Разработка теоретических основ методов противодействия современным формам информационной войны».

Цель диссертационного исследования:

Создание теоретико-алгебраических основ методов противодействия современным формам информационной войны, осуществляемых на уровне воздействия на социокультурный код.

Задачи исследования:

- Разработать метод приведения операций многозначной логики к алгебраическим выражениям для случая, когда не существует возможности установить однозначное соответствия между числом переменных многозначной логики и числом элементов поля Галуа, а также осуществить проверку данного метода с использованием электронных схем, реализуемых при помощи специализированных программных продуктов.
- Разработать алгоритм для последовательно-параллельного процессора, построенный на системе остаточных классов с использованием первых четырех квази-мерсенновских чисел, и осуществить проверку данного метода при помощи специально разработанных электронных схем.
- Разработать метод построения базисов цифровых ортогональных функций, позволяющих привести операцию вычисления цифровой свертки к вычислению парциальных сверток, каждая из которых отвечает определенному полю Галуа.
- Распространить метод нестандартных алгебраических расширений, основанный на использовании дополнительных формальных уравнений, на случай, отвечающий трехмерному пространству, с использованием приводимых алгебраических уравнений.
- На основе обобщающего анализа современных форм информационной войны и прогнозов в данной области продемонстрировать что решение задач, связанных с противодействием современным формам информационной войны, в том числе требует разработки новой алгоритмической основы вычислительной техники.

Предмет исследования – операции многозначной логики, цифровая свертка.

Методы исследования:

- методы абстрактной алгебры, в частности теория полей Галуа и теории конечных алгебраических колец;
- методы отработки электронных схем с использованием специализированных программных продуктов.

Основные положения, выносимые на защиту:

- метод приведения операций многозначной логики к алгебраическим выражениям с использованием алгебраической дельта-функции и операции цифрового логарифмирования, позволяющий корректно определять и компактно задавать эти операции в конечных полях;
- алгоритм для последовательно-параллельного процессора, построенный на системе остаточных классов с использованием первых четырех квази-мерсенновских чисел, который допускает реализацию в виде электронных схем;
- метод алгебраических расширений, который позволяет построить набор цифровых ортогональных функций, обеспечивающих приведение операции свертки к вычислению совокупности парциальных сверток, каждая из которых вычисляется в отдельном поле Галуа;
- метод нестандартных алгебраических расширений, основанный на использовании дополнительных формальных решений приводимых уравнений, распространенный на случай, отвечающий трехмерному пространству;
- демонстрация того, что решение задач, связанных с противодействием современным формам информационной войны, в том числе требует разработки новой алгоритмической основы вычислительной техники.

Основные результаты исследования:

Основным результатом диссертационной работы является формирование теоретико-алгебраических основ методов противодействия современным формам информационной войны, реализуемых на уровне воздействия на социокультурный код. В публикациях показано, что для эффективного противодействия на этом уровне требуются вычислительные модели, способные описывать не только технические сигнальные процессы, но и многозначные логические взаимосвязи, характерные для коллективного восприятия и трансляции информации. Обосновано, что переход от традиционной двоичной логики к многозначным алгебраическим структурам позволяет создать аппаратно-алгоритмические решения, обеспечивающие математическую базу для анализа и фильтрации информационных потоков с учётом их структурных и смысловых особенностей, связанных с процессами формирования и передачи социокультурных паттернов. Системная связь этих разработок с задачами противодействия на уровне социокультурного кода развернуто представлена в обзорной статье, где сформулированы

методологические основания и показана их применимость для решения соответствующих аналитических и технологических задач.

Конкретно, в результате проведенных исследований показано, что:

- решение задач, связанных с противодействием современным формам информационной войны, в том числе требует разработки новой алгоритмической основы вычислительной техники

- алгебраическая дельта-функция и построенная на ее использовании операция цифрового логарифмирования позволяет привести операции многозначной логики к алгебраическим выражениям в том случае, когда не существует возможности установить однозначного соответствия между числом переменных многозначной логики и числом элементов поля Галуа, а также осуществлена проверка данного вывода при помощи электронных схем, отработанных методами имитационного моделирования;

- последовательно-параллельный процессор, сопоставимый по разрядности с 16-ти разрядным двоичным процессором, может быть реализован на основе алгоритма, построенного на системе колец классов вычетов множества целых числе по первым четырем квази-мерсенновским числам.

- разработан метод построения базисов цифровых ортогональных функций, позволяющий привести операцию вычисления цифровой свертки к вычислению парциальных сверток, каждая из которых отвечает выполнению операций в определенном поле Галуа, причем доказано, что для построения таких базисов целесообразно использовать метод алгебраических расширений основных полей, а также показано, что данный метод позволяет привести анализ систем, описываемых цифровой сверткой, к описанию в терминах парциальных передаточных функций, каждая из которых также отвечает определенному полю Галуа.

- усовершенствован метод нестандартных алгебраических расширений, основанный на использовании дополнительных формальных решений приводимых уравнений, через распространение на случай, отвечающий трехмерному пространству, что позволяет построить дискретную координатную систему, в которой роль трех базисных векторов играют идемпотентные элементы кольца, получаемого нестандартным алгебраическим расширением.

Обоснование новизны, достоверности и важности полученных результатов, практическая ценность, рекомендации по использованию научных выводов:

Научная новизна. Впервые в диссертационной работе разработан комплекс алгебраических и аппаратно-алгоритмических методов цифровой обработки сигналов, применимых для задач противодействия современным формам информационной войны, в том числе при анализе процессов, затрагивающих социокультурный код общества. К числу новых научных результатов относятся:

1. Метод приведения операций многозначной логики к алгебраическим выражениям с использованием алгебраической дельта-функции и операции цифрового логарифмирования — позволяет корректно задавать и вычислять логические операции при отсутствии однозначного соответствия между числом переменных многозначной логики и размерностью поля Галуа.
2. Вариант операции цифрового логарифмирования, впервые предложенный для указанной задачи и проверенный схемотехнически на специализированных электронных схемах.
3. Алгоритм последовательно-параллельного процессора, построенный на системе остаточных классов с использованием первых четырёх квази-мерсенновских чисел, обеспечивающий аппаратную реализацию вычислений с производительностью, сопоставимой с 16-разрядным бинарным процессором.
4. Метод построения базисов цифровых ортогональных функций, позволяющий свести вычисление полной цифровой свёртки к совокупности парциальных свёрток, каждая из которых выполняется в своём поле Галуа; показано, что использование метода алгебраических расширений основных полей обеспечивает эффективное построение таких базисов.
5. Расширение метода нестандартных алгебраических расширений на трёхмерный случай, что позволило построить дискретную координатную систему, в которой роль базисных векторов играют идемпотентные элементы порождаемого кольца; такая система применима для обработки сигналов и анализа многомерных структур.

Важность и актуальность результатов. Современные формы информационной войны всё чаще нацелены на воздействие на социокультурный код общества — совокупность устойчивых ценностно-нормативных, языковых и символических паттернов, определяющих коллективное восприятие информации. В научной литературе и практике стратегических коммуникаций этот подход уже закрепился как важный уровень анализа наряду с когнитивным и техническим. Для разработки эффективных средств противодействия необходимо не только социально-гуманитарное осмысление феномена, но и строгие вычислительные модели, позволяющие формализовать процессы восприятия и передачи информации в среде, где бинарная логика оказывается недостаточной для описания сложных смысловых структур.

Именно поэтому в работе предложены методы приведения операций многозначной логики к алгебраическим выражениям и архитектуры цифровой обработки сигналов (в том числе RNS-процессор, ортогональные базисы парциальных свёрток и трёхмерные дискретные координатные системы), обеспечивающие возможность аппаратно-алгоритмического анализа и фильтрации информационных потоков на уровне семантических и культурно-

кодовых признаков. Такое сочетание технических решений напрямую отвечает заявленной цели — созданию теоретико-алгебраических основ методов противодействия современным формам информационной войны.

Практическая ценность

– На основе предложенного метода цифрового логарифмирования получен Патент РК № 36266 («Способ и устройство для умножения по модулю семь»), предназначенный для RNS-процессора из второго положения.

– Методы позволяют создавать цифровые процессоры и DSP-модули, работающие с многозначной логикой и парциальными свёртками, что сокращает количество умножений и повышает производительность при обработке сигналов и изображений.

– Полученные математические конструкции (ортогональные базисы, трёхмерные координатные системы) применимы в анализе сложных информационных потоков, распознавании паттернов, системах обработки изображений, UAV-навигации и могут быть использованы в технологиях аналитики и мониторинга в сфере информационной безопасности.

Достоверность результатов. Результаты подтверждены математическими доказательствами, имитационным моделированием и схемотехнической проверкой в CAD-системах. Все положения прошли апробацию в виде публикаций в рецензируемых международных журналах (Q1–Q2 Web of Science) и в патенте, что подтверждает воспроизводимость и значимость работы.

Рекомендации по использованию. Разработанные методы рекомендуется применять при проектировании RNS-вычислителей и DSP-устройств для цифровой обработки сигналов и изображений, в системах мониторинга и фильтрации информационных потоков, в исследованиях социокультурных паттернов и в образовательных платформах для формирования устойчивости к информационным атакам.

Соответствие направлениям развития науки или государственным программам:

Исследования выполнялись в соответствии с утвержденным планом исследований МНВО РК и в рамках научных проектов AP14870281 «Разработка новых подходов к цифровой обработке изображений с использованием сверточных нейронных сетей» (2022-2024), «Жас ғалым» AP 15473354 «Разработка нейросетевых алгоритмов макроскопического управления системами на основе гидрофильных полимеров» (2022-2024), AP23490107 «Разработка теоретико-информационных методов описания преобразователей волновых сигналов на основе использования конечных алгебраических структур» (2024-2026), AP26104635 «Разработка новых информационных технологий на основе формализации диалектической логики» (2025-2027).

Структура диссертационной работы, представленной в виде серии статей, опубликованных соискателем.

Диссертационная работа представлена в виде серии статей:

1. Suleimenov I. E., Vitulyova Ye.S., Kabdushev Sh.B., **Bakirov A.S.** Improving the efficiency of using multivalued logic tools: application of algebraic rings //Scientific Reports. – 2023. – Т. 13. – №. 1. – С. 22021. https://doi.org/10.1038/s41598-023-49593-1 **Q1 Web of Science JCR**. (Вклад соискателя – вместе с научным консультантом соискатель разрабатывал математический аппарат, участвовал в постановке задач и обсуждении результатов).

2. Shaltykova D., Vitulyova, Y. S., **Bakirov A.S.,** Suleimenov I. E. Formation of Periodic Mosaic Structures Using Operations in Galois Fields //Symmetry. – 2025. – Т. 17. – №. 9. – С. 1415. https://doi.org/10.3390/sym17091415 **Q2 Web of Science JCR.** (Вклад соискателя – соискатель разрабатывал вариант алгоритма и исследовал его применение, участвовал в обсуждении математических выводов с соавторами).

3. Kadyrzhan A., Kadyrzhan, K., **Bakirov, A.,** Suleimenov, I. Prospects for the Use of Quasi-Mersen Numbers in the Design of Parallel-Serial Processors //Applied Sciences. – 2025. – Т. 15. – №. 2. – С. 741. https://doi.org/10.3390/app15020741 **Q1 Web of Science JCR.** (Вклад соискателя – соискатель внёс основной вклад в создание алгоритмических решений, а также в анализ схемных характеристик).

4. Kadyrzhan A., **Bakirov A.S.,** Shaltykova D.B., Suleimenov I. E. Application of the Algebraic Extension Method to the Construction of Orthogonal Bases for Partial Digital Convolutions //Algorithms. – 2024. – Т. 17. – №. 11. – С. 496. https://doi.org/10.3390/a17110496 **Q2 Web of Science JCR.** (Вклад соискателя – соискатель принимал ключевое участие в разработке метода, а также в анализе математических свойств метода).

5. Suleimenov I. E., **Bakirov A.S.** Prospects for Using Finite Algebraic Rings for Constructing Discrete Coordinate Systems //Symmetry. – 2025. – Т. 17. – №. 3. – С. 410. https://doi.org/10.3390/sym17030410 **Q2 Web of Science JCR.** (Вклад соискателя – соискатель разрабатывал математическую модель и участвовал в интерпретации результатов).

6. **Bakirov A.S.,** Suleimenov I. E. Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare // Computers. – 2025. – Т. 14. – №. 10. – С. 410. https://doi.org/10.3390/computers14100410 **Q2 Web of Science JCR.** (Вклад соискателя – соискатель инициировал и подготовил основную часть обзорного исследования, сформулировал структуру разделов и синтезировал результаты предыдущих работ, участвовал в редакции и методологическом обсуждении с консультантами).

Также в рамках выполнения диссертационной работы был получен патент:

1. Пат. 36266. Способ и устройство для умножения по модулю семь /Сулейменов И.Э., Мун Г. А., Кабдушев Ш.Б., Байпакбаева С.Т., Витулёва

Е.С., Бакиров А.С.; опубл. 16.06.2023. (Вклад соискателя – вместе с научным консультантом соискатель предложил идею и принимал участие в разработке принципа работы устройства, внёс вклад в схемные решения и подготовку патентной документации).

Первое выносимое на защиту положение было доказано в статьях 1,2. Второе положение было доказано в статье 3. Третье положение было доказано в статье 4. Четвертое положение было доказано в статье 5. Пятое выносимое на защиту положение было доказано в статье 6. Также статья 6 является обзором, который с одной стороны является литературным обзором по тематике, а с другой обосновывает и подчеркивает вклад статей 1-5 в разработку теоретических основ в проблематике информационных войн. Патент № 36266 основан на применении операции цифрового логарифмирования из положения 1 и реализует аппаратный множитель mod 7 в архитектуре RNS-процессора из положения 2.

В статье 6 соискатель является первым автором, во всех остальных (1-5) является автором для корреспонденции. Все статьи (1-6) удовлетворяют требованиям пункта 5-1 «Правил присуждения степеней».

scientific reports

Check for updates

OPEN

Improving the efficiency of using multivalued logic tools: application of algebraic rings

Ibragim E. Suleimenov[1], Yelizaveta S. Vitulyova[1], Sherniyaz B. Kabdushev[1] & Akhat S. Bakirov[2,3]✉

It is shown that in order to increase the efficiency of using methods of abstract algebra in modern information technologies, it is important to establish an explicit connection between operations corresponding to various varieties of multivalued logics and algebraic operations. For multivalued logics, the number of variables in which is equal to a prime number, such a connection is naturally established through explicit algebraic expressions in Galois fields. It is possible to define an algebraic δ-function, which allows you to reduce any truth table to an algebraic expression, for the case when the number of values accepted by a multivalued logic variable is equal to an integer power of a prime number. In this paper, we show that the algebraic δ-function can also be defined for the case when the number of values taken by a multivalued logic variable is p − 1, where p is a prime number. This function also allows to reduce logical operations to algebraic expressions. Specific examples of the constructiveness of the proposed approach are presented, as well as electronic circuits that experimentally prove its adequacy.

Multivalued logic has been developing quite actively in recent decades[1,2]. Various varieties of multivalued logics have been developed, in particular, paralogics[3], including paracomplete[4] and paraconsistent[5] logic. Closely related to them, multivalued algebraic structures of various kinds also attract the attention of researchers[6,7]. Works in the field of multivalued logic are also aimed at practical application, in particular, various kinds of computational and expert systems using multivalued logic are being developed[8,9]. There are reports in the literature in which multivalued logic is used to improve neural networks[10,11].

The application of multivalued logic to the construction of neural networks obviously also has a pronounced philosophical aspect[12,13]. Human thinking obviously cannot be reduced to binary logic it operates with such categories as modality, which obviously do not correspond to concepts built on the opposition "True–False". It is appropriate to emphasize that it was precisely the attempts to go beyond this opposition that led to the appearance of the pioneering works of Lukasevich[14] and Vasiliev[15], which gave rise to research in the field of multivalued logic. Moreover, as shown in[13], a fundamental feature of human thinking is the ability to lie, which is inseparable from any form of creativity. At a minimum, the human mind can operate with contradictions as well, which determines the increased interest in paracomplete[4] and paraconsistent[5] logics.

Philosophical understanding of the essence of intelligence is becoming more and more in demand due to the need to improve artificial intelligence (AI) systems[16,17]. As emphasized in[18], discussions about whether this system can be considered as artificial intelligence or not are pointless, since the essence of intelligence as such remains undisclosed.

The question of what kind of "logic" the human intellect operates on remains open. Moreover, there is every reason to believe that he can "switch" from one "logic" to another.

This makes even more relevant the question of how logics of various types are related to each other, as well as the question of whether one or another of them can be reduced to others. This issue is far from being completely resolved[19], but there is no doubt that the reduction of multivalued logics to algebraic form[20] can become an important tool for solving it.

Reducing the operations of multivalued logic to an algebraic form is also of interest from the point of view of improving fuzzy logic[21–23], since the variables of multivalued logic can be put in correspondence with the variables of fuzzy logic. This issue is also of interest from the point of view of using multivalued logic to improve neural

[1]National Engineering Academy of the Republic of Kazakhstan, Bogenbai Batyr Str. 80, 050010 Almaty, Kazakhstan. [2]Gumarbek Daukeyev Almaty University of Power Engineering and Telecommunications, Baytursynov Str. 126/1, 050013 Almaty, Republic of Kazakhstan. [3]Al-Farabi Kazakh National University, Almaty 050040, Republic of Kazakhstan. ✉email: axatmr@mail.ru

networks[24,25]. Non-binary logics are of interest from the point of view of bringing algorithms for the functioning of neural networks to an explicit form[26,27].

Reducing the operations of multivalued logic to algebraic form is most easily done when it is possible to establish a one-to-one correspondence between the values of the variables of multivalued logic and the elements of some Galois field. This is possible only for p^n-logics, where p is a prime number, n is an integer. As follows from the theory of Galois fields[28], such fields can contain only p^n elements, including zero.

We emphasize that the following result, obtained within the framework of classical mathematical logic operating with binary variables, is fundamental for modern computer technology. Any binary operation can be reduced to two others. This allows us to reduce all binary logic operations to addition and multiplication operations in the Galois field $GF(2)$. The algebraic δ-function defined in[18] makes clear the previously made conclusion that if the number of values that a logical variable can take is equal to p^n, where n is an integer and p is a prime number, then all operations of such logic can also be reduced to the operations of addition and multiplication over the Galois field $GF(p^n)$.

The question arises as to what kind of algebraic operations the operations of multivalued logics that do not satisfy the above criterion can be reduced to.

Examples of such logics are known they include six-valued ones[29], as well as ten-valued logic, which is of direct practical interest, since the decimal number system remains the most common.

In this paper, we show that the approach proposed in[20] can be generalized to the case when the number of values of multivalued logic variables is equal to $p-1$.

Specifically, an algebraic δ-function for this case can also be introduced into consideration. Examples of such logics discussed in this work are six- and ten-valued logic.

The tool for generating the algebraic δ-function for the cases under consideration is the transition from the use of algebraic fields to finite algebraic rings, which are already widely used in information technology[30,31].

It is significant that the operations of the above logics turn out to be irreducible to the operations of addition and multiplication in conjugate algebraic structures. In relation to logics complementary to Galois fields $GF(p-1)$, it is required to use the digital logarithm operation, as well as its inverse.

Thus, we show that there are examples of logics whose algebraization requires the use of a larger number of operations than is the case in classical cases.

Further, along with the reduction of multivalued logic operations to an algebraic form, it is also of interest to develop devices, including electronic devices that implement such or similar operations[32,33]. They are also of direct practical interest, for example, for the development of measuring equipment[34].

Electronic circuits that implement basic operations for the six-valued logic case, which is important, are also presented in this paper. Among other things, this also makes it possible to verify the conclusions and calculations made using simulation tools.

We also note that the issues under consideration are also important from the point of view of improving the methods of digital signal and image processing. As shown in[30,35,36], it is permissible to use functions that take values in Galois fields and/or algebraic rings to simulate digital signals. This allows you to move on to signal processing tools based on multivalued logic.

Section "Reduction of operations of -valued logic to algebraic form" shows that there is an explicit expression that converts $p-1$-valued logic operations to algebraic form.

Section "Visual demonstration of the connection between algebraic rings and algebraic fields" shows a visual connection between Galois fields containing p elements and algebraic rings containing $p-1$ elements.

Section "Digital logarithm operation for the field and its circuit implementation" discusses the digital logarithm operation, which establishes a connection between Galois fields containing p elements and algebraic rings containing $p-1$ elements, in relation to an important special case of six-valued logic. An electronic circuit is presented that ensures the performance of the corresponding operations. It is proved that six-valued logic can be reduced to (2,3)-logic by using the theory of algebraic rings.

Section "Modulo 6 multiplication algorithm and multiplier circuit" discusses specific electronic circuits that prove the constructiveness of the proposed approach, in particular, circuits that perform the multiplication operation for (2,3) logic, to which six-valued logic is reduced.

Reduction of operations of $p-1$-valued logic to algebraic form

One of very interesting (and far from being completely solved) problems, important for further development of information technologies based on multivalued logic, is the development of digital logarithm methods[37,38]. The operation of digital logarithm allows to reduce the operation of multiplication of two Galois field elements to the operation of addition, and the operation of magnification to the operation of multiplication.

As noted in the "Introduction", for multi-valued logics, complementary Galois fields $GF(p^n)$ (i.e. for the case when the number of values that a logical variable can take is equal to p^n, where p is a prime number, n is an integer), any logical operations can be reduced to addition and multiplication operations in a complementary Galois field. For the case when this condition is not met, it is necessary to expand the list of operations used to reduce logical operations to algebraic ones. In the case under consideration, such an additional operation is the operation of digital logarithm, as well as its inverse.

Recall that any element of the Galois field $GF(p)$ satisfies the equality

$$x^{p-1}=1. \tag{1}$$

Each nonzero element of the field can be represented as

$$x=\theta^n, n=0,1,\ldots,p-1, \tag{2}$$

where θ-primitive element.

By virtue of relations (1) and (2) we have

$$\theta^n\theta^m = \theta^{n+m,mod(p-1)}. \tag{3}$$

Ratio (3) shows that the operation of multiplication modulo p, can be reduced to the operation of addition modulo $p-1$. This, however, requires a numerical logarithm operation, i.e., finding an algorithm that allows one to set the number n to a given x.

This problem can be solved, for example, starting from the analogue of the Zhegalkin polynomial given in[20], which can be constructed as follows. The following expression may be treated as a logical analogue of the δ-function[20].

$$\delta_i(x) = 1 - (x - x_i)^{p-1}, \tag{4}$$

where x_i is a fixed element of the field $GF(p)$.

Indeed, due to expression (1), functions $\delta_i(x)$ have the following property

$$\delta_i(x) = \begin{cases} 1, x = x_i \\ 0, x \neq x_i \end{cases}. \tag{5}$$

Let us consider next polynomial

$$F(x,y) = \sum_{i,j=0}^{i,j=p-1} f(x_i,y_j)\delta_i(x)\delta_j(y), \tag{6}$$

where the values $f(x_i, y_j)$ form a truth table.

When a particular pair of x_{i_0}, y_{j_0} elements corresponding Galois field is substituted into expression (6), all summands appearing in the sum in the right part of formula (6) turn to zero except the summand for which $i = i_0, j = j_0$ is satisfied. Hence,

$$F(x_{i_0},y_{j_0}) = f(x_{i_0},y_{j_0}). \tag{7}$$

Expression (6), among other things, makes it possible to reduce any binary operation of multivalued logic to an explicit algebraic expression when the number of variables of this logic is equal to a prime number, i.e., the set of logic variables can be put into a one-to-one correspondence with the set of elements of a certain Galois field.

Similarly, an expression can be constructed that provides the digital logarithm operation.

Indeed, expression (6) is built based on a table reflecting a specific binary operation of multivalued logic. A similar table can be constructed explicitly for the digital logarithm operation. Indeed, for each specific θ one can specify a specific integer n that corresponds to a given element of the field x.

Formally, we can write

$$dl(x) = \sum_{i=1}^{i=p-1} dl(x_i)\delta_i(x), \tag{8}$$

where $dl(x)$ denotes the digital logarithm of the field element x.

However, notation (8) makes sense only insofar as the value $dl(x_i)$ is an element of the Galois field used. This means that this expression is useful only when there is an easy way to specify another correspondence between the integers n and the elements of the Galois field being used.

Obviously, this is easiest to do when the fields $GF(p)$ are used. In this case, each element of the field can be given a corresponding integer or zero.

We also emphasize that in formula (8) the lower summation limit is changed to 1, which corresponds to the fact that the digital logarithm of zero does not make sense. Six non-zero elements of the field $GF(7)$ are associated with six elements of the same field. This set includes 0 but does not include the element corresponding to the number 6.

It is easy to pass from expression (8) to an expression that is applicable for the algebraic description of multivalued logic operations, the number of variables in which is equal to $p-1$.

$$Q(x,y) = \sum_{i,j=0}^{i,j=p-2} Q(x_i,y_j)\delta_i\left(\theta^{n(x)}\right)\delta_j\left(\theta^{n(y)}\right). \tag{9}$$

In this expression, the "algebraic δ-function"

$$\delta_i(x) = 1 - \left(\theta^{n(x)} - \theta^{n(x_i)}\right)^{p-1}, \tag{10}$$

applied to the power of the primitive element θ, which uses the correspondence between multivalued logic variables and integers.

In the written expressions, in fact, a well-defined mapping of the field $GF(p)$ onto an algebraic ring, which contains $p-1$ elements, is actually used. Let's consider this connection in more detail. This, among other things, is usefull for the construction of electronic circuits that perform the digital logarithm operation.

Visual demonstration of the connection between algebraic rings and algebraic fields

The number p is prime, but the number $p-1$ is no longer prime. The only exception is the case of $p=2$, which is of no practical interest.

Hence, there are zero divisors in the ring of modulo $p-1$ deduction classes, and their existence is a clear sign that distinguishes rings from fields. Otherwise, calculations using the transition from an element $x=\theta^n$ to n, actually corresponds to transition from calculations in terms of an algebraic field to calculations in terms of an algebraic ring.

The functioning algorithm of the considered electronic circuits, discussed below and used to illustrate the proposed approach, is based on the well-known theorem from the theory of algebraic rings, according to which there are rings R, decomposing into a direct sum of ideals r_i

$$R = r_1 + r_2 + \cdots + r_n. \tag{11}$$

Each of these ideals is generated by idempotent elements e_i

$$r_i = Re_i, \tag{12}$$

which cancel each other out

$$e_i e_j = 0, i \neq j;\ e_i e_i = e_i, \tag{13}$$

and their sum is equal to one of the ring under consideration

$$\sum_i e_i = 1. \tag{14}$$

An example of such a ring is a ring obtained through a homomorphic mapping of a ring of integers to a ring of classes of deductions modulo 6 (this ring can be assigned to a set of six-valued logic variables). In this case any positive integer less than 6 can be represented as

$$u = 3 \cdot u_1 + 4 \cdot u_2, \tag{15}$$

where $u_{1,2}$ take the following values

$$u_1 = 0, 1;\ u_2 = 0, 1, 2. \tag{16}$$

It can be seen that in operations modulo 6 the elements of the ring of deduction classes appearing in (15) really act as idempotent elements, i.e., the following takes place

$$3 \cdot 3 = 9 \equiv 3(6), 4 \cdot 4 = 16 \equiv 4(6). \tag{17}$$

Moreover, these elements cancel each other out,

$$3 \cdot 4 = 12 \equiv 0(6), \tag{18}$$

and their sum modulo 6 is one

$$4 + 3 = 7 \equiv 1(6). \tag{19}$$

One can see that the ring of deduction classes under consideration is indeed an example of the fulfillment of relations (11)–(14). Moreover, this example emphasizes that the number of elements in the ideals into which the ring splits does not necessarily have to be the same.

The number 6 is the product of prime numbers 3 and 2, so the ideals generated by the idempotent elements correspond to Galois fields $GF(3)$ and $GF(2)$. They contain 3 and 2 elements, respectively, as relations (16) show.

Accordingly, formula (15) can be viewed as a representation of a number in binary ternary logic. In particular, instead of the notation (15) one can use its abbreviated version

$$u = u_1 u_2, \tag{20}$$

where numbers $u_1 u_2$ и $u_1 u_2$ are treated as analogues of decimal places (the analogy with the writing of decimal numbers is obvious).

Note also that formula (8) also allows us to represent all non-zero elements of Galois field $GF(7)$ in the following form

$$x = \theta^{3 \cdot u_1} \theta^{4 \cdot u_2} = g_1^{u_1} g_2^{u_2}. \tag{21}$$

where elements g_i are determined from the conditions

$$g_1^2 = g_2^3 = 1. \tag{22}$$

Elements g_i for the case in question can be chosen as follows

$$g_1 = 6;\ g_2 = 2, \tag{23}$$

which is proved by direct verification.

This choice is not the only one, in particular, one can put $g_2 = 4$.

The advantage of representation (15) is that the digit analogs can be handled independently. Indeed, consider the product modulo 6 of two numbers written in the form (15)

$$u = e_1 u_1 + e_2 u_2. \tag{24}$$

Considering that $e_{1,2}$ are idempotent elements and that the sets of variable values $u_{1,2}$ are isomorphic to the Galois fields generated by prime numbers $p_{1,2}$, we have

$$u^{(1)} u^{(2)} = e_1 u_1^{(1)} u_1^{(2)} + e_2 u_2^{(1)} u_2^{(2)}. \tag{25}$$

The same result is true for the addition operation.

$$u^{(1)} + u^{(2)} = e_1 \left[u_1^{(1)} + u_1^{(2)} \right] + e_2 \left[u_2^{(1)} + u_2^{(2)} \right], \tag{26}$$

where the addition in square brackets is made by the modulus of the number specifying the corresponding digit analog.

Further, the formula (21) makes it possible to demonstrate the specificity of the search for primitive elements. In particular, it immediately follows that the primitive element in the choice of elements g_i according to formula (23) is

$$\theta = g_1 g_2 = 5. \tag{27}$$

Degrees of this element form gives all non-zero elements of field $GF(7)$.

Another important example involves converting ten-valued logic operations to algebraic form. This field in the sense of the algebraic delta function (10) is conjugate to the field $GF(11)$, i.e. operations in an algebraic ring corresponding to ten-valued logic are reduced to algebraic ones through the use of addition and multiplication operations in the $GF(11)$ field, as well as the operation of digital differentiation.

In this case, any positive integer less than 10 can be represented as

$$u = 5 \cdot u_1 + 6 \cdot u_2, \tag{28}$$

where $u_{1,2}$ take the following values

$$u_1 = 0, 1;\ u_2 = 0, 1, \ldots, 4. \tag{29}$$

It is easy to see that in this case analogues of formulas (17)–(19) are also satisfied, in particular

$$5 + 6 = 11 \equiv 1(10). \tag{30}$$

Accordingly, the field element $GF(11)$ included in the expression for the algebraic delta function (10) can be represented in a form similar to (21)

$$x = \theta^{5 \cdot u_1} \theta^{6 \cdot u_2} = g_1^{u_1} g_2^{u_2}. \tag{31}$$

where elements g_i of the $GF(11)$ field, are determined from next conditions

$$g_1^2 = g_2^3 = 1. \tag{32}$$

In particular, we can choose $g_1 = 10$; $g_2 = 3$.

Note that the case of 10-valued logic may be of interest, including from an applied point of view. Namely, computing systems based on non-trivial elemental base[39], including quasi-biological[40], are currently being actively developed. Since in the foreseeable future humanity is unlikely to abandon the decimal number system, bringing the operations of such logic to algebraic ones can potentially be used to create computing systems directly oriented towards the decimal number system.

Formulas (25) and (26) allow us to propose the algorithm of multiplication modulo 6 and the circuit of multiplier modulo 6 that implements it (a similar approach can be used for decimal logic). Its advantage is the ability to operate with the "digits" of the number represented by formula (20) independently. This algorithm is considered in section "Modulo 6 multiplication algorithm and multiplier circuit". However, it should be emphasized once again that the operations of addition and multiplication of ring elements do not provide the possibility of reducing all operations of $(p-1)$-logic to algebraic ones, as is the case in the fields $GF(p)$. These operations must be supplemented by the operation of digital logarithm and its inverse—exponentiation.

Digital logarithm operation for the $GF(7)$ field and its circuit implementation

The importance of the digital logarithm operation for the case of $(p-1)$-logic follows directly from formula (10). Indeed, the algebraic delta function, which, as follows from formula (9), makes it possible to reduce any operations of such logic to algebraic ones, takes values in the field $GF(p)$. In fact, formula (10) operates with a mapping of an algebraic ring containing $(p-1)$ onto the field $GF(p)$. Therefore, to return to the original ring, i.e., to really ensure the execution of operations in terms of $p-1$-logic, it is necessary to have a tool that will provide the reverse transition. This is the digital logarithm operation.

Let us consider how exactly we can make the transition from $x = \theta^n$ to n, i.e., perform the operation of digital logarithm for the field $GF(7)$. More precisely, we will show that, using relation (8), it is possible not only to provide such a transformation, but also to propose an electronic circuit that performs the digital logarithm operation.

For this purpose, we first transform relation (10). The next relation is proven in theory of algebraic fields

$$(y \pm x)^q = y^q \pm x^q, \tag{33}$$

where q is the characteristic of the field.

For fields $GF(p)$ the number p coincides with the characteristic.

Direct verification proves the validity of the equality

$$y^p - x^p = (y - x)\left(y^{p-1} + y^{p-2}x + \cdots + yx^{p-2} + x^{p-1}\right). \tag{34}$$

Substituting the ratio (33) in the right part of formula (34), we get

$$(y - x)^{p-1} = y^{p-1} + y^{p-2}x + \cdots + yx^{p-2} + x^{p-1}. \tag{35}$$

For the special case of the field $GF(7)$, this relation becomes

$$(y - x)^6 = 1 + y^5x + \cdots + yx^5 + 1. \tag{36}$$

We will use representation (21) for the elements of the field under consideration. Then, after simple transformations, expression (36) can be reduced to the form

$$(y - x)^6 - 1 = \left(g_1^n g_1^m + 1\right)\left(g_2^{2n} g_2^m + g_2^n g_2^{2m} + 1\right), \tag{37}$$

where $x = g_1^n g_2^n$; $y = g_1^m g_2^m$ and the relation (22) was used.

Substituting specific values, we get

$$-\delta(x, y) = (y - x)^6 - 1 = \left(2^{2n}2^m + 2^n 2^{2m} + 1\right)\left(6^n 6^m + 1\right). \tag{38}$$

It can be seen that for the case under consideration, the algebraic δ-function is factorized, since we have

$$2^{2n}2^m + 2^n 2^{2m} + 1 = \begin{cases} 3, m + n \equiv 0(3) \\ 0, m + n \not\equiv 0(3) \end{cases}, \tag{39}$$

$$6^n 6^m + 1 = \begin{cases} 2, m + n \equiv 0(2) \\ 0, m + n \not\equiv 0(2) \end{cases}. \tag{40}$$

In the case when the right side of expression (38) is not equal to 0, it is equal to 6, which in the field $GF(7)$ corresponds to the inverse (by addition) elements with respect to 1.

Expressions (39) and (40) can be put in accordance with the operations carried out in the binary representation of the elements of the field under consideration.

Indeed, the prime number 7 is a special case of Mersenne prime numbers represented as $2^q - 1$. Such numbers have the following property. When you multiply a number written in binary form by 2 (modulo equal to a Mersenne number), there is a cyclic permutation of characters. In particular,

$$2 \cdot a_2a_1a_0 =_{(7)} a_1a_0a_2, \tag{41}$$

where a_i—binary characters.

The binary digits of all numbers N_0 corresponding to non-zero elements of the field $GF(7$ are presented in Table 1. It also presents the degrees of n primitive elements $\theta = 5$ and $\theta = 3$, which correspond to these elements.

This table emphasizes that the nonzero elements of the field $GF(7)$ decompose into two subsets corresponding to formulas (39) and (40). In each of them, the sequences of binary symbols corresponding to the field elements relate to each other by cyclic permutation (42).

Element 6, for which connection $1 + 6 \equiv 0(3)$ is valid, provides a transition from element to the element inverse by addition. Namely,

$$6 \cdot a_2a_1a_0 =_{(7)} \overline{a}_2\overline{a}_1\overline{a}_0, \tag{42}$$

where the slash above the symbol corresponds to the logical operation of inversion (logical 0 turns into one and vice versa).

N_0	1	2	4	3	6	5
a_2	0	0	1	0	1	1
a_1	0	1	0	1	1	0
a_0	1	0	0	1	0	1
$n; \theta = 5$	$6 \equiv 0(6)$	4	2	5	3	1
$n; \theta = 3$	$6 \equiv 0(6)$	2	4	1	3	5

Table 1. Binary representation of non-zero elements of the field $GF(7$ and their corresponding degrees of primitive elements.

The fact that the element $\overline{a}_2\overline{a}_1\overline{a}_0$ is the inverse of $a_2a_1a_0$ is also proved directly

$$a_2a_1a_0 + \overline{a}_2\overline{a}_1\overline{a}_0 = 111 =_{(7)} 000. \tag{43}$$

The specificity of the field $GF(7)$, expressed in Table 1 and formula (22), allows to realize the following circuit, performing the operation of digital logarithm (Fig. 1).

At the input of the circuit the binary signals a_i, corresponding to the elements of the field $GF(7)$, Table 1, are received. The purpose of this circuit is to convert such signals into a set of binary signals b_i, corresponding to the exponent of degree n at a certain choice of a primitive element. Concretely, the considered scheme corresponds to the case $\theta = 5$.

Elements 1_{1-3} and element 2 provide the transformation of the set of input signals into the format when only one of them is non-zero. This corresponds to the use of the second factor on the right side of formula (38). As follows from Table 1, the conversion to such format is performed by inversion of all signals a_i, which is performed if the sum of $\sum a_i$ exceeds one.

Specifically, three elements 1, 2, and 4 from the original field (Table 1) differ from elements 3, 5, and 6 in that for the elements of the first of these groups, the sum of the values of all three digits is equal to 1, and for the second, it is equal to 2. At the same time, as follows from formula (42), there is a one-to-one relationship between the elements of each of these groups, determined by logical inversion, in which the value of the digit 0 goes to 1 and vice versa.

Therefore, it is possible to determine by simple means which of the groups a particular element belongs to, displayed by a sequence of binary characters $a_2a_1a_0$, which correspond to the values at the inputs of the circuit, Fig. 1.

This operation is performed by block 2, Fig. 1, which performs the summation of the values of the bits $\sum a_i$. At the output of this block is formed the logical one if $\sum a_i > 1$ and logical zero otherwise.

Further, the signals a_i are fed to the EXCLUSIVE OR elements 1_{1-3}, to the second inputs of which the signal from element 2 is fed. As a result, elements 1_{1-3} carry out a logical inversion of each of the signals arriving at the inputs of the circuit in Fig. 1 if $\sum a_i > 1$ and leave them unchanged otherwise.

Further operations, performed by the circuit of Fig. 1, correspond to Table 2. In this table, the elements of the $GF(7)$ field are grouped in the same way as in Table 1. The difference is that in Table 2 shows not the values of the binary digits themselves, corresponding to the signals coming to the input of the circuit Fig. 1, but the values of the bits $\widetilde{a}_j$, formed at the outputs of elements 1_{1-3}, i.e. the values for elements 1, 2 and 4 remain unchanged, and the values of the bits for elements 3, 6 and 5 are changed to logically inverted. This is emphasized by the first line of Table 1, which indicates the algebraic operation (multiplication by the element 6 in the Galois field $GF(7)$), which provides the inversion.

For comparison, in the same table, the values of the bits b_j are indicated, which correspond to the values of the digital logarithms of the elements under consideration for the case $\theta = 5$, i.e. the powers to which the primitive element $\theta = 5$ must be raised in order to obtain the required element of the field $GF(7)$.

From Table 2 the value of the b_0 bit is determined only by the belonging of the considered field to one of the above sets. This corresponds to the factorization expressed by formulas (39) and (40). Therefore, the value of the bit b_0 corresponds to the signal generated at the output of block 2 of the circuit in Fig. 1.

In turn, this means that the operation of digital logarithm for the case under consideration is reduced to operations associated with setting the values of the two most significant digits at the output of the circuit in Fig. 1.

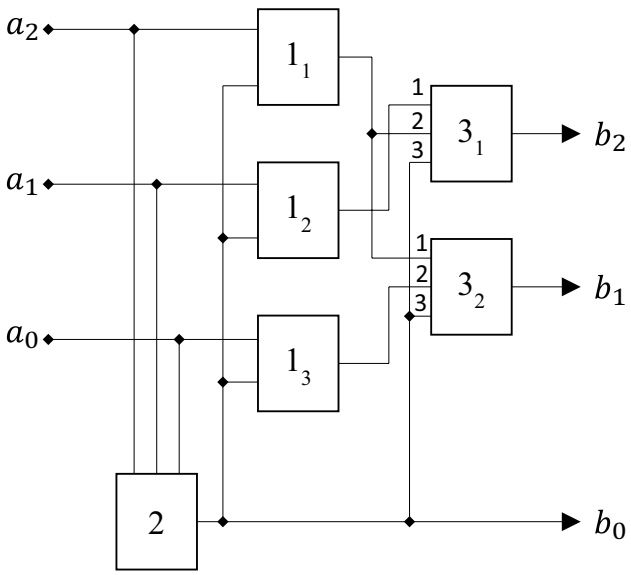


Figure 1. Circuit, performing the operation of digital logarithm.

	No inversion			Inversion		
	1	**2**	**4**	**6*3**	**6*6**	**6*5**
$\widetilde{a}_2$	0	0	1	1	0	0
$\widetilde{a}_1$	0	1	0	0	0	1
$\widetilde{a}_0$	1	0	0	0	1	0
	No inversion			**Inversion**		
	0 (6)	**4**	**2**	**5**	**3**	**1**
b_2	0	1	0	1	0	0
b_1	0	0	1	0	1	0
b_0	**0**	**0**	**0**	**1**	**1**	**1**

Table 2. Table of logical conversion of digit values at digital logarithm in the field $GF(7)$. Significant values are in bold.

This problem is solved using switches $3_{1,2}$ as follows. Both among the input (for the switch block $3_{1,2}$), and among the output signals, there is a maximum of only one that differs from zero. Therefore, the transition from the set of logical variables $\widetilde{a}_j$ to the set of variables $b_{1,2}$ can only be ensured by the nature of the connection between the elements of the circuit. This is shown in Table 3, which shows which output of the circuit in Fig. 1 must be supplied with that of the signals $\widetilde{a}_j$, which is non-zero for the digital logarithm operation to be performed.

The signals from the outputs of elements 1_{1-3} are fed to switches $3_{1,2}$ which perform the following operation.

The first input of each of these switches receives the signal taken from the output of the element 1_{1-3} which corresponds to the first part of Table 3 (no inversion). The second input receives the signal corresponding to the second part of this table (inversion). The switch is controlled by a signal taken from block 2. If this signal equals zero, the state of the commutator output coincides with the state of the output of the first input, if one—with the state of the second input. As a result, the signals corresponding to the two high digits of value the digital logarithm in binary representation are formed at the outputs of the switches.

The lower digit is exactly equal to the value of logic variable formed at the output of element 2.

Thus, for the considered Galois field the execution of a digital logarithm calculation can be carried out by a quite simple scheme.

We emphasize that the presented scheme reflects a fundamental fact. The proposed approach to performing the digital logarithm operation is since the number $p-1$, where p is prime, is decomposed into the product of some factors. Therefore, if the digital logarithm of the elements of an arbitrary Galois field is a mapping of the given field onto some ring, which, generally speaking, contains zero divisors and several idempotent elements.

The ring generated by the field $GF(7)$ in passing to the digital logarithm has two mutually canceling elements corresponding to simpler Galois fields. One of them corresponds to the field $GF(2)$. It is this fact that made it possible to classify the field elements (in the transition to digital logarithm) according to the value of the sum of the number of digits. A similar approach can be implemented for other Galois fields, since the digital logarithm in any case involves a mapping of its nonzero elements onto some algebraic ring.

Based on discussed above scheme, it is possible to propose various variants of other schemes, for example, implementing multiplication operation, six-digit logic operations, etc.

Let's move on to the consideration of electronic circuits providing multiplication by modulo 6. This scheme is intended to show that it is possible to implement calculations according to formula (9) or similar ones even in the case when the number of arguments of a logical operation becomes sufficiently large. The circuit considered below corresponds to the representation of six-valued logic in (2.3) logic, which also corresponds to formula (38). Figure 2 shows a circuit that performs digital logarithm, implemented by software NI Multisim.

Modulo 6 multiplication algorithm and multiplier circuit

The scheme considered below is intended to demonstrate the following fundamental circumstance, which is expressed by formula (26). It is possible to represent the element of the ring in the "hybrid" number system, formula (20). The digits of this number, if the operations proceed within the corresponding ring, can be handled independently.

This approach can be applied to various rings, but for the primary proof of its effectiveness in terms of implementation in the form of electronic circuits, it is permissible to restrict ourselves to the simplest example, which corresponds to the case of six-valued logic.

	No inversion	Inversion
$\widetilde{a}_2$	b_1	b_2
$\widetilde{a}_1$	b_2	–
$\widetilde{a}_0$	–	b_1

Table 3. Correspondence between the numbers of outputs of the block elements 1_{1-3} and the numbers of inputs of the switch block $3_{1,2}$, corresponding to the digital logarithm operation.

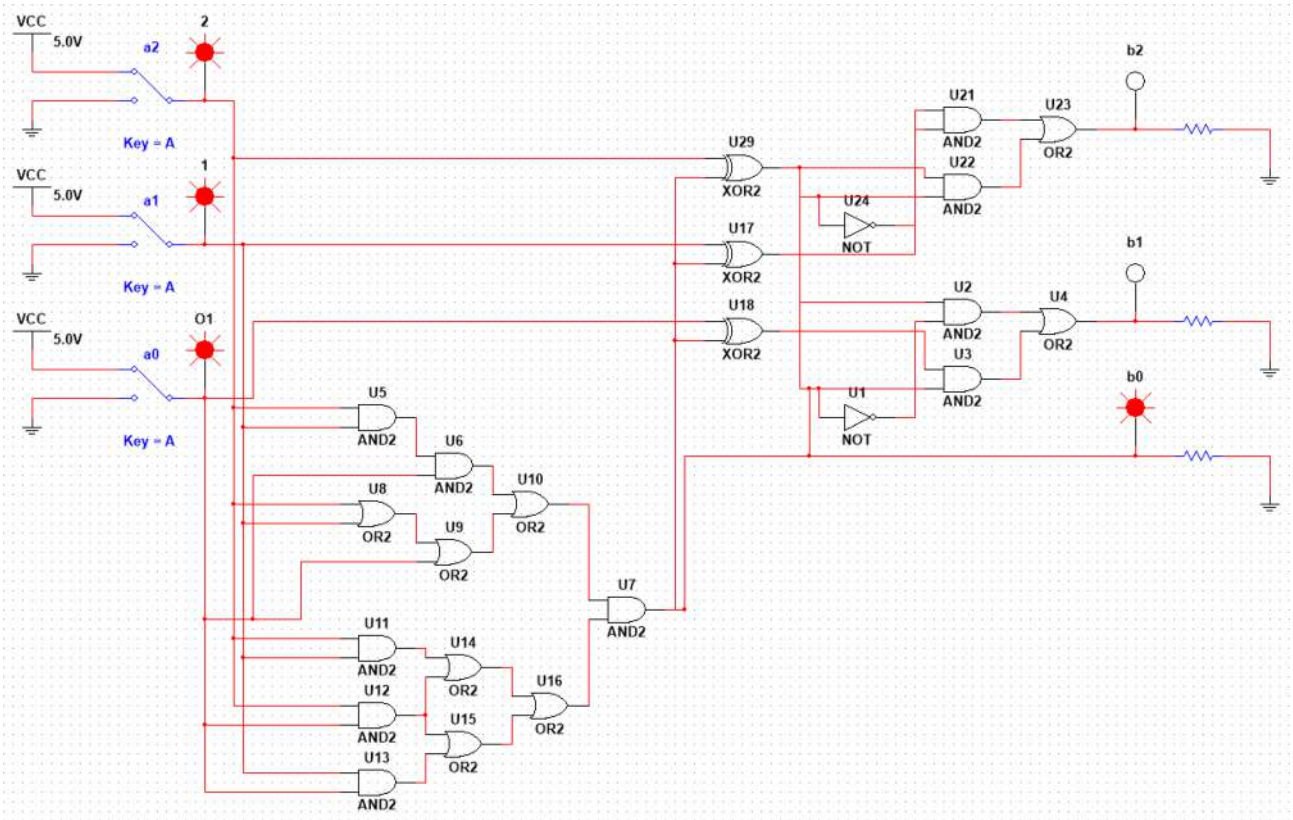


Figure 2. Digital logarithm performing scheme implemented by software NI Multisim.

The modulo 6 multiplication algorithm involves the following operations, to which the individual blocks of the electronic circuit correspond. The list of operations includes:

- conversion of multiplied numbers in binary representation to binary numbers modulo 6,
- conversion of the numbers in binary encoding to encoding in (2;3)-logic representation,
- multiplication of numbers in (2;3)-logic representation,
- conversion of the number representation in the (2;3)-logic to the usual binary representation.

Scheme of the block to convert the initial numbers in the binary representation to binary numbers modulo 6 (Fig. 3) is since the numbers 6 and 7 in the binary representation are written as 110 and 111 respectively. When

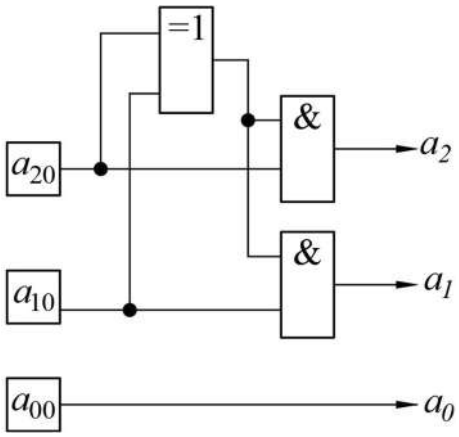


Figure 3. Schematic diagram of the block to convert the original numbers in binary representation to binary numbers modulo 6.

passing to calculations modulo 6, these numbers correspond to zero and one, i.e., for this case it is sufficient to replace the two most significant digits with zeros.

The EXCLUSIVE OR element in Fig. 3 compares the values of the two most significant digits. If they are the same, the output is a logical zero. The signal from the output of this element is fed to the elements of AND, the second output of which is fed signals corresponding to the values of a_{01} and a_{02}, as a result of their output signals equal to a_{01} and a_{02}, if the output of EXCLUSIVE OR is formed a logical unit (ie, the values of a_{01} and a_{02} do not coincide). On the contrary, if these values are the same, then at the output of the AND elements, logical zeros are formed.

Otherwise, the relationship between the values of variables on the input a_{i0} and the output a_i is given by the following logical formulas

$$a_2 = a_{20}(a_{10} + a_{20}), \tag{44}$$

$$a_1 = a_{10}(a_{10} + a_{20}), \tag{45}$$

$$a_0 = a_{00}. \tag{46}$$

Let us consider an algorithm of functioning of the block of conversion of numbers in binary encoding to encoding in (2;3)-logic representation (Table 3). The first line of this table contains numbers n from 0 to 5; this set corresponds to operations modulo 6. The next three lines present binary variables corresponding to the bits when writing the number n in binary encoding.

The next two lines represent the numbers u_1 and u_2, corresponding to the bits modulo 2 and 3 in the (2;3)-logic representation, respectively. This corresponds to the representation of the considered numbers in the hybrid number system in accordance with formula (20). We emphasize that each of the digits in this formula corresponds to a certain Galois field, specifically, the six-valued logic leads to (2;3)-logic, which is formed by the Galois fields $GF(2)$ and $GF(3)$. Each of the numbers appearing in the bits of such a representation, in turn, can be represented in binary encoding. For the elements of the $GF(2)$ field, it is sufficient to use only one binary digit, the values of which are presented in the fifth row of this Table 4. The field $GF(3)$ needs two such bits.

Respectively, the two bottom lines represent the binary variables u_{21} and u_{20} corresponding to the representation of numbers u_2 in binary logic.

It follows directly from this table that in the (2;3)-logic representation $u_1 = a_0$

Let us consider next expression, where all quantities are treating as logical binary variables

$$q = a_2 + a_1 a_0 \tag{47}$$

Direct calculations show that this expression is equal to zero for numbers 0,1,2 and equal to one for numbers 3,4,5, which is proved by direct calculation. In particular, the value of a_2 (the most significant bit) is zero for numbers 0,1,2, and the product of $a_1 a_0$ is also zero, since for numbers 0,1,2 only one of the two least significant bits is non-zero. The product $a_1 a_0$ is equal to 1 only for the initial number 3 from the set under consideration, and for the initial numbers 4 and 5 it also vanishes. But, since the value a_2 also appears in the sum (47), then for the initial numbers 3,4 and 5, the q parameter is equal to 1.

The q parameter is auxiliary, its calculation allows one to find direct connection between values of digits b_1 and b_2 with initial values a_i.

Specifically, this relationship is expressed by the following logical formulas

$$b_2 = a_1 + q a_0, \tag{48}$$

$$b_1 = a_0 + q, \tag{49}$$

$$b_0 = a_0. \tag{50}$$

For the case of numbers 0, 1 and 2 $q = 0$, and formulas (48) and (49) take the form that corresponds to the relationship between the considered quantities, determined by the second, third, and fourth columns of Table 4.

n	0	1	2	3	4	5
a_2	0	0	0	0	1	1
a_1	0	0	1	1	0	0
a_0	0	1	0	1	0	1
u_1	0	1	0	1	0	1
u_2	0	1	2	0	1	2
$u_{21} = b_2$	0	0	1	0	0	1
$u_{20} = b_1$	0	1	0	0	1	0

Table 4. Transition from binary encoding to encoding in (2;3)-logic representation.

$$b_2 = a_1, \tag{51}$$

$$b_1 = a_0. \tag{52}$$

Indeed, as Table 4 shows, for the numbers 0, 1 and 2, the value of the bit b_1 is the same as the value of a_0, and the value of b_2 is the same as the value of a_1.

For the case of numbers 3, 4 and 5 $q = 1$, and formulas (51) and (52) take the form that corresponds to the relationship between the considered quantities, determined by the last three columns of Table 4.

$$b_2 = a_1 + a_0, \tag{53}$$

$$b_1 = a_0 + 1. \tag{54}$$

Indeed, as Table 4 shows, for the numbers 3, 4, and 5, the value of the bit b_1 is associated with the value of a_0 by a logical inversion (or sum modulo 2), and the value of b_2 can be obtained as the sum of the values of a_1 and a_0 modulo 2.

Calculations in accordance with formulas (48)–(50) are carried out by a fragment of the multiplier circuit modulo 6, shown in Fig. 4.

Due to relation (50), the lowest bit in the encoding used remains the same $b_0 = a_0$.

Two other binary digits corresponding to value u_2 are formed by next elements of the circuit, presented on Fig. 4.

The AND (1) and EXCLUSIVE OR (2) elements calculate the auxiliary boolean variable q. These elements perform the operation reflected by formula (47).

Signals a_0 and q are sent to element AND (3), which corresponds to the calculation of the product qa_0 in formula (48). The signal from the output of this element is fed to the input of another EXCLUSIVE OR element (4) whose second input receives the signal corresponding to the value a_1, i.e., this part of the circuit implements the logical formula (48), i.e. at the output of the element, a signal is generated corresponding to the value b_2.

The signals a_0 and q are also fed to the EXCLUSIVE OR element input (5), which thus performs the logical operation given by formula (49), i.e., its output generates a signal corresponding to the value of b_1.

The considered block (Fig. 4), in essence, performs only an intermediate transformation. Specifically, it provides a transition from the encoding corresponding to the variables of six-valued logic to the "hybrid" number system, reflected by formula (20), which in the case under consideration corresponds to the case of (2,3)-logic.

The main convenience of the transition to such logic is demonstrated by the modulo 6 multiplier circuit considered below, which is a circuit implementation of formula (25), which shows that when switching to a “hybrid” number system corresponding to the use of algebraic rings,

The main convenience of the transition to such logic is demonstrated by the modulo 6 multiplier circuit considered below, which is a circuit implementation of formula (25), which shows that when switching to a “hybrid” number system corresponding to the use of algebraic rings, operations are performed in terms of binary and ternary logic. The logic is reduced to a simpler one.

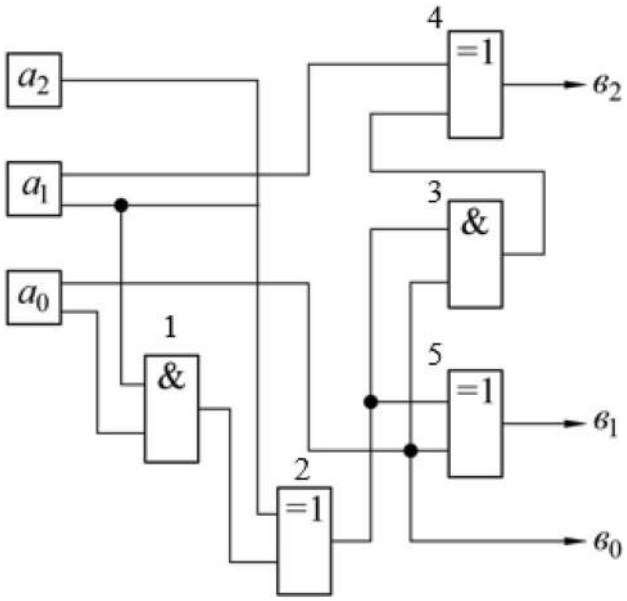


Figure 4. Schematic of the block to convert the numbers in binary encoding to encoding in the (2;3)-logic representation.

The resulting circuit of modulo 6 multiplier includes two similiar converters forming on its output one binary digit each corresponding to values $u_1^{(1)}$ and $u_1^{(2)}$, and two digits each corresponding to values $u_2^{(1)}$ and $u_2^{(2)}$. According to formula (15) presented above, the multiplication of these numbers is done independently, with one case multiplied modulo 2, and the other case multiplied modulo 3. To carry out the first of these operations it is sufficient to use the element AND (Fig. 4), i.e., $z_0 = b_0^{(1)} b_0^{(2)}$.

Let's consider elements of the circuit that perform the second of these operations (Fig. 5). The table of multiplication by modulo 3 (Table 5) can be reduced to a form which specifies values z_2 and z_1, i.e., binary variables corresponding to high and low binary digits of multiplication result (Tables 6 and 7).

The above tables show that

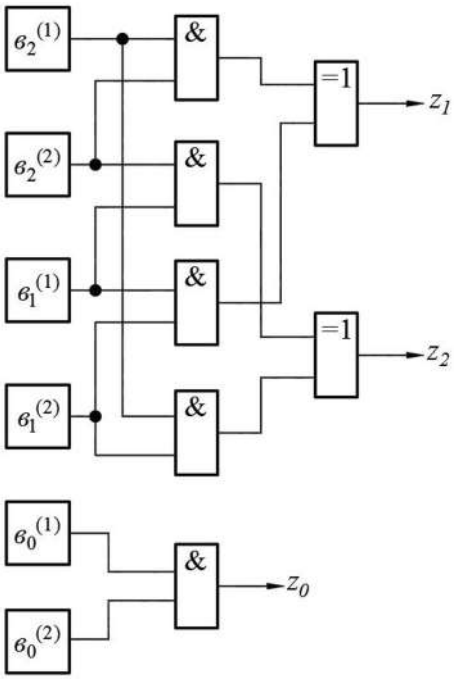


Figure 5. Diagram of the number multiplication block in (2;3)-logic representation.

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Table 5. Multiplication table modulo 3.

	00	01	10
00	0	0	0
01	0	1	0
10	0	0	1

Table 6. Table of least significant digits in modulo 3 multiplication.

	00	01	10
0	0	0	0
01	0	0	1
10	0	1	0

Table 7. Table of high digit values for multiplication by modulo 3.

$$z_1 = b_1^{(1)} b_1^{(2)} + b_2^{(1)} b_2^{(2)}, \tag{55}$$

$$z_2 = b_1^{(1)} b_2^{(2)} + b_2^{(1)} b_1^{(2)}, \tag{56}$$

where all values are treated as binary logic variables.

The scheme in Fig. 5 uses two AND elements for each of these operations (calculating the product modulo 2) and one OR circuit (calculating the sum).

Consider the inverse transformation to the representation of the result of the product in three-digit binary form (Fig. 4).

Possible encodings formed at the output of the circuit of Fig. 5 are shown in Table 8. The task is to convert them electronically into values corresponding to c_2 and c_1, which correspond to the product calculation result in the initial representation, $c_0 = z_0$ and require no transformation. The required result is shown in Table 9. The given values of logical variables, in essence, coincide with those reflected in Table 4, but we present them here for clarity of comparison again.

Directly from Table 8 you can see that the first and second triplets of numbers are classified by the values z_1 and z_0. If these values coincide, then the number in question takes the value 0, 1, or 2. If not—3, 4 or 5. Otherwise, the difference between one triplet and another is the value of the logical variable

$$w = z_1 + z_0. \tag{57}$$

For the first triplet w is 0, and for the second triplet it is 1.

Further, for the first triplet, we can proceed from the pair z_1 and z_2 to the pair c_2 and c_1 by adding the value of z_1 as a logical variable to the value z_0. For the first triplet, the latter differs from zero only for $n = 1$. That is, for the first three we have

$$c_2 = z_1 + z_0, \tag{58}$$

$$c_1 = z_2. \tag{59}$$

For the second triplet, the transition from the pair z_1 and z_2 to the pair c_2 and c_1 is provided by adding the value of z_0 to the two-digit binary number $z_1 z_2$.

This corresponds to logical expressions

$$c_1 = z_2 + z_0, \tag{60}$$

$$c_2 = z_1 + z_0 z_2. \tag{61}$$

Using (57), the written formulas can be combined as

$$c_1 = z_2 + (z_1 + z_0) z_0, \tag{62}$$

$$c_2 = z_1 + (z_1 + z_0 + 1) z_0 + (z_1 + z_0) z_0 z_2. \tag{63}$$

The last expression can be simplified

$$c_2 = (z_1 + z_0)(1 + z_0(1 + z_2)). \tag{64}$$

These expressions are realized by the scheme shown in Fig. 6. It is taken into account that the logical addition with one corresponds to the inversion operation.

n	0	1	2	3	4	5
z_1	0	1	0	0	1	0
z_2	0	0	1	0	0	1
z_0	0	1	0	1	0	1

Table 8. Values of the logical variables corresponding to the integers at the output of the circuit in Fig. 5 (at the input of the circuit in Fig. 6).

n	0	1	2	3	4	5
c_2	0	0	0	0	1	1
c_1	0	0	1	1	0	0

Table 9. The value of the logical variables that need to be generated at the output of the circuit of Fig. 6.

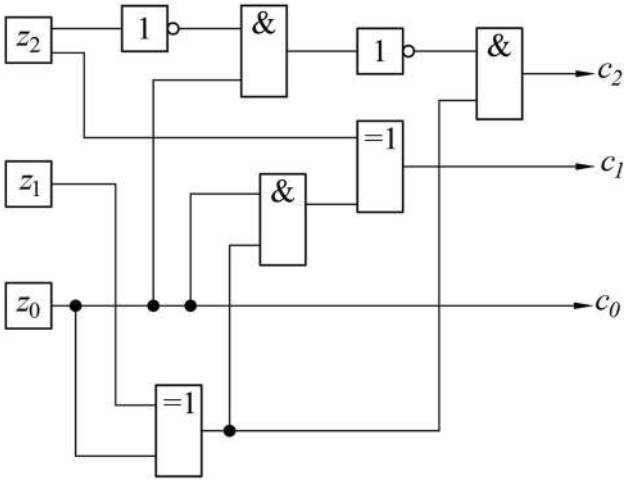


Figure 6. Schematic of the block for converting a number representation in (2;3)-logic to the usual binary representation.

Thus, the operation of multiplication of two numbers modulo 6 can really be implemented by rather simple electronic circuits (including those implemented by simulation methods), which use only standard elements of binary logic.

The general electronic circuit that combines the blocks shown in Figs. 3, 4, 5, 6, shown in Fig. 7. This scheme is implemented using software NI Multisim, i.e., with its help, the efficiency of the proposed approach is proved directly.

Conclusion

The increasing use of multivalued logics makes it relevant to reduce logical operations to algebraic ones. For those logics in which the number of values of a boolean variable is equal to p^n, where p is a prime number and n is an integer, this problem is solved by establishing a correspondence with Galois fields.

In this case, any logical operations can be reduced to operations of addition and multiplication in Galois fields, and there is an explicit tool that allows you to do this—the algebraic delta function, the usefulness and

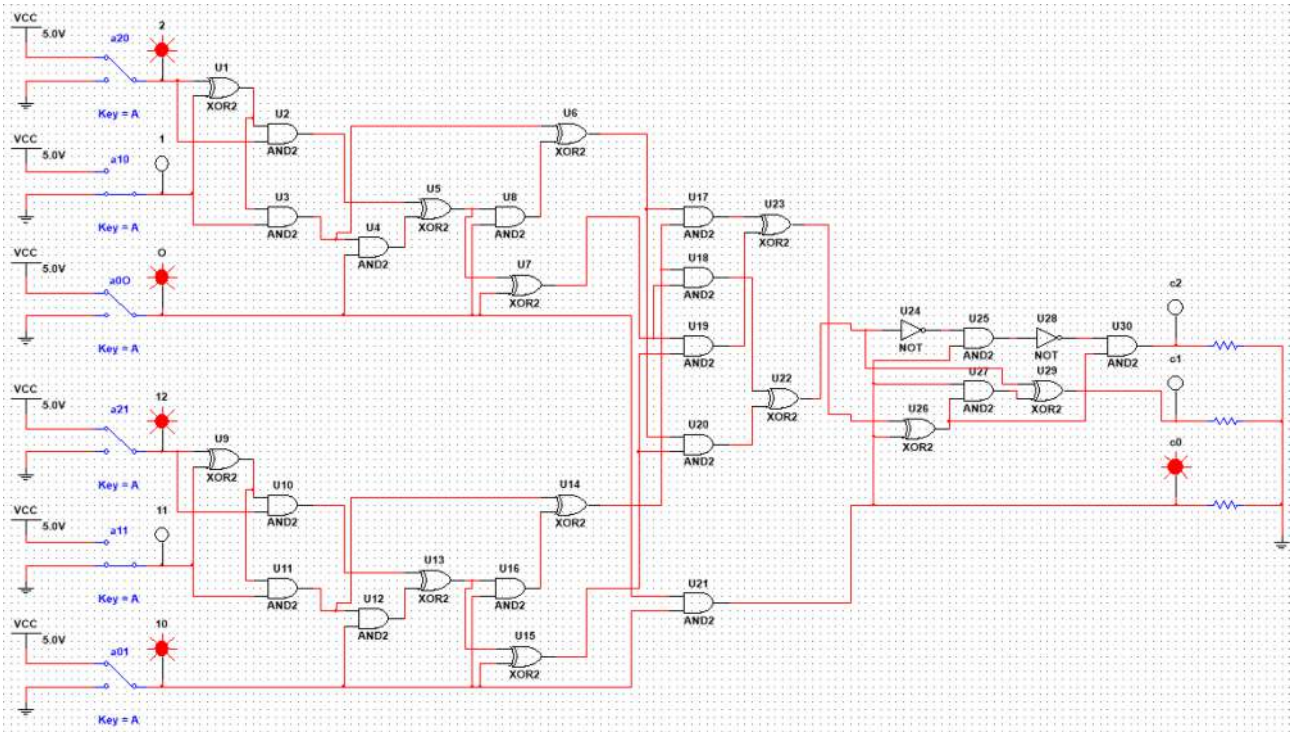


Figure 7. Modulo 6 multiplication scheme implemented by software NI Multisim.

q_4	q_3	q_2	q_1	$M = q_1q_2 \dots q_s$	p	Mp
–	–	3	2	6	7	42
–	–	5	2	10	11	110
–	–	11	2	22	23	506
–	5	3	2	30	31	930
–	7	3	2	42	43	1806
–	11	3	2	66	67	4422
–	7	5	2	70	71	4970
–	17	3	2	102	103	10,506
–	13	5	2	130	131	17,030

Table 10. Factors q_i giving examples of numbers of the form $q_1q_2 \dots q_s = p - 1$.

convenience of which was demonstrated in[20]. This function, in particular, allows one to write in explicit form an expression for an analogue of the Zhegalkin polynomial for arbitrary Galois fields.

However, there are several important logics (for example, six-valued and ten-valued logics), for which the reduction of logical operations to algebraic ones presents a certain problem.

This paper shows that it is possible to construct an algebraic delta function for the case when the number of values that a Boolean variable takes is $p - 1$.

This case, among other things, demonstrates the fundamental difference between logics that allow direct comparison with Galois fields, and such logics, the number of variable values in which is not equal to p^n, where p is a prime number and n is an integer.

In the latter case, the reduction of logical operations to algebraic ones cannot be reduced only to addition and multiplication, it is required to use a larger number of operations. For $p - 1$-logics such operations are the operation of digital logarithm and its inverse. Such operations, as shown in this work, allow us to bring the operations performed for $p - 1$-logic to the operations performed in the field $GF(p)$.

The adequacy of the proposed approach is demonstrated on the example of electronic circuits, which allow reducing the operations of six-valued logic to algebraic ones, which can be technically implemented even based on standard logical electronic components.

The proposed approach is of interest for the development of logic circuits based on a non-standard element base, for example, on a quasi-biological basis. The development of such systems returns to the question of how exactly computer systems should be implemented that are complementary to the usual decimal number system. There is no need to prove that bringing calculations in the binary number system to decimal form requires additional computer resources. New computing systems may well be based on a combined number system, on (2.5), a logic that is complementary to the Galois field $GF(11)$.

The advantage of this approach is the simplification of addition and multiplication operations by technical devices, which follows from formulas (25), (26), as well as the possibility of its extension to other logics, the number of variable values in which is equal to the product of prime numbers $q_1q_2 \dots q_s$, the value of which itself equals $p - 1$, where p is a prime number: $q_1q_2 \dots q_s = p - 1$.

Examples of such numbers are presented in Table 10.

Indeed, in this case it becomes possible to reduce the operations of logic, the number of values of the variables of which is equal to $p - 1$, to operations in algebraic rings corresponding to the product $p_1p_2 \dots p_s$.

This significantly expands the list of multivalued logics, the operations in which are reducible to algebraic ones, which, however, requires additional research.

In addition, the use of multi-valued logics is a promising tool for improving the means of digital signal and image processing. Solving problems of this kind requires reducing logical operations to algebraic ones, which determines the prospects for further research in this direction. In particular, the task of further weakening the restrictions imposed on the number of values that a boolean variable can take is topical.

Data availability

All data generated or analysed during this study are included in this published article.

Received: 3 September 2023; Accepted: 9 December 2023
Published online: 12 December 2023

References

1. Sokolov, A., & Zhdanov, O. Prospects for the application of many-valued logic. *Funct. Cryptogr. 331–339*. https://doi.org/10.1007/978-3-319-91008-6_33 (2018).
2. Schurz, G. Meaning-preserving translations of non-classical logics into classical logic: Between pluralism and monism. *J. Philos. Log.* **51**, 27–55. https://doi.org/10.1007/s10992-021-09608-6 (2021).
3. Karpenko, A., & Tomova, N. Bochvar's three-valued logic and literal paralogics: Their lattice and functional equivalence. *Logic Logic. Philos.* **26**(2), 207–235. https://doi.org/10.12775/LLP.2016.029 (2017).
4. Hernández-Tello, A., Macías, V. B. & Coniglio, M. E. Paracomplete logics dual to the genuine paraconsistent logics: The three-valued case. *Electron. Notes Theor. Comput. Sci.* **354**, 61–74. https://doi.org/10.1016/j.entcs.2020.10.006 (2020).

5. Zamansky, A. On recent applications of paraconsistent logic: An exploratory literature review. *J. Appl. Non-Classical Logics* **29**(4), 382–391. https://doi.org/10.1080/11663081.2019.1656393 (2019).
6. Senturk, I. A view on state operators in Sheffer stroke basic algebras. *Soft Comput.* **25**(17), 11471–11484. https://doi.org/10.1007/s00500-021-06059-8 (2021).
7. Oner, T. & Senturk, I. The Sheffer stroke operation reducts of basic algebras. *Open Math.* **15**(1), 926–935. https://doi.org/10.1515/math-2017-0075 (2017).
8. Jo, S. B., Kang, J. & Cho, J. H. Recent advances on multivalued logic gates: A materials perspective. *Adv. Sci.* **8**(8), 2004216. https://doi.org/10.1002/advs.202004216 (2021).
9. Yoo, H. & Kim, C. H. Multi-valued logic system: New opportunities from emerging materials and devices. *J. Mater. Chem. C* **9**(12), 4092–4104. https://doi.org/10.1039/D1TC00148E (2021).
10. Sun, J. *et al.* Bi-objective elite differential evolution algorithm for multivalued logic networks. *IEEE Trans. Cybern.* **50**(1), 233–246. https://doi.org/10.1109/TCYB.2018.2868493 (2018).
11. Bykovsky, A. Y. Multiple-valued logic and neural network in the position-based cryptography scheme. *J. Russ. Laser Res.* **42**(5), 618–630. https://doi.org/10.1007/s10946-021-10000-7 (2021).
12. Kahane, H., Hausman, A., & Boardman, F. *Logic and philosophy: A modern introduction* (Hackett Publishing, 2020).
13. Gabrielyan, O., Vitulyova, E., & Suleimenov, I. Multi-valued logics as an advanced basis for artificial intelligence (as an example of applied philosophy). *Wisdom* **21**(1), 170–181. https://doi.org/10.24231/wisdom.v21i1.721 (2022).
14. Lukasiewicz, J. On three-valued logic. Polish Rev. 43–44 (1968).
15. Gomes, E. L. Thinking about contradictions: The Imaginary Logic of Nikolai Aleksandrovich Vasil'ev: V. Raspa, Translated by Peter N. Dale. Heidelberg, New York: Springer International Publishing AG, 2017. xxi+ 160 pp. Hardcover US 109.99,e-bookUS 84.99. Hardcover ISBN 978-3-319-66085-1. eBook ISBN 978-3-319-66086-8. https://doi.org/10.1080/01445340.2019.1591669 (2019).
16. Shankar, S. Lessons from nature for computing: looking beyond moore's law with special purpose computing and co-design*. *IEEE High Perf. Extreme Comput. Conf. (HPEC)* **2021**, 1–8. https://doi.org/10.1109/HPEC49654.2021.9622865 (2021).
17. Zhang, Y. *et al.* A system hierarchy for brain-inspired computing. *Nature* **586**, 378–384. https://doi.org/10.1038/s41586-020-2782-y (2020).
18. Suleimenov, I. E., Vitulyova, Y. S., Bakirov, A. S., & Gabrielyan, O. A. Artificial Intelligence: what is it? In *Proceedings of the 2020 6th International Conference on Computer and Technology Applications* (pp. 22–25). https://doi.org/10.1145/3397125.3397141 (2020).
19. Cotnoir, A. J. Logical nihilism. In *Pluralisms in truth and logic* (pp. 301–329). Palgrave Macmillan, Cham. DOI: https://doi.org/10.1007/978-3-319-98346-2_13 (2018).
20. Suleimenov, I. E., Vitulyova, Y. S., Kabdushev, S. B. & Bakirov, A. S. Improving the efficiency of using multivalued logic tools. *Sci. Rep.* **13**(1), 1108. https://doi.org/10.1038/s41598-023-28272-1 (2023).
21. Franzoi, L. Jaccard-like fuzzy distances for computational linguistics. In *2017 19th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)* (pp. 196–202). IEEE. https://doi.org/10.1109/SYNASC.2017.00040 (2017).
22. Sedova, N., Sedov, V., Bazhenov, R. & Bogatenkov, S. Neural network classifier for automatic course-keeping based on fuzzy logic. *J. Intell. Fuzzy Syst.* **40**(3), 4683–4694. https://doi.org/10.3233/JIFS-201495 (2021).
23. Sharma, R., Bhasin, S., Gaur, P. & Joshi, D. A switching-based collaborative fractional order fuzzy logic controllers for robotic manipulators. *Appl. Math. Model.* **73**, 228–246. https://doi.org/10.1016/j.apm.2019.03.041 (2019).
24. Gan, L., Kuang, K., Yang, Y., & Wu, F. Judgment prediction via injecting legal knowledge into neural networks, 12866–12874. https://doi.org/10.1609/aaai.v35i14.17522 (2021).
25. Williamson, I. *et al.* Reprogrammable electro-optic nonlinear activation functions for optical neural networks. *IEEE J. Select. Top. Quant. Electron.* **26**, 1–12. https://doi.org/10.1109/JSTQE.2019.2930455 (2019).
26. Suleimenov, I. E. *et al.* Distributed memory of neural networks and the problem of the intelligences essence. *Bull. Electr. Eng. Inf.* **11**(1), 510–520. https://doi.org/10.11591/eei.v11i1.3463 (2022).
27. Suleimenov, I. E., Bakirov, A. S. & Matrassulova, D. K. A technique for analyzing neural networks in terms of ternary logic. *J. Theor. Appl. Inf. Technol.* **99**(11), 2537–2553 (2021).
28. Harari, D. *Galois cohomology and class field theory* (Springer International Publishing, 2020).
29. Cantú, L. & Figallo, M. On the logic that preserves degrees of truth associated to involutive Stone algebras. *Log. J. IGPL* **28**, 1000–1020. https://doi.org/10.1093/JIGPAL/JZY071 (2018).
30. Matrassulova, D. K., Vitulyova, Y. S., Konshin, S. V. & Suleimenov, I. E. Algebraic fields and rings as a digital signal processing tool. *Indones. J. Electr. Eng. Comput. Sci.* **29**(1), 206–216. https://doi.org/10.11591/ijeecs.v29.i1.pp206-216 (2023).
31. Razaq, A., Ahmad, M., Yousaf, M. A. & Masood, S. A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption. *Multimed. Tools Appl.* **80**(13), 20191–20215 (2021).
32. Inumarty, H., & Basiri, M. Reconfigurable hardware design for polynomial galois field arithmetic operations. In *2020 24th International Symposium on VLSI Design and Test (VDAT)*, 1–5. https://doi.org/10.1109/VDAT50263.2020.9190485 (2020).
33. Kalimoldayev, M., Tynymbayev, S., Gnatyuk, S., Ibraimov, M. & Magzom, M. The device for multiplying polynomials modulo an irreducible polynomial. *News Natl. Acad. Sci. Republic Kazakhstan Ser. Geol. Tech. Sci.* **2**(434), 199–205. https://doi.org/10.32014/2019.2518-170X.55 (2019).
34. Matrassulova, D. K., Kabdushev, S. B., Bakirov, A. S., & Suleimenov, I. E. Algorithm for Analyzing Rotating Images Based on the Fourier-Galois Transform. In *2023 15th International Conference on Computer Research and Development (ICCRD)* (pp. 204–209). IEEE. https://doi.org/10.1109/ICCRD56364.2023.10080084 (2023).
35. Moldakhan, I., Matrassulova, D. K., Shaltykova, D. B. & Suleimenov, I. E. Some ad vantages of non-binary Galois fields for digital signal processing. *Indones. J. Electr. Eng. Comput. Sci.* **23**(2), 871–877. https://doi.org/10.11591/ijeecs.v23.i2.pp871-878 (2021).
36. Vitulyova, E. S., Matrassulova, D. K. & Suleimenov, I. E. New application of non-binary Galois fields Fourier transform: Digital analog of convolution theorem. *IJEECS* **23**(3), 1718. https://doi.org/10.11591/ijeecs.v23.i3.pp1718-1726 (2021).
37. Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., & Zimmermann, P. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. In *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II 40* (pp. 62–91). Springer International Publishing (2020).
38. Pershina, R., Soppe, B. & Thune, T. M. Bridging analog and digital expertise: Cross-domain collaboration and boundary-spanning tools in the creation of digital innovation. *Res. Policy* **48**(9), 103819 (2019).
39. Liu, P., Xing, Q., Wang, D. & Oeser, M. Application of dynamic analysis in semi-analytical finite element method. *Materials* **10**(9), 1010. https://doi.org/10.3390/ma10091010 (2017).
40. Lei, Z. & Wu, P. Bioinspired quasi-solid ionic conductors: Materials, processing, and applications. *Accounts Mater. Res.* **2**(12), 1203–1214. https://doi.org/10.1021/accountsmr.1c00165 (2021).

Author contributions

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by I.E.S., Y.S.V., S.B.K., A.S.B. The first draft of the manuscript was written by I.E.S., A.S.B. and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding
This research has been/was/is funded by the Science Committee of the Ministry of Higher Education and Science of the Republic of Kazakhstan (Grant no. AP15473354).

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to A.S.B.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

symmetry

MDPI

Article

Formation of Periodic Mosaic Structures Using Operations in Galois Fields

Dina Shaltykova [1], Yelizaveta Vitulyova [1,2], Akhat S. Bakirov [3,*] and Ibragim Suleimenov [1]

[1] National Engineering Academy of the Republic of Kazakhstan, Almaty 050010, Kazakhstan; shaltykova.d@mail.ru (D.S.); lizavita@list.ru (Y.V.); esenych@yandex.kz (I.S.)
[2] JSC «Institute of Digital Engineering and Technology», Almaty 050013, Kazakhstan
[3] Institute of Communication and Space Engineering, Gumarbek Daukeev Almaty University of Power Engineering and Communications, Almaty 050013, Kazakhstan
* Correspondence: axatmr@mail.ru

Abstract

Mosaic ornaments and periodic geometric patterns are deeply rooted in cultural heritage and contemporary design, where symmetry plays a fundamental role in both aesthetic and cognitive perception. This study develops an algebraic method for generating symmetrical and periodic mosaic structures using operations in Galois fields. The approach demonstrates that the intrinsic properties of finite fields naturally give rise to symmetry and periodicity, eliminating the need for specific initial patterns, even when applied to relatively simple algebraic expressions such as the Bernoulli lemniscate and the cissoid of Diocles. The proposed algorithm offers the advantages of simplicity and the ability to provide gradual transitions from one mosaic structure to another. Furthermore, it is demonstrated that standardization of algebraic expressions used for mosaic generation can be efficiently achieved through discrete logarithm operations. A novel method for computing discrete logarithms is introduced. The results confirm that symmetrical structures of high complexity can be obtained through simple expressions, and their periodicity becomes more pronounced with increasing field characteristics. This approach offers practical applications in textile and wallpaper design, smart materials, and psychological testing, while also suggesting new perspectives for the analysis of mosaic-like natural systems where symmetry is a defining property.

Keywords: mosaics; periodic structures; Galois fields; algebraic extensions; primitive element; discrete logarithm; monitoring object modeling

Academic Editor: Calogero Vetro

Received: 24 July 2025
Revised: 17 August 2025
Accepted: 25 August 2025
Published: 1 September 2025

Citation: Shaltykova, D.; Vitulyova, Y.; Bakirov, A.S.; Suleimenov, I. Formation of Periodic Mosaic Structures Using Operations in Galois Fields. *Symmetry* **2025**, *17*, 1415. https://doi.org/10.3390/sym17091415

1. Introduction

Mosaic ornaments and geometric patterns, characterized by a high degree of symmetry, constitute an integral part of the cultural heritage of various nations across the world [1–3].

Such ornaments have been employed for centuries, including as elements of frescoes and in the architectural decoration of buildings, such as churches and cathedrals [4], mosques and mausoleums [5], as well as Hindu and Buddhist temples [6]. Geometric mosaic patterns remain widely used today, for instance in urban architectural design, as well as in the production of textiles, carpets, and related artifacts.

The advancement of technologies for the production of textiles, carpets, and other household items (including the increasing adoption of 3D printing [7–9]) requires an expansion of the spectrum of design methods available for the generation of patterns.

An illustrative example is the development of smart textiles [10,11], which opens new opportunities for the creation of nontrivial and innovative designs.

These possibilities can be employed to enhance psychological comfort for consumers [11,12], including for the correction of psychological states [12,13]. Moreover, several hypotheses have been proposed suggesting that mosaics may be considered as a paradigm of visual construction that extends beyond the scope of decorative art [14]. This perspective is consistent with conclusions drawn in earlier studies [15,16].

At present, the costs of producing textile, wallpaper, and related patterns remain relatively high, as they require the involvement of highly paid professional designers [17]. In the literature, attempts have been reported to improve [18,19] and to algorithmize [20–22] the process of pattern generation. However, these approaches do not enable the efficient production of a wide variety of designs at high speed, nor do they facilitate the creation of sequences of patterns that gradually transform from one into another. These aspects are of particular importance for allowing consumers to select the most suitable designs, especially when patterns are employed for psychological correction.

Mosaic structures generated automatically (including in high-frame-rate modes) are of interest for the advancement of psychological testing methods, particularly in projective techniques [23,24]. One of the most widely used among these is the psychogeometric test developed by Susan Dellinger [25]. The application of such techniques is often met with criticism [26], which can be addressed by selecting appropriate geometric structures capable of evoking associations, including at the archetypal level [27]. The variability of patterns used in psychological testing also facilitates the refinement of association-based methodologies, the most renowned of which is the Rorschach test [28,29]. This is particularly relevant in the context of testing large population groups.

The objective of this study is to develop a relatively simple and efficient method for generating periodic mosaic structures, including those characterized by a high degree of symmetry, as well as the possibility of ensuring smooth transitions from one mosaic to another.

The algorithm employs Galois fields, which are increasingly applied in digital image processing [30,31] and in other digital technologies [32,33], including elliptic curve cryptography (ECC) [34,35]. For the purpose of mosaic generation, particularly in applications related to psychological testing, however, such algebraic structures have not previously been utilized. This problem is addressed for the first time in the present work. It should be emphasized that studies on mosaic structures, including two-dimensional ones, are well known (in addition to the works mentioned above, see also [36,37]). Nevertheless, these studies have not addressed the problem of high-speed generation of such structures, and especially not the creation of mosaics capable of gradually transforming from one into another.

The principal tool enabling sequential transitions between mosaic structures is the novel method for computing discrete logarithms in Galois fields, introduced here for the first time. This method is based on the application of an algebraic delta function [38]. In the cryptographic literature, it is widely acknowledged that until recently, the problem of computing discrete logarithms remained intractable [39]. In particular, it has been noted that the first practical public-key cryptosystem, the Diffie–Hellman key exchange algorithm, relies on the assumption that discrete logarithms are computationally hard. This assumption, characterized as a hypothesis, underpins the presumed security of various other public-key schemes and, as emphasized in [39], remains a formidable challenge. At the time of publication [39], this hypothesis was the subject of extensive debate, and the discussion has continued in subsequent research [40].

In the present study, a novel approach to discrete logarithm computation is proposed, complementing the algorithm for mosaic generation. This algorithm is applicable, at least, to relatively small Galois fields $GF(p)$ (since the use of fields with very large values of p is not meaningful for mosaic construction) and is introduced here for the first time.

The study also discusses potential directions for further application of the proposed framework. One promising avenue arises from the observation that many natural objects, including those of critical importance for agricultural land monitoring, exhibit structures closely resembling mosaics [41–43].

2. Methods

Various functions $F(x, y)$ that take values in the field $GF(p)$ are employed. The arguments of these functions are also elements of the same Galois field. The elements of this field are represented in the following form (the validity of this representation is most clearly demonstrated in [44]):

$$GF(p) \leftrightarrow \left\{ -\frac{p-1}{2},\ -\frac{p-1}{2}+1, \ldots,\ -1, 0, 1, \ldots, \frac{p-1}{2} \right\} \tag{1}$$

This representation is adequate because, except for the case of $p = 2$ which is not of interest, the number p is odd. This representation, among other things, makes the use of the minus sign in all subsequent calculations completely correct [44].

A discrete two-dimensional Cartesian coordinate system was employed, in which each integer value of both coordinates is associated with an element of the field $GF(p)$. This approach corresponds to the partitioning of the image plane into individual pixels, each of which is assigned discrete values $n_x,\ n_y$, with $0 \le n_{x,y} \le p-1$. It should be emphasized that pixel-based image partitioning is also employed in other studies on mosaic generation, in particular in [20]. For each pixel, a specific function $F(x, y)$, was computed, also taking values in this field. This operation is essentially equivalent to calculating the remainder of the division of $F(x, y)$ by the prime number p.

Subsequently, the values of the function were mapped onto the set $\{-1,\ 1\}$:

$$Q[F(x,y)] = \begin{cases} -1, F(x,y) < 0 \\ 1, F(x,y) \ge 0 \end{cases} \tag{2}$$

It should be emphasized that Formula (2) provides a natural way to assign a specific discrete indicator to each pixel. In the case of two-color mosaics, this indicator assumes two values determined by the sign of the function defined over the Galois field. Furthermore, as will become evident in the subsequent discussion, it is precisely the properties of the Galois field that ensure the periodic nature of the generated mosaics, despite the fact that the employed functions, when considered over continuous variables, do not exhibit such periodicity.

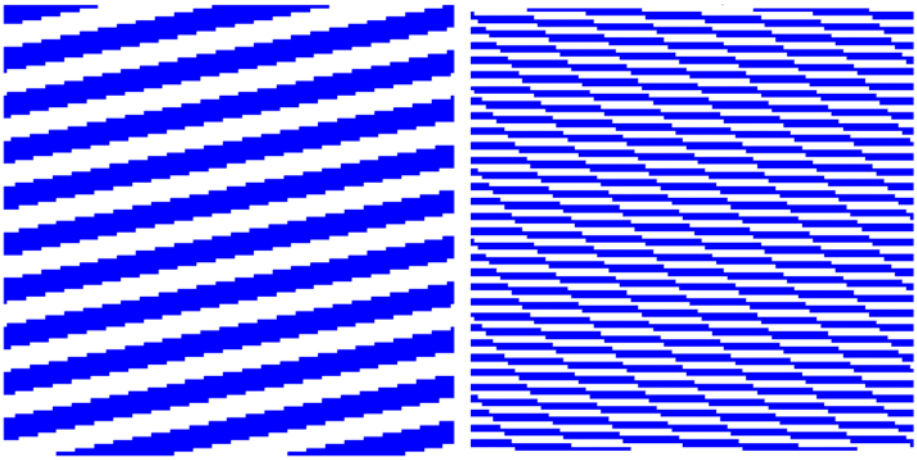
The results of this mapping constitute mosaics (where the minus sign corresponds to white fields and the plus sign to colored ones), which are analyzed below. The principal distinction of the present method from approaches such as those described in [20–22] lies in the fact that, in this case, a single function $F(x, y)$ can be employed to describe the mosaic, and the computations are carried out using the simple expression (2), which significantly simplifies the algorithmic implementation of mosaic generation. The programming code is particularly straightforward when the function $F(x, y)$ is applied without additional correction. This code is provided in Supporting Information S1.

3. Results

Let us consider specific examples of mosaics that can be generated using mapping (2). For this purpose, the programming code provided in Supporting Information S1 was used. Figures 1–4 correspond to the case where the field $GF(61)$ is used. In these figures, as well as in all other figures presented in this study, the size of the field along both the horizontal and vertical axes is equal to twice the value of p, corresponding to the utilized field $GF(p)$. Specifically, Figure 1 shows a mosaic formed by means of the following function:

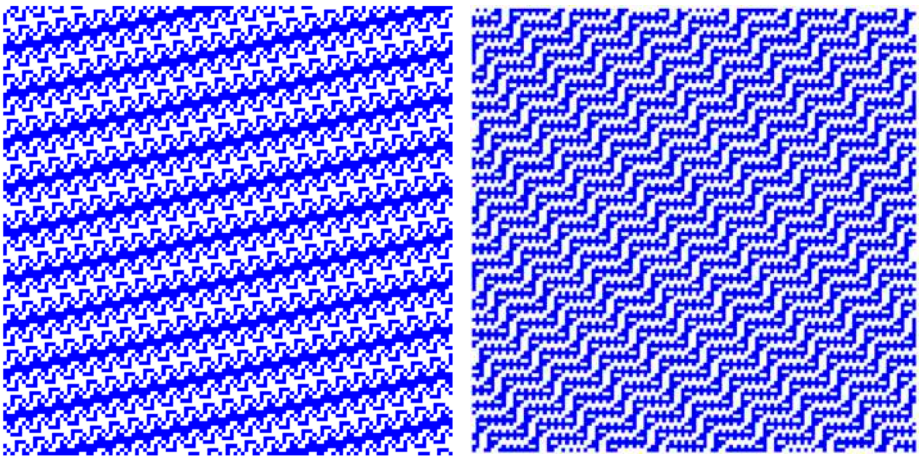
$$f(x, y) = x + ay \tag{3}$$

for parameter values $a = 5$ and $a = 45$, respectively.



(**a**) (**b**)

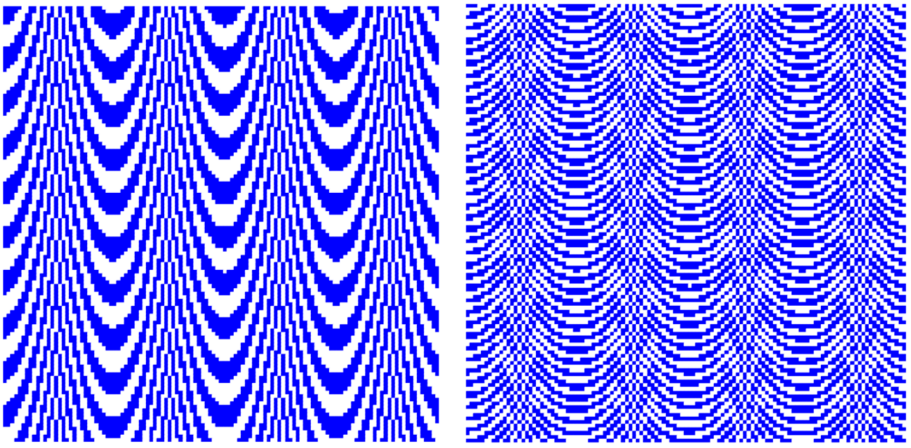
Figure 1. Mosaics generated using Formula (3); $a = 5$ (**a**), $a = 45$ (**b**); the field used is $GF(61)$.



(**a**) (**b**)

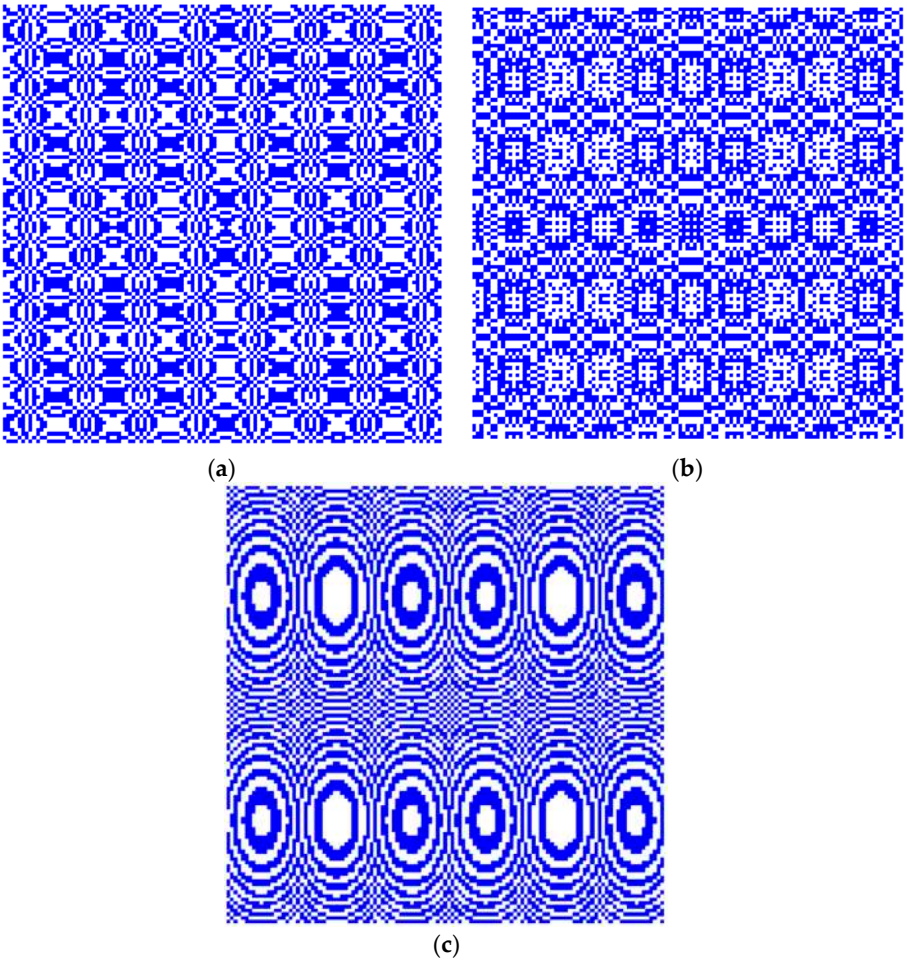
Figure 2. Mosaics generated using Formula (4); $a = 5$ (**a**), $a = 45$ (**b**); the field used is $GF(61)$.

It can be observed that the simplest linear equation gives periodic structures that, up to discretization accuracy, resemble a system of equidistant parallel stripes. It should be noted that even this simplest example demonstrates the advantages of using Galois fields for constructing periodic mosaics. The original function, when considered as a function over the set of real numbers, does not inherently produce periodicity. However, when functions taking values in Galois fields are employed, such periodicity becomes apparent, even in the most elementary case.



(**a**) (**b**)

Figure 3. Mosaics generated using Formula (5); $a = 5$ (**a**), $a = 19$ (**b**); the field used is $GF(61)$.



(**a**) (**b**)

(**c**)

Figure 4. Mosaics generated using Formula (6); $a = 5$ (**a**), $a = 19$ (**b**), $a = 30$ (**c**); the field used is $GF(61)$.

Figure 2 presents a mosaic, characterized by a high degree of symmetry, generated using the following function:

$$f(x, y) = (x + ay)^2 \tag{4}$$

for $a = 5$ and $a = 45$, respectively.

It can be observed that in this case the primary structure corresponding to a system of equidistant stripes is preserved, although the internal structure of the stripes undergoes a transformation. It is worth emphasizing once again that the structure shown in Figure 2 reflects the distinctive properties of Galois fields. If the original function, including (4), is considered over the set of real variables, it is not periodic. Periodicity emerges when the function takes values in a Galois field, and the resulting mosaic structure becomes highly nontrivial, despite the fact that the underlying equation remains relatively simple.

Figure 3 presents a mosaic generated using the following function:

$$f(x, y) = x^2 + ay \tag{5}$$

(the parameter values are indicated in the figure caption).

It can be observed that periodicity is again evident in this case, driven by the operation of taking the remainder modulo the prime number p, that defines the field $GF(p)$. The underlying structure of the mosaics shown in Figure 3 corresponds to a system of parabolas, shifted relative to one another along the vertical axis.

Figure 4 presents a mosaic generated using the Bernoulli lemniscate for parameter values $a = 3$ $a = 15$ and $a = 30$ respectively.

$$f(x, y) = \left(x^2 + y^2\right) - a^2\left(x^2 - y^2\right) \tag{6}$$

It can be observed that a relatively minor complication of the employed function results in the emergence of a highly nontrivial mosaic structure, the characteristics of which strongly depend on the value of the control parameter a, while still retaining a high degree of symmetry.

This provides evidence that the proposed approach enables the generation of a wide variety of mosaic structures using comparatively simple means. Moreover, it also allows for a sequential transition from one mosaic to another by gradually varying the control parameter in small increments.

Figure 5 shows mosaics also generated using function (6), but for the field $GF(127)$. As in previous cases, the field size along each axis equals twice the value of p, corresponding to the employed Galois field.

It can be observed that when transitioning from the field $GF(61)$ to $GF(127)$, the characteristics of the mosaics generated using Equation (6) remain similar (for the same value of the single control parameter). The difference lies in the fact that, as the level of mosaic detail increases with the field characteristic, the periodic nature of the resulting structures becomes more pronounced. In particular, the structure shown in Figure 5c can be interpreted as the result of an "interference" between periodically repeating systems of concentric circles, whereas this feature is far less evident in Figure 4c. It can also be noted that for practical purposes such as generating patterns for textiles, floor tiles, wallpapers, and similar applications, it is sufficient to use Galois fields with relatively small characteristics, i.e., without excessively increasing the level of detail in the generated structures. The same applies to mosaics intended for psychological testing.

Thus, even the relatively simple algebraic expression, the Bernoulli lemniscate (6), allows for the generation of a wide variety of mosaics. Evidently, a considerable number of different algebraic expressions can be proposed, including those based on heuristic considerations. Therefore, it is reasonable to consider the possibility of unifying the generation of such mosaics. This task is feasible precisely due to the specific properties of Galois fields (finite commutative fields) and their algebraic extensions.

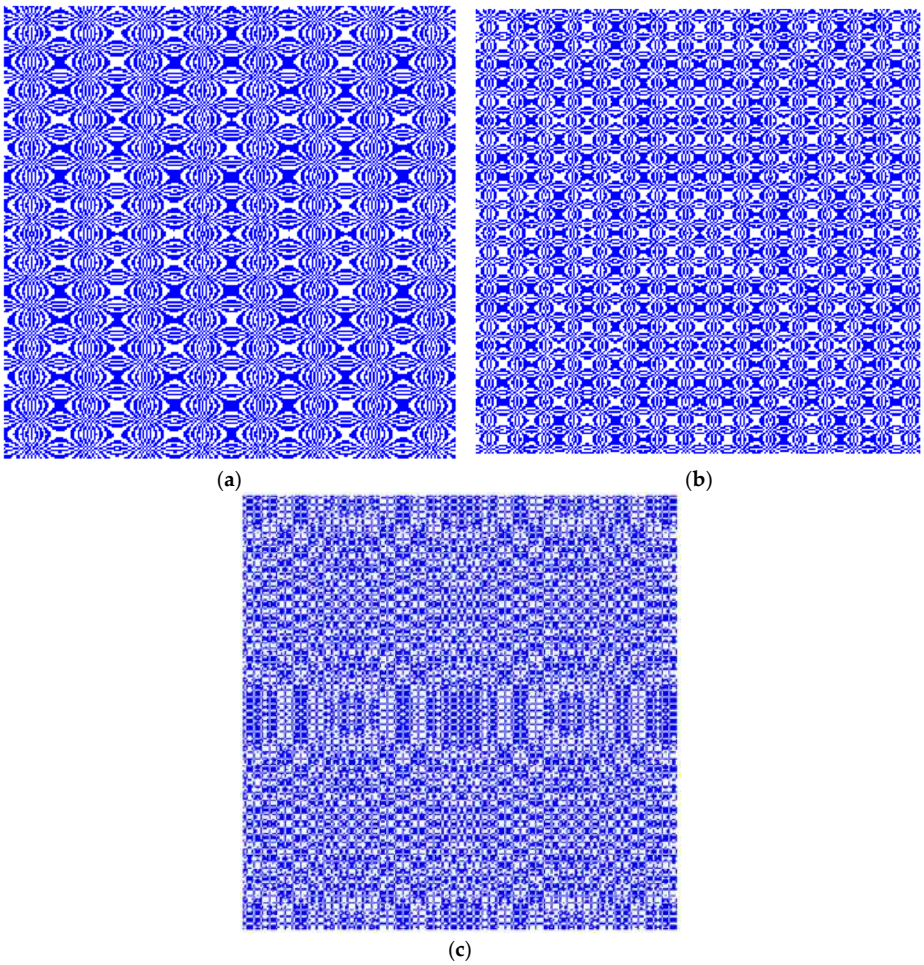


Figure 5. Mosaics generated using Formula (6); $a = 3$ (**a**), $a = 5$, (**b**), $a = 15$, (**c**), the field used is $GF(127)$.

Indeed, if expression (6) is regarded as a polynomial dependent on y, then its factorization into linear factors can be considered by using Equation (6) in its transformed form:

$$y^2\left(1 + a^2\right) + x^2\left(1 - a^2\right) = 0 \tag{7}$$

It can be seen that this equation is a particular case of an equation of the following form:

$$y^2 - f(x) = 0 \tag{8}$$

where the function $f(x)$, in general, depend on one or several additional parameters.

Consequently, the question of factorization of a polynomial of the form (8) reduces to the question of factorization of the following equation:

$$y^2 - b = 0, \ \forall b \in GF(p) \tag{9}$$

for arbitrary values of b.

Let us clarify why factorization is of interest in the context of mosaic generation using the proposed algorithm. When Equation (8) is expressed in terms of functions over real variables and $f(x) > 0$, Equation (8) can be decomposed into two equations that may be considered independently. Specifically, in this case, Equation (8) can be written as

$$\left(y - \sqrt{f(x)}\right)\left(y + \sqrt{f(x)}\right) = 0 \tag{10}$$

Equation (10) is evidently satisfied if $y - \sqrt{f(x)} = 0$ or $y + \sqrt{f(x)} = 0$, i.e., one can reduce the problem to the consideration of equations linear in y. However, when the function $f(x)$ takes values in a Galois field, the analog of the square root operation exhibits well-defined specific characteristics. These characteristics are as follows.

All nonzero elements b of the field $GF(p)$ satisfy the equation [45]

$$b^{p-1} - 1 = 0 \tag{11}$$

Each such element can be expressed as a power of a primitive element θ_0, the number of which depends on the prime p.

$$b_n = \theta_0^n; n = 0, 2, \ldots, p-2 \tag{12}$$

Consequently, it is permissible to distinguish between elements that are even and odd powers of θ_0

$$b_n = \theta_0^k \theta_0^{2m};\ k = 0, 1; m = 0, 1, \ldots, \frac{p-1}{2} \tag{13}$$

As a result, the set of equations of the form (9) splits into two subsets corresponding to the following formulas:

$$y^2 - \theta_0^{2m} = 0 \tag{14}$$

$$y^2 - \theta_0 \theta_0^{2m} = 0 \tag{15}$$

Equation (14) is solved straightforwardly. Since division by nonzero elements is allowed in Galois fields, we achieve the following formula:

$$\left(\frac{y}{\theta_0^m}\right)^2 = 1;\ y = \pm\theta_0^m \tag{16}$$

Therefore, in this case, the following is true:

$$y^2 - b = (y + \theta_0^m)(y - \theta_0^m) \tag{17}$$

Equation (15) has no solution within the base Galois field. Otherwise, the square root can be extracted only for half of the elements of the field $GF(p)$. However, the specific properties of Galois fields allow this problem to be resolved. Specifically, solutions of Equation (15) arise when passing to algebraic extensions, which are constructed precisely through irreducible algebraic equations [46,47]. This method is analogous to the construction of complex numbers, which are defined by the following equation:

$$y^2 + 1 = 0 \tag{18}$$

whose solution is the imaginary unit i, such that $i^2 = -1$.

An analog of the imaginary unit for Galois fields $GF(p)$ can be constructed using the following equation, which, as noted above, has no solution in the base field $GF(p)$.

$$y^2 - \theta_0 = 0 \tag{19}$$

This analog, as discussed in [48], provides the possibility to interpret the solution of Equation (19) as a logical imaginary unit, since the set of elements of the Galois field $GF(p)$ can be put into correspondence with the set of values of a variable in p-valued logic. The same notation will be used for this analog, i.e.,

$$i^2 = \theta_0 \tag{20}$$

It can be easily shown that any equation of the form (15) can be solved using this logical imaginary unit. Indeed, rewriting it as follows:

$$\left(\frac{y}{\theta_0^m}\right)^2 = \theta_0, \tag{21}$$

we obtain the following:

$$y = \pm i\theta_0^m \tag{22}$$

Thus, for the considered polynomial, factorization into linear factors can be indicated in this case as well:

$$y^2 - b = (y + i\theta_0^m)(y - i\theta_0^m) \tag{23}$$

Combining expressions (17) and (23), it follows that any polynomial of the form (9) can be factorized as follows:

$$y^2 - b(x) = (y + w(x))(y - w(x)) \tag{24}$$

where the function $w(x)$ takes values in an algebraic extension of the base Galois field.

Although the reasoning underlying this result is elementary from the perspective of abstract algebra, it is significant for constructing mosaics of the considered type, since any algebraic expression involving y^2, can be brought to the form (24), which is an analog of the expression corresponding to two intersecting lines (see Figure 6):

$$f(x, y) = y^2 - a^2x^2 = (y + ax)(y - ax) \tag{25}$$

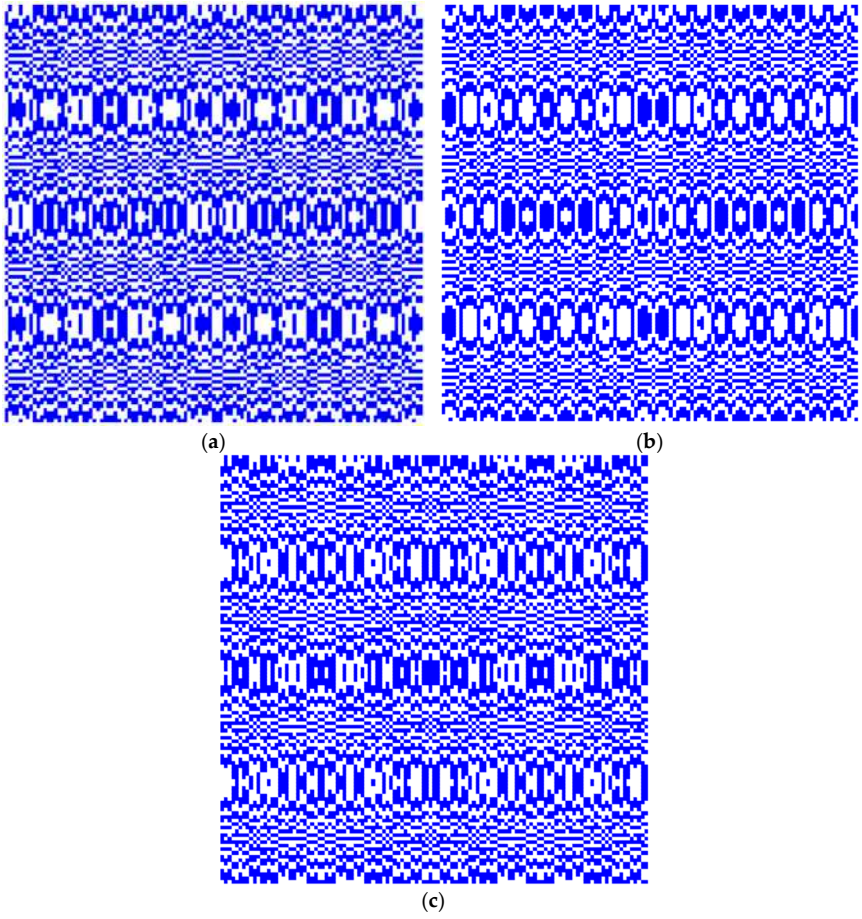


Figure 6. Mosaics generated using Formula (25); $a = 3$ (**a**), $a = 5$, (**b**), $a = 15$, (**c**), the field used is $GF(61)$.

Furthermore, from Formulas (14) and (15), it follows that the key operation for finding the function $w(x)$ given a known function $b(x)$ is the operation of discrete logarithm calculation, which allows determining the exponent of the primitive element for any nonzero element of the field $GF(p)$. This operation, in particular, enables the extraction of the square root of any element of $GF(p)$ when passing to its algebraic extension corresponding to the introduction of a logical imaginary unit. This operation can be expressed by the following formula:

$$x = \theta^n \to n \tag{26}$$

The discrete logarithm operation has been considered in numerous studies. Notably, Joux's algorithm [49], the baby-step giant-step algorithm [50,51], and the Pohlig–Hellman algorithm [52,53], among others, are well known. In the realm of quantum computing, Shor's algorithm is of particular interest [54,55]. As noted in the aforementioned studies [39,40], a significant limitation of existing methods for computing discrete logarithms is the substantial computational resources required. In the present work, the method previously proposed in [56] is employed, which is based on representing a primitive element as a product of factors, thereby substantially simplifying the computations. The method can be described as follows.

Let the number $p-1$ be factorized into the following product of powers of prime numbers p_i:

$$p - 1 = p_1^{q_1} p_2^{q_2} \dots p_k^{q_k} \tag{27}$$

Then, an arbitrary nonzero element of the field $GF(p)$ can be represented as the following product:

$$z = g_1^{s_1} g_2^{s_2} \cdots g_k^{s_k} \tag{28}$$

where the exponents s_i vary within the range from 0 to $s_{im} = p_1^{q_1}$, and g_i are elements of the considered field satisfying the following condition:

$$g_i{}^{p_1^{q_1}} = 1 \tag{29}$$

For illustration, let us consider the specific example of the field $GF(61)$. In this case, the following:

$$60 = 2^2 \cdot 3 \cdot 5 \tag{30}$$

Based on Formula (30), it is straightforward to observe that any element of this field can be expressed in the form (28), specifically as follows:

$$z = g_1^{s_1} g_2^{s_2} g_3^{s_3} \tag{31}$$

where the elements g_i can be chosen as follows $g_1 = -11$; $g_2 = 13$; $g_3 = -3$. Some arbitrariness in the choice of these elements exists because Equation (29) may be satisfied by various g_i. Furthermore, the following relations hold:

$$g_1^4 = 1;\ g_2^3 = 1;\ g_3^5 = 1 \tag{32}$$

Consequently, the exponents s_i vary within the ranges $s_1 = 0, 1, 2, 3$; $s_2 = 0, 1, 2$; $s_3 = 0, 1, 2, 3, 4$, since due to (32) the exponents in expression (31) are effectively computed modulo the powers of prime numbers appearing in the factorization (30), i.e., modulo 4, 3, and 5, respectively.

Let us consider the important particular case $s_{1,2,3} = 1$. Then the product is computed modulo 61, as follows:

$$z_0 = g_1 g_2 g_3 = 2 \tag{33}$$

Let us consider the next expression in which the product is also computed modulo 61:

$$(z_0)^r = g_1^r g_2^r g_3^r \tag{34}$$

By virtue of property (32), this expression can be rewritten as follows:

$$(z_0)^r = g_1^{r(mod4)} g_2^{r(mod3)} g_3^{r(mod5)} \tag{35}$$

It can be observed that the exponents of the elements g_i n the given expression vary within the same ranges as the exponents s_i in Formula (31). Moreover, the set of powers of the element z_0 exhausts all possible combinations of the exponents s_i. Therefore, the element z_0, appearing in Formula (33) is primitive, i.e.,

$$z_0 = \theta_0 \tag{36}$$

The obtained result is illustrated in Table 1. The first three columns of this table indicate the factors entering the product (35). The fourth column shows the element of the base Galois field formed according to Formula (35). The fifth column presents the corresponding power of the primitive element. It is evident that the values in the first three columns vary periodically with periods 4, 3, and 5, respectively, which fully corresponds to Formula (35). For clarity, the unit elements in the first three columns are highlighted in bold; these elements mark the periods of variation in the quantities $g_i^{r(mod4)}$. Table 1 also expresses the direct relationship between the considered field element and its discrete logarithm.

Table 1. The nature of the relationship between a field element and its discrete logarithm.

$g_1^{r(mod4)}$	$g_2^{r(mod3)}$	$g_3^{r(mod5)}$	$(z_0)^r$	r
−11	13	-3	2	1
−1	−14	9	4	2
11	**1**	−27	8	3
1	13	20	16	4
−11	−14	**1**	−29	5
−1	**1**	−3	3	6
11	13	9	6	7
1	−14	−27	12	8
−11	**1**	20	24	9
−1	13	**1**	−13	10
11	−14	−3	−26	11
1	**1**	9	9	12
−11	13	−27	18	13
−1	−14	20	−25	14
11	**1**	**1**	11	15
1	13	−3	22	16
−11	−14	9	−17	17
−1	**1**	−27	27	18
11	13	20	−7	19
1	−14	**1**	−14	20
−11	**1**	−3	−28	21
−1	13	9	5	22
11	−14	−27	10	23
1	**1**	20	20	24
−11	13	**1**	−21	25
−1	−14	−3	19	26

Table 1. *Cont.*

$g_1^{r(mod4)}$	$g_2^{r(mod3)}$	$g_3^{r(mod5)}$	$(z_0)^r$	r
11	**1**	9	−23	27
1	13	−27	15	28
−11	−14	20	30	29
−1	**1**	**1**	−1	30
11	13	−3	−2	31
1	−14	9	−4	32
−11	**1**	−27	−8	33
−1	13	20	−16	34
11	−14	**1**	29	35
1	**1**	−3	−3	36
−11	13	9	−6	37
−1	−14	−27	−12	38
11	**1**	20	−24	39
1	13	**1**	13	40
−11	−14	−3	26	41
−1	**1**	9	−9	42
11	13	−27	−18	43
1	−14	20	25	44
−11	**1**	**1**	−11	45
−1	13	−3	−22	46
11	−14	9	17	47
1	**1**	−27	−27	48
−11	13	20	7	49
−1	−14	**1**	14	50
11	**1**	−3	28	51
1	13	9	−5	52
−11	−14	−27	−10	53
−1	**1**	20	−20	54
11	13	**1**	21	55
1	−14	−3	−19	56
−11	**1**	9	23	57
−1	13	−27	−15	58
11	−14	20	−30	59
1	**1**	**1**	1	60

The method for calculating the discrete logarithm used in [56] is based on determining the exponents s_i. These exponents, corresponding to each element of the considered field, are presented in Table 2. The first three columns of this table contain the three values of s_i, which can be referred to as partial discrete logarithms. For clarity, the unit values of s_i are highlighted in bold in the table, marking the periods and emphasizing the periodic nature of their variation. The fourth column shows the element u of the considered Galois field corresponding to the given set of s_i values. The fifth column presents the discrete logarithm of this element, denoted as Dlu. It can be seen that it is precisely the mismatch of the periods of s_i, that allows the computation of the discrete logarithms of all nonzero elements of the considered field. The fifth and sixth columns display the exponents corresponding to the real and imaginary parts of the value w, respectively. It can be observed that, in this case, the values in the first three columns also exhibit periodic variation. Additionally, this table enables the determination of the function $w(x)$ from the function $b(x)$.

Table 2. Relationship of partial discrete logarithms with imaginary and real values of the square root.

s_1	s_2	s_3	u	Dlu	$Re(w)$	$Im(w)$
1	**1**	**1**	2	1		0
2	2	2	4	2	1	
3	0	3	8	3		1
0	**1**	4	16	4	2	
1	2	0	−29	5		2
2	0	**1**	3	6	3	
3	**1**	2	6	7		3
0	2	3	12	8	4	
1	0	4	24	9		4
2	**1**	0	−13	10	5	
3	2	**1**	−26	11		5
0	0	2	9	12	6	
1	**1**	3	18	13		6
2	2	4	−25	14	7	
3	0	0	11	15		7
0	**1**	**1**	22	16	8	
1	2	2	−17	17		8
2	0	3	27	18	9	
3	**1**	4	−7	19		9
0	2	0	−14	20	10	
1	0	**1**	−28	21		10
2	**1**	2	5	22	11	
3	2	3	10	23		11
0	0	4	20	24	12	
1	**1**	0	−21	25		12
2	2	**1**	19	26	13	
3	0	2	−23	27		13
0	**1**	3	15	28	14	
1	2	4	30	29		14
2	0	0	−1	30	15	
3	**1**	**1**	−2	31		15
0	2	2	−4	32	16	
1	0	3	−8	33		16
2	**1**	4	−16	34	17	
3	2	0	29	35		17
0	0	**1**	−3	36	18	
1	**1**	2	−6	37		18
2	2	3	−12	38	19	
3	0	4	−24	39		19
0	**1**	0	13	40	20	
1	2	**1**	26	41		20
2	0	2	−9	42	21	
3	**1**	3	−18	43		21
0	2	4	25	44	22	
1	0	0	−11	45		22
2	**1**	**1**	−22	46	23	
3	2	2	17	47		23
0	0	3	−27	48	24	
1	**1**	4	7	49		24
2	2	0	14	50	25	
3	0	**1**	28	51		25
0	**1**	2	−5	52	26	

Table 2. *Cont.*

s_1	s_2	s_3	u	Dlu	$Re(w)$	$Im(w)$
1	2	3	−10	53		26
2	0	4	−20	54	27	
3	**1**	0	21	55		27
0	2	**1**	−19	56	28	
1	0	2	23	57		28
2	**1**	3	−15	58	29	
3	2	4	−30	59		29
0	0	0	1	60	30	

The relationship between the exponents s_i and the value of the discrete logarithm follows from the following considerations. The computation of the discrete logarithm represents a mapping from the Galois field to the ring of residue classes modulo $p-1$.

Elements of such a ring, in the most general case, admit the following representation through idempotent elements, as employed, among others, in [57]:

$$s \equiv e_1 s_1 + e_2 s_2 + \ldots + e_N s_N,\ mod(p-1) \tag{37}$$

where e_i are idempotent mutually annihilating elements, and $s_i = 0, 1, 2, \ldots, p_i^{q_i} - 1$.

Formula (37) is given for the set of exponents s_i, corresponding to the exponent r, i.e., the discrete logarithm of a certain element of the considered Galois field. The idempotent elements are formed according to the rule [57]:

$$e_i = \alpha_i \prod_{i \neq j}^{N} p_j \tag{38}$$

where α_i is an integer. The choice of these integers is made under the following condition:

$$e_i e_i = 1 \tag{39}$$

The following is evident from the construction:

$$e_i p_i \equiv 0(P) \tag{40}$$

because any product of the form (40) contains the factorization $p - 1 = p_1 p_2 \ldots p_N$.

For the particular case $GF(61)$ Formula (37) takes the following form:

$$r \equiv 45 \cdot s_1 + 40 \cdot s_2 + 36 \cdot u_3,\ mod(60) \tag{41}$$

whereas before, $s_1 = 0, 1, 2, 3$; $s_2 = 0, 1, 2$; $s_3 = 0, 1, 2, 3, 4$. The fact that the numbers 45, 40, and 36 are idempotent elements modulo 60 can be verified directly.

Therefore, as employed in [56], by determining the exponents s_i, one can compute the value of the discrete logarithm according to Formula (39). This methodology also enables deriving the explicit form of the function $w(x)$, which, according to Formula (24), defines a specific mosaic. To achieve this, it suffices to separate the even and odd values of r, then compute either $\frac{r}{2}$ (for even r) or $\frac{r-1}{2}$ (or odd r). The values of the function $w(x)$ are then calculated as either $\theta_0^{\frac{r}{2}}$, or $i\theta_0^{\frac{r-1}{2}}$.

The method to identify the values of s_i, is based on the following reasoning. In [38], the algebraic delta function was defined as follows:

$$\delta(x - x_i) = 1 - (x - x_i)^{p-1}, \tag{42}$$

where x_i is a fixed element of the field $GF(p)$.

It has the following property, which follows from relation (11):

$$\delta(x - x_i) = \begin{cases} 1, & x = x_i \\ 0, & x \neq x_i \end{cases}. \tag{43}$$

Next, let us consider the following polynomial:

$$F(x) = \sum_{m=0}^{m=p-1} Dl(\theta^m)\delta(x - \theta^m), \tag{44}$$

where $Dl(\theta^m) = m$ corresponds to the discrete logarithm values (an example is contained in Table 1). When a particular element $x = \theta^{m_0}$ of the corresponding Galois field is substituted into expression (44), all summands in the sum vanish except the one where $m = m_0$. Hence,

$$F(x) \to m. \tag{45}$$

It can be observed that the use of the algebraic delta function indeed allows the problem of computing discrete logarithms to be resolved in an exceptionally transparent manner. The elements $x_m = \theta^m$ enter Formula (44) directly in the order corresponding to the computation of the discrete logarithm; therefore, when summing the polynomial in (44), its value is obtained automatically.

However, computing large powers according to Formula (42) is not an optimal procedure. It is much more convenient to consider the identifiers s_i, i.e., values, the number of which is significantly smaller than the total number of field elements. The corresponding function is given by the following:

$$S_i(x) = \sum_{k=0}^{k=p-1} s_i(\theta^m)\delta(x - \theta^m),\ i = 1, 2, 3, \tag{46}$$

In this expression, $s_i(\theta^m)$ represents the value of s_i for the k-th nonzero field element, i.e., element $x_k = \theta_0^k$ (the numbering of field elements can be chosen arbitrarily). As emphasized by Table 2, the functions $s_i(x_k)$, are periodic. For the specific field $GF(61)$ their periods are 4, 3, and 5, respectively. We will demonstrate that the periodic nature of these functions significantly simplifies the computation of expressions of the form (44) or (46).

In the theory of algebraic fields, the following is proved [45]:

$$(y \pm x)^q = y^q \pm x^q \tag{47}$$

where q is the characteristic of the field.

For fields $GF(p)$ the number p coincides with the characteristic. Direct verification proves the validity of the following equality:

$$y^p - x^p = (y - x)\left(y^{p-1} + y^{p-2}x + \ldots + yx^{p-2} + x^{p-1}\right) \tag{48}$$

Substituting the ratio (47) in the right part of Formula (48), we get the following:

$$(y - x)^{p-1} = y^{p-1} + y^{p-2}x + \ldots + yx^{p-2} + x^{p-1} \tag{49}$$

Consequently, the expression (44) can be represented as follows:

$$S_i(x) = \left(1 - x^{p-1}\right)\sum_{k=0}^{k=p-1} s_i(x_k) - \sum_{k=1}^{k=p-1} x^{p-1-k}Q_k \tag{50}$$

where

$$Q_k = \sum_{l=1}^{l=p-1} s_i(x_l) x_l^k = \sum_{l=1}^{l=p-1} s_i\left(\theta^l\right)\theta^{kl}, \quad (51)$$

The first term in (50) vanishes by virtue of relation (11).

Sequences

$$w_m = \left(1, \theta^m, \theta^{2m}, \theta^{3m}, \ldots, \theta^{(p-2)m}\right) \quad (52)$$

form [57] a complete orthogonal basis on the interval containing p-1 cycles, i.e.,

$$\sum_{j=0}^{j=p-2} w_{k_1}^{(j)} w_{k_2}^{(j)} = \begin{cases} 1, k_1 \equiv k_2 (mod\ (p-1)) \\ 0, k_1 \not\equiv k_2 (mod (p-1)) \end{cases} \quad (53)$$

Therefore, the Q_k values are non-binary Galois fields Fourier transform functions $s_i\left(\theta^l\right)$:

$$Q_k = \hat{F}[s_i(x)] = \sum_{l=1}^{l=p-1} s_i\left(\theta^l\right)\theta^{k \cdot l} \quad (54)$$

Importantly, the functions $s_i\left(\theta^l\right)$ are periodic with a relatively small number of periods. For example, if a function has period 5, then the number of nonzero spectral components cannot exceed 5. Consequently, an expression of the form (51) contains no more than five terms in this case, which significantly simplifies computational procedures.

A block diagram illustrating the generalized procedure for computing the discrete logarithm using the proposed methodology is shown in Figure 7.

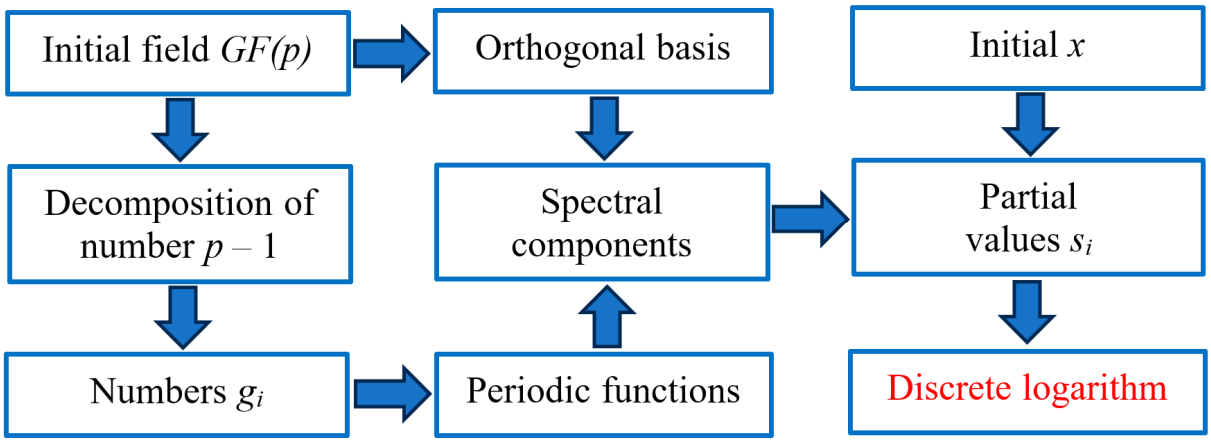


Figure 7. Block diagram of operations enabling the computation of the discrete logarithm using the partial values s_i.

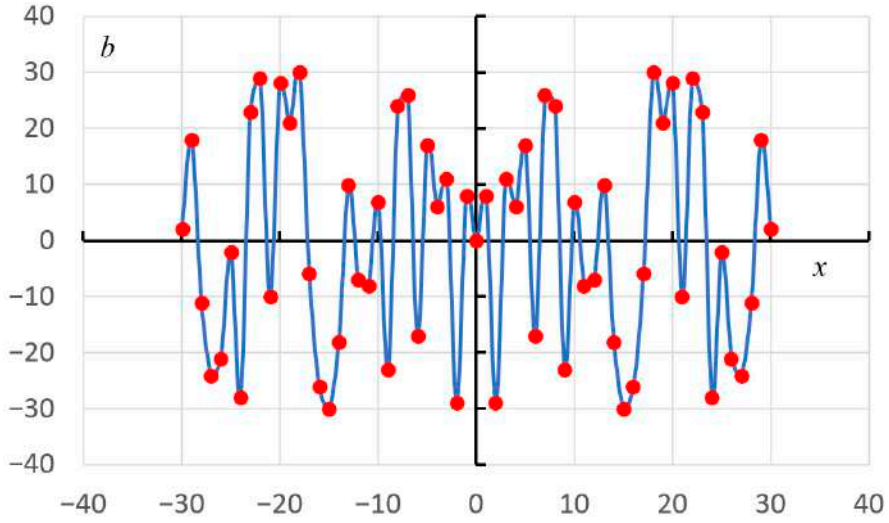
The initial step involves selecting the Galois field to be used for mosaic construction ("Initial field *GF(p)*"). Next, according to Formula (27), the number $p-1$ is factorized into prime factors ("Decomposition of number $p-1$"). Based on these values, the values g_i are selected ("Numbers g_i"), which allow the primitive element to be represented as a product of roots of unity in accordance with Formula (31). Finding such values constitutes an independent task; however, as follows from the results presented below, for applied purposes related to mosaic generation, it is sufficient to use Galois fields with relatively small characteristics. Since the number of primes in the range from 1 to 300 is limited, pre-tabulated values can be used when implementing the algorithm.

Using the values of g_i, periodic functions ("Periodic functions") entering Formula (46) are then constructed. Examples of such functions are presented in Table 2, columns 1–3. In parallel, an orthogonal basis ("Orthogonal basis") is formed, determined by the employed Galois field according to Formula (53). Using this basis, the spectral components of the

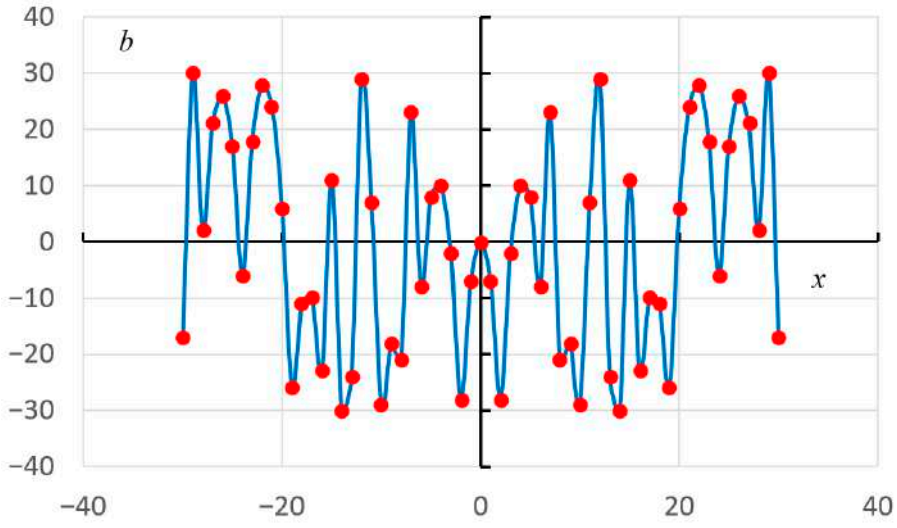
functions in Formula (46) are computed ("Spectral components"). On this basis, the quantities s_i ("Partial values s_i") are calculated, from which, using Formula (37), the discrete logarithm ("Discrete logarithm") for a given number x ("Initial x") is determined. An example of programming code implementing the discrete logarithm operation is provided in Supporting Information S2.

Examples of the application of the discrete logarithm computation algorithm are illustrated in Figures 8 and 9. Figure 8 shows examples of functions $b(x)$ corresponding to mosaics constructed using Formula (7), i.e.,

$$b(x) = x^2\left(a^2 - 1\right)\left(1 + a^2\right)^{-1} \tag{55}$$

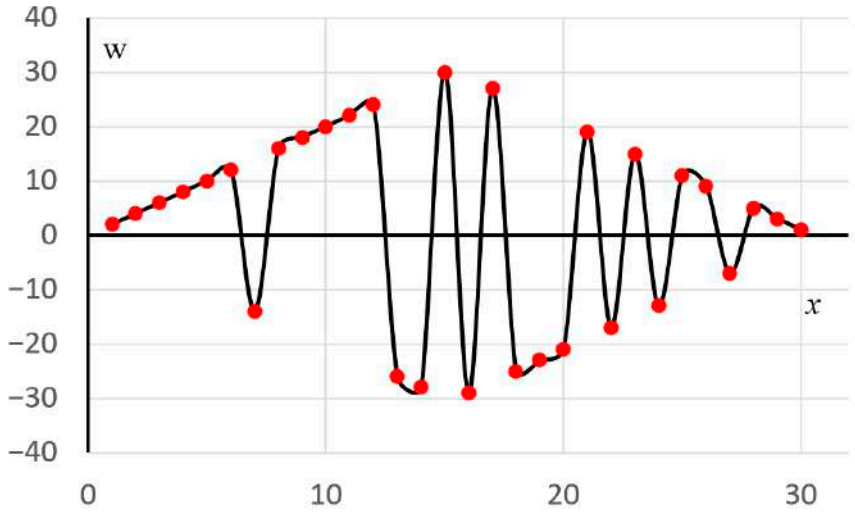


(**a**)

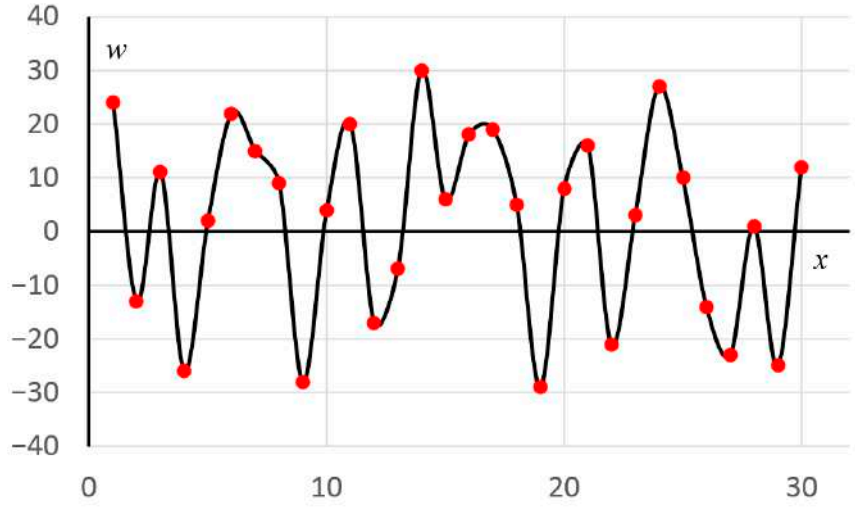


(**b**)

Figure 8. Examples of functions $b(x)$, corresponding to mosaics constructed using the algebraic expression (7) and Formula (55); $a = 5$ (**a**), $a = 30$ (**b**).



(**a**)



(**b**)

Figure 9. Imaginary parts of the square root of the functions shown in Figure 8a (**a**) and Figure 8b (**b**).

Figure 9 presents the functions corresponding to the solutions of Equations (15) for these particular cases. Figure 9a and 9b correspond to the imaginary parts of the extracted square root for the cases of Figure 8a and 8b, respectively.

Notably, in the calculation according to Formula (55), the inverse element of the sum $1 + a^2$ within the sense of the employed Galois field is used (fractional values do not arise).

It can be observed that the considered algorithm indeed allows the description of rather complex mosaics to be reduced to relatively simple functions, albeit taking values in an algebraic extension of the base Galois field. On this basis, it is possible, in perspective, to develop a method for generating mosaics by directly specifying the functions $w(x)$. In particular, it is permissible to construct mosaics in which the functions $w(x)$ take only real values. The first step in this direction involves a method in which the functions $b(x)$, initially computed based on polynomial functions, are subsequently modified in various ways. At the next stage, it becomes possible to implement an algorithm that ensures a gradual (stepwise) transition from one type of mosaic to another. A preliminary experiment demonstrating the potential of this approach is presented in Supporting Information S3. In this experiment, the programming code provided in Supporting Information S3 was used. The code employs the same mosaic generation algorithm as that in Supporting Information

S1, with the exception that every second computed value is artificially set to zero. The examples presented in Supporting Information S3 show that, in this case, the resulting mosaic structures approximate configurations that visually decompose into fragments corresponding to parallel ornamented bands. For generality, the code reads the functions $b(x)$ from a separate file.

Despite the simplicity of expression (25), this expression enables the generation of a wide range of nontrivial mosaics. In particular, Figures 10–15 present mosaics obtained using the following algebraic expression:

$$f(x, y) = y^2(a - x) - x^2 \tag{56}$$

It can be seen that the polynomial on the right-hand side can also be brought to the form (25), since it can be transformed into the following equality:

$$y^2 - x^2(a - x)^{-1} = 0 \tag{57}$$

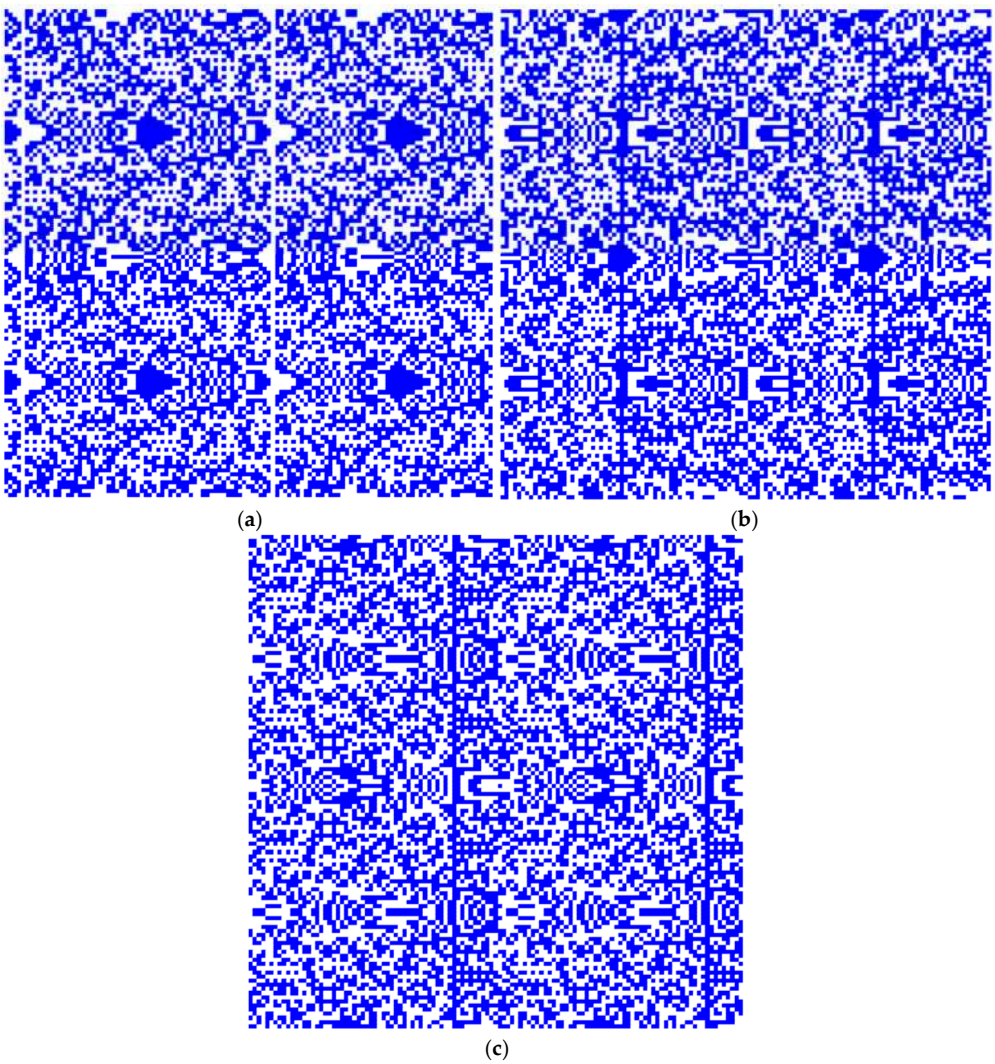
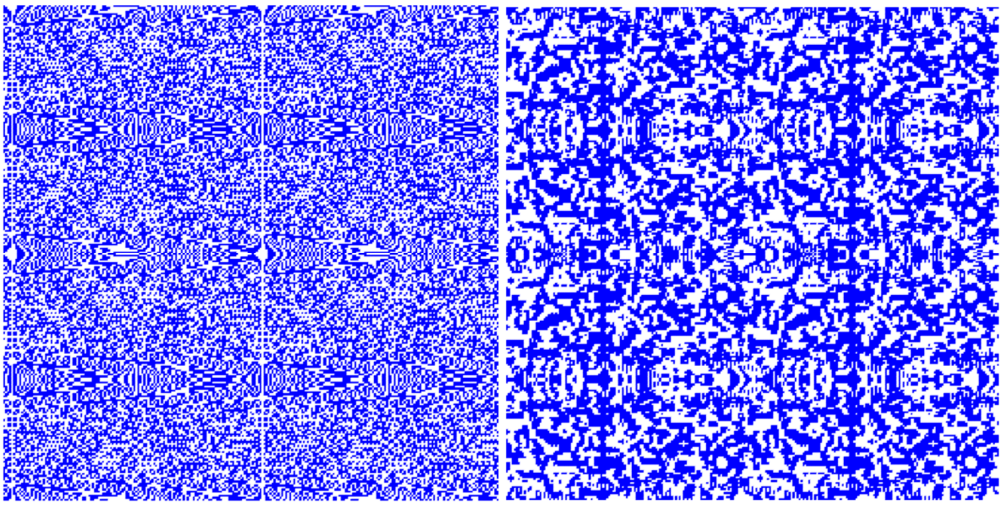
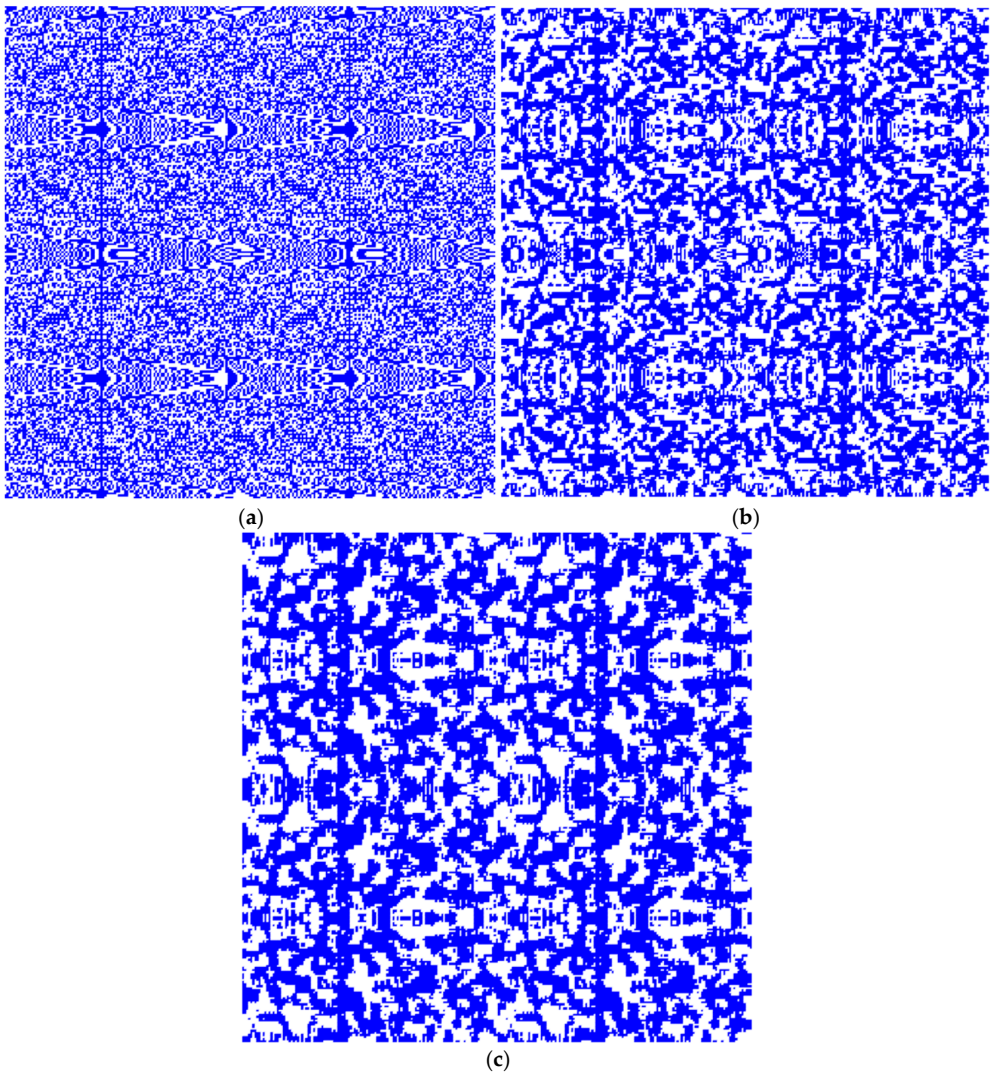


Figure 10. Mosaics obtained using Formula (56); $a = 5$ (**a**), $a = 30$, (**b**), $a = 50$, (**c**), with the Galois field $GF(61)$.



(**a**) (**b**)

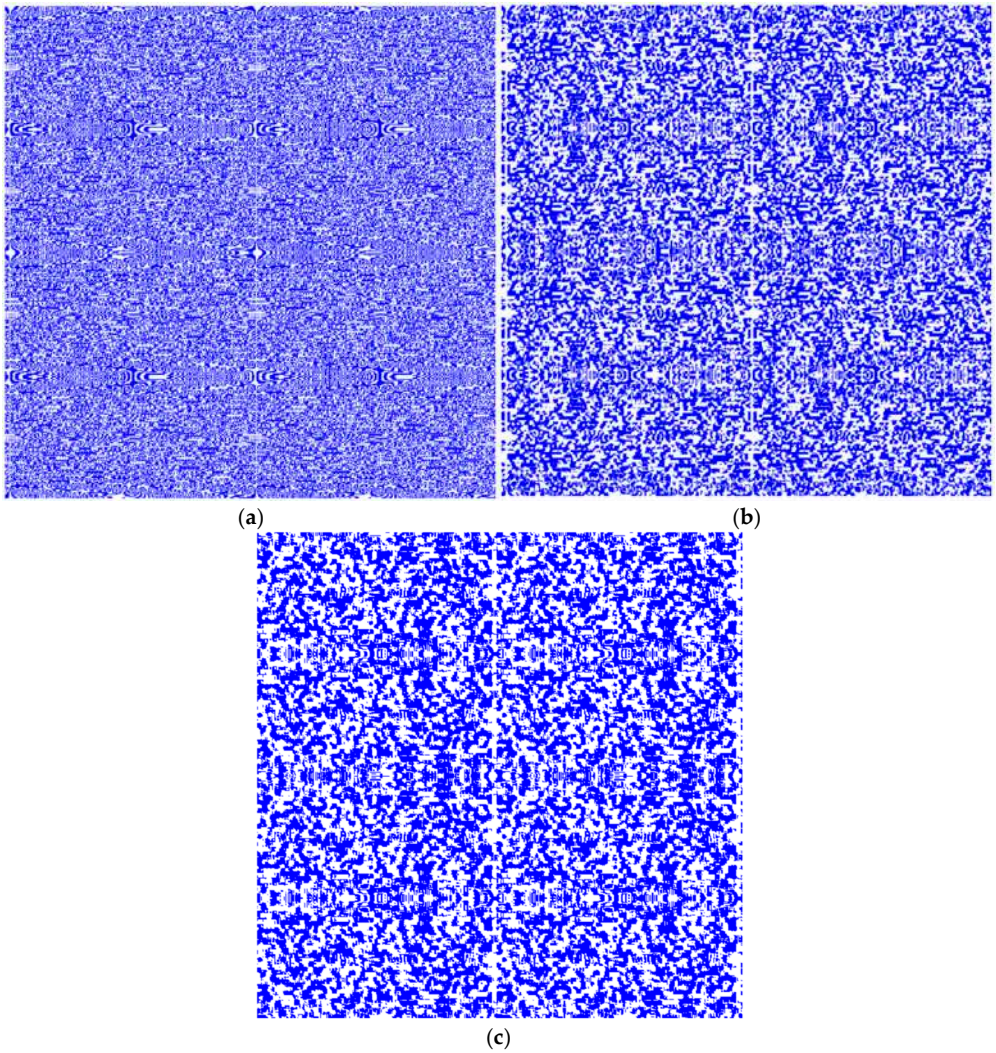
Figure 11. Mosaics obtained using Formula (56); $a = 5$, Galois field $GF(127)$, (**a**) original mosaic, (**b**) result after smoothing.



(**a**) (**b**)

(**c**)

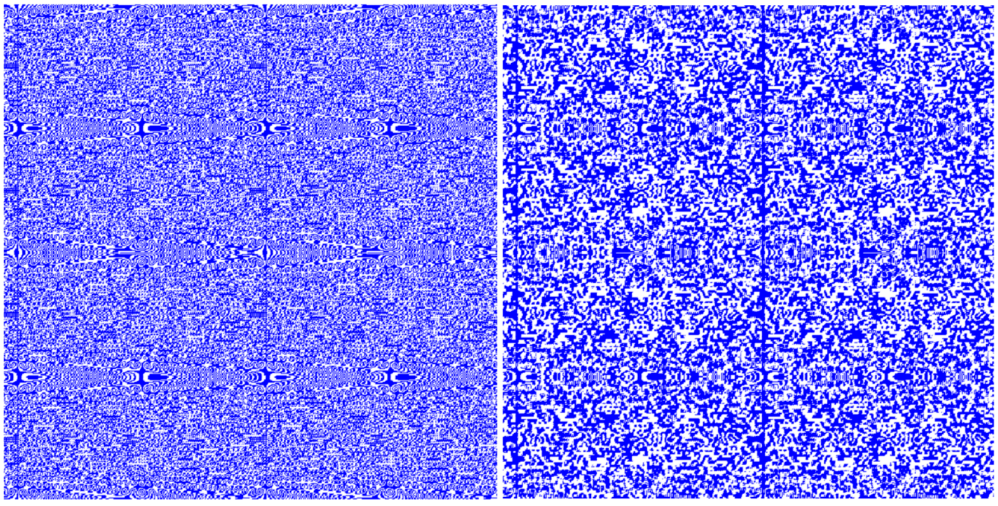
Figure 12. Mosaics obtained using Formula (56); $a = 50$, Galois field $GF(127)$, (**a**) original mosaic, (**b**) result after smoothing over 9 pixels, (**c**) result after smoothing over 25 pixels.



(**a**) (**b**)

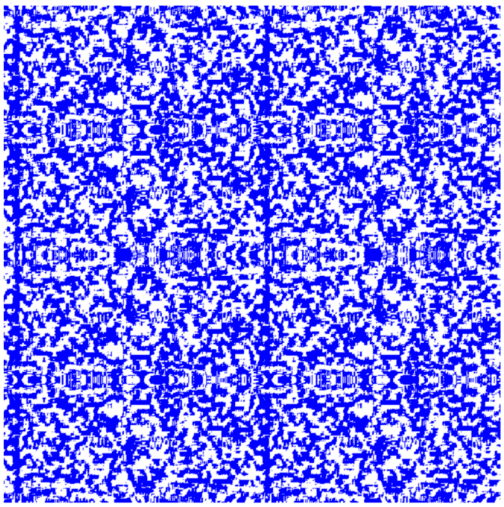
(**c**)

Figure 13. Mosaics obtained using Formula (56); $a = 5$, Galois field $GF(257)$, (**a**) original mosaic, (**b**) result after smoothing over 9 pixels, (**c**) result after smoothing over 25 pixels.



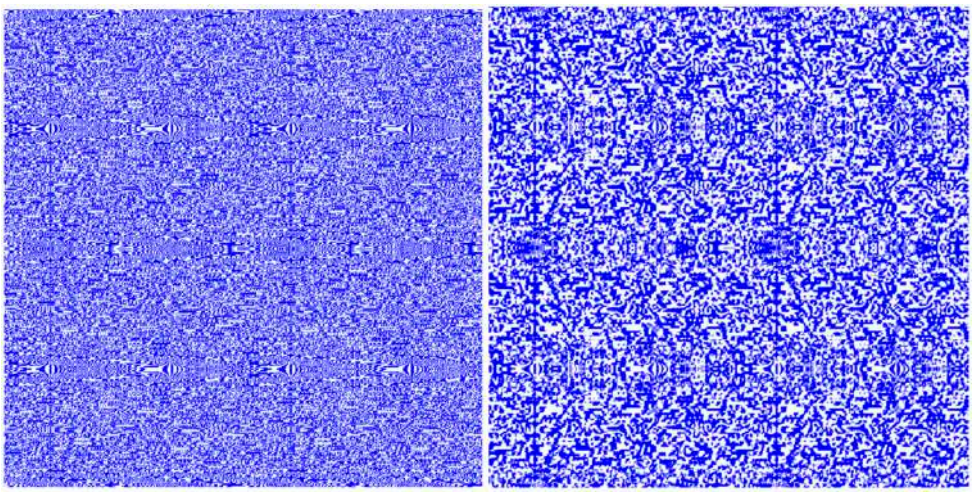
(**a**) (**b**)

Figure 14. *Cont.*

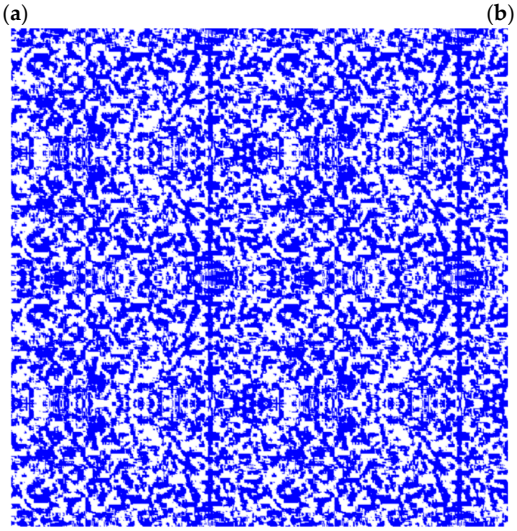


(**c**)

Figure 14. Mosaics obtained using Formula (56); $a = 15$, Galois field $GF(257)$, (**a**) original mosaic, (**b**) result after smoothing over 9 pixels, (**c**) result after smoothing over 25 pixels.



(**a**) (**b**)



(**c**)

Figure 15. Mosaics obtained using Formula (56); $a = 50$, Galois field $GF(257)$, (**a**) original mosaic, (**b**) result after smoothing over 9 pixels, (**c**) result after smoothing over 25 pixels.

In the construction of the mosaics presented in Figures 11–15, smoothing of the resulting structures was also applied. An algorithm analogous to the moving average method was employed. For each pixel with coordinates i, j, a square centered at that pixel is considered. For Figures 11b, 12b, 13b, 14b and 15b, this square includes 9 pixels (including the central pixel), while for Figures 12c, 13c, 14c and 15c, it includes 25 pixels. The resulting color is determined based on the majority of pixels (white or colored) within the selected square.

The resulting mosaics demonstrate that the smoothing procedure allows the periodic nature of mosaics generated using Galois fields with relatively large characteristics to be clearly revealed. Smoothing also provides an additional tool for mosaic generation, since increasing the field characteristic (even only up to 257) produces an excessively complex mosaic, which is unlikely to be of practical interest, particularly for applications such as textile or wallpaper pattern design. The use of excessively complex mosaics in psychological testing is also not justified.

For comparison, Figure 16 presents mosaics formed using the cissoid of Diocles.

$$f(x, y) = y^2(a - x) - x^3 \tag{58}$$

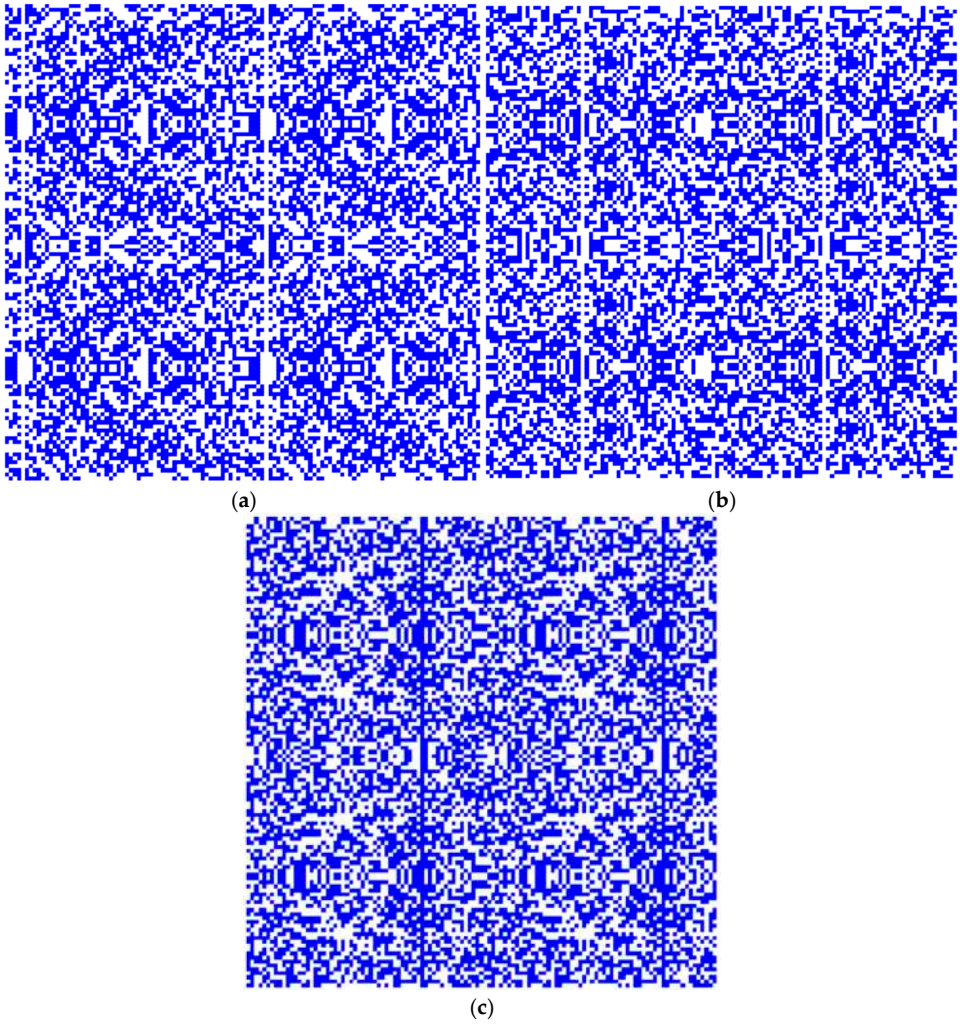


Figure 16. Mosaics obtained using Formula (56); $a = 5$ (**a**), $a = 25$, (**b**), $a = 45$, (**c**), with the Galois field $GF(61)$.

The presented mosaics indicate that, in terms of mosaic generation, transitioning to more complex equations (even cubic equations) is not always justified. Visually, mosaics corresponding to an equation containing a variable to the third power are similar to those

generated using simpler equations. This observation, of course, does not preclude potential applications of more complex equations in the future. However, for the purposes of psychological testing and for generating patterns used in the production of textiles, wallpapers, and similar materials, it is sufficient to employ relatively simple algebraic expressions.

4. Discussions

The use of Galois fields enables the development of a relatively simple algorithm for generating mosaics suitable for applied purposes, such as the production of textiles, including smart textiles [10], wallpapers, floor coverings, and similar applications. Modern manufacturing technologies allow for the production of wallpapers, carpets, and similar products tailored to individual preferences [12,17]. Many commonly used patterns are geometric in nature and closely resemble the mosaics examined in this study. Therefore, there is potential to select mosaic patterns not only for aesthetic appeal but also for enhancing psychological comfort in living environments.

Another promising area of application for such mosaics is the development of novel approaches to improving established psychological testing methods, in particular those such as the Rorschach test [28,29]. It should be noted that other commonly used tests also employ well-defined images (in particular, the Szondi Test [24] and Susan Dellinger's psychogeometric test [25], both of which were mentioned above). These techniques have been subject to considerable criticism [26], which also applies to the Rorschach test [58]. The automatic generation of mosaics capable of evoking specific associations in test subjects offers a pathway to improving association-based methods, as suggested in [27]. Crucially, the link between mosaics and algebraic structures is essential for the statistical analysis and validation of the obtained results.

The main advantage of using Galois fields for these purposes lies in the possibility of employing extremely simple algebraic expressions to generate relatively complex mosaics. A comparison of the main characteristics of the proposed approach with previously known methods is presented in Table 3. It should be emphasized that this table does not consider the metric of mosaic generation speed. This metric is not critical, as practical applications in the contexts under consideration only require reaching a rate of 24 frames per second, which corresponds to the existing standard. Achieving higher speeds is not meaningful.

The simplicity and convenience of mosaic generation using the proposed algorithm (Supporting Information S1) also enable the development of a comprehensive psychological testing methodology, simultaneously oriented toward analyzing the current psychological state of the subject and identifying factors corresponding to archetypal levels. As demonstrated in [1,2], cited in the Introduction, mosaic ornaments are an integral part of the cultural heritage of many nations worldwide. Accordingly, there is reason to believe that the corresponding patterns, in one way or another, correlate with archetypes. On this basis, a comprehensive psychological testing methodology could be developed in the future, in which both mosaics correlating with culturally traditional patterns and responses to specific questions are employed.

For the development of such methodologies (as well as for the refinement of psychological testing methods based on the findings of [27] and similar studies), the ability to generate mosaic structures that transition stepwise from one to another is of crucial importance. The feasibility of implementing such an approach is confirmed by the results presented in Supporting Information S3. It should also be noted that the transition from one mosaic structure to another is of interest for applications such as the advancement of smart textiles.

Table 3. Comparison of the main characteristics of the proposed approach with previously known methods.

Criterion	Proposed Approach	Previously Known Approaches
Mosaic periodicity	Periodicity arises automatically due to the properties of Galois fields, even for simple algebraic expressions	Periodicity must be imposed artificially, typically requiring a special algorithm [15,18,20]
Need for an initial pattern	Not required	An initial pattern is necessary [15,18,20]
Mosaic modification and control	Stepwise transitions between different types of mosaics are possible	Mechanisms for transitioning between patterns of different types are either not provided [15,20] or require direct operator intervention [18,19,22]
Implementation complexity	The code is extremely simple (example—SI-1); computations use only integers	Algorithm implementation involves computational complexities [19,21,22] or requires searching for the initial pattern [15,18,20]
Scalability/detail level	Details can be enhanced straightforwardly by increasing the field characteristic	Detail enhancement is possible, but operations required for it are comparable in complexity to generating a new mosaic [15,18–21]
Post-processing/complexity management	Simple smoothing (analogous to 3×3 or 5×5 moving window) helps reveal periodicity and reduce excessive complexity	The use of smoothing filters is not provided [15,18,20,21]
Limitations	Requires a simple modulus pp; special cases for pp of the form 2 m -1 (quasi-Mersenne primes), and the possibility to relax the requirement via finite rings	Limitations depend on the method (tiling rules, geometric/numerical constraints, etc.)

It is emphasized that this capability is enabled, in particular, by the properties of Galois fields, which allow mosaics to be realized using maximally simple algebraic expressions. The transition from one such expression to another can be defined algorithmically. Additional possibilities in this regard are provided by the transition to algebraic extensions of Galois fields, where the relevant polynomials decompose into linear factors. For equations of the form (8), all polynomial roots can be found using discrete logarithm computation. It should also be noted that equations of the form (8), corresponding to binomial polynomials, represent a specific case. However, the proposed approach can be readily generalized to equations of the following form:

$$y^N - b(x) = 0 \tag{59}$$

The use of relations of the type (59) for the aforementioned purposes generally requires the computation of discrete logarithms. This methodology is also presented in the current work. Regarding the operation of discrete logarithm computation, there is a specific nuance. For fields associated with primes of the form $p = 2^k + 1$, relation (27) becomes degenerate. These primes can be interpreted as quasi-Mersenne numbers [59]. However, in such cases, the discrete logarithm operation can be performed using the results from the cited work. Furthermore, the limitation on mosaic dimensions, determined by the requirement that p be prime, can be at least partially relaxed by employing the results of [60]. In this case, finite algebraic rings are used instead of Galois fields, and it can be anticipated that mosaic construction in the future may be implemented

through logical operations, as described in the cited source. The solution to this problem, however, remains a matter for future research.

In a broader perspective, the proposed method for generating mosaic structures can be used to develop techniques for diagnosing structures similar to mosaics based on the use of radio waves. As shown in [41–43], cited in the Introduction, the analysis of mosaic-like structures is of interest for monitoring agricultural lands.

In [61], it was demonstrated that the description of any radiation transformer obeying the Helmholtz equation or its analog can be reduced to a discrete form. This conclusion is based on the fact that the classical Huygens–Fresnel principle can also be expressed in discrete form, which is particularly relevant for addressing problems in radio holography, an area currently undergoing active development [62–64].

For the development of such methods, especially those oriented toward practical applications (as dictated, for example, by mosaic-like structures occurring naturally [41–43]), it is expedient to employ certain test structures, which can be generated using the proposed method.

5. Conclusions

The generation of large arrays of diverse mosaics can be achieved through the use of an algorithm based on Galois fields and simple algebraic expressions (including classical expressions, such as the Bernoulli lemniscate or the Diocles' cissoid). The advantage of this approach lies in the simplicity of implementing the computational algorithm, as well as the possibility of ensuring a gradual transition from one mosaic to another. The proposed method allows for generalization through the use of algebraic extensions of the base field, as well as the computation of discrete logarithms.

The proposed method for constructing complex mosaic structures holds promise for a variety of practical applications, including psychological testing. The most immediate application lies in expanding the design possibilities of wallpapers, fabrics, and related products—particularly with the aim of enhancing psychological well-being for consumers.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/sym17091415/s1, Supporting Information S1: Python code for mosaic generation using the function F(x,y); Supporting Information S2: Python code for discrete logarithm computation in GF(p); Supporting Information S3: Program code for conducting experiments on artificial variation of the function b(x) and experimental results obtained using this code.

Author Contributions: Conceptualization, I.S.; data curation, D.S. and Y.V.; formal analysis, A.S.B.; funding acquisition, D.S., Y.V. and I.S.; methodology, I.S.; project administration, Y.V.; resources, D.S.; software, A.S.B.; supervision, Y.V.; validation, A.S.B.; visualization, A.S.B.; writing—original draft, I.S.; writing—review and editing, D.S. and Y.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26104635).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: Author Yelizaveta Vitulyova was employed by the JSC "Institute of Digital Engineering and Technology". The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Pintus, R.; Pal, K.; Yang, Y.; Weyrich, T.; Gobbetti, E.; Rushmeier, H. A survey of geometric analysis in cultural heritage. *Comput. Graph. Forum* **2016**, *35*, 4–31. [CrossRef]
2. Sobh, H.; Samy, H.A. Islamic geometric patterns as timeless architecture. *J. Al-Azhar Univ. Eng. Sect.* **2018**, *13*, 1074–1088. [CrossRef]
3. Jebur, A.K. The techniques of cultural heritage: Literature review. *Saudi J. Civ. Eng.* **2022**, *6*, 108–114. [CrossRef]
4. Jabi, W.; Potamianos, I. Geometry, light, and cosmology in the church of Hagia Sophia. *Int. J. Archit. Comput.* **2007**, *5*, 303–319. [CrossRef]
5. Thalal, A.; Aboufadil, Y.; Elidrissi Raghni, M.A.; Jali, A.; Oueriagli, A.; Ait Rai, K. Symmetry in art and architecture of the Western Islamic world. *Crystallogr. Rev.* **2018**, *24*, 102–130. [CrossRef]
6. Xu, P. The Mandala as a cosmic model used to systematically structure the Tibetan Buddhist Landscape. *J. Archit. Plan. Res.* **2010**, *27*, 181–203.
7. Xiao, Y.-Q.; Kan, C.-W. Review on Development and Application of 3D-Printing Technology in Textile and Fashion Design. *Coatings* **2022**, *12*, 267. [CrossRef]
8. Liu, J.; Jiang, S. Textile-Based 3D Printing and Traditional Chinese Geometric Patterns for Fashion Textile Development. *J. Text. Inst.* **2024**, *116*, 2087–2099. [CrossRef]
9. Arikan, C.O.; Doğan, S.; Muck, D. Geometric structures in textile design made with 3D printing. *Tekstilec* **2022**, *65*, 307–321. [CrossRef]
10. Nilsson, L.; Vallgårda, A.; Worbin, L. Designing with Smart Textiles: A New Research Program. In Proceedings of the Nordes Making Design Matter, Helsinki, Finland, 29–31 May 2011.
11. Matté, L.L.; Broega, A.C. The Evaluation of (Social-) Psychological Comfort in Clothing: A Possible Approach. *IOP Conf. Ser. Mater. Sci. Eng.* **2017**, *254*, 182008. [CrossRef]
12. Stylios, G.K.; Chen, M. The concept of psychotextiles; interactions between changing patterns and the human visual brain, by a novel composite SMART fabric. *Materials* **2020**, *13*, 725. [CrossRef]
13. Zeng, F.; Wang, G.; Qiao, J.; Wang, Q.; Wu, M.; Zeng, X.; Hong, X. Modeling the Relationship between Fabric Textures and the Evoked Emotions through Different Sensory Perceptions. *J. Eng. Fibers Fabr.* **2024**, *19*, 15589250241248761. [CrossRef]
14. de Melo, M.J. *Mosaic as an Experimental System: Materials, Practices and Knowledges in Art and Science*; University of Amsterdam: Amsterdam, The Netherlands, 2019.
15. Zhang, J.; Zhang, K.; Peng, R.; Yu, J. Parametric modeling and generation of mandala thangka patterns. *J. Comput. Lang.* **2020**, *58*, 100968. [CrossRef]
16. Suleimenov, I.E.; Gabrielyan, O.A.; Bakirov, A.S. Neural network approach to the interpretation of ancient Chinese geomancy feng shui practices. *Eur. J. Sci. Theol.* **2023**, *19*, 39–51.
17. Teixeira, T.G.B.; de Medeiros, J.F.; Kolling, C.; Duarte Ribeiro, J.L.; Morea, D. Redesign in the Textile Industry: Proposal of a Methodology for the Insertion of Circular Thinking in Product Development Processes. *J. Clean. Prod.* **2023**, *397*, 136588. [CrossRef]
18. An, M.H.; Jang, A.R. Development of textile pattern design by MC Escher's tessellation technique using chaekgeori icons. *Fash Text* **2023**, *10*, 15. [CrossRef]
19. Liu, S. A Method for Image Mosaic of Textile Printing Fabric Based on SIFT Feature Matching. In Proceedings of the 6th International Conference on Management, Education, Information and Control (MEICI 2016), Shenyang, China, 23–25 September 2016; Atlantis Press: Dordrecht, The Netherlands, 2016; pp. 953–957.
20. Kunkhet, A.; Chudasri, D. Design Approaches for Tile Pattern Designs Inspired by Traditional Textiles. *Processes* **2022**, *10*, 1460. [CrossRef]
21. Massarwe, K.; Verner, I.; Bshouty, D.; Verner, I. An ethnomathematics exercise in analyzing and constructing ornaments in a geometry class. *J. Math. Cult.* **2010**, *5*, 1–20.
22. Wang, W.; Zhang, G.; Yang, L.; Wang, W. Research on garment pattern design based on fractal graphics. *J. Image Video Proc.* **2019**, *2029*, 29. [CrossRef]
23. Furrer, W. Psychiatric test methods, especially the Lüscher color test. *Ther. Present* **1967**, *106*, 1290–1300.
24. Borstelmann, L.J.; Klopfer, W.G. The Szondi Test: A review and critical evaluation. *Psychol. Bull.* **1953**, *50*, 12. [CrossRef]
25. Mayall, K.; Dellinger, S. *Your Personal Communication Style (Parenting Shape eBook) (Kindle Edition)*; Jade Ink: Oakland, CA, USA, 1953.
26. Paluchowski, W.J.; Stemplewska-Żakowicz, K. The reliability of projective techniques as tools of psychological assessment. Part 1: Why it is unjustified to describe some of them as projective. *Probl. Forensic Sci.* **2013**, *93*, 421–430.
27. Suleimenov, I.; Kostsova, M.; Grishina, A.; Matrassulova, D.; Vitulyova, Y. Empirical validation of the use of projective techniques in psychological testing using Galois fields. *Front. Appl. Math. Stat.* **2024**, *10*, 1455500. [CrossRef]

28. Pianowski, G.; Villemor-Amaral, A.E.D.; Meyer, G.J. Comparing the validity of the Rorschach Performance Assessment System and Exner's Comprehensive System to differentiate patients and nonpatients. *Assessment* **2023**, *30*, 2417–2432. [CrossRef]
29. Khadivi, A. Review of a Special Issue of Rorschachiana: The Rorschach Test Today: An Update on the Research. *J. Personal. Assess.* **2023**, *105*, 578–579. [CrossRef]
30. Bhaskar, R.; Dubey, P.K.; Kumar, V.; Rudra, A. Efficient Galois field arithmetic on SIMD architectures. In Proceedings of the 15th Annual ACM Symposium on Parallel Algorithms and Architectures (SPAA'03), San Diego, CA, USA, 7–9 June 2003; pp. 256–257. [CrossRef]
31. Vitulyova, Y.S.; Bakirov, A.S.; Suleimenov, I.E. Galois fields for digital image and signal processing: Evidence for the importance of field specificity. In Proceedings of the 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), Chengdu, China, 19–21 August 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 637–642.
32. Kuang, R.; Perepechaenko, M.; Barbeau, M. A new quantum-safe multivariate polynomial public key digital signature algorithm. *Sci. Rep.* **2022**, *12*, 13168. [CrossRef]
33. Thi, H.P.; Lee, H. Basic-Set Trellis Min–Max Decoder Architecture for Nonbinary LDPC Codes with High-Order Galois Fields. In *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*; IEEE: Piscataway, NJ, USA, 2018; Volume 26, pp. 496–507. [CrossRef]
34. Alinejad, M.; Hassan Zadeh, S.; Biranvand, N. Digital Signature with Elliptic Curves over the Finite Fields. *J. Discret. Math. Sci. Cryptogr.* **2022**, *25*, 1289–1301. [CrossRef]
35. Larasati, H.T.; Kim, H. Quantum cryptanalysis landscape of shor's algorithm for elliptic curve discrete logarithm problem. In *International Conference on Information Security Applications*; Springer: Cham, Switzerland, 2021; pp. 91–104.
36. O'Keeffe, M.; Treacy, M.M.J. The Symmetry and Topology of Finite and Periodic Graphs and Their Embeddings in Three-Dimensional Euclidean Space. *Symmetry* **2022**, *14*, 822. [CrossRef]
37. Evans, M.E.; Robins, V.; Hyde, S.T. Ideal geometry of periodic entanglements. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **2015**, *471*, 20150254. [CrossRef]
38. Suleimenov, I.E.; Vitulyova, Y.S.; Kabdushev, S.B.; Bakirov, A.S. Improving the efficiency of using multivalued logic tools. *Sci. Rep.* **2023**, *13*, 1108. [CrossRef]
39. Odlyzko, A. Discrete Logarithms: The Past and the Future. *Des. Codes Cryptogr.* **2000**, *19*, 129–145. [CrossRef]
40. Sarkar, A.; Guha Roy, D.; Datta, P. An Overview of the Discrete Logarithm Problem in Cryptography. In *Proceedings of Third International Conference on Advanced Computing and Applications*; ICACA 2024; Lecture Notes in Networks and Systems; Giri, D., Das, S., Corchado Rodríguez, J.M., De, D., Eds.; Springer: Singapore, 2024; Volume 1045. [CrossRef]
41. Mukhamediev, R.I.; Merembayev, T.; Kuchin, Y.; Malakhov, D.; Zaitseva, E.; Levashenko, V.; Popova, Y.; Symagulov, A.; Sagatdinova, G.; Amirgaliyev, Y. Soil Salinity Estimation for South Kazakhstan Based on SAR Sentinel-1 and Landsat-8,9 OLI Data with Machine Learning Models. *Remote Sens.* **2023**, *15*, 4269. [CrossRef]
42. Atzberger, C. Advances in Remote Sensing of Agriculture: Context Description, Existing Operational Monitoring Systems and Major Information Needs. *Remote Sens.* **2013**, *5*, 949–981. [CrossRef]
43. Mukhamediev, R.I.; Terekhov, A.; Amirgaliyev, Y.; Popova, Y.; Malakhov, D.; Kuchin, Y.; Sagatdinova, G.; Symagulov, A.; Muhamedijeva, E.; Gricenko, P. Using Pseudo-Color Maps and Machine Learning Methods to Estimate Long-Term Salinity of Soils. *Agronomy* **2024**, *14*, 2103. [CrossRef]
44. Suleimenov, I.E.; Bakirov, A.S.; Matrassulova, D.K. A technique for analyzing neural networks in terms of ternary logic. *J. Theor. Appl. Inf. Technol.* **2021**, *99*, 2537–2553.
45. van der Waerden, B.L. *Algebra*; Springer-Verlag New York, Inc.: New York, NY, USA, 1991; Volume 1, 265p.
46. Tudunkaya, S.M.; Kiri, A.I. Galois groups of polynomials and the construction of finite fields. *Pure Appl. Math. J.* **2012**, *1*, 10–16. [CrossRef]
47. Kim, K.-S.; König, J. On Galois extensions with prescribed decomposition groups. *J. Number Theory* **2021**, *220*, 266–294. [CrossRef]
48. Vitulyova, E.S.; Matrassulova, D.K.; Suleimenov, I.E. Construction of generalized Rademacher functions in terms of ternary logic: Solving the problem of visibility of using Galois fields for digital signal processing. *Int. J. Electron. Telecommun.* **2022**, *68*, 237–244. [CrossRef]
49. Adj, G.; Menezes, A.; Oliveira, T.; Rodriguez-Henriquez, F. Computing discrete logarithms using Joux's algorithm. *ACM Commun. Comput. Algebra* **2015**, *49*, 60. [CrossRef]
50. Galbraith, S.D.; Wang, P.; Zhang, F. *Computing Elliptic Curve Discrete Logarithms with Improved Baby-Step Giant-Step Algorithm*; Cryptology ePrint Archive; American Institute of Mathematical Sciences: Springfield, MI, USA, 2015.
51. Rubinstein-Salzedo, S. The Diffie–Hellman key exchange and the discrete logarithm problem. In *Cryptography*; Springer International Publishing: Cham, Switzerland, 2018; pp. 99–112.
52. Pohlig, S.C.; Hellman, M.E. An improved algorithm for computing logarithms over GF (p) and its cryptographic significance. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 415–430.

53. Lin, K.; Wang, W.; Wang, L.; Zhao, C.A. An alternative approach for computing discrete logarithms in compressed SIDH. *arXiv* **2021**, arXiv:2111.10226. [CrossRef]
54. Shor, P.W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS'94), Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134. [CrossRef]
55. Ekerå, M. Revisiting Shor's quantum algorithm for computing general discrete logarithms. *arXiv* **2019**, arXiv:1905.09084.
56. Kadyrzhan, K.; Kaldybekov, D.; Baipakbaeva, S.; Vitulyova, Y.; Matrassulova, D.; Suleimenov, I. Electronic Fourier–Galois Spectrum Analyzer for the Field GF(31). *Appl. Sci.* **2024**, *14*, 7770. [CrossRef]
57. Suleimenov, I.; Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y. Peculiarities of Applying Partial Convolutions to the Computation of Reduced Numerical Convolutions. *Appl. Sci.* **2024**, *14*, 2076–3417. [CrossRef]
58. Areh, I.; Verkampt, F.; Allan, A. Critical review of the use of the Rorschach in European courts. *Psychiatry Psychol. Law.* **2022**, *29*, 183–205. [CrossRef]
59. Bakirov, A.; Matrassulova, D.; Vitulyova, Y.; Shaltykova, D.; Suleimenov, I. The specifics of the Galois field GF (257) and its use for digital signal processing. *Sci. Rep.* **2024**, *14*, 15376. [CrossRef]
60. Suleimenov, I.E.; Vitulyova, Y.S.; Kabdushev, S.B.; Bakirov, A.S. Improving the Efficiency of Using Multivalued Logic Tools: Application of Algebraic Rings. *Sci. Rep.* **2023**, *13*, 22021. [CrossRef]
61. Vitulyova, Y.; Kadyrzhan, K.; Kadyrzhan, A.; Shaltykova, D.; Suleimenov, I. Reducing the description of arbitrary wave field converters to tensor form. *Int. J. Inf. Technol.* **2024**, *17*, 1–10. [CrossRef]
62. Ivashov, S.I.; Capineri, L.; Bechtel, T.D.; Razevig, V.V.; Inagaki, M.; Gueorguiev, N.L.; Kizilay, A. Design and Applications of Multi-Frequency Holographic Subsurface Radar: Review and Case Histories. *Remote Sens.* **2021**, *13*, 3487. [CrossRef]
63. SIvashov, I.; Razevig, V.V.; Vasiliev, I.A.; Zhuravlev, A.V.; Bechtel, T.D.; Capineri, L. Holographic Subsurface Radar of RASCAN Type: Development and Applications. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **2011**, *4*, 763–778. [CrossRef]
64. Lombardi, F.; Lualdi, M. Step-Frequency Ground Penetrating Radar for Agricultural Soil Morphology Characterisation. *Remote Sens.* **2019**, *11*, 1075. [CrossRef]

applied sciences

MDPI

Article

Prospects for the Use of Quasi-Mersen Numbers in the Design of Parallel-Serial Processors

Aruzhan Kadyrzhan [1], Kaisarali Kadyrzhan [2], Akhat Bakirov [1,2,*] and Ibragim Suleimenov [2]

[1] Department of Telecommunication Engineering, Institute of Communications and Space Engineering, Gumarbek Daukeev Almaty University of Power Engineering and Communications, Almaty 050040, Kazakhstan; aru.kadyrzhan@gmail.com
[2] National Engineering Academy of the Republic of Kazakhstan, Almaty 050010, Kazakhstan; kaisarali1997ss@gmail.com (K.K.); esenych@yandex.ru (I.S.)
* Correspondence: axatmr@mail.ru

Abstract: It is shown that a serial-parallel processor, comparable in bit capacity to a 16-bit binary processor, can be implemented based on an algorithm built on the residue number system, a distinctive feature of which is the use of the first four quasi-Mersenne numbers, i.e., prime numbers representable as $p_k = 2^k + 1,\ k = 1, 2, 3, 4$. Such a set of prime numbers satisfies the criterion $2p_1p_2p_3p_4 + 1 = P$, where P is also a prime number. Fulfillment of this criterion ensures the possibility of convenient use of the considered RNS for calculating partial convolutions developed for the convenience of using convolutional neural networks. It is shown that the processor of the proposed type can be based on the use of a set of adders modulo a quasi-Mersenne number, each of which operates independently. A circuit of a modulo $2^k + 1$ adder is proposed, which can be called a trigger circuit, since its peculiarity is the existence (at certain values of the summed quantities) of two stable states. The advantage of such a circuit, compared to known analogs, is the simplicity of the design. Possibilities for further development of the proposed approach related to the use of the digital logarithm operation, which allows reducing the operations of multiplication modulo $2^k + 1$ to addition operations, are discussed.

Keywords: quasi-Mersen numbers; trigger adder; effective bit depth of adder; computing performance; parallel-serial computing; residue number system (RNS)

Academic Editor: Alessandro Lo Schiavo

Received: 4 September 2024
Revised: 7 January 2025
Accepted: 7 January 2025
Published: 13 January 2025

Citation: Kadyrzhan, A.; Kadyrzhan, K.; Bakirov, A.; Suleimenov, I. Prospects for the Use of Quasi-Mersen Numbers in the Design of Parallel-Serial Processors. *Appl. Sci.* **2025**, *15*, 741. https://doi.org/10.3390/app15020741

1. Introduction

At present, there is considerable interest in increasing the productivity of computing equipment [1–4]. One approach to solving this problem is the use of parallel-sequential calculations [5,6], which are implemented, among other methods, using the residue number system (RNS) [7,8]. In this case, each integer x is represented as $(x_1, x_2, \ldots, x_n)$, where $x_i = x \bmod m_i$, $m_i; i = 1, 2, \ldots n$ are integers that form the RNS [9]. The moduli m_i are generally assumed to be pairwise coprime.

The advantage of RNS is its ability to independently operate with individual remainders x_i, in particular, $z_i = x_i + y_i$, if $z = x + y$ (similarly for multiplication). Such properties allow the move from sequential to parallel-sequential computations, since, when $x < M = m_1m_2 \ldots m_n$, each set of residues $(x_1, x_2, \ldots, x_n)$ represents exactly one integer x. Consequently, as long as this inequality is satisfied, computations using integers can be reduced to computations in RNS. From the perspective of computer technology, this limitation is not significant. In any case, the range within which standard processors operate is also limited (e.g., 16-bit adders).

The question of choosing a concrete set of moduli m_i from the perspective of computer technology is not trivial. In particular, in the case that all numbers m_i are prime, i.e., $m_i = p_i$, the computations corresponding to each component x_i of the number x are de facto performed in the Galois field $GF(p_i)$. Currently, numerous different types of electronic circuits are known that are designed to perform addition and multiplication operations in such fields, i.e., adders and multipliers modulo a prime number [10–13]. They differ significantly from one another in their design, which, moreover, significantly depends on the choice of the modulus, as is proven, in particular, by report [14]. Moreover, it was noted in [15] that different Galois fields have different specifics.

Consequently, there is every reason to assert that the choice of a set of moduli m_i should be determined, first, by the specifics of the problems being solved. The technical implementation of this approach is facilitated by the widespread use of microcircuits with a reconfigurable logical structure [16–18]. Accordingly, it is permissible to raise the question of developing calculators oriented towards solving a certain range of problems.

In [19], it was shown that for calculating digital convolutions, it is convenient to use an RNS corresponding to a set of prime numbers p_i, such that $p_1 p_2 \dots p_n + 1 = P$, where P is also a prime number. In this case, it becomes possible to reduce the discrete scale corresponding to the result of calculating the convolution to a discrete scale corresponding to the original function, without using fractional values.

This paper shows that a serial-parallel processor, comparable in bit depth to a 16-bit binary processor, can be implemented based on an algorithm built on the residue number system. The distinctive feature of this processor is the use of the first four quasi-Mersenne numbers, i.e., prime numbers representable as $p = 2^k + 1$.

The basis of such a processor is an adder modulo a quasi-Mersenne prime number. A specific electronic circuit of such an adder is presented, which can be called a trigger, since it can be in two different states. Its advantage over known analogs is the simplicity of the design.

It should be noted that Mersenne primes are currently widely used in information technology. In particular, these numbers are used to generate pseudorandom numbers [20]. Specifically, a pseudorandom number generator called the Mersenne Twister, developed in 1997 by Japanese scientists M. Matsumoto and T. Nishimura [21], is directly based on the use of Mersenne numbers.

Some reports demonstrating the expediency of using such numbers for data transmission are presented in the current literature [22,23], etc. Mersenne codes 3, 7, and 11 provide greater noise immunity and an increased probability of correct detection in radar channels, offering a potential alternative to Barker codes for noise-resistant data transmission in radio channels [24]. Modified RSA algorithm, using fixed Mersenne prime numbers, improves encryption in medical ultrasound imaging while maintaining adequate elapsed time for image transfer [25].

From the perspective of performing calculations modulo an integer, these numbers are particularly convenient because the multiplication of a number a written in binary form by two modulo the Mersenne number is reduced to cyclic permutation of characters. For example, for calculations in the field $GF(7)$, the next equality is true

$$2 \cdot a_2 a_1 a_0 =_{(7)} a_1 a_0 a_2 \quad (1)$$

Relation (1) reflects the uniqueness of Mersenne primes. Quasi-Mersenne numbers are also unique, which is demonstrated in report [26]. Their uniqueness is due to the fact that the operation of digital logarithm, the study of which has recently received very serious attention [27–29], has a pronounced specificity in the case under consideration. Namely, the operation of digital logarithm allows us to reduce the operation of multiplication in a

Galois field to the operation of addition. However, this operation is applicable only to non-zero elements of Galois fields. In Galois fields $GF(p)$, corresponding to quasi-Mersenne numbers $p = 2^k + 1$, the number of non-zero elements is obviously equal to 2^k, i.e., the multiplication operation (after using the digital logarithm operation) is de facto reduced not simply to an addition operation, but to an addition operation in terms of ordinary binary logic, easily implemented on the existing element base (addition modulo 2^k is operationally reduced to discarding the most significant digits in the binary representation of a number).

It is appropriate to emphasize that the uniqueness of quasi-Mersenne numbers has not previously received the attention that they deserve. Evidence for this is provided in our recent report [26], where it was shown that it is possible to implement a simple and convenient method of digital logarithm specifically for such fields.

We also note that the approach using a specific Galois field (or varieties of such fields) is not fundamentally new. Modern binary computing technology is de facto built on the use of a specific field, GF(2). Consequently, the question of developing computing technology that uses the specifics of a particular type of Galois fields in a certain sense corresponds to the existing tradition.

2. Results

2.1. RNS Used

The RNS used is formed by the following quasi-Mersenne numbers (Table 1) and the prime number 2.

Table 1. Quasi-Mersenne numbers used.

k	1	2	4	8
$P = 2^k + 1$	3	5	17	257

Equality holds

$$2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 + 1 = 131,071 \quad (2)$$

It is significant that the number 131,071 is prime. This means that this set of numbers satisfies the criterion formulated in [19], i.e.,

$$p_1 p_2 \ldots p_n + 1 = P \quad (3)$$

where P is also a prime number.

This criterion is very important, in particular, from the perspective of performing operations that are used by convolutional neural networks. As noted in [20], the following problem arises when digital convolutions are being used. The discretization scale of the convolution result may differ from the discretization scale of the original signal. To make the discretization step of these scales the same, one can use, for example, the operation of rounding to an integer. From a computational point of view, however, this is not convenient, since it is more convenient for any electronic devices to perform calculations in integers. As shown in [19], if criterion (1) is satisfied, then there is a simple and convenient way to reduce the above scales to a single format in which only calculations in integers are used. Thus, the fulfillment of criterion (1) for the first quasi-Mersenne numbers is additional evidence of their uniqueness.

In addition, $\log_2 131,071 \approx 16.999978$. This means that the range of integers with which a processor built on the RNS under consideration can work with exceeds a typical 16-bit processor in terms of effective bit depth.

This fact also testifies in favor of the uniqueness of the set of prime numbers presented in Table 1. Calculations using the RNS corresponding to such a system correspond in their capabilities to one of the existing standards, but, as will become clear, there is an opportunity to move on to serial-parallel calculations. In this regard, it is appropriate to note that any existing technical standard (including those in the field of computer technology) is deliberately oriented towards specific quantitative indicators. The simplest example is the existing television standards, which fix the number of lines and the number of pixels in a line [30,31]. It is important that these standards can have a fairly large variety, as demonstrated by the standards corresponding to information display systems. Similarly, based on considerations of convenience and efficiency, a set of standards corresponding to computer technology can be implemented. In this regard, it is appropriate to note once again that the existing digital technology is de facto oriented towards a very specific standard associated with the choice of a specific Galois field $GF(2)$. It is precisely in this field that existing binary adders and other elements of binary logic are built.

This field has well-defined specifics, as well as well-defined advantages. This, however, does not exclude the possibility of using other Galois fields. Based on the analogy with existing processors, it seems advisable to begin by developing an adder modulo quasi-Mersenne numbers. For the processor under consideration, such an adder plays the same role as the classical binary adder in the most common processors. It is also important that the circuit for the developed adder be oriented toward the use of components that correspond to binary logic, since these are the ones that are produced industrially. Thus, this paper substantiates the possibility of using another standard of computer technology, one which has the same computing capabilities as existing 16-bit processors but allows for serial-parallel computations using a well-defined RNS. This approach is particularly convenient for computations corresponding to convolutional neural networks due to the fulfillment of criterion (2). In addition, as will become clear, it is the use of quasi-Mersenne numbers that allows us to propose fairly simple computing devices based on standard elements developed for binary logic.

2.2. Basic Scheme of Operation of the Calculators of the Proposed Type

The operational scheme of the proposed type of calculators is based on the following properties of algebraic rings, of which RNS is a special case, as emphasized in the report [19]. Such rings R decompose into a direct sum of ideals r_i

$$R = r_1 + r_2 + \cdots + r_n \tag{4}$$

Each of the ideals r_i is generated by its complementary idempotent element e_i

$$r_i = Re_i, \tag{5}$$

The elements e_i cancel each other out

$$e_i e_j = 0,\ i \neq j;\ e_i e_i = e_i \tag{6}$$

The sum of these elements is equal to the unit of the ring R

$$\sum_i e_i = 1 \tag{7}$$

Examples of such rings are given by rings of residue classes modulo a number p, representing the product of prime numbers $p = p_1 p_2 \ldots p_n$. In this case, idempotent elements can be formed according to the rule used, in particular, in [20]

$$e_i = \alpha_i \prod_{j \neq i} p_j \tag{8}$$

where α_i is an integer that is not a multiple of p_i. The choice of these numbers is based on the condition

$$e_i e_i = 1 \tag{9}$$

It is obvious that by construction we have

$$e_i p_i \equiv 0(P) \tag{10}$$

since any product of the form (10) contains the factor $p = p_1 p_2 \dots p_N$.

With the choice of integers α_i made, it also holds

$$e_1 + e_2 + \dots + e_N \equiv 1(P) \tag{11}$$

In the case under consideration, an arbitrary element of the ring R can be represented as

$$u = e_1 u_1 + e_2 u_2 + \dots + e_N u_N \tag{12}$$

where e_i are idempotent mutually canceling elements, and $u_i = 0, 1, 2, \dots, p_i$.

The convenience of representing (12) in calculations is that the elements u_i are multiplied independently, and the multiplication is performed modulo p_i. Indeed, since e_i are mutually annihilating idempotent elements, the product of two numbers $u^{(1)}$ and $u^{(2)}$ is expressed as

$$u^{(1)} u^{(2)} = e_1 u_1^{(1)} u_1^{(2)} + e_2 u_2^{(1)} u_2^{(2)} + \dots + e_N u_N^{(1)} u_N^{(2)} \tag{13}$$

A similar formula is valid for the addition operation, which was also used in report [19]

$$u^{(1)} + u^{(2)} = e_1 \left(u_1^{(1)} + u_1^{(2)} \right) + e_2 \left(u_2^{(1)} + u_2^{(2)} \right) + \dots + e_N \left(u_N^{(1)} + u_N^{(2)} \right) \tag{14}$$

Formulas (13) and (14) allow us to implement the following circuits of the multiplier and adder modulo the number $p = p_1 p_2 \dots p_N$, where p_i are prime numbers (Figures 1 and 2, respectively). Common to these circuits are elements (1_i) and (2_i), which ensure the reduction of the original numbers to values modulo each of the prime numbers p_i. From the algebraic-theoretical perspective, such elements correspond to the transition to the use of calculations in Galois fields complementary to the ideals r_i. Blocks (3_i) perform multiplication or addition modulo prime numbers p_i, i.e., multiplication or addition in terms of Galois fields $GF(p_i)$. As follows from Formulas (13) and (14), the multiplication and addition of individual "components" of the original number can indeed be performed independently. Block (4) returns the calculation result to the number in the original representation in accordance with Formula (12).

Let us emphasize that formally the calculations using the presented schemes are performed modulo the integer p. However, if the result of addition and multiplication does not exceed p, it coincides with the result of calculations using ordinary arithmetic operations. For any physically implemented processor, the range in which the result of calculations fits is finite. This is particularly true for existing 16-bit processors. As follows from Table 1, the product $2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 = 131,070$ corresponds to approximately the same range. It is this fact that allows calculations to be performed in accordance with the proposed schemes without changing the result in the traditional "arithmetic" sense.

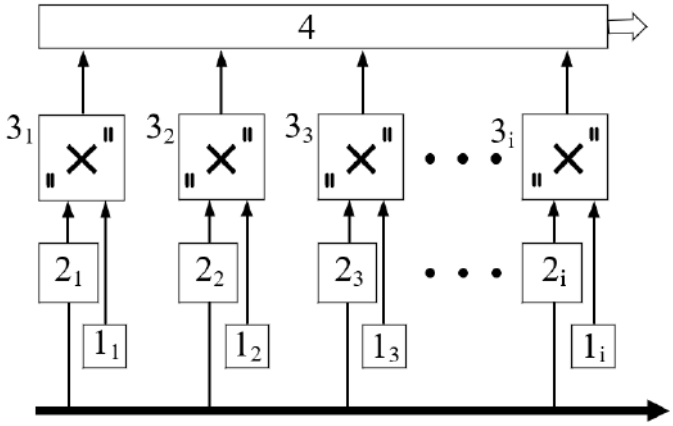


Figure 1. General diagram of a multiplier built based on Formula (13).

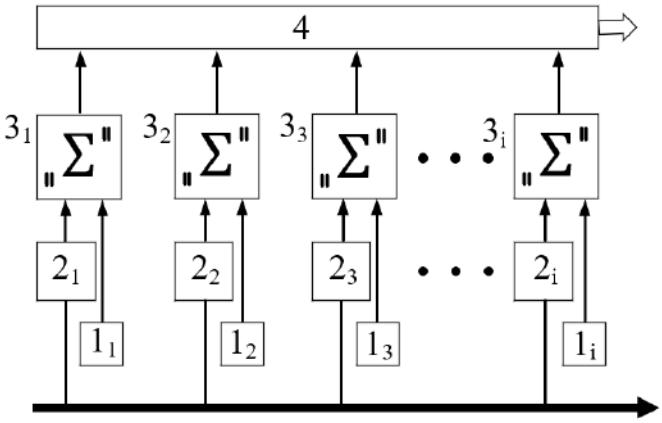


Figure 2. General diagram of an adder built based on Formula (14).

The circuits in Figures 1 and 2 are applicable to any numbers $p = p_1 p_2 \dots p_N$, where p_i are prime numbers. However, there is a significant nuance. As will become clear, the degree of complexity of electronic circuits that perform calculations in different Galois fields varies. One of the simplest types of such calculators corresponds to the case where all the prime numbers in the above product are representable as $p_i = 2^{k_i} + 1$, i.e., quasi-Mersenne numbers. For this reason, we focus on the use of such numbers in advanced processor technology, especially for that which ensures the implementation of convolutional neural networks.

2.3. Scheme of a Trigger Adder Modulo a Quasi-Mersenne Number

This section considers a specific design of adders, which have numbers (3_i) in the diagram in Figure 2. The proposed design is common to all adders modulo the quasi-Mersenne number.

The proposed adder circuit differs significantly from the modulo integer adder circuits reported in the current literature [32,33], including patents [34,35]. The adder circuits known in the literature are built entirely on direct logical operations, excluding the use of more than one stable state of the circuit. The paper [32] presents a modulo 2^n adder using the carry-save method. The circuit contains 48 logical elements and provides high performance for residual class systems. The paper [33] describes a unified modulo adder/subtractor designed for arbitrary modules. Its architecture uses 58 elements and a universal algorithm to improve hardware efficiency. Patent [34] describes a modular binary adder circuit that uses field-effect transistors to minimize computational delays. This patent includes 48 elements to ensure high-speed operation. Patent [35] describes a circuit that

uses iterative calculations to obtain a residual value through multi-step addition, which significantly improves efficiency in systems that handle large numbers. This circuit uses 56 elements, including multiple operation units to improve accuracy and speed.

The fundamental difference between the proposed circuit and the known ones is that it is essentially an analog of a trigger, i.e., it is capable of being in two different stable states. This allows us to significantly reduce the number of logical elements used, as shown below. It is also significant that such circuits, which can be called trigger circuits, are quite simple to implement, especially when the addition is performed modulo a quasi-Mersenne number.

The circuit diagram of the proposed adder is shown in Figure 3. It includes two sets of conventional single-digit adders (1_i) and (2_i), where $i = 1, 2, \ldots, k+1$, logical AND elements (3) and (4), and a rectangular pulse generator (5).

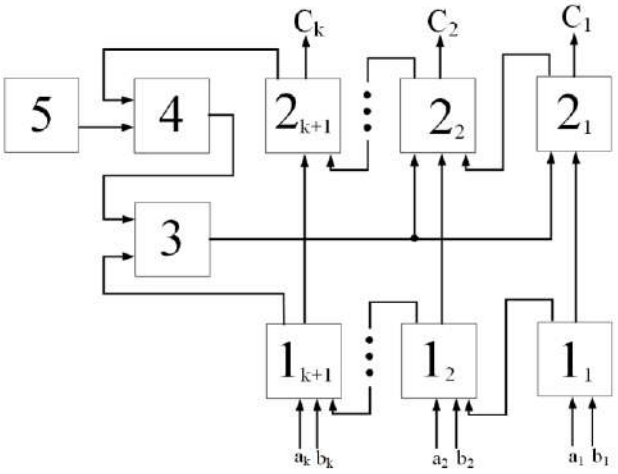


Figure 3. Circuit diagram of a modulo $2^k + 1$ trigger adder.

The circuit is designed for summation modulo $2^k + 1$ of numbers represented in binary form and lying in the range

$$0 \leq a \leq 2^k \tag{15}$$

It is thus assumed that, before the summation operation, the original numbers have already been reduced to a value modulo the number over which the summation is performed. Thus, this circuit performs summation in the field $GF\left(2^k + 1\right)$. In particular, this means that the largest number that this circuit operates, when represented in binary form, is written as

$$a_{max} = 1\underbrace{00\ldots0}_{k} \tag{16}$$

In particular, this means that when summation is performed in the Galois field $GF(17)$, it is assumed that the inputs of the adder are fed signals corresponding to numbers in the range $0 \leq a \leq 16$.

The circuit operates as follows. Binary signals corresponding to the representation of integers a and b in binary format are fed to the inputs a_i *and* b_i. The first line of adders (1_i) ensures the summation of these numbers in the usual binary representation. The second line of adders (2_i) is designed to reduce the sum to the sum modulo $2^k + 1$.

Looking ahead, we note that the part of the circuit involving the second line of adders can also be used to calculate the components of the original numbers according to the rule $x_i = x \ mod \ m_i$. As noted above, it is assumed that before performing the operations implemented using the circuit in Figure 3, the numbers being summed have already been reduced to the format $x_i = x \ mod \ m_i$.

Let us consider the operation of the circuit in Figure 3 in more detail, taking into account that the nature of its functioning depends on the specific value of the summation result, which corresponds to the signals generated at the output of adders (1_i). In particular, the case when two numbers corresponding to the binary representation of the form (4) are summed is exceptional. The logical AND element (3) takes this exceptional case into account. When two numbers of the form (16) are summed, a logical one is formed at the output of the adder carry bit (1_{k+1}). Accordingly, a logical one is also formed at the output of element (3), which is transferred to the second gatherings of adders in the second line with numbers from 1 to k. The adder with number $k+2$ is absent in the second line. Consequently, transferring a logical one to the inputs of the adders indicated above effectively means that the number 2^{k+1} is subtracted from the number formed at the output of the first line of adders, and a number that contains exactly k ones in binary representation is added.

We emphasize that the circuit in Figure 3 includes not k, but $k+1$ adders. This is necessary because there is an exceptional case when the output of the adder (2_{k+1}) differs from one. This case corresponds to the maximum number that can arise in calculations within the Galois field corresponding to a quasi-Mersenne number, i.e., a number that in binary representation has the form (16). Accordingly, when two numbers of the form (16) are summed modulo 2^k+1, the number 2^k+1 should be subtracted from the result of direct summation. This corresponds to subtracting the number 2^{k+1}, which is achieved by the absence of an adder numbered $k+2$ in the circuit under consideration, followed by the addition of the number $2^{k+1}-2^k-1=2^k-1$. In binary representation, the last number is displayed as follows: The number 2^k in binary form is written similarly to Formula (16)

The difference $2^{k+1}-2^k=2^k$ is written as

$$2^k = 1\underbrace{00\ldots0}_{k} \tag{17}$$

Therefore, the number $q=2^{k+1}-2^k-1$ is written as

$$q = 2^{k+1}-2^k-1 = 0\underbrace{11\ldots1}_{k} \tag{18}$$

This formula shows that technically, bringing the summation result to a value modulo 2^k+1 in the case under consideration essentially involves adding ones to all digits from the first to the digit with number k. This is the operation performed by the circuit in Figure 3, or more precisely, by the adders in the second line (2_i). It is appropriate to emphasize that in this circuit, additional ones are fed to the inputs of adders with numbers 1 through k, but are not fed to the adder numbered $k+1$.

As an example, let us consider the case when summation is performed modulo $2^2+1=5$. In this case, both lines (1_i) and (2_i) of the adder in Figure 3 contain three single-digit adders. The maximum value of the numbers being summed is 4, or 100 in binary representation. Note again that in this case, the most significant digit with the number $k+1$ (in this case, with the number 3), is used only to represent this special case. When calculating in the Galois field $GF(5)$, the two least significant digits are sufficient to represent the remaining elements. The sum of two numbers, 4, is equal to 8, or 1000 in binary representation. By discarding the most significant digit as a result of summation and adding the number 3 (written as 11 in binary representation), we exactly subtract the number 5, which gives the correct answer when summing modulo 5, i.e., 3.

Thus, element (3) allows us to obtain an adequate answer in the special case considered above. All other summation results can be classified as follows.

$$z : \begin{cases} 0 \le z < 2^k \\ z = 2^k \\ 2^k < z \le 2^{k+1} - 1 \end{cases} \tag{19}$$

In relation to the modulo 5 adder, this classification looks like this:

$$z : \begin{cases} 0 \le z < 4 \\ z = 4 \\ 4 < z \le 7 \end{cases} \tag{20}$$

In the cases corresponding to the first line of Formula (19), the second line of adders does not perform any actions. Integers lying in the range $0 \le z < 2^k$ do not require reduction to a value modulo 2^{k+1}. In this case, the variable formed at the output of the adder (2_{k+1}) is zero. It is non-zero in the cases corresponding to the second and third lines of Formula (5). The difference between these cases is that the number $z = 2^k$ does not require reduction modulo 2^{k+1}, and the numbers corresponding to the range $2^k < z \le 2^{k+1} - 1$—vice versa.

Reducing a number in the above range $2^k < z \le 2^{k+1} - 1$ to a number modulo 2^{k+1} means that the number 2^{k+1} should be subtracted from the given number and, as in the case considered above, adding a number that in binary representation contains exactly k ones, i.e., adding the number $q = 2^{k+1} - 2^k - 1$.

Let us emphasize once again that for the binary representation of the number 2^{k+1}, $k + 2$ binary digits are required. For example, the number 8 in binary representation is 1000. The second line of adders in the circuit in Figure 3 contains $k + 1$ single-digit adders. This means that the number 2^{k+1} will be automatically subtracted when it is used, even when a logical one is formed at the output of the carry bit of the adder with the number $k + 1$.

The addition of the number $q = 2^{k+1} - 2^k - 1$, composed in binary representation from k ones, according to the circuit in Figure 3 is carried out in a manner similar to that discussed above.

The carry-out output of the single-digit adder (2_{k+1}) is connected by feedback to adders (2_i), $i = 1, 2.., k$ via the "logical AND" element (4). Consequently, the number q, given by Formula (16), will be added to the result of the primary summation (the first line of adders) if a logical one is formed at the output of the adder (2_{k+1}) or at the output of the generator (5).

The above feedback forms an analog of a trigger. Namely, if the result of the summation lies in the range $2^k < z \le 2^{k+1} - 1$, then the circuit can be in two stable states. Indeed, adding the number q results in the formation of a logical one at the carry-out output of the adder (2_{k+1}), which supports summation with the above number q. This represents one of the two stable states. The second stable state occurs when a logical zero is formed at the output of the adder carry bit (2_{k+1}). In this case, the number q is not added to the result of the primary summation.

The generator (5) ensures switching between the two specified stable states. It transfers the circuit to the state "add the number q to the primary summation result". This reduces the result of the primary summation to the sum modulo $2^k + 1$.

An exception arises when the result of the primary summation corresponds to Formula (16) or the second line in Formula (19). In these cases, it should also remain unchanged (for example, the number 4 does not require reduction modulo 5). This is also ensured by the circuit in Figure 3. To prove this, consider the following summation result

$$1\underbrace{00\ldots0}_{k} + 0\underbrace{11\ldots1}_{k} = 1\underbrace{11\ldots1}_{k} \tag{21}$$

This result does not lead to the formation of a logical unit at the input of the adder bit carry (2_{k+1}). Therefore, after switching off the generator (5), a return to the initial state corresponding to the number $1\underbrace{00\ldots0}_{k}$ will be performed.

Thus, in all three cases corresponding to Formula (19), the proposed circuit actually provides summation modulo $2^k + 1$. Let us consider the results of testing the proposed circuit.

It should also be noted that the circuit in Figure 3 clearly demonstrates the advantages of using quasi-Mersenne numbers, as well as the possibility of generalizing the proposed approach to summation modulo other numbers. Namely, if we use the algebraic scheme for reducing the direct summation result to the summation result modulo, then depending on the value of the result, it is necessary to ensure that a certain value is subtracted from it, with a coefficient equal to 1 or 0. Taking into account the discarding of the most significant digit, this means that a number equal to the corresponding difference should be added to the summation result. With regard to quasi-Mersenne numbers, this is the number specified by Formula (18). With the same success, we can use other numbers whose binary representation contains k digits. The transition to using other numbers is reduced to changing the nature of the connections between the output of element (3) and the inputs of the adders in the second line in the circuit in Figure 3. However, when quasi-Mersenne numbers are used, this method corresponds to the possibility of feeding the same signal corresponding to a logical unit to the second inputs of the adders in the second line (Figure 3). While this may not be fundamentally important from the perspective of implementing electronic circuits, this does not diminish the convenience of using prime numbers of the type under consideration for building calculators designed to perform digital convolution operations and similar tasks. There is another significant argument in favor of using quasi-Mersenne numbers, considered in the Section 3. As shown in [26], for such numbers, it is quite simple to implement the digital logarithm operation, which allows us to reduce multiplier circuits in Galois fields to adder circuits in terms of ordinary binary logic.

2.4. Test Result of the Proposed Trigger Adder Circuit

Initial testing of the proposed schemes was carried out in the Proteus program. Figure 4 shows the results of testing the proposed adder circuit in Proteus for the case of the quasi-Mersenne number $2^2 + 1 = 5$. Figure 5 shows a similar result for a processor that provides summation modulo $2^4 + 1 = 17$. It is evident that the circuit operates in full accordance with the algorithm described above.

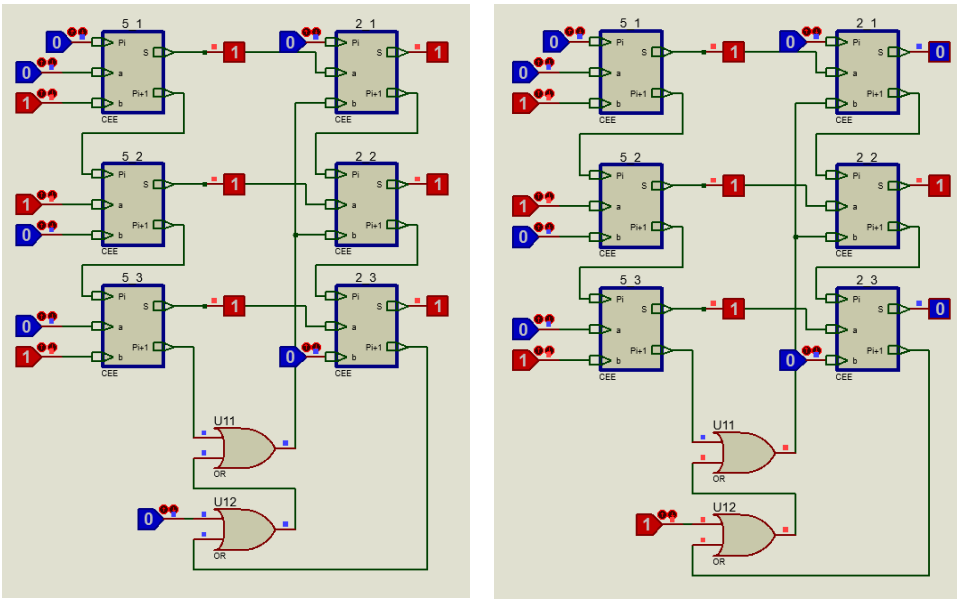
The circuits in Figures 4 and 5 fully correspond to the circuit in Figure 3, or rather, are its specifications. These figures use standard notations for adders and logical AND elements. Figures 4a and 5a correspond to the case when a logical zero is formed at the output of the rectangular pulse generator, which ensures the transition of the circuit from one stable state to another, and Figures 4b and 5b correspond to the case when a logical one is formed at its output. The circuit shows that, when a logical one is formed at the output of the specified generator, the primary result of summation is reduced to the value of the sum modulo the number 5 (Figure 4) or 17 (Figure 5).

To test the functionality and correctness of the project written in VHDL, Testbench is used, which is a simulation environment.

To test the logic circuit, the input data consists of 5-bit binary numbers for the modulo 17 adder and 3-bit binary numbers for the modulo 5 adder. These adders were designed using Verilog. The program listing is attached in the Supplementary Materials.

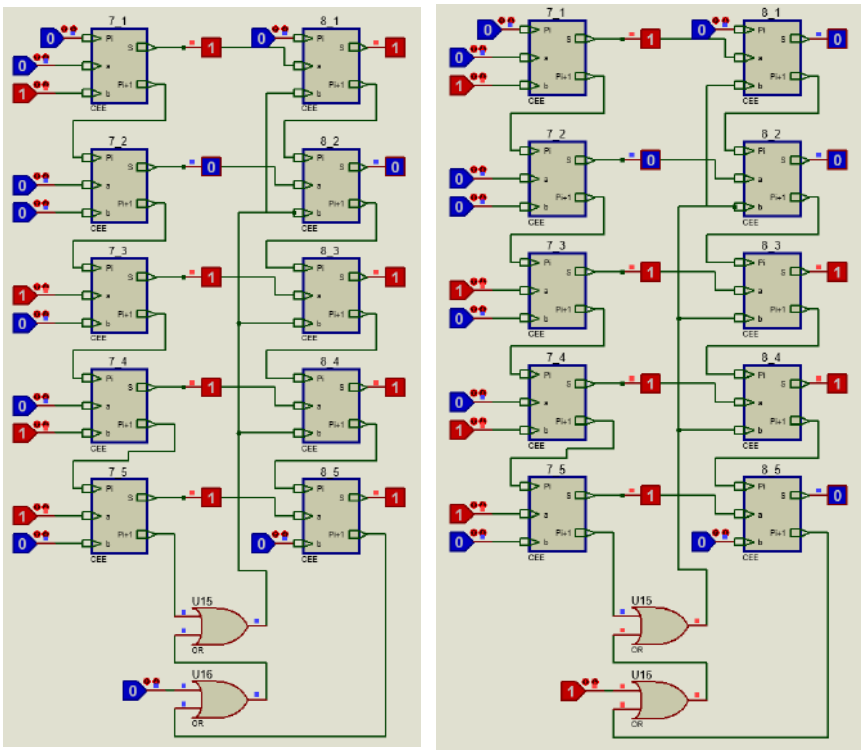
The program for conducting testbench iterates over input binary 5-bit numbers from 0 to 31 (i, j) inside the program cycle. If the sum of the input binary numbers is greater than or equal to 17 (if sum_ij $\geq$ 17), the U14_Control input of the generator is activated.

The results of the circuit's operation are visible on the timing diagram of the ModelSim simulator (Figure 6).



(**a**) (**b**)

Figure 4. Illustration of the existence of two stable states in the circuit of a trigger adder of the proposed type; adder modulo 5, example of adding two numbers 5 and 2; (**a**)—state before reducing the result to a sum modulo 5; (**b**)—after.



(**a**) (**b**)

Figure 5. Illustration of the existence of two stable states in the circuit of a trigger adder of the proposed type; adder modulo 17, example of adding two numbers 20 and 9; (**a**)—state before the result is transferred to the sum modulo 5; (**b**)—after.

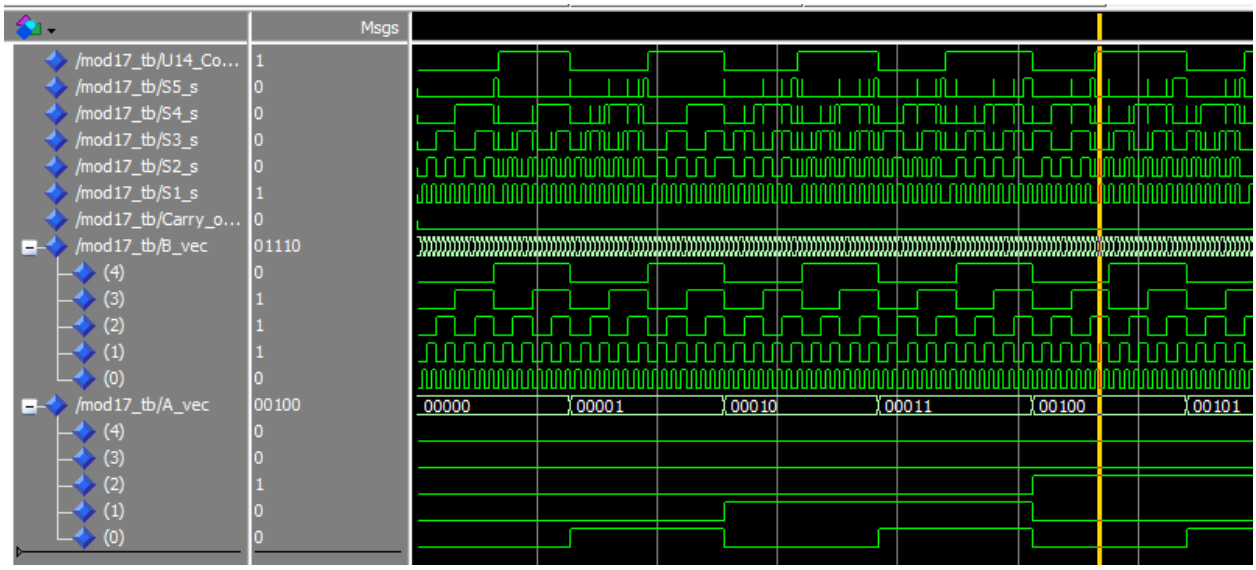


Figure 6. ModelSim testbench result (mod17).

3. Discussion

The proposed scheme for the adder modulo a quasi-Mersen number allows for the future to implementation of a processor that performs serial-parallel calculations due to the built in algorithm, built on a very specific RNS. As outlined in Section 2, the fact that this RNS is built on quasi-Mersen numbers allows to implement a relatively simple (compared with existing analogs) adder scheme. The basis of this processor is a set of adders in the fields $GF\left(2^k+1\right)$, each of which operates independently.

The simplest architecture of this processor can be implemented by analogy with existing processors, in which the basic operation is addition. The difference is that all numbers inputted into the calculator are initially converted into a format corresponding to the RNS of the proposed type. Consequently, further operations with each "component" of each number are carried out independently. Specifically, this means that the performance of such a processor is minimally affected by the units that provide the reduction of a number to a set of numbers modulo the first quasi-Mersenne numbers (the same applies to the inverse operation). Performance is determined solely by the adder itself, and the limiting factor (in terms of calculation speed, etc.) is associated with the adder containing the maximum number of elements (i.e., the adder modulo 257). This number corresponds to an 8-bit adder, while the adder as a whole corresponds to a 16-bit adder in terms of performance.

The prospects for the widespread use of a processor of this type may still be debatable; however, it is possible to indicate a very specific range of problems for which this processor is either optimal or close to optimal. For example, this applies to the calculation of partial convolutions, considered in [19].

There is no need to emphasize that the development of devices that calculate digital convolutions is becoming increasingly relevant. In particular, this is due to the increasingly widespread use of convolutional neural networks [36–38], which are used, among other things, for primary data processing by onboard computing systems installed on devices for various purposes. In particular, the development of onboard computing systems that perform primary image processing during remote sensing of the Earth is relevant. Specifically, it is necessary to exclude the transmission of images in cases where the surface is covered by cloud cover [39,40].

To solve such problems, it is advisable to use a processor of the proposed type precisely because it operates independently with different components of an integer. Consequently, it can be used both for standard calculations and for calculations oriented towards the use of partial convolutions, as described in [19], which is specially designed for the implementation of convolutional neural network algorithms.

Examples from other fields can also be provided, in which the proposed approach may be in demand. This applies, in particular, to the development of new measuring devices using the Fourier-Galois transform. An example of such a device (a viscometer), using the GF(31) field, was considered in [41]. Other devices of this type, in which the electronic unit is significantly modernized [42], could be oriented towards other fields. However, the most important thing is that, in this case, the range of numbers in which the calculations are performed remains limited. Another non-trivial field of application for the developed approach in the future may be electronics implemented on a non-standard element base. The search for such an element base is currently being pursued very actively (for example, this concerns the development of neuromorphic materials [43–45], optical computers [46,47], etc.). Promising neuromorphic materials are very diverse. In particular, it has been proposed to use organic electronics for this purpose [48,49], including those that use organic transistor [50] and optoelectronic elements [51]. A distinctive feature of such elements is ion-electron conductivity [52], which raises the question of developing an algorithmic basis complementary to the presence of charge carriers of several types. It should also be considered that developments in this area are focused on the use of non-trivial memory cells [53]. Moreover, the results reflected in [54,55] suggest that it is possible for materials representing a "hybrid" of neural networks and classical logical electronics to be implemented on the basis of polymeric materials that form memory cells due to their physical and chemical properties. This is due to the specificity of these environments, in which the manifestations of the phase transition [56] are accompanied by the so-called "multidimensional" hysteresis [57]. As emphasized in [54], the non-trivial element base of computing technology inevitably requires significant modernization of the algorithmic basis for performing calculations.

Furthermore, the use of quasi-Mersenne numbers as the basis for the RNS used in the processor algorithm offers another advantage. Namely, as shown in [26], for the Galois fields $GF(17)$ and $GF(257)$, a relatively simple algorithm for digital logarithm can be proposed, which allows the multiplication operation to be reduced to the addition operation.

This algorithm implements the mapping of any non-zero element of the Galois field, represented as

$$x = \theta^n, \tag{22}$$

where θ is a primitive element of the field, on n: $x = \theta^n \rightarrow n$. Recall that a primitive element exists in any Galois field $GF(p)$, and its powers from 1 to $p-1$ exhaust all elements of this field.

The number of non-zero elements of the Galois field $GF(p)$ is $p-1$, and the digital logarithm operation provides a mapping of the fields $GF(17)$ and $GF(257)$ onto the Galois fields $GF(2^4)$ and $GF(2^8)$, respectively [26]. This means that the multiplication operation, when using the digital logarithm operation, is reduced to standard addition operations, which can be performed using standard processors.

Thus, the combination of a processor of the proposed type, built on adders in the fields $GF\left(2^k+1\right)$, creates additional prospects for increasing the performance of computing equipment by transitioning to parallel-sequential calculations.

4. Conclusions

Thus, a purely mathematical fact—the existence of a unique prime number 131,071, representable as $P = p_1p_2p_3p_4p_5 + 1$, where $p_1 = 2$ and the remaining p_i represent the first four quasi-Mersenne numbers, paves the way for the future implementation of a serial-parallel processor comparable in equivalent binary capacity to a classical 16-bit binary processor. This processor assumes independent operation with each component of an integer, representable in RNS, formed by the first four prime quasi-Mersenne numbers (3, 5, 17, and 257) and the number two. The architecture of such a processor, such as its classical analog, are adders, but for the proposed type of processor, these are adders modulo quasi-Mersenne numbers. The specificity of these numbers enables the implementation of a relatively simple circuit of a modulo adder. The simplicity of its design (compared to existing analogs) is ensured by the transition to a trigger circuit, where for certain values of the summed numbers, the circuit can be in two different stable states. Further development of the proposed approach can be based on the use of the digital logarithm operation. In this case, the multiplication operations in individual Galois fields corresponding to individual RNS components are reduced to addition operations, which are performed using conventional binary adders. The developed approach is applicable in cases where calculations are obviously carried out within a limited range of numerical values. In particular, for a processor built on the use of the first quasi-Mersenne numbers, the results obtained during calculations should not exceed 131,070. However, this is sufficient for many practical applications, particularly for the implementation of measuring devices built on the analysis of Fourier-Galois spectra.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/app15020741/s1. The program listing written in VHDL is attached in the Supplementary Materials.

Author Contributions: Conceptualization, K.K. and I.S.; methodology, I.S., A.B. and A.K.; formal analysis, A.K., K.K., A.B. and I.S.; writing—original draft preparation, A.K., K.K., A.B. and I.S.; writing—review and editing, A.K., K.K., A.B. and I.S.; visualization, K.K. and I.S.; supervision, I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been/was/is funded by the Science Committee of the Ministry of Higher Education and Science of the Republic of Kazakhstan (Grant No. AP23490107).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article/Supplementary Materials, further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Brynjolfsson, E.; Hitt, L.M. Computing productivity: Firm-level evidence. *Rev. Econ. Stat.* **2003**, *85*, 793–808. [CrossRef]
2. Leiserson, C.E.; Thompson, N.C.; Emer, J.S.; Kuszmaul, B.C.; Lampson, B.W.; Sanchez, D.; Schardl, T.B. There's plenty of room at the Top: What will drive computer performance after Moore's law? *Science* **2020**, *368*, eaam9744. [CrossRef] [PubMed]
3. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2462–2488. [CrossRef]
4. Schweikl, S.; Obermaier, R. Lessons from three decades of IT productivity research: Towards a better understanding of IT-induced productivity effects. *Manag. Rev. Q.* **2020**, *70*, 461–507. [CrossRef]
5. Umuroglu, Y.; Conficconi, D.; Rasnayake, L.; Preusser, T.B.; Själander, M. Optimizing bit-serial matrix multiplication for reconfigurable computing. *ACM Trans. Reconfig. Technol. Syst. (TRETS)* **2019**, *12*, 1–24. [CrossRef]

6. Moss, D.J.; Boland, D.; Leong, P.H. A two-speed, radix-4, serial–parallel multiplier. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2018**, *27*, 769–777. [CrossRef]
7. Isupov, K. Using floating-point intervals for non-modular computations in residue number system. *IEEE Access* **2020**, *8*, 58603–58619. [CrossRef]
8. Peng, J.; Sun, S.; Narayana, V.K.; Sorger, V.J.; El-Ghazawi, T. Residue number system arithmetic based on integrated nanophotonics. *Opt. Lett.* **2018**, *43*, 2026–2029. [CrossRef]
9. Mohan, P.A.; Mohan, P.A. *Residue Number Systems*; Birkhäuser: Cham, Switzerland, 2016; pp. 16–24.
10. Efstathiou, C.; Kouretas, I.; Kitsos, P. On the modulo 2n+1 addition and subtraction for weighted operands. *Microprocess. Microsyst.* **2023**, *101*, 104897. [CrossRef]
11. Patel, B.K.; Kanungo, J. Efficient Tree Multiplier Design by using Modulo 2 n+ 1 Adder. In Proceedings of the 2021 Emerging Trends in Industry 4.0 (ETI 4.0), Raigarh, India, 19–21 May 2021; pp. 1–6. [CrossRef]
12. Irkhin, V.P.; Glazkov, E.B.; Lukyanov, M.A.; Dolgachev, A.A.; Kryukov, Y.G. Device for Addition and Subtraction of Numbers Modulo. 2020. Available online: https://patenton.ru/patent/SU1599857A1 (accessed on 12 August 2024).
13. Ahmadifar, H.; Torabi, Z. Adder-Only Reverse Converters for 5-Moduli Set {2 q, 2 q− 1, 2 q+ 1±1, 2 q+ 2− 1}. *IETE J. Res.* **2024**, *70*, 7346–7353. [CrossRef]
14. Suleimenov, I.E.; Vitulyova, Y.S.; Kabdushev, S.B.; Bakirov, A.S. Improving the efficiency of using multivalued logic tools: Application of algebraic rings. *Sci. Rep.* **2023**, *13*, 22021. [CrossRef] [PubMed]
15. Vitulyova, Y.S.; Bakirov, A.S.; Suleimenov, I.E. Galois Fields for Digital Image and Signal Processing: Evidence for the Importance of Field Specificity. In Proceedings of the 2022 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), Chengdu, China, 19–21 August 2022; pp. 637–642.
16. Pan, C.; Wang, C.Y.; Liang, S.J.; Wang, Y.; Cao, T.; Wang, P.; Miao, F. Reconfigurable logic and neuromorphic circuits based on electrically tunable two-dimensional homojunctions. *Nat. Electron.* **2020**, *3*, 383–390. [CrossRef]
17. Wei, S. Reconfigurable computing: A promising microchip architecture for artificial intelligence. *J. Semicond.* **2020**, *41*, 020301. [CrossRef]
18. Luo, S.; Song, M.; Li, X.; Zhang, Y.; Hong, J.; Yang, X.; You, L. Reconfigurable skyrmion logic gates. *Nano Lett.* **2018**, *18*, 1180–1184. [CrossRef]
19. Suleimenov, I.; Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y. Peculiarities of Applying Partial Convolutions to the Computation of Reduced Numerical Convolutions. *Appl. Sci.* **2024**, *14*, 6388. [CrossRef]
20. Bhattacharjee, K.; Das, S. A search for good pseudo-random number generators: Survey and empirical studies. *Comput. Sci. Rev.* **2022**, *45*, 100471. [CrossRef]
21. Matsumoto, M.; Nishimura, T. Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator. *ACM Trans. Model. Comput. Simulat.* **1998**, *8*, 3–30. [CrossRef]
22. Smirnov, A.A.; Bondar, V.V.; Rozhenko, O.D.; Mirzoyan, M.V.; Darjania, A.D. Mersenne Numbers in the Bases of Systems of Residual Classes when Transmitting Data in Serial Communication Channels. *J. Math. Sci.* **2022**, *260*, 241–248. [CrossRef]
23. Ali, S.; Cenk, M. Faster residue multiplication modulo 521-bit Mersenne prime and an application to ECC. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *65*, 2477–2490. [CrossRef]
24. Nenashev, V.A.; Sergeev, A.M.; Kapranova, E.A. Research and analysis of autocorrelation functions of code sequences formed on the basis of monocyclic quasi-orthogonal matrices. *Inf. Control Syst.* **2018**, *4*, 9–14. [CrossRef]
25. Shin, S.H.; Yoo, W.S.; Choi, H. Development of modified RSA algorithm using fixed mersenne prime numbers for medical ultrasound imaging instrumentation. *Comput. Assist. Surg.* **2019**, *24* (Suppl. S2), 73–78. [CrossRef] [PubMed]
26. Bakirov, A.; Matrassulova, D.; Vitulyova, Y.; Shaltykova, D.; Suleimenov, I. The specifics of the Galois field GF (257) and its use for digital signal processing. *Sci. Rep.* **2024**, *14*, 15376. [CrossRef] [PubMed]
27. Yin, W.; Wen, Q.; Li, W.; Zhang, H.; Jin, Z. An anti-quantum transaction authentication approach in blockchain. *IEEE Access* **2018**, *6*, 5393–5401. [CrossRef]
28. Turner, C.S. A fast binary logarithm algorithm [DSP tips & tricks]. *IEEE Signal Process. Mag.* **2010**, *27*, 124–140. [CrossRef]
29. Sinha, S.K.; Kumari, S.; Kataria, A.; Thangarasu, N.; Sahoo, G.S. Blockchain empowerment: Investigating integration with software-defined networks and its impact on IoT privacy. *Multidiscip. Rev.* **2023**, *6*, e2023ss073. [CrossRef]
30. Chen, X.; Zhang, Z.; Ren, J.S.; Tian, L.; Qiao, Y.; Dong, C. A new journey from SDRTV to HDRTV. In Proceedings of the IEEE/CVF International Conference on Computer Vision, Virtual, 11–17 October 2021; pp. 4500–4509.
31. Arnold, J.; Frater, M.; Pickering, M. *Digital Television: Technology and Standards*; John Wiley & Sons: Hoboken, NJ, USA, 2007.
32. Hiasat, A.A. High-speed and reduced-area modular adder structures for RNS. *IEEE Trans. Comput.* **2002**, *51*, 84–89. [CrossRef]
33. Tay, T.F.; Chang, C.H. A new unified modular adder/subtractor for arbitrary moduli. In Proceedings of the 2015 IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, Portugal, 24–27 May 2015; pp. 53–56. [CrossRef]
34. Maitland, D.S.; Chumbley, S.L.; Bradley, H.E. Modular Binary Half-Adder. U.S. Patent No. 4,054,788, 18 October 1977. Available online: https://patents.google.com/patent/US4054788A/en (accessed on 12 August 2024).

35. Lin, W.C. Modular Operation Circuit Adopting Iterative Calculations. U.S. Patent No. 11,662,978, 30 May 2023. Available online: https://patents.google.com/patent/US11662978B2/en (accessed on 12 August 2024).
36. Gu, J.; Wang, Z.; Kuen, J.; Ma, L.; Shahroudy, A.; Shuai, B.; Chen, T. Recent advances in convolutional neural networks. *Pattern Recognit.* **2018**, *77*, 354–377. [CrossRef]
37. Afridi, M.J.; Ross, A.; Shapiro, E.M. On automated source selection for transfer learning in convolutional neural networks. *Pattern Recognit.* **2018**, *73*, 65–75. [CrossRef]
38. Li, Z.; Liu, F.; Yang, W.; Peng, S.; Zhou, J. A survey of convolutional neural networks: Analysis, applications, and prospects. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *33*, 6999–7019. [CrossRef]
39. Sun, L.; Zhang, Y.; Chang, X.; Wang, Y.; Xu, J. Cloud-aware generative network: Removing cloud from optical remote sensing images. *IEEE Geosci. Remote Sens. Lett.* **2019**, *17*, 691–695. [CrossRef]
40. Li, X.; Wang, L.; Cheng, Q.; Wu, P.; Gan, W.; Fang, L. Cloud removal in remote sensing images using nonnegative matrix factorization and error correction. *ISPRS J. Photogramm. Remote Sens.* **2019**, *148*, 103–113. [CrossRef]
41. Kadyrzhan, K.; Kaldybekov, D.; Baipakbaeva, S.; Vitulyova, Y.; Matrassulova, D.; Suleimenov, I. Electronic Fourier–Galois Spectrum Analyzer for the Field GF (31). *Appl. Sci.* **2024**, *14*, 7770. [CrossRef]
42. Suleimenov, I.E.; Mun, G.A.; Kabdushev, S.B.; Alikulov, A.; Shaltykova, D.B.; Moldakhan, I. The design of viscometer with smartphone controlling. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *27*, 366–374. [CrossRef]
43. Torres, F.; Basaran, A.C.; Schuller, I.K. Thermal management in neuromorphic materials, devices, and networks. *Adv. Mater.* **2023**, *35*, 2205098. [CrossRef] [PubMed]
44. Sangwan, V.K.; Hersam, M.C. Neuromorphic nanoelectronic materials. *Nat. Nanotechnol.* **2020**, *15*, 517–528. [CrossRef]
45. Oh, S.; Hwang, H.; Yoo, I.K. Ferroelectric materials for neuromorphic computing. *APL Mater.* **2019**, *7*, 091109. [CrossRef]
46. Zhu, H.H.; Zou, J.; Zhang, H.; Shi, Y.Z.; Luo, S.B.; Wang, N.; Liu, A.Q. Space-efficient optical computing with an integrated chip diffractive neural network. *Nat. Commun.* **2022**, *13*, 1044. [CrossRef]
47. Kazanskiy, N.L.; Butt, M.A.; Khonina, S.N. Optical computing: Status and perspectives. *Nanomaterials* **2022**, *12*, 2171. [CrossRef]
48. Krauhausen, I.; Koutsouras, D.A.; Melianas, A.; Keene, S.T.; Lieberth, K.; Ledanseur, H.; Sheelamanthula, R.; Giovannitti, A.; Torricelli, F.; Mcculloch, I.; et al. Organic Neuromorphic Electronics for Sensorimotor Integration and Learning in Robotics. *Sci. Adv.* **2021**, *7*, eabl5068. [CrossRef]
49. Krauhausen, I.; Coen, C.; Spolaor, S.; Gkoupidenis, P.; Van De Burgt, Y. Brain-Inspired Organic Electronics: Merging Neuromorphic Computing and Bioelectronics Using Conductive Polymers. *Adv. Funct. Mater.* **2024**, *34*, 2307729. [CrossRef]
50. Giovannitti, A.; Sbircea, D.-T.; Inal, S.; Nielsen, C.B.; Bandiello, E.; Hanifi, D.A.; Sessolo, M.; Malliaras, G.G.; McCulloch, I.; Rivnay, J. Controlling the Mode of Operation of Organic Transistors through Side-Chain Engineering. *Proc. Natl. Acad. Sci. USA* **2016**, *113*, 12017–12022. [CrossRef] [PubMed]
51. Wu, X.; Wang, S.; Huang, W.; Dong, Y.; Wang, Z.; Huang, W. Wearable In-Sensor Reservoir Computing Using Optoelectronic Polymers with through-Space Charge-Transport Characteristics for Multi-Task Learning. *Nat. Commun.* **2023**, *14*, 468. [CrossRef] [PubMed]
52. Zhang, Y.; Van Doremaele, E.R.W.; Ye, G.; Stevens, T.; Song, J.; Chiechi, R.C.; Van De Burgt, Y. Adaptive Biosensing and Neuromorphic Classification Based on an Ambipolar Organic Mixed Ionic–Electronic Conductor. *Adv. Mater.* **2022**, *34*, 2200393. [CrossRef] [PubMed]
53. Zhang, B.; Chen, W.; Zeng, J.; Fan, F.; Gu, J.; Chen, X.; Yan, L.; Xie, G.; Liu, S.; Yan, Q.; et al. 90% Yield Production of Polymer Nano-Memristor for in-Memory Computing. *Nat. Commun.* **2021**, *12*, 1984. [CrossRef]
54. Suleimenov, I.; Gabrielyan, O.; Kopishev, E.; Kadyrzhan, A.; Bakirov, A.; Vitulyova, Y. Advanced Applications of Polymer Hydrogels in Electronics and Signal Processing. *Gels* **2024**, *10*, 715. [CrossRef]
55. Suleimenov, I.; Bakirov, A.; Moldakhan, I. Formalization of ternary logic for application to digital signal processing. In *Energy Management of Municipal Transportation Facilities and Transport*; Springer International Publishing: Cham, Switzerland, 2019; pp. 26–35. [CrossRef]
56. Shaikhutdinov, R.; Mun, G.; Kopishev, E.; Bakirov, A.; Kabdushev, S.; Baipakbaeva, S.; Suleimenov, I. Effect of the Formation of Hydrophilic and Hydrophobic–Hydrophilic Associates on the Behavior of Copolymers of N-Vinylpyrrolidone with Methyl Acrylate in Aqueous Solutions. *Polymers* **2024**, *16*, 584. [CrossRef]
57. Suleimenov, I.E.; Gabrielyan, O.A.; Bakirov, A.S. Initial study of general theory of complex systems: Physical basis and philosophical understanding. *Bull. Electr. Eng. Inform.* **2025**, *14*, 774–789. [CrossRef]

algorithms

MDPI

Article

Application of the Algebraic Extension Method to the Construction of Orthogonal Bases for Partial Digital Convolutions

Aruzhan Kadyrzhan [1], Akhat Bakirov [1,2,*], Dina Shaltykova [2] and Ibragim Suleimenov [2]

[1] Institute of Communications and Space Engineering, Gumarbek Daukeev Almaty University of Power Engineering and Communications, Almaty 050040, Kazakhstan; aru.kadyrzhan@gmail.com
[2] National Engineering Academy of the Republic of Kazakhstan, Almaty 050010, Kazakhstan; dina65@mail.ru (D.S.); esenych@yandex.ru (I.S.)
* Correspondence: axatmr@mail.ru

Abstract: Mathematical tools have been developed that are analogous to the tool that allows one to reduce the description of linear systems in terms of convolution operations to a description in terms of amplitude-frequency characteristics. These tools are intended for use in cases where the system under consideration is described by partial digital convolutions. The basis of the proposed approach is the Fourier–Galois transform using orthogonal bases in corresponding fields. As applied to partial convolutions, the Fourier–Galois transform is decomposed into a set of such transforms, each of which corresponds to operations in a certain Galois field. It is shown that for adequate application of the Fourier–Galois transform to systems described by partial convolutions, it is necessary to ensure the same number of cycles in each of the transforms from the set specified above. To solve this problem, the method of algebraic extensions was used, a special case of which is the transition from real numbers to complex numbers. In this case, the number of cycles varies from p to p^n/k, where p is a prime number, n and k are integers, and an arbitrary number divisor of p^n can be chosen as k. This allows us to produce partial Fourier–Galois transforms corresponding to different Galois fields, for the same number of cycles. A specific example is presented demonstrating the constructiveness of the proposed approach.

Keywords: orthogonal bases; algebraic extensions; digital convolutions; Fourier–Galois transforms; transfer function; linear systems

Citation: Kadyrzhan, A.; Bakirov, A.; Shaltykova, D.; Suleimenov, I. Application of the Algebraic Extension Method to the Construction of Orthogonal Bases for Partial Digital Convolutions. *Algorithms* **2024**, *17*, 496. https://doi.org/10.3390/a17110496

Academic Editor: Meng Liu

Received: 30 August 2024
Revised: 20 October 2024
Accepted: 25 October 2024
Published: 3 November 2024

1. Introduction

The application of the Fourier–Galois transform covers a wide range of scientific and technical disciplines [1–3], where it is used for signal analysis, solving differential equations, and optimization in various systems. This transform combines the algebraic methods of Galois theory with the harmonic analysis of the Fourier transform, which makes it especially useful in problems involving the use of symmetrical features and group structure. One of the important areas of application of the Fourier–Galois transform is coding theory and cryptography [4,5]. It is used to analyze and create resistant ciphers based on Galois theory [6,7]. For example, working with finite fields and cyclic groups, which are used in modern encryption systems such as RSA and ECC, can be simplified using this transform [8,9]. The Fourier–Galois transform has found application in digital signal processing [10,11], where it helps to solve problems of filtering, compression and signal analysis. An example is in the efficient recovery of signals from noisy data, where the symmetric properties of the transform in question help improve the filtering of high-frequency noise [12,13].

In mathematical physics, the Fourier–Galois transform is used to solve linear differential equations, especially those involving operators with certain symmetric properties [14,15]. An example is the solution of equations in electrodynamics or quantum

mechanics, where the symmetry of the system allows for simpler calculations [16]. In number theory, the Fourier–Galois transform is used to study the properties of numbers and to solve problems related to the distribution of prime numbers [17]. For example, it is used in the analysis of algebraic structures of number fields [18] and in solving problems related to the distribution of residues by modules [19].

In the field of computational mathematics, the Fourier–Galois transform is used to optimize FFT algorithms in systems with finite fields [20]. This is relevant in problems related to big data processing and modeling of complex systems, such as meteorological models or control systems. In quantum information science, the Fourier–Galois transform is used to develop quantum algorithms [21]. For example, it is used in factorization and period search problems [22], which is important for quantum cryptography and quantum search algorithms.

In telecommunications, the Fourier–Galois transform helps improve modulation and signal coding systems. An example is its application in OFDM (Orthogonal Frequency Division Multiplexing) [23–25], where it is used to improve noise immunity and increase data transmission speed. Thus, the Fourier–Galois transform finds application in a wide range of disciplines, from number theory and cryptography to quantum information science and digital signal processing, offering powerful tools for solving problems related to symmetry and algebraic structures. A number of other areas of application of the Fourier–Galois transform, as well as the Fourier transform, are associated with systems described by the convolution operation.

Indeed, it is permissible to pose the question that the description of a system, reduced to the operation of digital convolution, can then be reduced to a description in terms of the transformation of the spectrum formed based on the corresponding orthogonal set of basis functions. There is an obvious analogy here. Linear systems of arbitrary nature, possessing the property of invariance with respect to the time shift operation, are described by the operation of classical (analog) convolution, which is used, for example, in Fourier optics [26]. One of the key applications of the convolution theorem is signal and image filtering [27]. In filtering, such as smoothing or removing noise from an image, convolution allows filters to be applied efficiently. With the Fourier transform, filtering is accomplished by multiplying the transformed signal with a filter in the frequency domain, and then performing the inverse transform to return the processed signal or image.

A special case in the field of application of this theorem is linear radio circuits formed from passive elements. The classical convolution theorem [28] allows us to move on to describing the circuit in terms of the frequency range, since the Fourier transform of the convolution is the product of the Fourier transforms of the functions under its sign. In particular, this fundamental theorem allows us to correctly justify the use of such terms as the amplitude–frequency characteristic, the frequency range of the radio signal, etc. [29]. For systems described by the digital analog of the convolution theorem, a similar theorem is valid, a visual proof of which (from the point of view of digital signal processing) was given in [30] based on the results of [31]. Therefore, it is permissible to pose the question of reducing the description of any systems whose behavior is described by the operation of digital convolution (including convolutional neural networks) to a description in terms of spectra and their transformations, similar to how this is the case for classical linear radio circuits.

This issue is also relevant to the description of convolutional neural networks (CNNs). Such networks have a number of advantages that have made them indispensable in various tasks for computer vision, signal processing, and data analysis [32]. The main advantage of CNNs is their ability to automatically extract features from data, especially from images, without the need for manual feature selection. This is achieved using convolutional layers that identify local patterns in the data (e.g., edges, textures, and shapes in images) and can combine them into more complex features as the depth of the network increases. Another important advantage of CNNs is the ability to reduce the number of parameters with

convolutional filters with shared weights [32,33]. This reduces computational complexity and makes the networks more resistant to overfitting.

The main applications of CNNs are related to pattern recognition, object detection and image segmentation. They are widely used in medical diagnostics (e.g., for analyzing X-ray and MRI images [34,35]), in security systems for facial recognition [36], and in autonomous vehicles for recognizing objects on the road [37]. CNNs can also effectively be used to analyze time series and signals such as sound and text [38,39]. For example, they are used to recognize speech and music, as well as to analyze texts in classification tasks, such as when working with the sentiment of texts or analyzing the syntactic structure.

However, the digital convolution theorem in the formulation in [40] and similar ones solve the problem of transitioning to a description of a linear system in terms of a spectrum only partially. Indeed, the theorem under consideration in the formulation indicated above is valid only for the case when the function describing the digital signal in terms of the Galois field $GF(p)$ is a periodic piecewise constant function, and the period contains exactly p-1 clock cycles. This makes the issue of constructing orthogonal bases for which this requirement is not satisfied very relevant. Note that a very wide range of orthogonal bases is currently known, used to calculate the spectra of digital functions. In particular, the Walsh basis is known, which is an orthogonal system of functions used in various applications of digital signal processing [41,42] and in problems related to the analysis of light neural networks [43]. Unlike the Fourier basis, which is based on sinusoids and cosines, the Walsh basis consists of piecewise constant functions called Walsh functions. These functions have only values of +1 or -1 and change sign at certain intervals, which makes them especially convenient for digital signal processing, where discrete levels are easier to process.

In addition to the Walsh basis, there are other orthogonal bases that allow one to move to the spectra of digital functions. One of them is the Haar basis [44], which consists of piecewise constant functions that divide segments into two parts. The Haar basis is used for data compression and the analysis of signals with abrupt changes [45,46]. Another important example is the discrete cosine transformation, which is often used in image processing such as JPEG compression [47]. It is effective for computing convolution in problems involving low-frequency components of an image.

The next step in this direction is the transition to bases constructed using the Residue Number System (RNS). It is appropriate to note that RNSs are currently increasingly used, including for fast arithmetic [48,49]. The RNS has a number of significant advantages that make it attractive for use in computing systems, especially in parallel processors and cryptography. The first advantage of RNS is that it breaks long integers into several smaller numbers that can be processed independently of each other. This property allows arithmetic operations to be performed in parallel, which significantly speeds up computations, especially in systems where high processing speed is important, such as digital signal processing [50,51] or cryptographic systems [52,53].

The second advantage of RNS is that it reduces the complexity of arithmetic operations. Unlike a traditional number system, where addition, subtraction, and multiplication require carries, in a remainder system, modulo operations are performed for each separately, eliminating the need for carries. This results in simpler and faster operations, especially for large numbers. RNS also makes it easy to implement complex operations such as modulo inverses, making it particularly useful for cryptographic applications such as RSA encryption [54].

Finally, RNS is highly error-tolerant and secure. Because each number is represented as a set of remainders over different moduli, single errors in one of the remainders do not always cause serious failures in the system. This property can be used to design systems with increased reliability [55], as well as to build schemes that are resistant to side-channel attacks in cryptography.

Furthermore, the digital convolution theorem applies to functions that take values in Galois fields. It is worth emphasizing that a function that takes values in any finite

algebraic system (Galois field, finite algebraic ring, etc.) can serve as a model of any digital signal that changes in a finite range of amplitudes. It is only important that the number of signal levels does not exceed the number of elements in the given system.

Traditionally, signal models are functions that take values on a set of real or complex numbers, but this is nothing more than a matter of agreement and convenience [40]. When using a function that takes values in some finite algebraic ring containing zero divisors, the convolution operation is decomposed into a set of convolutions that can be called partial, and which are calculated in terms of the corresponding Galois fields [56].

This work is the next step in relation to the work [56]. Namely, the goal of this work is to find such sets of basis functions that would allow partial convolutions (in calculations in algebraic rings) to be reduced to operations on the Fourier–Galois spectra of their individual components. Thus, this work allows us to find an analog of transfer functions for any systems that are described by partial convolutions.

2. Methods

The paper considers the mapping of a signal in the form of a function that takes values in a finite algebraic ring containing zero divisors. The choice of this approach is due to the following considerations.

For many problems of practical interest, the result of performing the convolution of two digital functions lies in a limited range of values. This paper considers such convolution operations whose values do not exceed a certain number P, which is the product of prime numbers.

$$P = p_1 p_2 \dots p_S \tag{1}$$

When this condition is satisfied, the result of the convolution in calculations modulo the number P, coinciding with the result of calculations in the sense of ordinary arithmetic operations.

The transition to residue classes modulo the numbers p_i allows us to consider any number $u < P$, which can be included as an element of the algebraic ring of residue classes modulo P. Specifically,

$$u \equiv e_1 u_1 + e_2 u_2 + \dots + e_N u_N (P) \tag{2}$$

where e_i are idempotent mutually canceling elements, and $u_i = 0, 1, 2, \dots, p_i - 1$.

The idempotent elements are formed according to the rule

$$e_i = \alpha_i \prod_{i \neq j}^{N} p_j \tag{3}$$

where α_i is an integer. The choice of these numbers is based on the condition

$$e_i e_i = 1 \tag{4}$$

It is obvious that by construction we have [56]

$$e_i p_i \equiv 0 (P) \tag{5}$$

since any product of the form (5) contains a factor $P = p_1 p_2 \dots p_N$.

With the choice of integers α_i made, it also holds.

$$e_1 + e_2 + \dots + e_N \equiv 1 (P) \tag{6}$$

Consider the product of two numbers written in the form (2). Since e_i are mutually annihilating idempotent elements, we have

$$u^{(1)} u^{(2)} = e_1 u_1^{(1)} u_1^{(2)} + e_2 u_2^{(1)} u_2^{(2)} + \dots + e_N u_N^{(1)} u_N^{(2)} \tag{7}$$

In this case, the calculation of the products $u_i^{(1)}u_i^{(2)}$ is actually performed in the sense of the multiplication operation in the Galois field $GF(p_i)$, since the multiplication operation is performed modulo p_i. This conclusion is also true for the addition operation [56].

Let us consider the convolution written in the form

$$U_{out}(i) = \sum_j K(j)\, U_{in}(i-j) \tag{8}$$

where $K(j)$ is the kernel of the convolution operator, and $U_{out}(i)$ and $U_{in}(i)$ are functions that we will treat as "output" and "input", respectively.

If the condition is satisfied

$$U_{out}(i) < p_1 p_2 \dots p_N, \tag{9}$$

then, in Formula (9) we can substitute the expansion through idempotent elements (2), both for $K(j)$ and for $U_{in}(i)$. We have:

$$U_{out}(i) = \sum_j \left(\sum_m e_m K_m(j)\right)\left(\sum_m e_m U_{m,in}(i-j)\right) \tag{10}$$

By swapping the summation signs, we obtain [56]

$$U_{out}(i) = \sum_m e_m \left(\sum_j K_m(j) U_{m,in}(i-j)\right) \tag{11}$$

It can be seen that the convolution operation is factorized. Each component of the functions used can be operated on in a completely independent manner.

Accordingly, in this case it is permissible to speak of partial convolutions, each of which corresponds to a certain digit in the hybrid number system. We have:

$$U_{out,m}(i) = \sum_j K_m(j) U_{m,in}(i-j) \tag{12}$$

3. Statement of the Problem

A digital convolution theorem of the form [40] is applicable to each of the partial convolutions (12).

It consists of the following:

Sequences of the following form a complete basis [40].

$$\vec{w}_k = \left(\theta^k, \theta^{2k}, \theta^{3k}, \dots, \theta^{(p-2)k}, 1\right), \tag{13}$$

where θ is a primitive element whose powers up to and including the $(n-1)$th are given by all nonzero elements of the used Galois field $GF(p)$, $k = 1, \dots, p-1$. The last element in this sequence is always equal to 1, since any nonzero element of the Galois field satisfies the equation

$$x^{p-1} - 1 = 0 \tag{14}$$

where p is the number of elements of the field, including the zeroth one.

Sequences (13) can also be considered as piecewise constant functions taking values in the field $GF(p)$. They are direct "digital" analogs of harmonic functions; in particular, they form a complete basis and are orthogonal in the following sense [40]

$$\sum_{j=1}^{j=p-1} w_{k_1}^{(j)} w_{k_2}^{(j)} = \begin{cases} \text{“}n\text{”}, k_1 + k_2 \equiv 0 (mod\ p-1) \\ 0, k_1 + k_2 \not\equiv 0 (mod\ p-1) \end{cases} \tag{15}$$

Formula (15) contains the notation "n" in quotation marks. This notation implies that if the condition $k_1 + k_2 \equiv 0 (mod\ p-1)$ is met, all terms under the sum sign on the left side of this formula turn into 1. However, the sum of n units, generally speaking, in different

Galois fields (even if the number of such terms remains the same) can take on different values.

The condition on the right side of Formula (15) is an analog of the following relation for harmonic functions

$$\int_0^{2\pi} \exp\left(-i\frac{2\pi mt}{T_0}\right)\exp\left(i\frac{2\pi nt}{T_0}\right) \sim \delta_{m,n} \tag{16}$$

That is, the fulfillment of the condition $k_1 + k_2 \equiv 0(mod\ p-1)$ means that the sequences $w_{k_2}^{(j)}$ and $w_{k_1}^{(j)}$ are conjugate to each other.

For a sequence conjugate to a sequence $\vec{w}_j$, the notation $\vec{w}_j^T$ will be used below.

Relation (16) allows us to immediately move on to the spectral representation of the signal in the form

$$\vec{u} = \sum_{j=1}^{j=p-1} z_j \vec{w}_j \tag{17}$$

where the spectral components (Fourier–Galois spectrum) can be calculated as

$$z_j = q(\vec{u},\vec{w}_j^T) \tag{18}$$

where q is a factor determined from the condition $q(\vec{w}_j, \vec{w}_j^T) = 1$, which is different for different Galois fields.

It is essential that the spectrum defined by Formula (18) describes the piecewise constant function (or sequence) $\vec{u}$ with exhaustive completeness, provided that this function is periodic, and its period contains exactly $p-1$ cycles.

The digital convolution theorem is expressed by the formula [40]

$$\left(\vec{U}_{out,m}, \vec{w}_j^T\right) \sim \left(\vec{K}_m, \vec{w}_j^T\right)\left(\vec{U}_{m,in}, \vec{w}_j^T\right) \tag{19}$$

It can be seen that it is a complete analog of the classical convolution theorem.

However, there is a significant nuance. Sequences of (13), as emphasized above, contain exactly $p-1$ elements. Accordingly, for different numbers p_i, which are factors of the number P, the number of cycles on which the orthogonal basis is determined will also be different. This does not allow for applying the convolution theorem in the form (19) to Formula (10) directly.

The problem solved in this paper can be formulated as follows.

Find such orthogonal bases that will allow applying the digital convolution theorem to Formula (10), thereby determining the transfer function for digital convolution, represented through a set of partial convolutions.

This problem is solved using the method of algebraic extensions.

4. Results

4.1. Using Algebraic Extensions to Construct Orthogonal Bases

Recall that an algebraic extension is formed by adjoining, to the ground field, the root of an irreducible equation, i.e., an equation that has no solution in the ground field.

In particular, the complex numbers $x = a_1 + ia_2$ are formed by adjoining to the set of real numbers the root of the equation

$$x^2 + 1 = 0 \tag{20}$$

which has no real roots.

Galois fields $GF(p^n)$ are constructed by adjoining to the field $GF(p)$ the root θ of an irreducible equation of degree n.

Let us consider as an example the construction of the fields $GF(5^2)$ and $GF(7^2)$.

The field $GF(5^2)$ is constructed as an algebraic extension of the field $GF(5)$. The elements $0, 1, 2, 3, 4$ are chosen as the elements of the field $GF(5)$.

Equation (20) in the field $GF(5)$ has a solution. Therefore, the irreducible equation is used [19]

$$x^2 = 3 \tag{21}$$

Element 3 in the field $GF(5)$ is the inverse of element 2. Accordingly, if we select elements of this field in the form $-2, -1, 0, 1, 2$, then instead of Equation (21), we could use the equation $x^2 + 2 = 0$, similar to (20). If there are no negative numbers in the set used, then the correct form is (21).

Accordingly, the elements of the field $GF(5^2)$ can be represented in the form [57]

$$x = a_1 + ia_2 \tag{22}$$

where i is the root of the irreducible Equation (21), which can also be interpreted as a logical imaginary unit.

The multiplication of elements of the form (22), therefore, is carried out according to the rule

$$xy = (a_1 + ia_2)(b_1 + ib_2) = (a_1b_1 + 3a_2b_2) + i(a_2b_1 + a_1b_2) \tag{23}$$

where the calculation of expressions in brackets is carried out in the sense of the field $GF(5)$.

The field $GF(7^2)$ is constructed as an algebraic extension of the field $GF(7)$. The elements $0, 1, 2, 3, 4, 5, 6$ are chosen as the elements of the field $GF(7)$.

In this field, Equation (20) is irreducible; therefore, for this case, $i^2 = -1$. However, if negative elements are not used, then the correct form is $x^2 = 6$. Accordingly, the multiplication of the field elements is carried out according to the rule

$$xy = (a_1 + ia_2)(b_1 + ib_2) = (a_1b_1 + 6a_2b_2) + i(a_2b_1 + a_1b_2) \tag{24}$$

where the calculation of expressions in brackets is carried out in the sense of the field $GF(7)$.

Orthogonal bases in the fields $GF(5^2)$ and $GF(7^2)$ can also be constructed according to rule (13). The first elements of such sequences are all nonzero elements of the fields under consideration that satisfy the equation

$$x^{q-1} = 1 \tag{25}$$

where $q = p^n$ is the number of elements of the field, including zero.

Therefore, the length of such sequences for the field $GF(5^2)$ is 24 cycles, and for the field $GF(7^2)$—48 cycles.

However, there is an important nuance.

Sequences of (13) obviously have different periodicity [58]. This can be proven as follows. All elements of any Galois field satisfy Equation (25). The number $q - 1$ is not necessarily prime. In particular, it can contain a factor q_1. This means that there are $\frac{q-1}{q_1}$ elements satisfying the equation

$$x^{\frac{q-1}{q_1}} - 1 = 0 \tag{26}$$

The roots of this equation are obviously representable as θ^{q_1}, where θ is a primitive element of the field under consideration.

All such quantities appear as the first elements of sequences (13) in their general list. These sequences have a period that contains not $q - 1$, but $\frac{q-1}{q_1}$ cycles.

In particular, for the case of the field $GF(7^2)$, the value $q - 1 = 48$. This number contains the factor $q_1 = 2$, i.e., among sequences of the form (13) in this case there are 24 sequences that have a period containing 24 cycles (or less).

The first elements of such sequences satisfy the equation over the field $GF(7^2)$

$$x^{24} - 1 = 0 \tag{27}$$

For an interval containing 24 bars, they also form a complete orthogonal basis, and orthogonality is proved in the same way as for sequences (13).

Let us form two sequences of the form (13).

$$\vec{w}_{1,2} = \left(\xi_{1,2}^{1}, \xi_{1,2}^{2}, \xi_{1,2}^{3}, \ldots, \xi_{1,2}^{23}, 1\right), \tag{28}$$

where ξ_i^1 is root of Equation (27).

Their scalar product with each other is

$$\left(\vec{w}_1, \vec{w}_2\right) = \sum_{m=1}^{24} (\xi_1 \xi_2)^m, \tag{29}$$

The solutions of Equation (27) obviously form a group under multiplication. Consequently, the product $\xi_1\xi_2$ is also an element of this group, i.e., the root of (27). On the right-hand side of (29) is the sum of a geometric progression; therefore, for $\xi_1\xi_2 \neq 1$ we have

$$\left(\vec{w}_1, \vec{w}_2\right) = \frac{1 - (\xi_1\xi_2)^{24}}{1 - \xi_1\xi_2} = 0 \tag{30}$$

It remains to clarify the values of the multiplier q for the cases under consideration. As noted above, the multiplier q is determined from the condition

$$q\left(\vec{w}_j, \vec{w}_j^{T}\right) = 1 \tag{31}$$

where $\vec{w}_j^{T}$ is a sequence conjugate of sequence $\vec{w}_j$.

According to Formula (27), the number of elements in the sequences under consideration is 24. Therefore, with respect to the field $GF\left(7^2\right)$, q is exactly the inverse element to the element that is equal to the number 24 taken modulo 7. For the field $GF\left(5^2\right)$, it is taken modulo 5.

The number 24 modulo 5 is 4. This element in the field $GF(5)$ is inverse to itself $4^2 \equiv 1 \bmod 5$, whence

According to Formula (27), the number of elements in the considered

$$q_{(5)} = 4 \tag{32}$$

Likewise,

$$q_{(7)} = 5 \tag{33}$$

Since $3{\cdot}5 \equiv 1 \bmod 7$; $24 \equiv 3 \bmod 7$.

Thus, algebraic extensions of the fields under consideration allow us to construct orthogonal bases corresponding to intervals containing the same number of cycles.

This allows us to use them to apply the digital convolution theorem to partial convolutions.

4.2. Application of the Digital Convolution Theorem to Partial Convolutions

Let us show, with a specific example, that the use of algebraic extensions, which allow us to reduce the calculations of partial convolutions to Fourier–Galois bases containing the same number of cycles, allows us to extend the theorem on digital convolution to the case when the convolution is represented as a sum of partial convolutions.

Let us consider the convolution

$$U_1(j) = \sum_{1}^{24} K(j-i)U_0(i) \tag{34}$$

We will assume that the maximum value of the functions U_1, K, and U_0 does not exceed 34; i.e., it is permissible to assume that these functions take values in the ring of residue classes modulo 35. We will also assume that the function $U_0(i)$ is periodic, and

its period is 24 cycles, and that the domain of the definition of the function K fits into this interval. In the ring under consideration, each number can be represented in the form

$$u \equiv 21 \cdot u_1 + 15 \cdot u_2 (mod\ 35) \tag{35}$$

where $u_1 = 0, 1, 2, 4$, $u_2 = 0, 1, \ldots, 6$; and the numbers 21 and 15 are idempotent elements, which, in particular, satisfy relation (4), which can be verified by direct verification.

We apply the general Formulas (11)–(34), representing all the functions appearing in (34) in the form (35). Then

$$U_1(j) \equiv 21 \cdot \sum_1^{24} K_1(j-i) U_{01}(i) + 15 \cdot \sum_1^{24} K_2(j-i) U_{02}(i) (mod\ 35) \tag{36}$$

In this formula, the functions $K_{1,2}$ and $U_{01,2}$ are defined as

$$U_{01} \equiv U_0 (mod\ 5);\ U_{02} \equiv U_0 (mod\ 7);\ K_1 \equiv K (mod\ 5);\ K_2 \equiv K (mod\ 7) \tag{37}$$

The possibility of such a representation follows directly from general Formula (6).

It is essential that the convolution $\sum_1^{24} K_1(j-i) U_{01}(i)$ is calculated in the field $GF(5^2)$, and the convolution $\sum_1^{24} K_2(j-i) U_{02}(i)$ is calculated in the field $GF(7^2)$, i.e., the digital convolution theorem in the form [40] is applicable to both of them.

Specifically, the Fourier–Galois transform of the first of the convolutions under consideration, $F_1(K_1 * U_{01})$, is

$$F_1(K_1 * U_{01}) = q_1 \sum_{j=1}^{24} \xi^{\bar{k}j} \sum_{i=1}^{24} K_1(j-i) U_{01}(i) = q_1 \sum_{i=1}^{24} U_{01}(i) \sum_{j=1}^{24} \xi^{\bar{k}j} K_1(j-i) \tag{38}$$

where the bar over the symbol $\bar{k}$ means that the calculations use the number (degree) corresponding to the conjugate sequence, i.e., the sequence determined by condition (15).

In the right part of Formula (38) the order of summation is changed.

The next identity is valid:

$$\sum_{i=0}^{23} \xi^{\bar{k}j} K_1(j-i) = \xi^{\bar{k}j} \sum_{j=0}^{23} \xi^{\bar{k}(j-i)} K_1(j-i) \tag{39}$$

The sum on the right side of Formula (39) is exactly the result of the Fourier–Galois transform of function K_1, since all the functions under consideration change cyclically. Substituting (39) into (38), we obtain

$$F_1(K_1 * U_{01}) = q_1^{-1} F_1(K_1) F_1(U_{01}) \tag{40}$$

It is easy to show that a similar formula is also valid for the second of the convolutions under consideration.

$$F_2(K_2 * U_{02}) = q_2^{-1} F_2(K_2) F_2(U_{02}) \tag{41}$$

The difference is that the Fourier–Galois transforms for these convolutions are performed using different bases corresponding to algebraic extensions of different Galois fields.

It can be seen that in the case under consideration it is permissible to speak of partial transfer functions $F_1(K_1)$ and $F_2(K_2)$, which exhaustively describe the result of the convolution operation. In particular, to return to the function $U_1(j)$, it is necessary to perform inverse Fourier–Galois transforms in the corresponding fields.

It is easy to see that the obtained result can be generalized to an arbitrary number of terms in the formula for partial convolutions (11). To do this, it is necessary to ensure such a choice of algebraic extensions that would allow the Fourier–Galois bases to be reduced to the same number of cycles.

Let us consider a specific example for clarity.

4.3. Example

The convolution of the model function shown in Figure 1, curve 1 with the model convolution kernel, Figure 2, is used. The function, curve 1, takes discrete integer values in the range from 0 to 6 on discrete values of the current integer variable k. These values are shown by blue dots (similarly for the curve in Figure 2). The type of model function was chosen based on the convenience of demonstrating the results obtained. Curve 2 in Figure 1 is the result of calculating the convolution using the rules of ordinary arithmetic. It also takes values on discrete values of the current integer variable k (red dots), but the range of its variation increases.

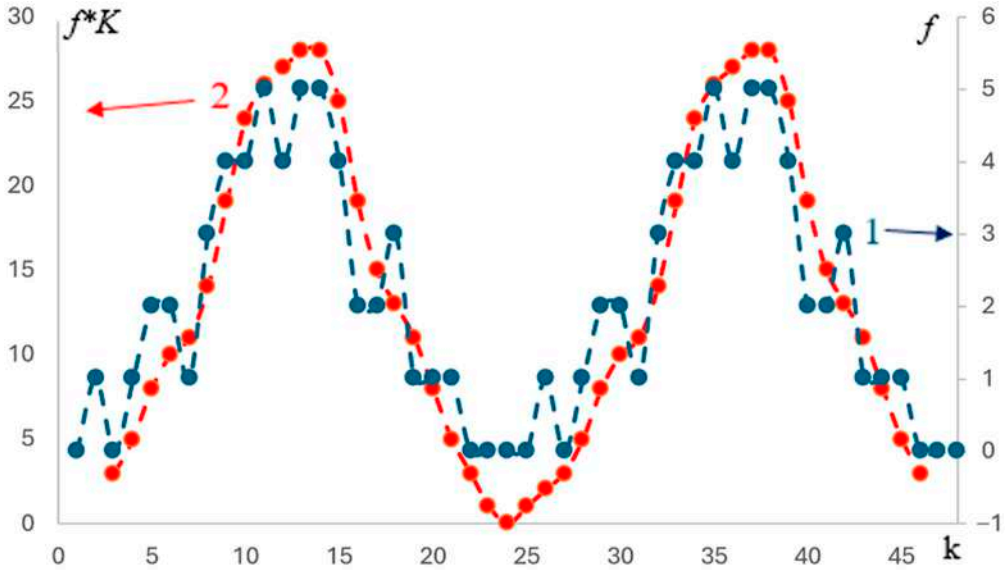


Figure 1. Model function f, curve 1, and the result of the convolution $f * K$ of this function with the model convolution kernel K, Figure 2 (curve 2).

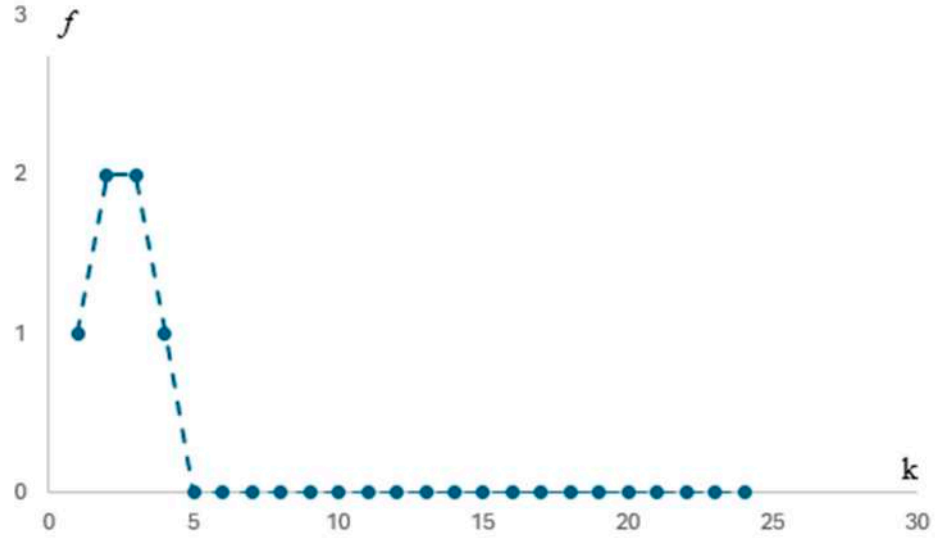


Figure 2. Model convolution kernel K.

Let us show that the result of the convolution operation, shown in Figure 1, curve 2, can also be obtained by using the digital convolution theorem for a set of partial convolutions.

The table in supplemental materials File S1 presents functions corresponding to 24-cycle bases in the fields $GF(5^2)$ and $GF(7^2)$, respectively.

More precisely, functions with a 24-term period were selected from the basis functions corresponding to the field $GF(7^2)$.

These bases were used to calculate the real and imaginary parts of the Fourier–Galois spectra of the functions

$$f_1 \equiv f(mod\ 5);\ f_2 \equiv f(mod\ 7);\ K_1 \equiv K(mod\ 5);\ K_2 \equiv K(mod\ 7) \tag{42}$$

The calculations were carried out in a Python program; the program code is presented in supplemental materials File S2. In the diagrams in Figures 3 and 4, the real and imaginary components of the Fourier–Galois spectra of the functions f_1 and f_2 are shown separately as an example.

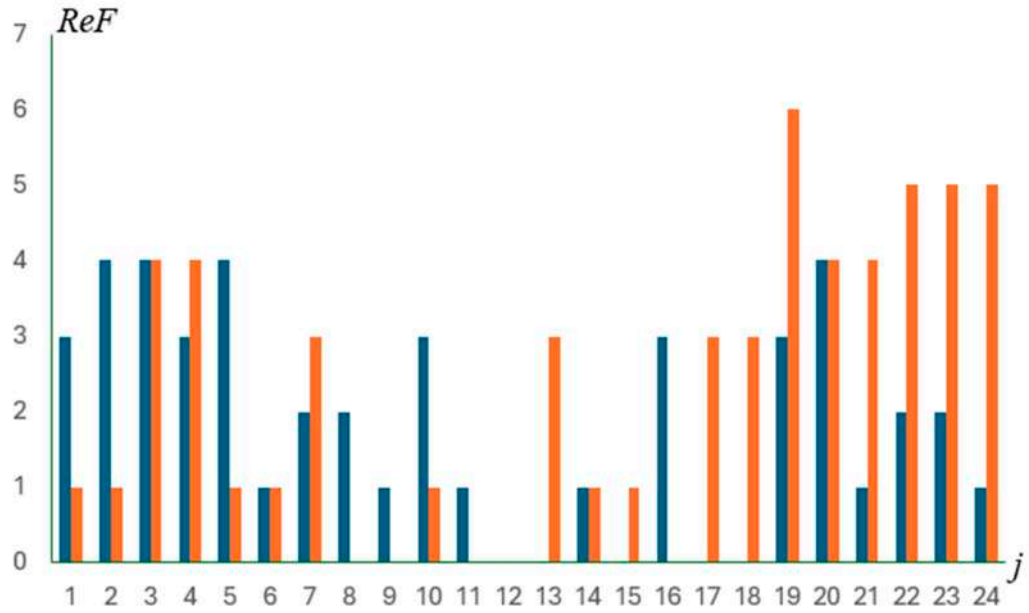


Figure 3. Real parts of the Fourier–Galois spectra $ReF[f_1]$ and $ReF[f_2]$ of the functions f_1 and f_2, defined in the fields $GF(5)$ and $GF(7)$, respectively; blue color—field $GF(5)$; red color—field $GF(7)$.

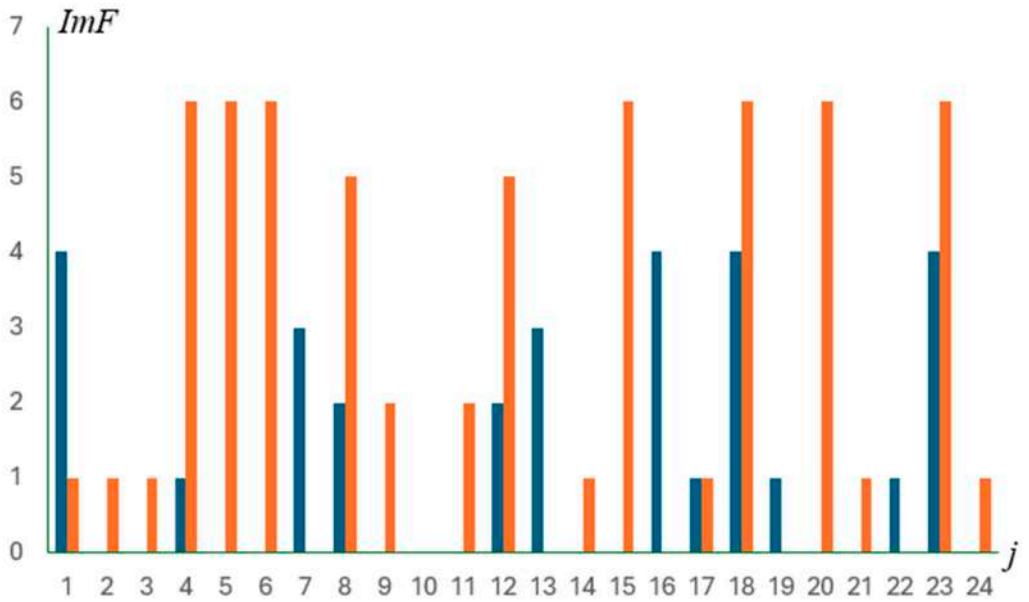


Figure 4. Imaginary parts of the Fourier–Galois spectra $ImF[f_1]$ and $ImF[f_2]$ of the functions f_1 and f_2, defined in the fields $GF(5)$ and $GF(7)$, respectively; blue color—field $GF(5)$; red color—field $GF(7)$.

The calculations were carried out using the formulas

$$F_1(f_1) = q_1 \sum_{j=1}^{24} \theta^{\bar{k}j} f_1(j) \tag{43}$$

where θ is a primitive element of the field $GF(5^2)$, and

$$F_2(f_2) = q_2 \sum_{j=1}^{24} \xi^{\bar{k}j} f_1(j) \tag{44}$$

where ξ is the square of the primitive element of the field $GF(7^2)$, the bar over the symbol $\bar{k}$ means that the number (degree) corresponding to the conjugate sequence is used in the calculations.

Similar formulas were used to calculate the components of the spectrum of the kernels K_1 and K_2.

At the next step, the products $F_1(K_1)F_1(f_1)$ and $F_2(K_2)F_2(f_2)$ were calculated. We emphasize that these products were calculated in the sense of the fields $GF(5^2)$ and $GF(7^2)$, respectively; i.e., in one case, Formula (23) was used, and in the other, (24).

The corresponding diagrams are shown in Figures 5 and 6. The diagrams also show the real and imaginary components separately.

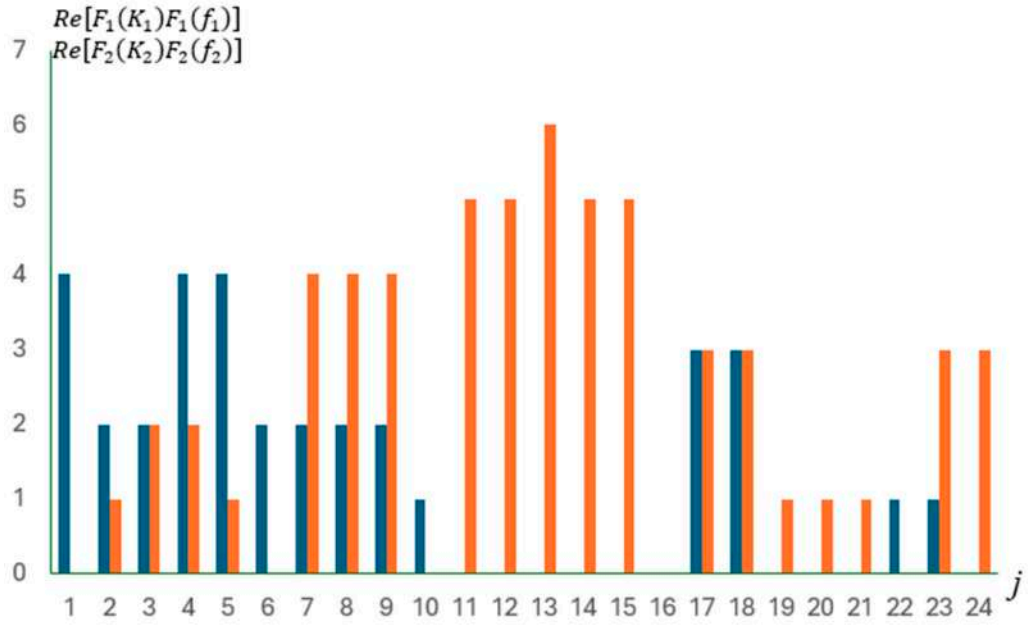


Figure 5. Real parts of the products $F_1(K_1)F_1(f_1)$ (blue) and $F_2(K_2)F_2(f_2)$ (red).

Then, the reverse transition to partial convolutions $K_1 * f_1$ and $K_2 * f_2$ was carried out according to the following formulas:

$$K_1 * f_1 = q_1^{-1} \sum_{j=1}^{24} \theta^{kj} z_1(j) \tag{45}$$

$$K_2 * f_2 = q_2^{-1} \sum_{j=1}^{24} \xi^{kj} z_2(j) \tag{46}$$

where $z_1(j)$ is the j-th component of the spectrum $F_1(K_1)F_1(f_1)$, and $z_2(j)$ is the j-th component of the spectrum $F_2(K_2)F_2(f_2)$.

The results of partial convolution calculations are shown in Figures 7 and 8. The same figures show the results of direct calculation of these convolutions for comparison. For clarity, the result of direct convolution calculation corresponds to the scale of the left axis, and the calculation using direct and inverse Fourier–Galois transforms corresponds to the right axis. As a result, one of the graphs is shifted relative to the other by one along the

ordinate axis. We emphasize that these graphs actually represent the same curve. The shift is introduced artificially in order to demonstrate that the results of calculations carried out in two different ways coincide (if the shift is not introduced, the curves will exactly overlap each other). This is emphasized by the designations of the right and left axes.

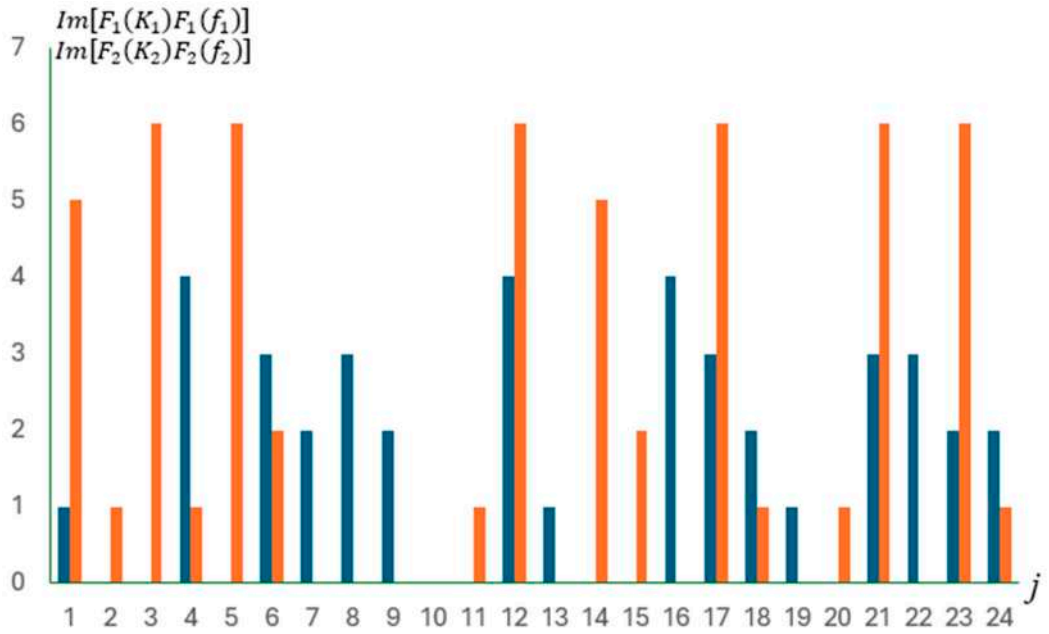


Figure 6. Imaginary parts of the products $F_1(K_1)F_1(f_1)$ (blue) and $F_2(K_2)F_2(f_2)$ (red).

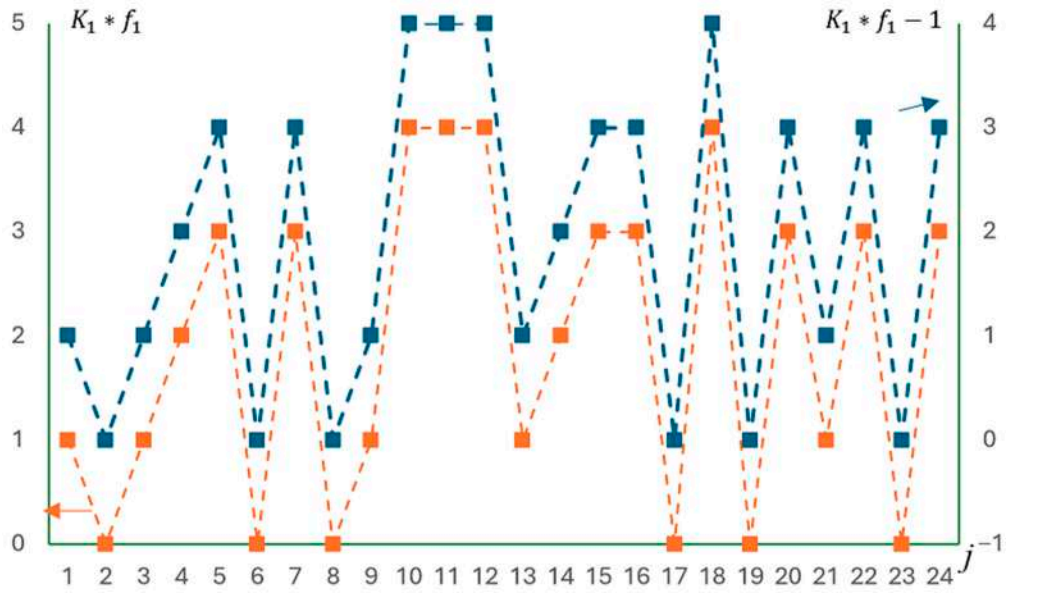


Figure 7. Comparison of the results of calculating the partial convolution $K_1 * f_1$ using the direct method (red, left axis) and the method using the direct and inverse Fourier–Galois transforms (blue, right axis).

A comparison of different methods for calculating the convolution is shown in Figure 9. Here, too, for clarity, an artificial shift of one unit is used due to differences in the scales of the right and left axes. The convolution value was calculated using the formula

$$U_1(j) \equiv 21 \cdot K_1 * f_1 + 15 \cdot K_2 * f_2 (mod\ 35) \quad (47)$$

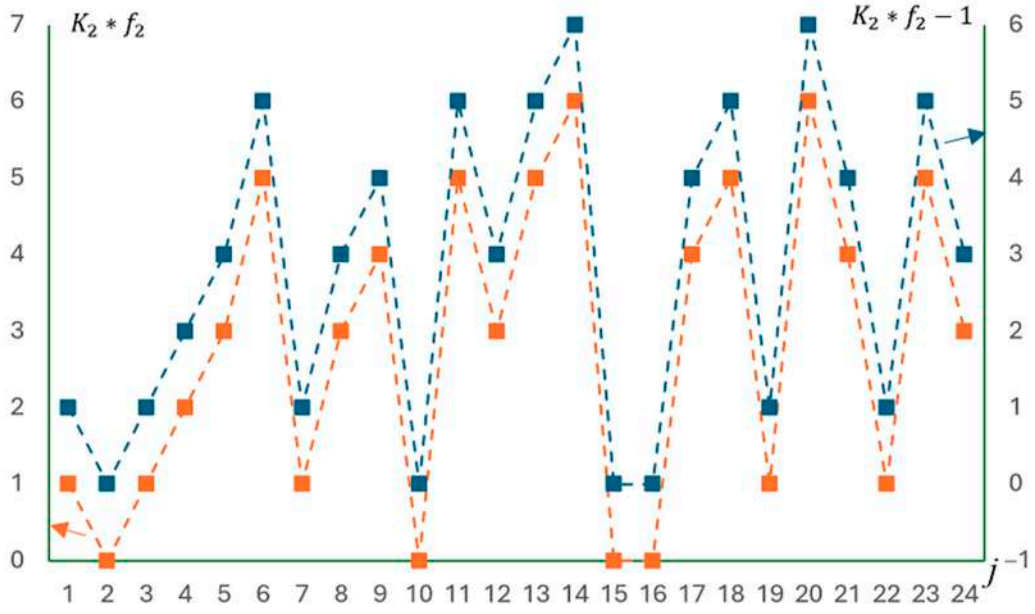


Figure 8. Comparison of the results of calculating the partial convolution $K_2 * f_2$ using the direct method (red, left axis) and the method using the direct and inverse Fourier–Galois transforms (blue, right axis).

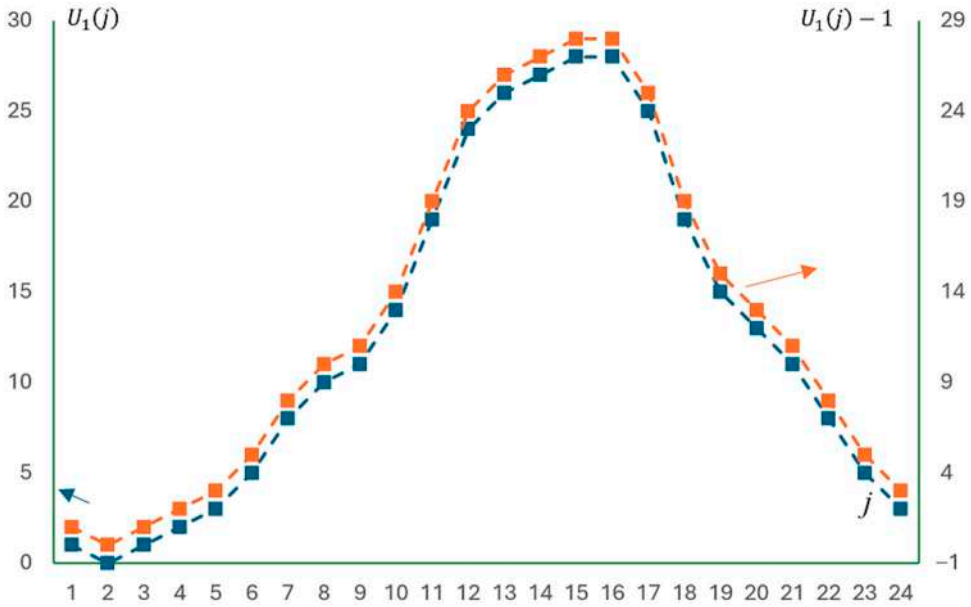


Figure 9. Comparison of the results of calculating the convolution $U_1(j) = \sum_1^{24} K(j-i)U_0(i)$ by the direct method (red color, right axis) and the method using the direct and inverse Fourier–Galois transforms (blue color, left axis).

Thus, it can be seen that the proposed approach does indeed allow one to move from a description in terms of partial convolutions to a description in terms of partial transfer functions. The proposed approach, among other things, can be considered as a generalized reduction of the description of linear systems of various natures in terms of the convolution operation to a description in terms of spectra and, consequently, in terms of transfer functions of linear systems widely used in electronics, Fourier optics, etc. Accordingly, the application of the proposed approach should be oriented towards very specific fields of interest for applied purposes. In particular, the results obtained are of greatest interest for describing convolutional neural networks, especially in cases where they can be described in terms of partial convolutions. In this case, it becomes possible to

reduce the description of such a neural network to a transfer function. In the long term, this allows us to simplify the training procedures for such neural networks, including when starting from a given transfer function.

5. Conclusions

Thus, along with the concept of "partial convolutions", it is advisable to use the concept of "partial Fourier–Galois transforms". These transforms can be applied, for example, to various components of the representation of natural numbers in RNS. In this case, a Fourier–Galois transform corresponding to a certain Galois field is applied to each component.

The use of this approach, in turn, requires reducing the partial Fourier–Galois transforms to the same number of cycles. This problem is conveniently solved using the method of algebraic extensions. In the future, this approach will allow for describing convolutional neural networks in terms of transfer functions, including those using multi-valued logic.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/a17110496/s1, File S1: Table S1: Set of bases for $GF(5^2)$; Table S2: Set of bases for $GF(7^2)$; File S2: Listing for calculations.

Author Contributions: Conceptualization, A.B. and I.S.; methodology, I.S., A.B. and A.K.; formal analysis, A.K., A.B., D.S. and I.S.; writing—original draft preparation, A.K., A.B., D.S. and I.S.; writing—review and editing, A.K., A.B., D.S. and I.S.; visualization, A.B. and I.S.; supervision, I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been/was/is funded by the Science Committee of the Ministry of Higher Education and Science of the Republic of Kazakhstan (Grant No. AP14870281).

Data Availability Statement: The original contributions presented in the study are included in the article/Supplementary Materials; further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shi, L.; Zhang, W.; Chang, Y.; Wang, H.; Liu, Y. Blind Recognition of Reed-Solomon Codes Based on Galois Field Fourier Transform and Reliability Verification. *IEEE Commun. Lett.* **2023**, *27*, 2137–2141. [CrossRef]
2. Huang, Q.; Tang, L.; He, S.; Xiong, Z.; Wang, Z. Low-Complexity Encoding of Quasi-Cyclic Codes Based on Galois Fourier Transform. *IEEE Trans. Commun.* **2014**, *62*, 1757–1767. [CrossRef]
3. Wu, G.; Zhang, B.; Wen, X.; Guo, D. Blind recognition of BCH code based on Galois field fourier transform. In Proceedings of the 2015 International Conference on Wireless Communications & Signal Processing (WCSP), Nanjing, China, 15–17 October 2015; pp. 1–4. [CrossRef]
4. Liu, P.; Pan, Z.; Lei, J. Parameter identification of Reed-Solomon codes based on probability statistics and Galois field Fourier transform. *IEEE Access* **2019**, *7*, 33619–33630. [CrossRef]
5. Garcia, L.; Vazquez, E.; Sanchez, G.; Avalos, J.-G.; Sanchez, G. An ultra-compact and high-speed FFT-based large-integer multiplier for fully homomorphic encryption using a dual spike-based arithmetic circuit over GF(p). *Neurocomputing* **2022**, *507*, 54–66. [CrossRef]
6. Nardo, L.G.; Nepomuceno, E.G.; Bastos, G.T.; Santos, T.A.; Butusov, D.N.; Arias-Garcia, J. A reliable chaos-based cryptography using Galois field. *Chaos Interdiscip. J. Nonlinear Sci.* **2021**, *31*, 091101. [CrossRef]
7. Shah, D.; Shah, T. Binary Galois field extensions dependent multimedia data security scheme. *Microprocessors and Microsystems.* **2020**, *77*, 103181. [CrossRef]
8. Shah, D.; Shah, T. A novel discrete image encryption algorithm based on finite algebraic structures. *Multimed. Tools Appl.* **2020**, *79*, 28023–28042. [CrossRef]
9. Roy, D.B.; Mukhopadhyay, D. High-speed implementation of ECC scalar multiplication in GF (p) for generic Montgomery curves. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2019**, *27*, 1587–1600.
10. Alaeddine, H.; Charafeddine, K.; Vikhrov, M. A new efficient method of adaptive filter using the Galois field arithmetic. *IOP Conf. Ser. Mater. Sci. Eng.* **2019**, *663*, 012060. [CrossRef]
11. Ricaud, B.; Borgnat, P.; Tremblay, N.; Gonçalves, P.; Vandergheynst, P. Fourier could be a data scientist: From graph Fourier transform to signal processing on graphs. *Comptes Rendus. Physique.* **2019**, *20*, 474–488. [CrossRef]
12. Li, J.; Qin, G.; Li, Y.; Ruan, X. Research on power quality disturbance identification and classification technology in high noise background. *IET Gener. Transm. Distrib.* **2019**, *13*, 1661–1671. [CrossRef]

13. Wahab, M.F.; Gritti, F.; O'Haver, T.C. Discrete Fourier transform techniques for noise reduction and digital enhancement of analytical signals. *TrAC Trends Anal. Chem.* **2021**, *143*, 116354. [CrossRef]
14. Lenzmann, E.; Sok, J. A sharp rearrangement principle in Fourier space and symmetry results for PDEs with arbitrary order. *Int. Math. Res. Not.* **2021**, *2021*, 15040–15081. [CrossRef]
15. Lin, J.; Feng, W.; Reutskiy, S.; Xu, H.; He, Y. A new semi-analytical method for solving a class of time fractional partial differential equations with variable coefficients. *Appl. Math. Lett.* **2021**, *112*, 106712. [CrossRef]
16. Andrews, D.L. Symmetries, conserved properties, tensor representations, and irreducible forms in molecular quantum electrodynamics. *Symmetry* **2018**, *10*, 298. [CrossRef]
17. Balakrishnan, J.S.; Craig, W.; Ono, K.; Tsai, W.L. Variants of Lehmer's speculation for newforms. *arXiv* **2020**, arXiv:2005.10354. [CrossRef]
18. Biasse, J.F.; Fieker, C.; Hofmann, T.; Page, A. Norm relations and computational problems in number fields. *J. Lond. Math. Soc.* **2022**, *105*, 2373–2414. [CrossRef]
19. Ito, Y.; Takeuchi, K. On irregularities of Fourier transforms of regular holonomic D-modules. *Adv. Math.* **2020**, *366*, 107093. [CrossRef]
20. Wang, Z.; Baladron-Zorita, O.; Hellmann, C.; Wyrowski, F. Theory and algorithm of the homeomorphic Fourier transform for optical simulations. *Opt. Express* **2020**, *28*, 10552–10571. [CrossRef]
21. Vorobyov, V.; Zaiser, S.; Abt, N.; Meinel, J.; Dasari, D.; Neumann, P.; Wrachtrup, J. Quantum Fourier transform for nanoscale quantum sensing. *npj Quantum Inf.* **2021**, *7*, 124. [CrossRef]
22. Amico, M.; Saleem, Z.H.; Kumph, M. Experimental study of Shor's factoring algorithm using the IBM Q Experience. *Phys. Rev. A* **2019**, *100*, 012305. [CrossRef]
23. Berardinelli, G. Generalized DFT-s-OFDM waveforms without cyclic prefix. *IEEE Access* **2017**, *6*, 4677–4689. [CrossRef]
24. Yli-Kaakinen, J.; Loulou, A.; Levanen, T.; Pajukoski, K.; Palin, A.; Renfors, M.; Valkama, M. Frequency-domain signal processing for spectrally-enhanced CP-OFDM waveforms in 5G new radio. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 6867–6883. [CrossRef]
25. Yli-Kaakinen, J.; Levanen, T.; Renfors, M.; Valkama, M.; Pajukoski, K. FFT-domain signal processing for spectrally-enhanced CP-OFDM waveforms in 5G new radio. In Proceedings of the 2018 52nd Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 28–31 October 2018; IEEE: New York, NY, USA, 2019; pp. 1049–1056.
26. Hu, Z.; Li, S.; Schwartz, R.L.; Solyanik-Gorgone, M.; Nouri, B.M.; Miscuglio, M.; Gupta, P.; Dalir, H.; Sorger, V.J. Batch processing and data streaming fourier-based convolutional neural network accelerator. In Proceedings of the Emerging Topics in Artificial Intelligence (ETAI) 2022, San Diego, CA, USA, 21–26 August 2022; SPIE: Bellingham, Washington, USA, 2022; Volume 12204, pp. 68–74.
27. Wei, D.; Li, Y.M. Convolution and multichannel sampling for the offset linear canonical transform and their applications. *IEEE Trans. Signal Process.* **2019**, *67*, 6009–6024. [CrossRef]
28. Bäumer, B.; Lumer, G.; Neubrander, F. Convolution kernels and generalized functions. In *Generalized Functions, Operator Theory, and Dynamical Systems*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2021; pp. 68–78.
29. Zeng, Y.; Zhang, M.; Han, F.; Gong, Y.; Zhang, J. Spectrum analysis and convolutional neural network for automatic modulation recognition. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 929–932. [CrossRef]
30. Suleimenov , I.E.; Vitulyova , Y.S.; Matrassulova , D.K. Features of digital signal processing algorithms using Galois fields GF (2n + 1). *Plos one.* **2023**, *18*, 0293294. [CrossRef] [PubMed]
31. Moldakhan, I.; Matrassulova, D.K.; Shaltykova, D.B.; Suleimenov, I.E. Some advantages of non-binary Galois fields for digital signal processing. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *23*, 871–877. [CrossRef]
32. Yang, Y.; Yu, J.; Jojic, N.; Huan, J.; Huang, T.S. Fsnet: Compression of deep convolutional neural networks by filter summary. *arXiv* **2019**, arXiv:1902.03264.
33. Wang, Y.; Xu, C.; Xu, C.; Tao, D. Packing convolutional neural networks in the frequency domain. *IEEE Trans. Pattern Anal. Mach. Intell.* **2018**, *41*, 2495–2510. [CrossRef]
34. Bullock, J.; Cuesta-Lázaro, C.; Quera-Bofarull, A. XNet: A convolutional neural network (CNN) implementation for medical x-ray image segmentation suitable for small datasets. In Proceedings of the Medical Imaging 2019: Biomedical Applications in Molecular, Structural, and Functional Imaging, San Diego, CA, USA, 16–21 February 2019; SPIE: Boca Raton, FL, USA, 2019; Volume 10953, pp. 453–463.
35. Rao, L.J.; Ramkumar, M.; Kothapalli, C.; Savarapu, P.R.; Basha, C.Z. Advanced computerized Classification of X-ray Images using CNN. In Proceedings of the 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 August 2020; IEEE: New York, NY, USA, 2020; pp. 1247–1251.
36. Sahan, J.M.; Abbas, E.I.; Abood, Z.M. A facial recognition using a combination of a novel one dimension deep CNN and LDA. *Mater. Today Proc.* **2023**, *80*, 3594–3599. [CrossRef]
37. Uçar, A.; Demir, Y.; Güzeliş, C. Object recognition and detection with deep learning for autonomous driving applications. *Simulation* **2017**, *93*, 759–769. [CrossRef]
38. Sharan, R.V.; Xiong, H.; Berkovsky, S. Benchmarking audio signal representation techniques for classification with convolutional neural networks. *Sensors* **2021**, *21*, 3434. [CrossRef] [PubMed]
39. Kiskin, I.; Zilli, D.; Li, Y.; Sinka, M.; Willis, K.; Roberts, S. Bioacoustic detection with wavelet-conditioned convolutional neural networks. *Neural Comput. Appl.* **2020**, *32*, 915–927. [CrossRef]

40. Vitulyova, E.S.; Matrassulova, D.K.; Suleimenov, I.E. New application of non-binary Galois fields Fourier transform: Digital analog of convolution theorem. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *23*, 1718–1726. [CrossRef]
41. Thesing, L.; Hansen, A.C. Non-uniform recovery guarantees for binary measurements and infinite-dimensional compressed sensing. *J. Fourier Anal. Appl.* **2021**, *27*, 14. [CrossRef]
42. Guan, N.; Wu, N.; Wang, H. Model identification for digital predistortion of power amplifier with signed regressor algorithm. *IEEE Microw. Wirel. Compon. Lett.* **2018**, *28*, 921–923. [CrossRef]
43. Dokur, Z.; Ölmez, T. Heartbeat classification by using a convolutional neural network trained with Walsh functions. *Neural Comput. Appl.* **2020**, *32*, 12515–12534. [CrossRef]
44. Moshtaghpour, A.; Bioucas-Dias, J.M.; Jacques, L. Close encounters of the binary kind: Signal reconstruction guarantees for compressive Hadamard sampling with Haar wavelet basis. *IEEE Trans. Inf. Theory* **2020**, *66*, 7253–7273. [CrossRef]
45. Yalcin, N.A.; Vatansever, F. A new hybrid method for signal estimation based on Haar transform and Prony analysis. *IEEE Trans. Instrum. Meas.* **2020**, *70*, 6501409. [CrossRef]
46. Pieraccini, M.; Rojhani, N.; Miccinesi, L. Compressive sensing for ground based synthetic aperture radar. *Remote Sens.* **2018**, *10*, 1960. [CrossRef]
47. Pang, C.Y.; Zhou, R.G.; Hu, B.Q.; Hu, W.; El-Rafei, A. Signal and image compression using quantum discrete cosine transform. *Inf. Sci.* **2019**, *473*, 121–141. [CrossRef]
48. Isupov, K. High-Performance Computation in Residue Number System Using Floating-Point Arithmetic. *Computation* **2021**, *9*, 9. [CrossRef]
49. Shirahatti, S.; Shettar, R.; Hongal, R.; Malenahalli, U. Performance Analysis of RNS Arithmetic Operations using Reversible Logic. In Proceedings of the 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 26–27 December 2022; pp. 1–5. [CrossRef]
50. Jyothi, G.N.; Sanapala, K.; Vijayalakshmi, A. ASIC implementation of distributed arithmetic based FIR filter using RNS for high speed DSP systems. *Int. J. Speech Technol.* **2020**, *23*, 259–264. [CrossRef]
51. Cardarilli, G.C.; Di Nunzio, L.; Fazzolari, R.; Nannarelli, A.; Petricca, M.; Re, M. Design space exploration based methodology for residue number system digital filters implementation. *IEEE Trans. Emerg. Top. Comput.* **2020**, *10*, 186–198. [CrossRef]
52. Schoinianakis, D. Residue arithmetic systems in cryptography: A survey on modern security applications. *J. Cryptogr. Eng.* **2020**, *10*, 249–267. [CrossRef]
53. Baagyere, E.Y.; Agbedemnab PA, N.; Qin, Z.; Daabo, M.I.; Qin, Z. A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers. *IEEE Access* **2020**, *8*, 100438–100447. [CrossRef]
54. Ochoa-Jiménez, E.; Rivera-Zamarripa, L.; Cruz-Cortés, N.; Rodríguez-Henríquez, F. Implementation of RSA signatures on GPU and CPU architectures. *IEEE Access* **2020**, *8*, 9928–9941. [CrossRef]
55. Tyncherov, K.T.; Mukhametshin, V.S.; Khuzina, L.B. Method to control and correct telemtry well information in the basis of residue number system. *J. Fundam. Appl. Sci.* **2017**, *9*, 1370–1374. [CrossRef]
56. Suleimenov, I.; Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y. Peculiarities of Applying Partial Convolutions to the Computation of Reduced Numerical Convolutions. *Appl. Sci.* **2024**, *14*, 6388. [CrossRef]
57. Matrassulova, D.K.; Vitulyova, Y.S.; Konshin, S.V.; Suleimenov, I.E. Algebraic fields and rings as a digital signal processing tool. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, *29*, 206–216. [CrossRef]
58. Vitulyova, E.S.; Matrassulova, D.K.; Suleimenov, I.E. Construction of generalized Rademacher functions in terms of ternary logic: Solving the problem of visibility of using Galois fields for digital signal processing. *Int. J. Electron. Telecommun.* **2022**, *68*, 237–244. [CrossRef]

symmetry

MDPI

Article

Prospects for Using Finite Algebraic Rings for Constructing Discrete Coordinate Systems

Ibragim Suleimenov [1] and Akhat Bakirov [1,2,*]

[1] National Engineering Academy of the Republic of Kazakhstan, Almaty 050010, Kazakhstan; esenych@yandex.ru
[2] Institute of Communication and Space Engineering, Gumarbek Daukeev Almaty University of Power Engineering and Communications, Almaty 050013, Kazakhstan
* Correspondence: axatmr@mail.ru

Abstract: The method of non-standard algebraic extensions based on the use of additional formal solutions of the reduced equations is extended to the case corresponding to three-dimensional space. This method differs from the classical one in that it leads to the formation of algebraic rings rather than fields. The proposed approach allows one to construct a discrete coordinate system in which the role of three basis vectors is played by idempotent elements of the ring obtained by a non-standard algebraic extension. This approach allows, among other things, the identification of the symmetry properties of objects defined through discrete Cartesian coordinates, which is important, for example, when using advanced methods of digital image processing. An explicit form of solutions of the equations is established that allow one to construct idempotent elements for Galois fields $GF(p)$ such that $p-1$ is divisible by three. The possibilities of practical use of the proposed approach are considered; in particular, it is shown that the use of discrete Cartesian coordinates mapped onto algebraic rings is of interest from the point of view of improving UAV swarm control algorithms.

Keywords: galois fields; algebraic rings; discrete Cartesian coordinates; idempotent elements; UAVs; information security; geometric problems

Academic Editor: Alexei Kanel-Belov

Received: 15 February 2025
Revised: 1 March 2025
Accepted: 7 March 2025
Published: 9 March 2025

Citation: Suleimenov, I.; Bakirov, A. Prospects for Using Finite Algebraic Rings for Constructing Discrete Coordinate Systems. *Symmetry* **2025**, *17*, 410. https://doi.org/10.3390/sym17030410

1. Introduction

Algebraic extensions of Galois fields based on irreducible polynomials and providing the formation of $GF(p^n)$ fields are increasingly used in practice. They play an important role in cryptography, coding theory, and digital signal processing. For example, in cryptography, operations in $GF(2^8)$ are used in encryption algorithms such as AES, as well as in the construction of elliptic curves, which ensures compact keys and a high degree of security [1–3]. In coding theory, Galois fields are used to develop error-correcting codes such as Reed–Solomon and BCH codes, which ensure reliable data transmission even under significant interference [4].

Modern research is focused on the development of algorithms for working with Galois fields $GF(p^n)$, including calculations in fields with large characteristics, which is especially important for applications in cryptography and computer algebra. For example, the ALDES/SAC2 systems implement algorithms for performing operations in large fields, such as $GF(3^{30})$ and $GF(7^{17})$, which makes it possible to efficiently implement computations [5,6]. Generators have been developed for creating hardware descriptions (VHDL) of multipliers applicable in digital systems. These tools make it possible to simplify the

design of high-performance cryptographic circuits [6,7]. Theoretical studies of structures associated with such extensions are also ongoing [8].

Such extensions are of interest for digital image processing, including volumetric images. Indeed, in the digital processing of planar images, they are divided into pixels, and in similar processing of volumetric images, into voxels [9]. In many problems of practical interest, the image size, and therefore the number of pixels (or voxels), is limited. An obvious example is the images displayed on the screen in existing standards [10,11]. In such cases, it is permissible to use discrete coordinates in terms of Galois fields. Indeed, the location of a single pixel of a particular image can be uniquely described through an element of the Galois field $GF(p^2)$, represented in the form

$$u = u_1 + \theta u_2 \tag{1}$$

where u_1 and u_2 are the elements of the main field $GF(p)$, θ is the root of the irreducible equation (an equation of the second degree that has no solution in the main field), and it is also assumed that $l_{1,2} < p$, where $l_{1,2}$ is the number of pixels in the image under consideration horizontally and vertically.

A similar approach can be used in other cases when a finite section of the plane is analyzed (for example, for the purposes of monitoring agricultural lands [12,13], soil conditions [14], forests [15], and environmental monitoring [16]).

Formula (1) can be considered as a discrete analogue of the representation of a complex value:

$$z = x + iy \tag{2}$$

This representation of the coordinates of a point on a plane is known to be widely used in many problems of hydrodynamics [17,18], electrostatics [19,20], etc. However, there is a significant nuance. A representation similar to (1) also exists for the "three-dimensional" case

$$u = u_1 + \theta u_2 + \theta^2 u_3 \tag{3}$$

where θ is the root of an irreducible equation of the third degree.

At the same time, there is no analogue of formula (2) for the three-dimensional case. There are only "four-dimensional" complex numbers—Hamilton quaternions [21]. The advantages of representation (3) are obvious: starting from it, one can try to develop a discrete analogue of the theory of functions of a complex variable for the three-dimensional case. This formulation of the question is justified by the following considerations. As noted in [22], the model of a digital signal can, among other things, comprise functions that take values in Galois fields. Indeed, if a digital (discrete) signal changes in a finite range of amplitudes, then the number of its levels is obviously finite. Consequently, any planar digital image can be described through a function whose domain of definition is the field $GF(p^2)$ and which takes values in the same field. The same is true for three-dimensional images: it is sufficient to move to the fields $GF(p^3)$. Note also that it is possible to represent any functions of this type in the form of explicit algebraic expressions [23].

For many problems that are important from a practical point of view, the algebraic representation of coordinate transformations is also of interest. Such problems arise, for example, in the development of control algorithms for UAV swarms [24–26], which are increasingly used for both civilian [27–29] and military [30–32] purposes. To control a swarm of UAVs, it is often necessary to recalculate the coordinates of each drone relative to the reference point (e.g., the leading drone) between the above-mentioned coordinate systems [33,34]. In this case, it is often necessary to ensure the transition from the global coordinate system (e.g., GPS in the latitude and longitude format) to a local one, for example, NED (North–East–Down) and ENU (East–North–Up), and it is necessary to distinguish

between the local coordinate system of the swarm leader, the local coordinate system of the swarm center, or an individual drone (Body Frame) [35–37]. It is significant that in this case, such three-dimensional coordinate systems as the Global Rectangular system (ECEF—Earth-Centered, Earth-Fixed) and the Global Geographic system (LLA—Latitude, Longitude, Altitude) [38,39] are used.

To describe coordinate transformations, non-trivial algebraic structures such as Clifford algebra [33] and Hamiltonian quaternions [40] are used, which provide a compact and stable representation of rotation. Quaternions can be used both to describe the UAV orientation [40] and directly in control, for example, to find the orientation error [41], correct the angular velocity [42], or control the rotation, including for UAV stabilization [43]. The advantage of using quaternions is that they allow one to remove the difficulties associated with the "Gimbal Lock" problem (Euler angle singularity) [44]. Note that in practice, UAV coordinates are always specified with finite accuracy; therefore, it is permissible to use a discrete coordinate grid (discrete Cartesian coordinates). This significantly expands the list of algebraic structures that can be used for the above purposes. In particular, finite algebraic rings can be used, the advantages of which are as follows.

The classical form of representation of the coordinates of a point in a multidimensional space is the representation through orthogonal basis vectors $\boldsymbol{e}_i$:

$$\boldsymbol{u} = u_1\boldsymbol{e}_1 + u_2\boldsymbol{e}_2 + u_3\boldsymbol{e}_3 \tag{4}$$

where $\boldsymbol{e}_i\boldsymbol{e}_j = 0; i \neq j$.

In the theory of algebraic rings, it is proved that there exist rings that can be represented as a direct sum of algebraic ideals [45]. In this case, each element of the ring can be represented as

$$r = r_1e_1 + r_2e_2 + \cdots + r_ne_n \tag{5}$$

where e_i are idempotent elements with the following properties:

$$e_ie_j = 0; i \neq j, \tag{6}$$

$$e_1 + e_2 + \cdots + e_n = 1 \tag{7}$$

$$e_i^2 = e_i. \tag{8}$$

Comparison of formulas (4) and (5), which include elements that cancel each other, shows that a deep analogy can be established between algebraic rings and discrete vector spaces, and a deeper analogy than, say, between a two-dimensional vector space and complex numbers. Namely, unlike structures such as complex numbers or Galois fields, zero divisors appear in algebraic rings, which allows us to specify an analog of basis vectors that cancel each other when calculating the scalar product, as well as analogs of vector subspaces, which are ideals of the form r_ie_i. There is, however, an important nuance: in the case where, for example, residue number systems, RNSs [46–48], are used, ideals of the form r_ie_i contain a different number of elements. Accordingly, the above analogy is not complete.

Consequently, we can pose the question of finding an algebraic discrete analogue of formula (4), in which the role of basis vectors is played by idempotent elements. It is also desirable to ensure that all algebraic ideals of the form r_ie_i have the same number of elements. Such an approach, we emphasize once again, is of interest for numerous problems in which the coordinate grid can be reduced to a digital (discrete) form. In addition to the already mentioned problems, such an approach is of interest for constructing convolutional neural networks, which are currently finding an increasingly wide range of

applications [49–51]. As shown in [52], it is the use of finite algebraic structures that allows us to significantly modernize the operation of calculating digital convolutions.

In digital image processing using neural networks, problems are often encountered that require taking symmetry considerations into account. This is especially true for neural networks that allow the image under study to be represented as a set of fairly simple geometric elements. Such neural networks are widely used in practice and have proven themselves to be effective [53–57]. In this case, simple geometric elements can usually be brought to each other by means of coordinate transformations (including the operation of stretching along the coordinate axes). Coordinate transformations, as is known, have been and remain one of the main tools for studying the symmetry properties of not only flat but also spatial figures (symmetry corresponds to the invariance of a figure under a certain coordinate transformation). Since images (both flat and volumetric) are currently usually specified in discrete form, the development of a description of coordinate transformations in terms of finite algebraic structures is of interest from this point of view as well.

In this paper, we propose a specific algorithm for constructing representations of the form (5), intended for displaying digital (discrete) coordinates, based on the non-standard method of algebraic extensions proposed in [58]. The difference is that in the cited work, this method was applied to a two-dimensional space. In this paper, it is extended to the three-dimensional case. This requires the development of a non-trivial mathematical apparatus that allows solving systems of nonlinear equations whose coefficients belong to the main Galois field.

2. Methods

In the work [58], it was shown that along with the classical method of algebraic extensions, allowing the construction of fields $GF(p^n)$, it is also possible to propose a method of algebraic extensions, allowing the construction of algebraic rings. The difference is that the classical method of algebraic extensions is based on the use of irreducible equations of degree n, and the method proposed in [58] is based on the use of additional formal solutions of reducible equations. In the cited work [58], a non-standard method of forming algebraic extensions was considered as a special example of the field $GF(3)$, which corresponds to ternary logic [59], which is of interest for several applied problems [60–62]. In addition, in the cited work, a ring was considered, corresponding to a two-dimensional problem, i.e., containing two idempotent elements.

In this paper, the approach [58] is extended to the "three-dimensional" one, and it is proved that the fields $GF(p)$ corresponding to sufficiently large values of p, i.e., those of interest for solving "digital" problems encountered in practice, can be used as the main field.

3. Results

3.1. General Approach

Relation (6) can be used to find idempotent elements directly. We obtain the corresponding equations following the approach proposed in [58].

In accordance with the methodology [58], we assume that it is permissible to pass from the basic Galois field to its non-standard algebraic extension using some formal additional solution i of the reducible equation of the form

$$i^3 = k_0 + k_1 i + k_2 i^2 \tag{9}$$

We emphasize that an equation of the form (9) is used, which has a solution in the field under consideration. Our task is to find conditions under which it can have additional

formal solutions. Equation (9) is of the third order, which corresponds to finding an extension that can be put in correspondence with a discrete three-dimensional space.

In accordance with [63], the element i will be treated as a logical imaginary unit of the second kind. It is assumed that, using the element i, it is possible to construct three elements g_n, $n = 1, 2, 3$, satisfying condition (6), in the following form (for now, the elements g_n are considered, not e_n, since they can differ from each other by a factor):

$$g_n = 1 + a_n i + b_n i^2 \tag{10}$$

The element i is, strictly speaking, an abstraction, but the same is true for the algebraic elements by which extensions of Galois fields are constructed using the traditional method. In particular, this means that the meaning of the element i is given by the rules for operating with such an element. Let us establish these rules, while simultaneously clarifying the conditions under which relations (6) are satisfied. Let us emphasize that to establish the rules for operating with the element i, it is sufficient to find the coefficients k_m in formula (9), under which operations with i as a logical imaginary unit of the second kind will make sense.

Multiplying the elements g_1 and g_2 by each other, we obtain

$$g_1 g_2 = \left(1 + a_1 i + b_1 i^2\right)\left(1 + a_2 i + b_2 i^2\right) = c_{012} + c_{112} i + c_{212} i^2 \tag{11}$$

Or

$$g_1 g_2 = 1 + (a_1 + a_2) i + (a_1 a_2 + b_1 + b_2) i^2 + (a_2 b_1 + a_1 b_2) i^3 + b_1 b_2 i^4 \tag{12}$$

Considering formula (9), as well as condition (6), we have

$$c_{012} = 1 + (a_2 b_1 + a_1 b_2) k_0 + b_1 b_2 k_2 k_0 = 0 \tag{13}$$

$$c_{112} = a_1 + a_2 + (a_2 b_1 + a_1 b_2) k_1 + b_1 b_2 (k_0 + k_2 k_1) = 0 \tag{14}$$

$$c_{212} = a_1 a_2 + b_1 + b_2 + (a_2 b_1 + a_1 b_2) k_2 + b_1 b_2 \left(k_1 + k_2^2\right) = 0 \tag{15}$$

Three more such equations are obtained by considering two other pairs by replacing indices. Consequently, the system of equations that ensures the fulfillment of requirements (6) when representing elements e_n in the form (10) contains nine equations for nine unknowns.

Let us show that there is a very specific type of Galois field for which this system of equations has a non-trivial solution. These are the fields $GF(p)$, such that $p - 1$ is divisible by three.

In this case, the solutions of the system under consideration correspond to the following values of the sought parameters:

$$k_0 = 1;\ k_1 = 0;\ k_2 = 0 \tag{16}$$

$$a_n = b_n^2 \tag{17}$$

$$b_n = q_0^{n-1} \tag{18}$$

where m is an integer and q_0 is a primitive root of the equation

$$q^3 - 1 = 0 \tag{19}$$

Recalling that all non-zero elements of the field $GF(p)$ satisfy the equation

$$x^{p-1} - 1 = 0 \tag{20}$$

The use of the minus sign in formula (20) is legitimate, among other things, because, for the elements of the field $GF(p)$ it is permissible to use a representation containing negative numbers [59], for example

$$GF(7) = \{-3, -2, -1, 0, 1, 2, 3\} \tag{21}$$

From Equation (20) we can go to Equation (19) if $p - 1$ is divisible by three. Indeed

$$\left(x^{\frac{p-1}{3}}\right)^3 - 1 = 0 \tag{22}$$

Recall that the integer powers of the primitive root of the equation exhaust all possible solutions of the equation of the form (19) or (20). In particular, this means that there are three different solutions of Equation (19) q_1, q_2, q_3, which are elements of the field under consideration, and the sum of these three elements when added modulo p is identically equal to zero:

$$q_1 + q_2 + q_3 = 0 \tag{23}$$

Indeed, the solutions of Equation (19) form a group under multiplication, and there exists an element q_0 such that

$$q_n = q_0^n;\ n = 0, 1, 2 \tag{24}$$

Hence

$$q_1 + q_2 + q_3 = 1 + q_0 + q_0^2 \tag{25}$$

The identity holds

$$\left(1 + q_0 + q_0^2\right)(1 - q_0) = 1 - q_0^3 = 0 \tag{26}$$

From which follows (23), since $1 - q_0 \neq 0$. Using formula (23), it can be shown that the set of parameters specified by formulas (16)–(18) actually corresponds to the solution of the system of nine equations generated by conditions (6). Indeed, in the case when equalities (16) are satisfied, the first three equations from the considered system of equations take the form

$$c_{012} = 1 + (a_2 b_1 + a_1 b_2) = 0 \tag{27}$$

$$c_{112} = a_1 + a_2 + b_1 b_2 = 0 \tag{28}$$

$$c_{212} = a_1 a_2 + b_1 + b_2 = 0 \tag{29}$$

The remaining six equations are obtained by rearranging the indices. Substituting expressions (17) into formulas (27)–(29), we obtain

$$c_{012} = 1 + \left(b_2^2 b_1 + b_1^2 b_2\right) = 0 \tag{30}$$

$$c_{112} = b_1^2 + b_2^2 + b_1 b_2 = 0 \tag{31}$$

$$c_{212} = b_1^2 b_2^2 + b_1 + b_2 = 0 \tag{32}$$

It is easy to verify that, in this case, the expressions (18) really ensure the fulfillment of the system of equations under consideration. Indeed, in this case

$$c_{012} = c_{112} = c_{212} = 1 + q_0^2 + q_0^1 = 0 \tag{33}$$

Thus, expressions (16)–(18) define elements that mutually cancel each other. Expressions for these elements can be specified directly:

$$g_1 = 1 + i + i^2 \tag{34}$$

$$g_2 = 1 + q_0^2 i + q_0 i^2 \tag{35}$$

$$g_3 = 1 + q_0 i + q_0^2 i^2 \tag{36}$$

When deriving formula (36), it was considered that for the values of k_n specified by formula (18), the following holds:

$$q_0^3 = 1 \tag{37}$$

Summing up expressions (34)–(36), by virtue of (23) we obtain

$$g_1 + g_2 + g_3 = 3 \tag{38}$$

It is important that this result does not depend on the choice of the field $GF(p)$; it is only necessary that $p - 1$ be divisible by 3. Consequently, to ensure that relation (7) is satisfied, it is sufficient to multiply the obtained elements g_i by the normalization factor 3^{-1}, which is also the same for all fields of the type under consideration.

$$e_i = 3^{-1} g_i \tag{39}$$

It is worth emphasizing that the resulting elements automatically become idempotent. Indeed, multiplying (7) by e_i, we obtain

$$e_i(e_1 + e_2 + e_3) = e_i \tag{40}$$

From which we obtain the following:

$$e_i^2 = e_i \tag{41}$$

Thus, for a three-dimensional space, it is possible to propose an analog of a basis in which the role of basis vectors is played by idempotent elements of a finite algebraic ring, and the role of coordinates is played by elements of the Galois field $GF(p)$, where $p - 1$ is divisible by three. We emphasize that the proposed approach differs from existing methods of constructing algebraic rings in that the analogy between an algebraic ring of the type under consideration and a discrete vector space becomes complete. It follows from formula (5) that an arbitrary element of the ring z can be represented in the form

$$z = z_1 e_1 + z_2 e_2 + \cdots + z_n e_n \tag{42}$$

where z_i are elements belonging to the main field $GF(p)$, i.e., the number of elements corresponding to each of the coordinate analogues is the same, which is not the case, for example, for RNS [46–48].

For solving applied problems in which finite regions of space are considered, the latter limitation is not essential, since it is always possible to choose a field whose number of elements slightly exceeds the maximum discrete coordinate number.

3.2. Specific Examples

Let us consider, for clarity, specific examples of solutions to equations that allow us to construct idempotent elements capable of playing the role of basis vectors in three-dimensional space.

For illustration, Tables 1 and 2 present variants of solutions that correspond to formulas (16)–(18) for the cases of fields $GF(7)$ and $GF(13)$, respectively. The tables show that, as expected, solutions of this type correspond only to permutation of indices. The first six columns of Table 1 contain quantities whose third power in the field $GF(7)$ gives one, and similarly for Table 2.

Table 1. Solution options for the system of equations that meet condition (6) for the case of the field $GF(7)$.

a1	a2	a3	b1	b2	b3	k0	k1	k2
1	2	−3	1	−3	2	1	0	0
1	−3	2	1	2	−3	1	0	0
2	1	−3	−3	1	2	1	0	0
2	−3	1	−3	2	1	1	0	0
−3	1	2	2	1	−3	1	0	0
−3	2	1	2	−3	1	1	0	0

Table 2. Solution options for the system of equations that meet condition (6) for the case of a field $GF(13)$.

a1	a2	a3	b1	b2	b3	k0	k1	k2
1	3	−4	1	−4	3	1	0	0
1	−4	3	1	3	−4	1	0	0
3	1	−4	−4	1	3	1	0	0
3	−4	1	−4	3	1	1	0	0
−4	1	3	3	1	−4	1	0	0
−4	3	1	3	−4	1	1	0	0

Note that another type of solution to the system of equations generated by conditions (6) corresponds to the equation

$$y^3 + 1 = 0 \tag{43}$$

In this case, the solutions of the system of equations under consideration are given by the following formulas:

$$k_0 = -1;\ k_1 = 0;\ k_2 = 0 \tag{44}$$

$$a_n = -b_n^2 \tag{45}$$

$$b_n = q_0^{n-1} \tag{46}$$

Let us prove this statement. When substituting (44) into the initial system of equations generated by conditions (6), the following relations are formed:

$$c_{012} = 1 - (a_2 b_1 + a_1 b_2) \tag{47}$$

$$c_{112} = a_1 + a_2 - b_1 b_2 \tag{48}$$

$$c_{212} = a_1 a_2 + b_1 + b_2 \tag{49}$$

Six more equations from this system are obtained by permutations of indices. Substituting expressions (45) into (47)–(49), we obtain that the problem is reduced to the previous one:

$$c_{012} = 1 + \left(b_2^2 b_1 + b_1^2 b_2\right) = 0 \tag{50}$$

$$c_{112} = -\left(b_1^2 + b_2^2 + b_1 b_2\right) = 0 \tag{51}$$

$$c_{212} = b_1^2 b_2^2 + b_1 + b_2 = 0 \tag{52}$$

The only difference is the common minus sign in formula (51), which does not affect the final result. For clarity, possible solutions corresponding to formulas (44)–(46) are presented in Tables 3 and 4 for specific Galois fields $GF(7)$ and $GF(13)$, respectively. In this case, the solution options also differ from each other by the permutation of the coefficients.

Table 3. Solution options for the system of equations that meet condition (6) and Equation (43) for the case of a field $GF(7)$.

a1	a2	a3	b1	b2	b3	k0	k1	k2
3	−2	−1	2	−3	1	−1	0	0
3	−1	−2	2	1	−3	−1	0	0
−2	3	−1	−3	2	1	−1	0	0
−2	−1	3	−3	1	2	−1	0	0
−1	3	−2	1	2	−3	−1	0	0
−1	−2	3	1	−3	2	−1	0	0

Table 4. Solution options for the system of equations that meet condition (6) and Equation (43) for the case of a field $GF(13)$.

a1	a2	a3	b1	b2	b3	k0	k1	k2
4	−3	−1	3	−4	1	−1	0	0
4	−1	−3	3	1	−4	−1	0	0
−3	4	−1	−4	3	1	−1	0	0
−3	−1	4	−4	1	3	−1	0	0
−1	4	−3	1	3	−4	−1	0	0
−1	−3	4	1	−4	3	−1	0	0

A natural question arises as to how correct it is to use an additional algebraic element, interpreted as a logical imaginary unit of the second kind. To answer this question, it is advisable to use a matrix representation, simultaneously illustrating the nature of the results obtained using specific examples.

3.3. Justification of the Correctness of the Non-Standard Method of Algebraic Extensions

Let us emphasize once again that the element i that we use, interpreted as a logical imaginary unit of the second kind, is an abstraction. It is defined only by the rules of operation. For greater clarity, however, it makes sense to consider the question of what other form this element can be represented in, as well as the elements that are constructed with its help. In this section, it is proved that the above elements can be put in accordance with the matrices defined over the main Galois field, starting from which we construct algebraic rings. This will not only make the elements under consideration visual but also demonstrate the correctness of their use.

Let us start with specific examples of constructing idempotent elements e_i obtained by extending specific Galois fields. Specifically, in the field $GF(7)$, idempotent elements of the obtained type are displayed as

$$e_1 = 3^{-1}\left(1 + 3i + 2i^2\right) = -2 + i + 3i^2 \tag{53}$$

$$e_2 = 3^{-1}\left(1 - i + i^2\right) = -2 + 2i - 2i^2 \tag{54}$$

$$e_3 = 3^{-1}\left(1 - 2i - 3i^2\right) = -2 - 3i - i^2 \tag{55}$$

since in the field $GF(7)$ we have $3^{-1} = -2$.

This case corresponds to solutions corresponding to the equation

$$i^3 = -1 \tag{56}$$

A direct check can verify that these elements are indeed idempotent. For example, in the field $GF(7)$:

$$e_3^2 = \left(-2 - 3i - i^2\right)\left(-2 - 3i - i^2\right) = -3 - 2i - i^2 - i^3 + i^4 = -2 - 3i - i^2 = e_3 \tag{57}$$

This example is, of course, of a particular nature, but it allows us to demonstrate the correctness of using the element i by a method that allows an elementary generalization to all Galois fields of the type under consideration. Traditional algebraic extensions of Galois fields allow representations through matrices defined over the main Galois field. Similarly, a matrix representation can be used to represent the element i and those generated by it. Consider the product of the element i by an arbitrary element obtained with its help:

$$ia = i\left(a_1 + a_2 i + a_3 i^2\right) = a_3 + a_1 i - a_2 i^2 \tag{58}$$

$$i^2 a = i^2\left(a_1 + a_2 i + a_3 i^2\right) = -a_2 - a_3 i + a_1 i^2 \tag{59}$$

Transformation (58) can be considered as a transformation of a vector whose components are the quantities a_i. Such a transformation can be displayed by a matrix

$$i \leftrightarrow \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \tag{60}$$

Likewise,

$$i^2 \leftrightarrow \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \tag{61}$$

Moreover, the last representation could also be obtained immediately based on formula (59). Substituting the obtained matrix representations into formulas (10) and (39) and also taking into account the specific values of the coefficients for the case under consideration, we obtain a matrix representation of idempotent elements for the case of the field $GF(7)$.

$$e_1 \leftrightarrow -2\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + 3\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -2 & -3 & -1 \\ 1 & -2 & -3 \\ 3 & 1 & -2 \end{pmatrix}$$

$$e_2 \leftrightarrow -2\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}+2\begin{pmatrix}0&0&-1\\1&0&0\\0&1&0\end{pmatrix}-2\begin{pmatrix}0&-1&0\\0&0&-1\\1&0&0\end{pmatrix}=\begin{pmatrix}-2&2&-2\\2&-2&2\\-2&2&-2\end{pmatrix} \quad (62)$$

$$e_3 \leftrightarrow -2\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}-3\begin{pmatrix}0&0&-1\\1&0&0\\0&1&0\end{pmatrix}-\begin{pmatrix}0&-1&0\\0&0&-1\\1&0&0\end{pmatrix}=\begin{pmatrix}-2&1&3\\-3&-2&1\\-1&-3&-2\end{pmatrix}$$

The fact that these matrices, defined over the field $GF(7)$, are indeed idempotent and mutually annihilating can be verified directly by verification. Note that the matrix representation of the obtained algebraic elements is far from necessarily of practical interest. However, the very fact that additional formal solutions of the equation being reduced can be assigned specific matrices proves the correctness of their use.

4. Discussions

The proposed approach creates a basis for solving geometric problems in three-dimensional space in digital form. This approach is applicable to solving any geometric problems, including those related to coordinate transformations, in which the coordinates are specified with a certain accuracy, and the area to which the problem being solved relates is limited in space.

This is directly proved by formula (42), which is a complete analogue of formula (4), which expresses a vector in a multidimensional space through basis vectors and coordinate values. In formula (42), the role of basis vectors is played by idempotent elements of the ring constructed in this work, and the variables corresponding to coordinates in the chosen basis take values in the main Galois field.

Problems of a geometric nature that can be solved using the proposed approach are relevant, among other things, for improving methods of physical protection of information when transmitting commands to swarms of unmanned vehicles. It should be noted that the development of physical methods for protecting information is becoming increasingly important [64–66], including due to the improvement of electronic warfare methods. The method proposed in [67] is based on identifying the location of a radio signal source interpreted as "friend". Such a problem can be solved, including by determining the propagation time of a radio signal from a specific source to the elements of a UAV group. Geometrically, as in the case considered in [68], it comes down to finding the intersection point of hyperbolas (or hyperboloids, if the problem is solved in three-dimensional space). Problems of this kind can be solved in various ways [69–71]; however, to ensure information security by identifying the location of the signal source, high accuracy is not required, which allows the use of a sufficiently coarse discrete grid [72]. This allows us to raise the question of using finite algebraic structures to construct coordinate systems.

We emphasize that attention to this example is determined not only by demonstrating the relevance of the approach being developed. This example, among other things, demonstrates the importance of further development of the proposed approach, and specifically from the point of view of logical-algebraic problems.

Further development of the proposed approach, of course, requires solving several other problems. One of them is related to the question of how one should calculate the discrete distance between two points, provided that their coordinates are specified in a form corresponding to formula (5), i.e., it is necessary to answer the question of what should be understood by distance when the position of a point in a discrete three-dimensional space is specified through the elements of the ring constructed in this work.

We will show that this and similar problems can be solved by using the analogy between functions taking values in Galois fields $GF(p)$ and functions of multivalued logic.

We emphasize that the components of the analog of a three-dimensional vector in the case under consideration take values in the main Galois field. Consequently, for a given choice of idempotent elements (analogs of basis vectors), the position of a point in a discrete space is specified through a set of two or three variables taking values in the main field. Consequently, determining the distance in the case under consideration is reduced to finding a function taking values in the Galois field, the arguments of which also take values in the main Galois field.

Such a function can be constructed based on the results of [23], in which it was shown that it is possible to specify a specific algebraic expression for an arbitrary function of multivalued logic, provided that the number of values of the variables of such logic corresponds to the number of elements of the Galois field. For the case of two variables, such a function is written in the following form:

$$F(x,y) = \sum_{m,n} F(x_n, y_m) g(x - x_n) g(y - y_m), \tag{63}$$

where $g(x - x_n)$ is the algebraic δ-function:

$$g(x - x_n) = 1 - (x - x_n)^{p-1} = \begin{cases} 1, x = x_n \\ 0, x \neq x_n \end{cases}, \tag{64}$$

This allows us to specify a function describing the distance between points whose coordinates correspond to elements of the Galois field in the form of an analogue of the truth table and then use the relation (63). For clarity, Figure 1 shows a fragment of an analogue of the truth table for the case of the field $GF(31)$. The values given in this table correspond to discrete distances (true geometric distances rounded to integer values).

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	1	2	3	4	5	6
2	2	2	3	4	5	5	6
3	3	3	4	4	5	6	
4	4	4	5	5	6		
5	5	5	5	6			
6	6	6	6				

Figure 1. Fragment of an analogue of the truth table for the case of a field $GF(31)$. Blue—discrete values along the abscissa and ordinate axes, Red—Constant discrete distance from the origin.

The values presented in this table can also be interpreted as elements of the Galois field corresponding to discrete distances. For this, it is sufficient to choose p so that $p > \sqrt{2}N$ for the two-dimensional case and $p > \sqrt{3}N$ for the three-dimensional case (N is the maximum number of the discrete coordinate, if it is counted from zero). This allows us to use

formula (63) or its equivalent, which solves the problem. Similarly, using relation (63), we can obtain formulas for other geometric characteristics if necessary. Moreover, the proposed approach allows for further development due to the representation of linear operators through elements of algebraic structures. A similar problem has already been solved in [72], where it was shown that there is a large class of fields $GF(p)$ that simultaneously admit algebraic extensions both by the classical method and by the method proposed by us (i.e., using both irreducible and reducible algebraic equations). This approach allows us to represent arbitrary operators corresponding to 2×2 matrices (including operators corresponding to Galois transformations of plane coordinates) through algebraic elements formed by simultaneously using extensions of both types. The results presented in this paper allow us to implement a similar approach at the next stage of research for operators corresponding to 3×3 matrices, including operators describing transformations of three-dimensional coordinates.

Coordinate transformations are of interest for several practical applications, including for the method mentioned above, physical protection of information when controlling a group of UAVs in a line-of-sight zone, based on the definition of the operator's coordinates. This ultimately comes down to solving a geometric problem like that used in the "hyperbola method" [68]. The difference lies in the nature of the problem solution. In one case, the coordinates of the signal source are determined in terms of continuously changing coordinates, and in the other case, discrete ones. This is acceptable, since to identify the source of a signal interpreted as "one's own", its coordinates can be determined with a low accuracy. We emphasize that, in this case, the "accuracy" with which the operator's coordinates should be determined is determined by the nature of the use of the UAV swarm. A clear example proving this statement is related to the nature of the use of UAVs during the current military conflicts. Namely, drones controlled via fiber optics are increasingly being used. On the one hand, this automatically implies relatively short distances over which the control signal is transmitted. On the other hand, this implies that there is a fairly large distance between the drone operator and the location of any electronic warfare equipment used by the opposing side. As a rule, they are separated by the line of combat contact. Consequently, the accuracy of determining the operator's coordinates can indeed be made quite low; it is enough to determine the area of his location, for example.

We also note that the transition to controlling groups of unmanned vehicles using algorithms formulated in terms of finite algebraic structures is also of interest from the point of view of increasing the efficiency of computing systems, including onboard [73]. There is no doubt that computing systems built on calculations reduced to operations on integers have significant advantages over analogs forced to use fractional values in floating-point arithmetic, which requires additional processing for normalization and control of the accuracy of calculations [74–76]. Systems of this kind are currently being actively developed, for example, systems using residual classes (residue number system) [77,78], integer arithmetic in digital signal processors (DSP) [79,80], specialized processors for cryptography (e.g., hardware accelerators RSA and ECC) [81,82], as well as deep learning accelerators working with weight quantization (e.g., TPU and neuromorphic processors) [83,84]. It should be emphasized that computing systems directly based on operations in Galois fields (for example, systems that perform calculations modulo an integer [85,86]) are also being actively developed at the present time [87,88]. Not only do they obviously outperform algorithms that require fractional calculations in terms of performance, but they can also be used in the future to develop AI coupled with swarms of UAVs. Namely, as noted in [89], each command executed by a UAV can be assigned to a specific value of a variable of multi-valued logic, which, in turn, can be assigned to some non-zero element of a Galois field. This, among other things, makes it possible to reduce multi-valued logic opera-

tions to algebraic ones, and then use the potential of computing systems created based on neuromorphic materials [90,91] to implement specific forms of AI, the relevance of which was also substantiated in [92]. One of these specific forms of AI can be implemented for groups of unmanned vehicles. It is obvious that AI built on the use of Galois fields will be complementary to the representation of coordinate systems through such fields.

5. Conclusions

Thus, it is possible to extend the method of non-standard algebraic extensions to the case of three dimensions. This method differs from the classical one in that irreducible equations are not used, i.e., equations that have no solutions in the main Galois field. On the contrary, algebraic equations that have solutions in the field under consideration are used. The proposed method is needed since additional formal solutions of such equations are introduced into consideration, which do not coincide with the solutions that are elements of the main field. This method also differs from the classical one in that the extension does not result in a field, but an algebraic ring containing idempotent elements. It is also possible to write explicit algebraic equations that allow obtaining such elements in explicit form.

The proposed approach creates a basis for solving three-dimensional geometric problems in discrete (digital) form, since the idempotent elements of the ring obtained by the proposed method can be put in correspondence with unit vectors of the Cartesian coordinate system. The solution of geometric problems in digital form, in turn, is of interest, for example, for the development of methods for protecting information transmitted from the operator to the UAV group, based on determining the coordinates of the signal source by the onboard computing units of the UAV group. In this case, there is no need to determine the operator's coordinates with high accuracy, which justifies the transition to solving geometric problems in digital form.

Author Contributions: Conceptualization, A.B. and I.S.; methodology, A.B. and I.S.; formal analysis, A.B. and I.S.; writing—original draft preparation, A.B. and I.S.; writing—review and editing, A.B. and I.S.; visualization, A.B. and I.S.; supervision, I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been/was/is funded by the Science Committee of the Ministry of Higher Education and Science of the Republic of Kazakhstan (Grant No. AP23490107).

Data Availability Statement: The original contributions presented in the study are included in the article; further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kareem, S.M.; Rahma, A.M.S. New method for improving add round key in the advanced encryption standard algorithm. *Inf. Secur. J. A Glob. Perspect.* **2021**, *30*, 371–383. [CrossRef]
2. Roy, D.B.; Mukhopadhyay, D. High-speed implementation of ECC scalar multiplication in GF (p) for generic Montgomery curves. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2019**, *27*, 1587–1600.
3. Haider, M.I.; Ali, A.; Shah, D.; Shah, T. Block cipher's nonlinear component design by elliptic curves: An image encryption application. *Multimed. Tools Appl.* **2021**, *80*, 4693–4718. [CrossRef]
4. Bierbrauer, J. *Introduction to Coding Theory*; Chapman and Hall: London, UK; CRC: Boca Raton, FL, USA, 2016.
5. Calmet, J. Algebraic algorithms in GF (q). *Discret. Math.* **1985**, *56*, 101–109. [CrossRef]
6. Zholubak, I.; Hlukhov, V. Verification of Synthesized by the IP-core Generator Multipliers of Extended Galois Fields GF (p n) Elements. In Proceedings of the 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 13–15 October 2023; pp. 1–4.
7. Dey, S.; Chakrabarti, A.; Ghosh, R. Division Algorithm to search for monic irreducible polynomials over extended Galois Field GF (pˆ q). *Cryptol. ePrint Arch.* **2020**.

8. Koch, A.; Kohl, T.; Truman, P.J.; Underwood, R. Isomorphism problems for Hopf–Galois structures on separable field extensions. *J. Pure Appl. Algebra* **2019**, *223*, 2230–2245. [CrossRef]
9. Li, H.; Yang, X.; Zhai, H.; Liu, Y.; Bao, H.; Zhang, G. Vox-surf: Voxel-based implicit surface representation. *IEEE Trans. Vis. Comput. Graph.* **2022**, *30*, 1743–1755. [CrossRef]
10. Kou, W. *Digital Image Compression: Algorithms and Standards*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013; Volume 333.
11. Quigley, E.A.; Tokay, B.A.; Jewell, S.T.; Marchetti, M.A.; Halpern, A.C. Technology and technique standards for camera-acquired digital dermatologic images: A systematic review. *JAMA Dermatol.* **2015**, *151*, 883–890. [CrossRef]
12. Mukhamediev, R.I.; Yakunin, K.; Aubakirov, M.; Assanov, I.; Kuchin, Y.; Symagulov, A.; Levashenko, V.; Zaitseva, E.; Sokolov, D.; Amirgaliyev, Y. Coverage Path Planning Optimization of Heterogeneous UAVs Group for Precision Agriculture. *IEEE Access* **2023**, *11*, 5789–5803. [CrossRef]
13. Nakalembe, C.; Becker-Reshef, I.; Bonifacio, R.; Hu, G.; Humber, M.L.; Justice, C.J.; Keniston, J.; Mwangi, K.; Rembold, F.; Shukla, S.; et al. A review of satellite-based global agricultural monitoring systems available for Africa. *Glob. Food Secur.* **2021**, *29*, 100543. [CrossRef]
14. Mukhamediev, R.I.; Terekhov, A.; Amirgaliyev, Y.; Popova, Y.; Malakhov, D.; Kuchin, Y.; Sagatdinova, G.; Symagulov, A.; Muhamedijeva, E.; Gricenko, P. Using Pseudo-Color Maps and Machine Learning Methods to Estimate Long-Term Salinity of Soils. *Agronomy* **2024**, *14*, 2103. [CrossRef]
15. Nesha, M.K.; Herold, M.; De Sy, V.; Duchelle, A.E.; Martius, C.; Branthomme, A.; Garzuglia, M.; Jonsson, O.; Pekkarinen, A. An assessment of data sources, data quality and changes in national forest monitoring capacities in the Global Forest Resources Assessment 2005–2020. *Environ. Res. Lett.* **2021**, *16*, 054029. [CrossRef]
16. Tosato, P.; Facinelli, D.; Prada, M.; Gemma, L.; Rossi, M.; Brunelli, D. An Autonomous Swarm of Drones for Industrial Gas Sensing Applications. In Proceedings of the 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–6. [CrossRef]
17. Birkhoff, G. *Hydrodynamics*; Princeton University Press: Princeton, NJ, USA, 2015; Volume 2234.
18. Bonilla-Licea, M.; Schuch, D. Quantum hydrodynamics with complex quantities. *Phys. Lett. A* **2021**, *392*, 127171. [CrossRef]
19. Jonassen, N. *Electrostatics*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013.
20. Koehl, P. Electrostatics calculations: Latest methodological advances. *Curr. Opin. Struct. Biol.* **2006**, *16*, 142–151. [CrossRef]
21. Lam, T.Y. Hamilton's quaternions. In *Handbook of Algebra*; Elsevier: Amsterdam, The Netherlands, 2003; Volume 3, pp. 429–454.
22. Vitulyova, E.S.; Matrassulova, D.K.; Suleimenov, I.E. New application of non-binary Galois fields Fourier transform: Digital analog of convolution theorem. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *23*, 1718–1726. [CrossRef]
23. Suleimenov, I.E.; Vitulyova, Y.S.; Kabdushev, S.B.; Bakirov, A.S. Improving the efficiency of using multivalued logic tools: Application of algebraic rings. *Sci. Rep.* **2023**, *13*, 22021. [CrossRef]
24. Raj, A.; Ahuja, K.; Busnel, Y. AI algorithm for predicting and optimizing trajectory of massive UAV swarm. *Robot. Auton. Syst.* **2025**, *186*, 104910. [CrossRef]
25. Zaitseva, E.; Levashenko, V.; Mukhamediev, R.; Brinzei, N.; Kovalenko, A.; Symagulov, A. Review of Reliability Assessment Methods of Drone Swarm (Fleet) and a New Importance Evaluation Based Method of Drone Swarm Structure Analysis. *Mathematics* **2023**, *11*, 2551. [CrossRef]
26. Zhao, B.; Huo, M.; Li, Z.; Yu, Z.; Qi, N. Graph-based multi-agent reinforcement learning for large-scale UAVs swarm system control. *Aerosp. Sci. Technol.* **2024**, *150*, 109166. [CrossRef]
27. Dorigo, M.; Theraulaz, G.; Trianni, V. Swarm Robotics: Past, Present, and Future. *Proc. IEEE* **2021**, *109*, 1152–1165. [CrossRef]
28. Zaitseva, E.; Mukhamediev, R.; Levashenko, V.; Kovalenko, A.; Kvassay, M.; Kuchin, Y.; Symagulov, A.; Oksenenko, A.; Sultanova, Z.; Zhaxybayev, D. Comparative Reliability Analysis of Unmanned Aerial Vehicle Swarm Based on Mathematical Models of Binary-State and Multi-State Systems. *Electronics* **2024**, *13*, 4509. [CrossRef]
29. Bakirci, M. A drone-based approach to enhance spatial insight into surrounding air pollutant distributions for healthier indoor environments. *J. Build. Eng.* **2024**, *87*, 109023. [CrossRef]
30. Udeanu, G.; Dobrescu, A.; Oltean, M. Unmanned Aerial Vehicle in Military Operations. *Sci. Res. Educ. Air Force* **2016**, *18*, 199–206. [CrossRef]
31. Guitton, M.J. Fighting the locusts: Implementing military countermeasures against drones and drone swarms. *Scand. J. Mil. Stud.* **2021**, *4*, 26–36. [CrossRef]
32. Bakirci, M.; Ozer, M.M. Adapting swarm intelligence to a fixed wing unmanned combat aerial vehicle platform. In *Data Analytics and Computational Intelligence: Novel Models, Algorithms and Applications*; Springer Nature: Cham, Switzerland, 2023; pp. 433–479.
33. Nasry, H. Coordinate transformation in unmanned systems using Clifford algebra. In Proceedings of the 5th International Conference on Mechatronics and Robotics Engineering, Rome, Italy, 16–19 February 2019; pp. 167–170.
34. Cai, G.; Chen, B.M.; Lee, T.H.; Cai, G.; Chen, B.M.; Lee, T.H. Coordinate systems and transformations. In *Unmanned Rotorcraft Systems*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 23–34.

35. Fossen, T.I. An amplitude-phase representation of the North-East-Down kinematic differential equations. *IEEE Access* **2023**, *11*, 12587–12593. [CrossRef]
36. Yang, P.; Ye, G.Y.; Shao, C.L.; Yang, S.L.; Huang, Z.X. A distributed factor graph model solving method for cooperative localization of UAV swarms. *Meas. Sci. Technol.* **2024**, *36*, 016326. [CrossRef]
37. Chen, H.; Wang, X.; Shen, L.; Cong, Y. Formation flight of fixed-wing UAV swarms: A group-based hierarchical approach. *Chin. J. Aeronaut.* **2021**, *34*, 504–515. [CrossRef]
38. Kang, X.; Shao, Y.; Bai, G.; Sun, H.; Zhang, T.; Wang, D. Dual-UAV Collaborative High-Precision Passive Localization Method Based on Optoelectronic Platform. *Drones* **2023**, *7*, 646. [CrossRef]
39. Bober, T. Indirect Fire Target State Estimation and Prediction Using Aerial Scout Vehicles (No. 2024-01-4090). In *SAE Technical Paper*; SAE: Warrendale, PA, USA, 2024.
40. Wang, R.; Liu, J. Adaptive formation control of quadrotor unmanned aerial vehicles with bounded control thrust. *Chin. J. Aeronaut.* **2017**, *30*, 807–817. [CrossRef]
41. Wondosen, A.; Jeong, J.S.; Kim, S.K.; Debele, Y.; Kang, B.S. Improved attitude and heading accuracy with double quaternion parameters estimation and magnetic disturbance rejection. *Sensors* **2021**, *21*, 5475. [CrossRef]
42. Xian, B.; Diao, C.; Zhao, B.; Zhang, Y. Nonlinear robust output feedback tracking control of a quadrotor UAV using quaternion representation. *Nonlinear Dyn.* **2015**, *79*, 2735–2752. [CrossRef]
43. Cao, S.; Wang, X.; Zhang, R.; Peng, Y.; Yu, H. Aerobatic Maneuvering flight control of fixed-wing UAVs: An SE (3) approach using dual quaternion. *IEEE Trans. Ind. Electron.* **2024**, *71*, 14362–14372. [CrossRef]
44. Khoramshahi, E.; Oliveira, R.A.; Koivumäki, N.; Honkavaara, E. An image-based real-time georeferencing scheme for a UAV based on a new angular parametrization. *Remote Sens.* **2020**, *12*, 3185. [CrossRef]
45. Van Der Waerden, B.L. *Algebra*; Springer: Berlin/Heidelberg, Germany, 1993.
46. Schinianakis, D.; Stouraitis, T. Residue Number Systems in Cryptography: Design, Challenges, Robustness. In *Secure System Design and Trustable Computing*; Chang, C.-H., Potkonjak, M., Eds.; Springer: Cham, Switzerland, 2016; pp. 115–161. [CrossRef]
47. Givaki, K.; Hojabr, R.; Najafi, M.H.; Khonsari, A.; Gholamrezayi, M.H.; Gorgin, S.; Rahmati, D. Using Residue Number Systems to Accelerate Deterministic Bit-Stream Multiplication. In Proceedings of the 2019 IEEE 30th International Conference on Application-specific Systems, Architectures and Processors (ASAP), New York, NY, USA, 15–17 July 2019; p. 40. [CrossRef]
48. Valueva, M.V.; Nagornov, N.N.; Lyakhov, P.A.; Valuev, G.V.; Chervyakov, N.I. Application of the Residue Number System to Reduce Hardware Costs of the Convolutional Neural Network Implementation. *Math. Comput. Simul.* **2020**, *177*, 232–243. [CrossRef]
49. Li, Z.; Liu, F.; Yang, W.; Peng, S.; Zhou, J. A survey of convolutional neural networks: Analysis, applications, and prospects. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *33*, 6999–7019. [CrossRef]
50. Gu, J.; Wang, Z.; Kuen, J.; Ma, L.; Shahroudy, A.; Shuai, B.; Liu, T.; Wang, X.; Wang, G.; Cai, J.; et al. Recent advances in convolutional neural networks. *Pattern Recognit.* **2018**, *77*, 354–377. [CrossRef]
51. Wu, J. *Introduction to Convolutional Neural Networks*; National Key Lab for Novel Software Technology, Nanjing University: Nanjing, China, 2017; Volume 5, p. 495.
52. Suleimenov, I.; Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y. Peculiarities of Applying Partial Convolutions to the Computation of Reduced Numerical Convolutions. *Appl. Sci.* **2024**, *14*, 6388. [CrossRef]
53. Martel, J.; Lindell, D.; Lin, C.; Chan, E.; Monteiro, M.; Wetzstein, G. Acorn: Adaptive coordinate networks for neural scene representation. *ACM Trans. Graph. (TOG)* **2021**, *40*, 58. [CrossRef]
54. Rocco, I.; Arandjelović, R.; Sivic, J. Convolutional Neural Network Architecture for Geometric Matching. *IEEE Trans. Pattern Anal. Mach. Intell.* **2019**, *41*, 2553–2567. [CrossRef]
55. Ezuz, D.; Solomon, J.; Kim, V.; Ben-Chen, M. GWCNN: A Metric Alignment Layer for Deep Shape Analysis. *Comput. Graph. Forum* **2017**, *36*, 49–57. [CrossRef]
56. Altamirano-Escobedo, G.; Bayro-Corrochano, E. Geometric Algebra Quantum Convolutional Neural Network: A model using geometric (Clifford) algebras and quantum computing [Hypercomplex Signal and Image Processing]. *IEEE Signal Process. Mag.* **2024**, *41*, 75–85. [CrossRef]
57. Deng, Z.; Xiao, H.; Lang, Y.; Feng, H.; Zhang, J. Multi-scale hash encoding based neural geometry representation. *Comput. Vis. Media* **2024**, *10*, 453–470. [CrossRef]
58. Matrassulova, D.K.; Vitulyova, Y.S.; Konshin, S.V.; Suleimenov, I.E. Algebraic fields and rings as a digital signal processing tool. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, *29*, 206–216. [CrossRef]
59. Suleimenov, I.; Bakirov, A.; Moldakhan, I. Formalization of ternary logic for application to digital signal processing. In *Energy Management of Municipal Transportation Facilities and Transport*; Springer International Publishing: Cham, Switzerland, 2019; pp. 26–35.
60. Wang, X.Y.; Dong, C.T.; Wu, Z.R.; Cheng, Z.Q. A review on the design of ternary logic circuits. *Chin. Phys. B* **2021**, *30*, 128402. [CrossRef]

61. Suleimenov, I.E.; Bakirov, A.S.; Matrassulova, D.K. A technique for analyzing neural networks in terms of ternary logic. *J. Theor. Appl. Inf. Technol.* **2021**, *99*, 2537–2553.
62. Kim, S.; Lee, S.Y.; Park, S.; Kim, K.R.; Kang, S. A logic synthesis methodology for low-power ternary logic circuits. *IEEE Trans. Circuits Syst. I: Regul. Pap.* **2020**, *67*, 3138–3151. [CrossRef]
63. Vitulyova, E.S.; Matrassulova, D.K.; Suleimenov, I.E. Construction of generalized Rademacher functions in terms of ternary logic: Solving the problem of visibility of using Galois fields for digital signal processing. *Int. J. Electron. Telecommun.* **2022**, 237–244. [CrossRef]
64. Wang, D.; Bai, B.; Zhao, W.; Han, Z. A Survey of Optimization Approaches for Wireless Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1878–1911. [CrossRef]
65. Zoli, M.; Mitev, M.; Barreto, A.N.; Fettweis, G. Estimation of the secret key rate in wideband wireless physical-layer-security. In Proceedings of the 2021 International Symposium on Wireless Communication Systems (ISWCS), Berlin, Germany, 6–9 September 2021. [CrossRef]
66. Hamamreh, J.M.; Furqan, H.M.; Arslan, H. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1773–1828. [CrossRef]
67. Ermukhambetova, B.; Mun, G.; Kabdushev, S.; Kadyrzhan, A.; Kadyrzhan, K.; Vitulyova, Y.; Suleimenov, I.E. New approaches to the development of information security systems for unmanned vehicles. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, *31*, 810. [CrossRef]
68. Kuptsov, V.; Badenko, V.; Ivanov, S.; Fedotov, A. Method for Remote Determination of Object Coordinates in Space Based on Exact Analytical Solution of Hyperbolic Equations. *Sensors* **2020**, *20*, 5472. [CrossRef] [PubMed]
69. Barvinok, A.; Rudelson, M. When a system of real quadratic equations has a solution. *Adv. Math.* **2022**, *403*, 108391. [CrossRef]
70. Chi, Y.; Lu, Y.M. Kaczmarz method for solving quadratic equations. *IEEE Signal Process. Lett.* **2016**, *23*, 1183–1187. [CrossRef]
71. Huang, M.; Xu, Z. Solving systems of quadratic equations via exponential-type gradient descent algorithm. *arXiv* **2018**, arXiv:1806.00904. [CrossRef]
72. Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y.; Suleimenov, I. Discrete Cartesian Coordinate Transformations: Using Algebraic Extension Methods. *Appl. Sci.* **2025**, *15*, 1464. [CrossRef]
73. Zhang, J.; Zhou, L.; Zhou, F.; Seet, B.C.; Zhang, H.; Cai, Z.; Wei, J. Computation-efficient offloading and trajectory scheduling for multi-UAV assisted mobile edge computing. *IEEE Trans. Veh. Technol.* **2019**, *69*, 2114–2125. [CrossRef]
74. Panchekha, P.; Sanchez-Stern, A.; Wilcox, J.R.; Tatlock, Z. Automatically improving accuracy for floating point expressions. *Acm Sigplan Not.* **2015**, *50*, 1–11. [CrossRef]
75. Boldo, S.; Jeannerod, C.P.; Melquiond, G.; Muller, J.M. Floating-point arithmetic. *Acta Numer.* **2023**, *32*, 203–290. [CrossRef]
76. Chiang, W.F.; Baranowski, M.; Briggs, I.; Solovyev, A.; Gopalakrishnan, G.; Rakamarić, Z. Rigorous floating-point mixed-precision tuning. *ACM SIGPLAN Not.* **2017**, *52*, 300–315. [CrossRef]
77. Oke, A.A.; Nathaniel, B.A.; Bukola, B.F.; Ayopo, O.A. Residue number system based applications: A literature review. *Annals. Comput. Sci. Ser.* **2021**, *19*. Available online: https://anale-informatica.tibiscus.ro/download/lucrari/Vol19/19-1-20-Babatunde.pdf (accessed on 2 December 2024).
78. Kalmykov, I.A.; Pashintsev, V.P.; Tyncherov, K.T.; Olenev, A.A.; Chistousov, N.K. Error-correction coding using polynomial residue number system. *Appl. Sci.* **2022**, *12*, 3365. [CrossRef]
79. Madisetti, V.K.; Young, I.T. *The Digital Signal Processing Handbook-3 Volume Set*; CRC Press: Boca Raton, FL, USA, 2018.
80. Tan, L.; Jiang, J. *Digital signal Processing: Fundamentals and Applications*; Academic Press: Cambridge, MA, USA, 2018.
81. Park, J.Y.; Moon, Y.H.; Lee, W.; Kim, S.H.; Sakurai, K. A survey of polynomial multiplication with RSA-ECC coprocessors and implementations of NIST PQC Round3 KEM algorithms in Exynos2100. *IEEE Access* **2021**, *10*, 2546–2563. [CrossRef]
82. Parrilla, L.; Álvarez-Bermejo, J.A.; Castillo, E.; López-Ramos, J.A.; Morales-Santos, D.P.; García, A. Elliptic curve cryptography hardware accelerator for high-performance secure servers. *J. Supercomput.* **2019**, *75*, 1107–1122. [CrossRef]
83. Wang, Y.E.; Wei, G.Y.; Brooks, D. Benchmarking TPU, GPU, and CPU platforms for deep learning. *arXiv* **2019**, arXiv:1907.10701.
84. Indiveri, G.; Liu, S.C. Memory and information processing in neuromorphic systems. *Proc. IEEE* **2015**, *103*, 1379–1397. [CrossRef]
85. Didier, L.S.; Dosso, F.Y.; Véron, P. Efficient modular operations using the adapted modular number system. *J. Cryptogr. Eng.* **2020**, *10*, 111–133. [CrossRef]
86. Gong, Y.; Gan, L.; Liu, H. Multi-channel modulo samplers constructed from Gaussian integers. *IEEE Signal Process. Lett.* **2021**, *28*, 1828–1832. [CrossRef]
87. Huang, M.; Luo, J.; Ding, C.; Wei, Z.; Huang, S.; Yu, H. An integer-only and group-vector systolic accelerator for efficiently mapping vision transformer on edge. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2023**, *70*, 5289–5301. [CrossRef]
88. Li, X.; Wen, C.; Li, X.; He, J. Adaptive fractional-order backstepping control for a general class of nonlinear uncertain integer-order systems. *IEEE Trans. Ind. Electron.* **2022**, *70*, 7246–7256. [CrossRef]
89. Suleimenov, I.E.; Vitulyova, Y.S.; Kabdushev, S.B.; Bakirov, A.S. Improving the efficiency of using multivalued logic tools. *Sci. Rep.* **2023**, *13*, 1108. [CrossRef]

90. van De Burgt, Y.; Melianas, A.; Keene, S.T.; Malliaras, G.; Salleo, A. Organic electronics for neuromorphic computing. *Nat. Electron.* **2018**, *1*, 386–397. [CrossRef]
91. Cao, G.; Meng, P.; Chen, J.; Liu, H.; Bian, R.; Zhu, C.; Liu, F.; Liu, Z. 2D material based synaptic devices for neuromorphic computing. *Adv. Funct. Mater.* **2021**, *31*, 2005443. [CrossRef]
92. Kalimoldayev, M.N.; Pak, I.T.; Baipakbayeva, S.T.; Mun, G.A.; Shaltykova, D.B.; Suleimenov, I.E. Methodological basis for the development strategy of artificial intelligence systems in the Republic of Kazakhstan in the message of the president of the Republic of Kazakhstan dated October 5, 2018. *News Natl. Acad. Sci. Repub. Kazakhstan Ser. Geol. Tech. Sci.* **2018**, *6*, 47–54. [CrossRef]

computers

MDPI

Review

Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare

Akhat Bakirov [1,2,*] and Ibragim Suleimenov [2,*]

[1] Institute of Communication and Space Engineering, Gumarbek Daukeev Almaty University of Power Engineering and Communications, Almaty 050013, Kazakhstan
[2] National Engineering Academy of the Republic of Kazakhstan, Almaty 050010, Kazakhstan
* Correspondence: axatmr@mail.ru (A.B.); esenych@yandex.ru (I.S.)

Abstract

This review is devoted to a comprehensive analysis of modern forms of information warfare in the context of digitalization and global interconnectedness. The work considers fundamental theoretical foundations—cognitive distortions, mass communication models, network theories and concepts of cultural code. The key tools of information influence are described in detail, including disinformation, the use of botnets, deepfakes, memetic strategies and manipulations in the media space. Particular attention is paid to methods of identifying and neutralizing information threats using artificial intelligence and digital signal processing, including partial digital convolutions, Fourier–Galois transforms, residue number systems and calculations in finite algebraic structures. The ethical and legal aspects of countering information attacks are analyzed, and geopolitical examples are given, demonstrating the peculiarities of applying various strategies. The review is based on a systematic analysis of 592 publications selected from the international databases Scopus, Web of Science and Google Scholar, covering research from fundamental works to modern publications of recent years (2015–2025). It is also based on regulatory legal acts, which ensures a high degree of relevance and representativeness. The results of the review can be used in the development of technologies for monitoring, detecting and filtering information attacks, as well as in the formation of national cybersecurity strategies.

Keywords: information warfare; disinformation; cognitive biases; digital signal processing; Fourier–Galois transforms; platform moderation; ethical aspects

Academic Editor: George Angelos Papadopoulos

Received: 25 August 2025
Revised: 17 September 2025
Accepted: 22 September 2025
Published: 26 September 2025

Citation: Bakirov, A.; Suleimenov, I. Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare. *Computers* **2025**, *14*, 410. https://doi.org/10.3390/computers14100410

1. Introduction

Modern forms of information warfare are complex, multilevel and dynamically developing phenomena. Traditional methods of influence are complemented and enhanced by digital technologies. The development of information and communication systems, social networks, and automated platforms enables the dissemination of information at scale and in targeted ways, influencing public opinion, political stability, and social processes.

In the context of high-speed data exchange and global interconnectedness, information attacks are becoming increasingly covert and multifaceted. They can include targeted distortion of facts, manipulation of context, dissemination of disinformation, creation of artificial agendas, and use of automated bots to amplify the effect. At the same time, traditional approaches to counteraction are often insufficient. Since they are unable to ensure timely detection and analysis of hidden patterns in large, noisy data arrays.

The problem under consideration is distinctly interdisciplinary nature. Its solution, at a minimum, requires close integration of the humanities and technical sciences. The development of information technologies leads to transformations of society [1,2], which cannot always be explained using classical sociology and/or psychology. From our point of view, which underlies the methodology of this review, any attempt to create an effective method of counteracting modern forms of information warfare will highlight the difficulties of a fundamental nature as discussed in [3]. The cited work shows that the highly fragmented disciplinary structure of science that had developed by the early 21st century is often an obstacle to understanding modern societal processes as a whole. This conclusion applies not only to the problems associated with information warfare. Accordingly, in this review this particular problem is considered, among other things, to substantiate the concept discussed in [3]. Specifically, the issue of information warfare can be considered as the most illustrative example proving the adequacy of the thesis on the convergence of natural scientific, technical, and humanitarian knowledge. It is this thesis that underlies the methodology of this review.

An illustration of the importance of this thesis is the increasingly widespread use of generative artificial intelligence (GenAI [4]) in science and education. The nature of which causes numerous discussions [5–7]. GenAI is increasingly used to address a wide range of questions, including those of a humanitarian nature. The most general ideas about the essence of information warfare allow us to assert that GenAI can, depending on the algorithms embedded in it, prioritize the interests of certain political or other groups, etc. We emphasize that this does not imply outright falsehoods. Given the widespread use of such technologies, a relatively small (and often unnoticeable to the average user) shift in emphasis is sufficient.

This example clearly shows that the problem of information warfare is reaching a qualitatively new level. There is a famous expression attributed to Bismarck: "The Battle of Sadowa was won by a Prussian school teacher." This statement illustrates an obvious thesis—the worldview is determined by the education system. Consequently, if this system is transformed, then society is transformed as well. At a minimum, these processes are interconnected.

Consequently, the nature of the future development of computing systems that form the basis of AI for various purposes, particularly GenAI, cannot but influence society (at least in the long term). There is every reason to believe that the "information technology—society" system is currently at a bifurcation point [8], namely, there is a wide range of scenarios for the further development of this system.

Furthermore, evidence suggests that classical computing technology built on the von Neumann architecture has exhausted its development potential. This underscores the need to develop multiple types of neuromorphic systems [9,10]. Revies on this topic repeatedly emphasize that the von Neumann architecture has several significant shortcomings (at least relative to current demands). One of them is determined by the need for significant energy costs for data exchange between the actual computing nodes and memory blocks [11,12].

Developments in the field of neuromorphic materials, in turn, raise questions about the algorithmic principles underlying computing systems, including those implementing GenAI. As [13] shows, that computing systems based on neuromorphic materials will be complementary to logics that differ from binary. To an even greater extent, this conclusion is true for materials that represent a further development of neuromorphic materials [14]. In particular, attempts to create sociomorphic materials have already been reported in the literature [15].

In general, the analysis of problems related in one way or another to information warfare requires the integrated use of digital signal processing (DSP) methods, new-generation

computing architectures, and mathematical models capable of effectively identifying significant features and anomalies in information flows. Of particular importance are algorithms operating under modular arithmetic, as well as approaches that provide parallel data processing in real time. These technologies are used across military and government domains, and to protect critical infrastructure, financial systems, and media platforms.

This review is structured as follows. Section 2 details the review methodology (databases, search keywords and year coverage, inclusion/exclusion criteria, deduplication and screening) and reports the PRISMA flow. Section 3 develops the theoretical foundations of information influence, clarifying core concepts, mechanisms and levels of impact.

Section 4 surveys modern forms of information warfare, including coordinated online operations, platform-mediated manipulation, deepfakes and memetic tactics. Section 5 analyzes the impact on the sociocultural code—language, value-normative, symbolic, historical-narrative and social-institutional layers—with illustrative cases. Section 6 synthesizes methods of countering information attacks, spanning education and prebunking, platform-level interventions and detection pipelines (network, temporal, content and multimodal), as well as governance tools. Section 7 focuses on IoT/IIoT threat and mitigation patterns in the context of information warfare (e.g., segmentation/zero-trust, SBOM, MUD and industrial control security).

Section 8 discusses the evolution of information-processing systems relevant to counter-IO—linking digital signal processing and emerging computing architectures to scalable detection and filtering. Section 9 considers ethical and legal aspects (e.g., transparency, researcher access and accountability requirements).

Section 10 examines higher education in the context of information warfare and the need for a paradigm shift in curricula and training. Section 11 outlines future directions and a research agenda. Section 12 concludes. Map of the review presented in Table 1.

Table 1. Research Questions & Contribution Map.

Section	Research Questions (RQ)	Method/Evidence Base	Key Findings/Contribution	Cross-References
Introduction	What is the domain and why is a systematic review needed? What are the goals, scope, and novelty?	Problem framing; synthesis of key strands; articulation of objectives and the paper's structure.	Defines the field, consolidates motivation, and positions the review's theoretical and practical contribution.	See Section 2 (methodology), Sections 4–6 (core survey).
Review Methodology	How was the corpus constructed? Which databases, keywords, year coverage, and inclusion/exclusion criteria were used?	PRISMA flow: 1059 identified → deduplication/screening → 592 included search strings and year ranges are documented.	Transparency and reproducibility of selection; reduces risk of systematic bias.	PRISMA figure; groups × years table; see Sections 4–7 for use of the corpus.
Theoretical foundations of information influence	Which core concepts/mechanisms and levels of analysis are relevant to information influence?	Theoretical synthesis (communication, psychology, networks); mapping of mechanisms.	Unified vocabulary and level framework connecting micro/meso/macro processes.	See Section 4 (forms), Section 5 (sociocultural code).
Modern forms of information warfare	What is the taxonomy of contemporary forms and how are they evolving?	Systematization by tactics/channels: coordinated campaigns, platform manipulation, bots, memetics, deepfakes.	Coherent typology with observability indicators; links back to mechanisms in Section 3.	See Section 6 (countermeasures), Section 7 (IoT/IIoT context), Section 9 (law/ethics).
Impact on the sociocultural code: theory and practice	Which layers of the sociocultural code are vulnerable, and how is impact manifested in practice?	Layered analysis (linguistic, value-normative, symbolic, narrative-historical, institutional) + illustrative cases.	Explains channels/effects of long-term influence on identity, memory, and norms.	See Section 3 (mechanisms), cases across Sections 4 and 7.

Table 1. *Cont.*

Section	Research Questions (RQ)	Method/Evidence Base	Key Findings/Contribution	Cross-References
Methods of countering information attacks	Which strategic and operational countermeasures are effective against different forms?	Synthesis of education/pre-bunking, platform governance, and detection pipelines (network, temporal, content, multimodal).	Threat → indicator → measure → metric mapping; principles for multi-layer defense.	See Section 4 (threats), Section 7 (domain patterns), Section 9 (regulation).
IoT/IIoT Threats and Mitigation Patterns in the Context of Information Warfare	How does information warfare manifest in IoT/IIoT, and which threat/mitigation patterns matter?	2015–2025 survey + industry practice: segmentation/zero-trust, SBOM, MUD, ICS/SCADA context.	Domain-specific map of threats and measures at the cyber–information nexus in IIoT.	See Section 6 (methods), Section 8 (processing architecture).
Evolution of information-processing systems (DSP & emerging computing)	How do computing/DSP trends support scalable counter-IO (detection, filtering, resilience)?	Analytical review: digital signal processing and emerging architectures (e.g., neuromorphic, memory-centric).	Connect detection/filtering pipelines to hardware/architectural developments.	See Sections 6 and 7 (applications), Section 11 (R&D agenda).
Ethical and legal aspects of combating disinformation	How to balance counter-measures with rights/freedoms, transparency, and accountability?	Normative-legal and ethical analysis; comparison of regulatory approaches and practices.	Principled governance framework and constraints for counter-disinformation practices.	See Section 6 (methods), Section 10 (education), Section 11 (policy agenda).
Higher Education in the Context of Information warfare	What curricular and training changes are needed for resilience to information warfare?	Review of curricula and literacy practices; integration of technical-humanities modules.	Proposes paradigm shifts and learning pathways for robust knowledge ecosystems.	See Section 6 (countermeasures), Section 11 (implementation roadmap).
Future Directions and Research Agenda	What mid-/long-term priorities are required in methods, data, and infrastructure?	Synthesis of gaps; formulation of RQs/hypotheses; roadmaps for data, methods, and tooling.	Structured agenda—from detection methods to interdisciplinary impact metrics.	See Sections 6–9 (needs), Section 8 (architectures), summary in Section 12.
Conclusions	What is the overall contribution and the practical implications?	Synthesis of key results; alignment with goals stated in the Introduction.	Consolidated conclusions, limitations, and high-level recommendations for scholars and practitioners.	Back-references to Sections 2–11; notes on appendices/tables/figures.

The purpose of the review is to combine modern scientific and technological approaches in the field of countering information threats, providing a systemic understanding and a comprehensive view of possible methods of protection in the context of the rapid development of the digital environment.

2. Review Methodology

As noted above, the methodology of this review is based on the thesis of the convergence among natural science, technology, and humanities, whose significance is most evident in the problems of information warfare. Key evidence of the importance of interdisciplinary cooperation in this area is presented in Section 3, where the theoretical foundations of information influence are discussed.

The PRISMA 2020 methodology was used to prepare this review, ensuring transparency and reproducibility of the literature selection process. During the initial search, a total of 1059 publications were identified. After removing duplicates and sources that did not meet the formal criteria, 838 papers remained for screening. A step-by-step assessment was conducted. Based on the titles and abstracts, about 168 publications were excluded that were not related to the research focus or did not meet academic standards. The remaining articles underwent a full-text analysis, during which 78 more sources were excluded due to insufficient methodological rigor or limited relevance. As a result, the final sample included 592 publications, which formed the basis of the analysis. The chronological scope of coverage is broad: although the main focus was on studies of recent years (2015–2025). The review also included earlier works that are fundamental to forming a theoretical basis and

explaining the evolution of information impact methods. Thus, the final sample combines both contemporary studies reflecting current trends and challenges and classical works that allow us to trace the development of scientific thought in retrospect.

The literature search was conducted in leading international databases—Scopus, Web of Science, and Google Scholar, as well as in specialized academic publications. In addition, cross-references from review articles, monographs, and key publications were considered. When including sources, priority was given to publications in peer-reviewed journals and academic presses. This approach minimized the risk of bias and increased the reliability of the summarized data. To increase the completeness of the sample, a combination of keywords was used, including the terms "information warfare", "information operations", "propaganda", "disinformation", "hybrid warfare", "sociocultural code", "cognitive security", "digital platforms", "cybersecurity", as well as other equivalents. Table 2 provides information on source coverage, and Figure 1 shows a PRISMA-style diagram.

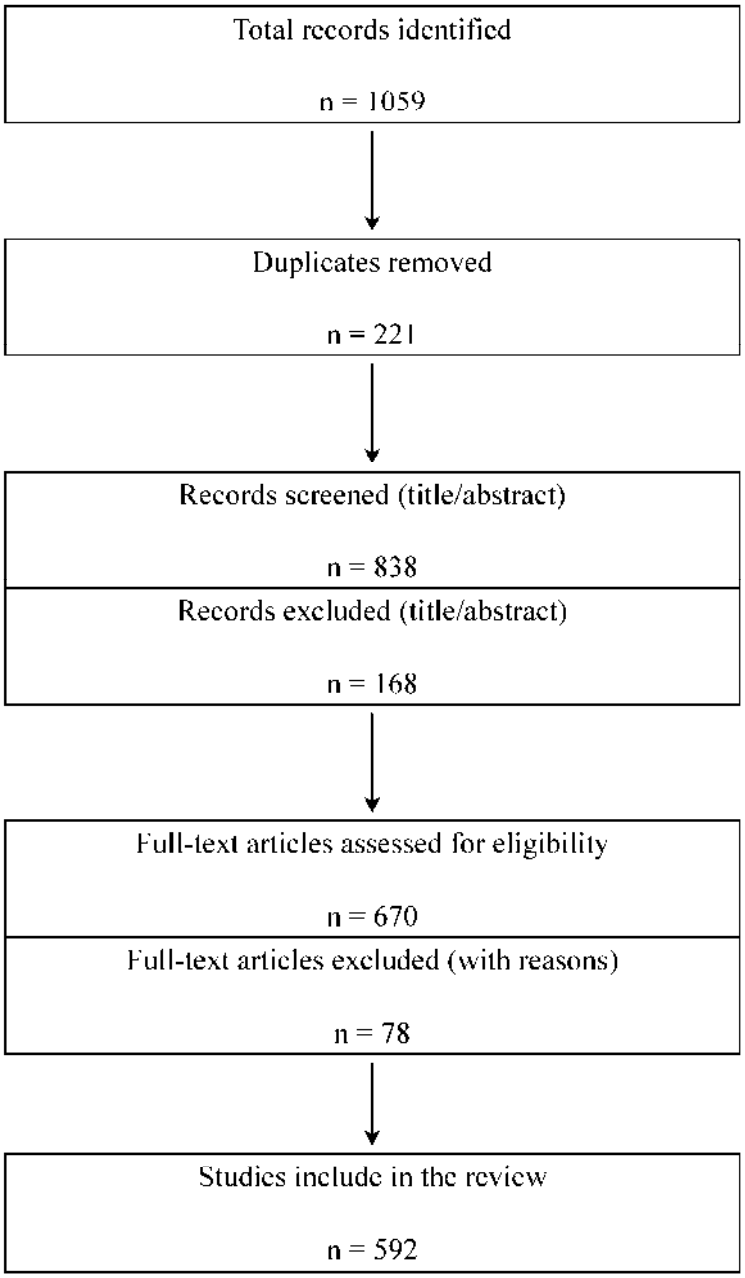


Figure 1. PRISMA style diagram.

Table 2. Coverage of Included Sources by Thematic Bucket and Period.

Group	Count	Share, %	<2000	2000–2014	2015–2025
General	164	27.7	11	28	125
Disinformation/Info Warfare	132	22.3	1	4	127
Communication Theory/Media Studies	93	15.71	15	21	57
Network Science & Diffusion	41	6.93	4	8	29
Policy/Doctrine/Law/Reports	32	5.41	0	0	32
Regional Cases	29	4.9	0	5	24
Sociocultural Code/Philosophy	27	4.56	6	9	12
Cognition/Biases/Psychology	20	3.38	6	9	5
Neuromorphic/Polymer/Memristor	15	2.53	0	0	15
Deepfakes & Synthetic Media	13	2.2	0	0	13
Memes & Digital Culture	10	1.69	0	1	9
AI/GAN/TTS/Diffusion Models	8	1.35	2	2	4
Digital Transformation & Higher Ed	6	1.01	0	1	5
Fact-checking/Verification	2	0.33	0	0	2

3. Theoretical Foundations of Information Influence

The study of information impact requires a comprehensive approach that combines knowledge from cognitive psychology, sociology, communication theory, cybernetics, and political science. In the context of digitalization and global interconnectedness of the media, the information environment has become not only a channel for transmitting information but also an arena for targeted manipulation of public opinion and behavioral patterns. Modern research emphasizes that the effectiveness of such impacts is determined by both individual cognitive mechanisms of perception and the structure of the information networks through which information disseminated. Fundamental theoretical models—from the concepts of cognitive biases and social epistemology to network and epidemiological theories—allow us to identify patterns in the formation, amplification, and replication of meanings in the collective consciousness. These same models underlie the development of information operations strategies, including military doctrines of cognitive actions, platform algorithms and the attention economy. This section presents a systematic review of the key theoretical approaches necessary to understand the nature and mechanisms of modern information impact.

3.1. Cognitive Biases and the Psychology of Perception

Cognitive biases are systematic deviations in the process of perceiving, processing, and memorizing information, that lead to persistent errors in judgment and decision making [16]. These phenomena are not random—they are associated with the characteristics of human memory, attention, and emotions, as well as evolved mechanisms for conserving cognitive resources [17]. In the context of information influence, cognitive biases are exploited to guide the interpretation of facts, evoke emotional reactions, and reinforce the desired attitudes in the collective consciousness [18]. One of the most studied is the confirmation bias, in which an individual tends to search for and interpret information so that it aligns with their existing beliefs [19]. In the context of digital platforms, this effect is amplified by content personalization algorithms that form "information bubbles" (filter bubbles), in which users mainly see information that confirms their worldview [20,21]. This not only reduces the likelihood of critical analysis but also makes the audience more receptive to targeted narratives.

The illusory truth effect is an increase in the perceived credibility of information through repetition [22]. Experiments show that even the refutation of an initially false message does not always reduce its subjective credibility, especially if repetitions occur in different contexts [23,24]. This phenomenon is widely exploited in propaganda campaigns, where key messages are regularly reproduced across multiple channels.

The anchoring effect demonstrates that initial numerical or verbal information exerts a disproportionate influence on subsequent evaluations [25]. For example, inflated or deflated statistics in news stories can change the perception of an issue, even when accurate information is subsequently presented [26].

Other significant cognitive biases used in information influence include:

- Halo effect—tendency to transfer positive or negative characteristics of an object to its other properties [27].
- Primacy and recency effects—better memorization of the first and last presented information [28].
- Selective perception—tendency to ignore data that does not meet expectations [29].
- Framing effect—change in the interpretation of information depending on the wording or context [30].

Psychological research shows that such biases are particularly pronounced under heightened emotional arousal [31]. High emotional load—fear, anger, a sense of threat—reduces cognitive control, shifts information processing to a heuristic level, and makes a person more susceptible to simplified, binary interpretations of events [32]. This explains why emotionally charged messages spread faster and more widely on social media [33]. In addition to individual cognitive biases, information campaigns rely on social cognitive effects. For example, the false consensus effect creates the impression that a certain position is widespread and supported by the majority [34]. The groupthink effect suppresses critical discussion within a group if it is assumed that there is general agreement [35].

Modern neurocognitive studies using functional magnetic resonance imaging (fMRI) show that cognitive biases are associated with activity in brain structures responsible for processing reward, social evaluation, and emotions, such as the prefrontal cortex and amygdala [36,37]. This opens up prospects for a deeper understanding of the mechanisms of manipulation and the development of methods of cognitive immunoprophylaxis.

Taken together, cognitive biases underpin manipulative influence, since they allow us to bypass rational filters of perception, appealing directly to automatic, emotionally charged mechanisms of information processing. Understanding these distortions is key to developing effective strategies to counter modern forms of information warfare.

3.2. Communication Theories and Social Epistemology

Communication theories play a fundamental role in understanding the mechanisms of information influence, because they allow us to conceptualize both the structure and dynamics of message dissemination across society. The evolution of communication models—from linear schemes of information transmission to multilevel network concepts—has reflected changes in the technological and media environments, as well as a shift in emphasis from data transmission to the construction of meanings and collective interpretations [38,39]. One of the early approaches that laid the foundation for the analysis of information processes was Las—swell's linear communication model, which reduces communication to the chain "who says—what—through which channel—to whom—with what effect" [40]. Despite its schematic nature, this model is still used in structuring information influence strategies and assessing the effectiveness of media campaigns [41].

In the context of information warfare, the linear model is important for mapping sources and target audiences, but insufficient for analyzing complex networks and feedback loops. A significant development of linear approaches was the two-stage communication model by Lazarsfeld and Katz, which identifies the role of "opinion leaders" in the transmission and interpretation of messages [42]. Opinion leaders, as highly trusted nodes in social networks, can amplify or weaken information signals, including disinformation [43]. Re-

cent empirical research shows that in the online environment, the role of opinion leaders is often played by micro-influencers or thematic communities, rather than large media figures. These "middle nodes" become key to the sustained dissemination of narratives [44]. With the transition to the digital age, interactive and transactional communication models have become widespread, emphasizing the bidirectional nature of information exchange [45]. Here, communication is viewed as a process of constant mutual influence, where the audience not only receives but also actively forms and redistributes content. This corresponds to the reality of social networks, where disinformation can be amplified through reposts, comments, and memetic transformations of original messages [46].

Social epistemology complements these models by focusing on how knowledge and beliefs are formed, disseminated, and legitimized in a collective context [47]. According to Goldman and Olson, social epistemology examines the institutions, technologies, and practices through which the "epistemic ecology" of society is shaped [48]. In the context of information warfare, epistemic ecology is under attack: alternative sources of legitimacy are created, standards of evidence are eroded, and trust in traditional knowledge institutions is undermined [49].

One of the key concepts of social epistemology is epistemic trust: the willingness to accept information from certain sources as true [50]. Manipulative information campaigns often aim to erode epistemic trust in independent media, scientific institutions, and government agencies, thereby opening space for the promotion of alternative narratives [51]. Recent research shows that loss of epistemic trust correlates with increased susceptibility to conspiracy theories and quasi-scientific claims [52]. Communication theories that consider the influence of network structures are particularly relevant for the analysis of disinformation. The network approach allows viewing the dissemination of messages as a process that depends on the topology of connections between participants [53]. For example, studies based on graph theory show that nodes with high betweenness centrality play a critical role in the transmission of information between clusters and can be targets for information intervention [54].

An important area is the integration of communication theories with epidemiological models, where information is viewed as an "infectious agent" [55]. These hybrid models enable to predict the dynamics of fake news spread and assess the effectiveness of "information quarantine" or prebunking strategies [56]. At the same time, social epistemology suggests that the speed of disinformation spread depends not only on network structure, but also on cultural norms, the level of media literacy, and trust in sources [57]. Framing and agenda-setting play a significant role in information impact. According to McCombs and Shaw, media do not so much tell people what to think as they determine what to think about [58].

Framing, in turn, determines the interpretive framework of events, influencing which aspects are perceived as significant [59]. In the modern digital environment, framing is often implemented through visual and memetic forms, which enhance its emotional and cognitive effectiveness [60]. Together, communication theories and social epistemology provide powerful tools for analyzing and countering information attacks. They allow identification of nodes and channels of dissemination, mechanisms for legitimizing knowledge, and weak points in the epistemic structure of society. For developers of information-security strategies, the key conclusion is the need to combine technical network analysis with a cultural and cognitive understanding of the processes that shape information perception.

3.3. Network and Epidemiological Models of Spread

Understanding the mechanisms of information dissemination in the modern media space is impossible without network and epidemiological models. These approaches help

to formalize complex message circulation processes, consider the structural features of communication systems, and predict the dynamics of information attacks. Network models are based on graph theory, in which the information ecosystem is represented as nodes (individual users, organizations, media accounts) and edges (connections between them, such as subscriptions, reposts, or mentions) [61]. Classic network analysis indicators—degree, betweenness centrality, closeness centrality, and eigenvector centrality—help identify key agents of message dissemination [53]. For example, nodes with high betweenness centrality are often "bridges" between clusters and can ensure the rapid transition of disinformation to new network segments [54]. One of the fundamental features of information networks is the small-world property, identified by Watts and Strogatz [62]. Even in large and sparse networks, there are relatively few steps needed to connect any two nodes. This property explains why disinformation can reach a global audience in a matter of hours, especially in the presence of viral content and memetic forms.

Another key characteristic is the scale-free (scale-invariant) degree distribution of networks, in which node degrees follow a power law [63]. Such networks are resilient to random failures but are extremely vulnerable to targeted interventions on hub nodes. Research shows that on Twitter and Facebook, about 1–5% of users can be responsible for more than 80% of the spread of certain narratives [64].

Based on network representations, diffusion models have been developed that integrate social and behavioral factors. The most well-known epidemiological models are the SIR (Susceptible-Infected-Recovered) type and its modifications—SIS, SEIR, SEIZ (where Z is the "zombie" state of a misinformed agent) [65]. In the context of information warfare, "infection" corresponds to the state of an individual who adopts and spreads disinformation, and "recovery" can mean either debunking or refusal to further spread the message [66].

The SIR model in the information context has been complemented by threshold models, in which an individual accepts information only when a certain number of signals from the environment are reached [67]. This allows us to describe the phenomenon of "viral breakout", when a narrative that has long remained on the periphery suddenly enters the mainstream.

Modern works demonstrate that classical epidemiological approaches need to be adapted to the specific features of digital platforms. For example, Borge-Holthoefer et al. [68] propose a SEIZ model in which state Z describes users who are resilient to refutation and continue to spread falsehoods despite access to corrective information. Such "infection resilience" is particularly characteristic of politically motivated disinformation campaigns.

An important area is the combination of network analysis and epidemiological models with agent-based modeling (ABM) methods [69]. ABM accounts for individual differences in agents—media literacy level, political orientation, emotional perception—and observe how these factors affect the macrodynamics of dissemination. For example, studies on COVID-19 show that misinformation about vaccines spread faster and deeper online than science-based messages due to emotional richness and algorithmic amplification [70]. Particular attention is paid to role structures in the network. The work of Lerman et al. [71] shows that "super-spreaders" and "super-receivers" are different categories of users, and counteraction strategies should take both into account. Eliminating super-spreaders slows the growth of misinformation, but long-term resilience is achieved by increasing the media literacy of super-receivers [72]. Hybrid approaches also use percolation models to describe cascade processes [73]. Here, dissemination is viewed as a process of penetration through a network, in which the "permeability" of nodes depends on trust, cultural factors, and personal experience. When a critical connection density is reached, a "percolation threshold" emerges, beyond which dissemination becomes uncontrollable.

In terms of countermeasures, network and epidemiological models allow testing the effectiveness of measures—from removing nodes to changing content delivery algorithms [74]. However, several studies [75] emphasize that without considering social context and cross-platform dynamics, such measures are short-lived.

Recent developments include the use of dynamic multilayer networks (multiplex networks), in which each layer represents a separate platform or type of interaction (e.g., public posts, private messages, offline meetings) [76]. Modeling on such structures reveals that disinformation often "migrates" between layers: blocking on one network causes an increase in activity in another. Network and epidemiological models of dissemination provide both an analytical and a predictive basis for understanding the dynamics of information attacks. Their strength lies in their ability to identify critical points, predict consequences, and evaluate the effectiveness of countermeasures. A key challenge for current research is integrating these models with cognitive and cultural factors to create more accurate and robust analytical tools.

3.4. Attention Economy and Platform Architecture

The concept of the attention economy dates back to the 1970s, when Herbert Simon pointed out that under information abundance, the scarce resource is not information but human attention [77]. In the modern digital space, this idea is of central importance, as user attention has become a key asset for which social networks, news aggregators, streaming services, and online platforms compete. The digital environment has transformed attention into a commodity subject to monetization through advertising models, targeting, and the sale of user-behavior data [78]. Platforms, relying on behavioral data, build algorithms that rank and personalize content to maximize user time on the platform. These algorithms work like digital "magnets", continuously optimizing the delivery of information to retain attention and stimulate repeat visits [79]. Modern platforms use a combination of recommender systems, ranking algorithms, and content-filtering systems based on machine learning and deep neural networks [80]. These mechanisms are trained on huge amounts of user data and, as recent studies show, tend to reinforce existing preferences, forming so-called "filter bubbles" and "echo chambers" [20].

The effect of algorithmic personalization has been documented in studies on Facebook and YouTube, where recommendation systems show a tendency to direct users to more polarized and emotionally charged content [81]. In the case of YouTube, algorithms increase the likelihood of being steered to conspiracy videos if users had previously interacted with similar content, even in the absence of an explicit search [82].

In the context of information warfare, platform architecture and the attention economy play a dual role. On the one hand, the highly competitive environment forces platforms to optimize algorithms for engagement metrics—clicks, likes, and reposts—without directly considering the credibility of the content [83]. On the other hand, this same mechanism creates conditions for increased amplification of disinformation, since false or sensational messages tend to evoke a stronger emotional response and accordingly, generate more interactions [84]. An empirical study shows that false news spreads faster on Twitter and reaches more users than true news, and this effect is not explained by bots—it is associated with the behavior of real users [64]. This indicates that the platform architecture focused on engagement metrics objectively amplifies narratives that correspond to attention patterns, rather than the quality of information.

The attention economy is closely related to cognitive psychology. People tend to pay more attention to information that evokes strong emotions (fear, outrage, surprise), which, in turn, encourages platforms to offer such content [33]. Algorithmic systems trained on

behavioral data unintentionally exploit cognitive biases, including confirmation bias and negativity bias [84].

From the perspective of military and strategic information operations doctrines, the attention economy and platform architecture create an infrastructure that enables large-scale and targeted manipulation of public opinion [85]. State and non-state actors, including online troll farms and coordinated botnets, use knowledge of algorithmic mechanisms to advance favorable narratives [86]. Modern NATO StratCom [87] and European External Action Service [88] reports indicate that the architecture of social platforms does not simply passively transmit information but actively shapes the context and trajectories of its dissemination, influencing the likelihood of users encountering a particular narrative.

One of the key challenges is the cross-platform migration of content. Disinformation blocked in one network can be instantly reproduced in another, and the architecture of interconnections (cross-posting, messengers, forums) helps bypass barriers [89]. Research shows that Telegram has become one of the main platforms—"recipients" of removed content from Facebook and Twitter, while maintaining a high speed of dissemination [90].

These features indicate the need to develop architectural solutions that can work not within a single platform but at the ecosystem level.

Thus, the attention economy and platform architecture are fundamental elements of the information impact infrastructure. Their key feature is algorithmic optimization for engagement metrics, which, although not initially aimed at disinformation, creates a favorable environment for its exponential spread. Understanding these mechanisms is a prerequisite for developing effective countermeasures to modern forms of information warfare.

3.5. Strategic and Military Doctrines of Cognitive Operations

Cognitive operations (CO) within a military context are the deliberate manipulation of the perceptions, thinking, emotions, and decision-making processes of target audiences to achieve strategic or operational objectives. The approach emerged at the intersection of psychological operations (PSYOPS), strategic communications (STRATCOM), information operations (IO), and cyber operations, but has become in its own right over the past two decades as a key dimension of modern conflict [91].

The origins of CO can be traced back to the Cold War military doctrines, when information and psychological warfare were viewed as an integral part of political struggle [92]. However, with the advent of digital communications and social media, the cognitive space has become an integral part of the "battlefield". A 2018 RAND report documents a shift from traditional "information superiority" to the concept of "cognitive superiority," in which the object of influence is no longer the communications infrastructure but the processes of perception and interpretation of information [93]. NATO doctrinal documents such as the Allied Joint Doctrine for Strategic Communications (AJP-10) define the cognitive domain as "the domain in which beliefs, values, and perceptions are formed and changed" [94]. Unlike the information domain, which describes the channels and technical means of data transmission, the cognitive domain focuses on subjective interpretations and their strategic management.

The United States developed the CO concept as part of a combination of PSYOPS, military information operations, and cyber operations. US Special Operations Command reports emphasize the need to integrate data on the cultural characteristics of target audiences into content impact algorithms [95]. The Pentagon views cognitive operations as a component of "Multi-Domain Operations" (MDO), in which psychological impact is synchronized with cyber and information attacks [96].

Russia officially uses the term "information-psychological impact" (IPI), which essentially overlaps with the concept of CO. The Russian Federation Information Security

Doctrine (2016) states that "information impact on collective consciousness" may aim to undermining cultural and spiritual values, as well as destabilizing the domestic situation [97]. Analysis by the NATO StratCom COE indicates that Russia systematically uses cognitive methods as part of hybrid strategies [98].

China, within the framework of the Three Warfares concept—psychological, legal, and media—emphasizes the cognitive effects of information campaigns [99]. The White Paper on National Defense of the PRC (2019) states that "victory in future wars will be determined by the ability to shape the perception and interpretation of events" [100].

Cognitive operations are embedded in a broader paradigm of hybrid warfare, in which military, diplomatic, economic, and information means are combined to achieve goals without direct armed conflict [101]. In this scheme, the cognitive component acts as a "force multiplier", since successfully changing the perception of the target audience can reduce the need to use kinetic means [102].

Cognitive operations use a wide range of methods, include [103]:

- targeted distribution of content based on behavioral data;
- creation and management of "frames" (narratives) with high emotional load;
- exploitation of cognitive biases (e.g., the anchoring effect and the confirmation effect);
- use of synthetic media (deepfakes) to enhance credibility.

A key feature of modern CO implementation is integration with platform architecture (see Section 3.4) and the use of algorithmic affordances of social media [104]. Research shows that the combination of algorithmic personalization and psychologically validated narratives can significantly increase the effectiveness of influence [105].

The doctrine of CO is being developed at the level of national strategies and international alliances. The 2021 NATO report "Cognitive Warfare" [106] explicitly states that cognitive space is a new domain of conflict along with land, sea, air, space, and cyberspace. The document warns that cognitive warfare is aimed not only at soldiers but also at civilians, including shaping the perception of threats and allies.

In 2020–2022, the United States conducted a series of exercises simulating operations in the cognitive domain, in which social media simulations were used to test the resilience of military units to information attacks [107]. Such training demonstrates an institutional recognition that winning future conflicts requires dominance in the cognitive domain.

Despite the growing attention to CO, there is a danger of an escalating "cognitive arms race" in which states invest in increasingly sophisticated methods of manipulating perceptions [108]. This raises serious ethical questions, including the balance between national security and the human right to freedom of thought and belief [109].

With the cognitive domain becoming an arena for strategic confrontation, developing countermeasures requires an interdisciplinary approach that combines political science, cognitive psychology, computer science, and international law.

4. Modern Forms of Information Warfare

The evolution of communication technologies and digital platforms has profoundly changed the nature of information conflicts. While in the past information warfare relied primarily on traditional media and propaganda channels. Today, the key arenas of confrontation have become social networks, instant messaging apps, video-hosting services, and interactive platforms. The development of personalization algorithms, tools for automated content distribution, and generative technologies has led to the emergence of new, more sophisticated forms of attack—from botnets and coordinated campaigns to synthetic media and memetic weapons. These forms often operate in a complex manner, reinforcing each other. These hybrid operations creating difficult-to-distinguish hybrid operations aimed at manipulating public consciousness, undermining trust in institutions,

and fragmenting the sociocultural space. This section examines the key manifestations of information warfare in their current technological and strategic context.

4.1. Disinformation, Fake News and False Narratives

In modern literature, it is suggested to distinguish between mis-, dis- and malinformation: errors and inaccuracies without the intention to mislead; deliberate lies; and accurate information disseminated with malicious intent (e.g., doxxing). This framework is outlined in the Council of Europe report [110], which also shows that the boundaries between categories are dynamic and context dependent (e.g., motives, production processes, and distribution routes). An important conclusion is that the source and process are at least as significant as the "factual result" itself, which is critical to developing countermeasures.

A philosophically precise definition of "disinformation" was proposed by Don Fallis: false (or misleading) content disseminated with the intent to mislead [111]. This definition emphasizes intent, distinguishing disinformation from unintentional error, and is aligns well with law-enforcement practice and communications ethics. In parallel, there is the term "fake news", which in academic usage has been typologized as: satire, parody, fabrication, manipulation (including deepfake editorials), advertising mimicry, and propaganda. This typology [112] notes that under one "umbrella" label are hidden different genres with different harmfulness and mechanisms of distribution—and therefore different response tools.

The review by Lazer et al. [113] in Science systematizes the empirical evidence: the role of platform algorithms, behavioral targeting, social context, and psychology. The authors emphasize that sustainable solutions go beyond simple "delete/tag" and include interface design, researchers' access to data, and prebunking (inoculation). The scale of impact in electoral contexts has been documented by a series of studies: the Oxford Internet Institute's report on the IRA account pool for the US Senate [114], Work on France's 2017 election [115], and an analysis of the "Brexit botnet" [116]. All of them document coordinated inauthentic behavior (CIB), the use of botnets, memetic formats, and cross-platform integration. This does not necessarily mean that each message is highly "persuasive," but it does demonstrate industrial-scale reach and repetition—two factors critical to the perpetuation of false narratives. At the same time, individual exposure to "untrusted domains" is heterogeneous: panel data from Guess, Nyhan, and Reifler [117] showed that a significant portion of the audience does not encounter such sources regularly, while small cohorts are overexposed and become "superconsumers" of inauthentic sites. For counter-policy, this means that targeted measures are needed, not just "platform-wide" regulation.

The cognitive side of the phenomenon explains the persistence of false narratives. The confirmation bias [118] inclines people to seek out and interpret information in support of their own beliefs. The "illusory truth effect" [119] shows that simple repetition increases subjective credibility even when a person knows the correct answer. Reviews of "post-truth" [120] highlight the limited effectiveness of post-factum refutations without changing frames and context. This explains the success of the "firehose of falsehood" [121], which relies on speed, volume, and variability rather than internal coherence. Finally, in times of crisis, an "infodemic" works: saturating the field with contradictory messages, in which the lack of trusted reference points (e.g., institutions and experts) makes the audience receptive to simple, emotionally charged explanations. WHO-The Lancet [122] observations during COVID-19 confirm that combating the infodemic requires a combination of technical filters, platform partnerships with fact-checking organizations, and media literacy measures [123–125].

4.2. Botnets, Trolling, and Coordinated Inauthentic Behavior

Among the most studied technological forms of modern information influence are botnets—automated or semi-automated accounts on social media that imitate the activity of

real users. Their key function is to scale content distribution, manipulate engagement metrics (likes, retweets, comments), and create the illusion of consensus on certain topics [126].

Botnet mechanisms are varied. In technical terms, they can be based on API access scripts to platforms (for example, Twitter API before the introduction of restrictions in 2023), use the infrastructure of "bot farms" with centralized control or distributed architectures via infected user devices (i.e., botnet models known from cybersecurity) [127]. In parallel, "human bots" are actively used—low-paid operators acting according to preset scenarios (troll farms), a pattern especially typical of political trolling [128]. Coordinated Inauthentic Behavior (CIB) as a concept is codified in the policies of Meta and other platforms and is studied in the academic community from the perspective of network analysis, anomaly detection, and digital attribution [129]. The key criterion is the presence of hidden centralized coordination aimed at misleading the audience about the true nature of the interaction.

Research by E. Ferrara and colleagues [130] shows that botnets can amplify both disinformation and legitimate political messages, which complicates the binary classification of "harm/benefit". At the same time, the pace of publications, the rhythm of daily activity, and the simultaneous distribution of the same URLs are reliable indicators of automation [131].

A classic example of a large-scale CIB operation is the activity of the Russian "troll factory" (Internet Research Agency, IRA), identified in the reports of the US Senate and analyzed in research [132]. Hundreds of pages and thousands of accounts aimed at polarizing society and interfering in the 2016 elections were identified on Facebook and Instagram.

Similar patterns are documented in other contexts: in the 2017 French elections [133], in the Catalan crisis [134], and in the media coverage of the Hong Kong protests [135]. In each case, campaigns are multilingual, integrated across cross-platform assets (Twitter, Facebook, YouTube, messaging apps), and use memetic content for organic reach.

The CIB problem is compounded by "digital astroturfing"—the imitation of grassroots support using synthetic accounts [136]. As experiments by Vosoughi, Roy, and Aral [137] show, false information spreads faster and more deeply on Twitter than truthful information, even without the use of bots; however, bots significantly accelerate the early stages of diffusion, increasing the chances of a narrative taking hold.

In response, platforms are implementing automatic detection methods: behavioral metrics, graph analysis, machine learning based on content features, and metadata [138]. However, as Keller and Klinger [139] note, each new detector quickly causes attackers to adapt—publication patterns, message frequency, and distribution by time zones change.

In the academic and applied context, interest in international regulation of CIB is growing. NATO StratCom COE [140] and the European External Action Service (EEAS) [141] reports point to the need to synchronize cybersecurity and information standards, since the boundaries between "purely technical" and "purely information" threats in the bot environment are blurred.

4.3. Deepfakes and Synthetic Media

Deepfakes are synthetic media files—images, audio, or video recordings, created or modified using deep learning algorithms, most often based on generative adversarial networks (GANs) [142]. Their key feature is a high degree of realism in the absence of an authentic source of an event or statement. Having emerged as an experimental direction in computer vision in the mid-2010s, deepfakes quickly became a tool for both entertainment and information attacks. The technological basis of deepfakes lies in the ability of GANs and their variants (StyleGAN, CycleGAN, and related models) to model data distributions and synthesize new samples that are visually indistinguishable from real ones [143]. For audio fakes, architectures based on voice conversion models and text-to-speech systems with deep learning are used [144]. With the advent of multimodal generators (e.g.,

DALL ·E 2, Imagen, and Sora), it became possible to create falsified content in several media channels simultaneously [145].

In the context of information warfare, deepfakes have two key application scenarios [146]:

1. Discrediting political figures and public leaders—creating false videos with statements or actions that did not occur.
2. Substitution of evidence: falsification of photo and video evidence used in the media and court proceedings.

Examples of this kind have been recorded in a number of countries. In 2019, a deepfake depicting Gabonese President Ali Bongo was distributed on Facebook and Twitter, which caused a political crisis and an attempted military coup [147]. In 2020, during the US elections, there were cases of using altered videos to discredit candidates [148]. Westerlund's research [149] points out that as generation algorithms develop, the risk of "invisible interference" in political processes through the mass production of synthetic materials increases.

The problem is exacerbated by the fact that the availability of generation tools has increased dramatically: the DeepFaceLab and the FaceSwap libraries, and cloud-based AI platforms enable deepfake creation without deep technical expertise [150]. At the same time, anti-detection methods are developing—including adding noise-like artifacts or using adaptive frame generation to bypass detection algorithms [151].

In terms of countermeasures, academic and corporate labs are developing methods for automatic detection of deepfakes based on analysis of facial microexpressions, blink rate discrepancies, lip movement patterns, and compression artifacts [152]. However, as Verdoliva [153] and Korshunov and Marcel [154] note, in the context of an "arms race", the accuracy of such methods decreases as new generative models appear. Organizations such as Europol and the UN view deepfakes as a threat to information security and public trust [155]. Europol's Facing Reality? (2022) report proposes including synthetic media in the list of priority threats to cyberspace. In 2023, the European Parliament began discussing legislation on labeling AI-generated content [156]. Deepfakes and synthetic media are therefore becoming an increasingly important element of the information warfare arsenal. Their danger lies in their ability to rapidly erode trust in visual and audio evidence, which undermines the basis of public consensus and makes rapid verification during crises nearly impossible.

4.4. Memetic Weapons and Infooperations in Social Networks

The term "memetic weapon" traces back to the concept of the meme proposed by R. Dawkins in the book "The Selfish Gene" (1976), where the meme is described as a unit of cultural information transmitted through imitation and communication [157]. In contemporary contexts, memes have become not only an object of study for cultural scientists, but also a tool for targeted information influence. In the context of information warfare, memetic weapons are understood as visual, textual, or audiovisual cultural artifacts created and distributed with the aim of changing the perceptions, beliefs or behaviors of target audiences [158].

Social networks have radically increased the potential of memetic communication due to the high speed of replication, algorithmic adjustment of news feeds and a low threshold for user participation [159]. Memes in the digital environment have several strategic properties [160]:

- Virality—the ability to spread exponentially in network structures.
- Brevity and density—the transmission of complex meanings in a minimal form.
- Emotional intensity—using humor, sarcasm, or outrage to enhance the response.
- Mimicry of "folk art"—which makes them difficult to attribute.

Within the framework of information operations, memes perform the following functions [161]:

- Cognitive contagion—introducing simplified and emotionally charged narratives that replace complex discussions.
- Discrediting the enemy—forming a negative image through an ironic or grotesque image.
- Signaling belonging—marking "us" and "them" in online communities.
- Triggering—activating certain reactions upon repeated contact with the meme.

Empirical studies show that memetic campaigns are often part of broader coordinated information operations. For example, Johnson et al. [162] analyzed Twitter activity during the 2016 US presidential election and identified network clusters that distributed political memes in conjunction with botnets. In [163] demonstrated that memes were used to increase polarization in Europe, with platform algorithms facilitating "echo chambers."

Memes play a special role in crisis and conflict situations. For example, during the conflict in eastern Ukraine, when visual jokes and caricatures become a tool for both mobilizing supporters and demoralizing opponents [164]. A study by Ylä-Anttila [165] shows that political memes on Facebook during campaigns can form stable emotional frames, shaping long-term perceptions of events.

The effectiveness of memetic weapons is due to cognitive mechanisms: ease of memorization, emotional coloring, conformity, and the effect of repetition [166]. These same mechanisms make counteraction difficult—memes quickly adapt, reformat, and integrate into new contexts.

Countermeasures include:

- automated meme detection using computer vision and contextual analysis [167];
- proactive creation of countermemes and positive narratives [168];
- media literacy and critical thinking as long-term protection [169].

However, as Phillips notes [170], excessive censorship of memes can be perceived as a restriction of freedom of expression, which in itself can become an object of information manipulation.

Thus, memetic weapons are an effective but difficult to control tool of information warfare, highly adaptable and able to penetrate the collective consciousness through everyday communication on social networks.

4.5. Geopolitical Cases

Analyses of the 2016 U.S. presidential election document systemic disinformation and coordinated operations using bots, targeted advertising, and memetic formats. Howard, Woolley, and Calo (JITP, 2018) [171] describe computational propaganda and challenges to voting rights; the DiResta (Tactics & Tropes) [172] team report and SSCI materials document IRA activities aimed at polarization and targeting vulnerable groups. The resulting estimates show uneven exposure and the contribution of small "superconsuming" cohorts, while simply increasing advertising transparency without cognitive prevention has limited impact [173–175]. In the European Union, information attacks are considered part of hybrid threats: the East StratCom Task Force maintains a case database (EUvsDisinfo), and the Joint Communication JOIN/2020/8 sets the framework for countering COVID-19 disinformation (rapid fact-checking, cooperation with platforms, and transparency). In parallel, "digital diplomacy against propaganda" is developing (Bjola and Pamment), but the constant dilemma is the balance with human rights protections [176–178]. Since 2014, information operations in Ukraine have been integrated with military actions; after 24 February 2022, there has been an increase in multilingual campaigns, deepfakes, operations on Telegram, and synchronization with cyberattacks. International studies document both state and civilian practices of digital resilience, OSINT and counter-memetic campaigns.

Current analytical reviews (Chatham House, Atlantic Council/DFRLab) and academic literature (International Affairs) converge in their assessment: the key factors are speed, cross-platform and narrative localization [179–182].

In East Asia, China's 'cognitive war' against Taiwan remains the most systemic. It combines psychological, legal, and "public opinion warfare" (the so-called "Three Warfares"). And manifests itself in electoral cycles through the fabrication of narratives, exploitation of vulnerabilities in the media environment, and the long-term "wear and tear" of trust in institutions [183–185].

In parallel, Hong Kong 2019–2020 has become a field of intense two-way struggle over meaning: studies document how "fakes" and rumors simultaneously served to delegitimize the protest and mobilize it, increasing polarization and networked forms of leadership [186].

In Southeast Asia, the most tragic case is Myanmar, where algorithmically amplified extremist speech and disinformation on Facebook were woven into a violent campaign against the Rohingya; academic works suggest moving away from the reduction to "hate speech" to the analysis of institutional and platform mechanisms of escalation [187,188]. The Philippines demonstrates a "production" model of online disinformation. In 2016, digital fan communities and informal "influencer" brokerage networks amplified the effect of offline mobilization of Duterte supporters. And in 2022, persistent narratives of "authoritarian nostalgia" and conspiracy theories contributed to the electoral dynamics, with the audience participating in the "co-production" of disinformation [189,190].

In South Asia, India has become a laboratory for "encrypted" information warfare: mass political communication via WhatsApp in the 2019 election campaign created opaque channels for the circulation of statements that are poorly amenable to platform moderation control. Empirical studies show that "tiplines" (crowdsourced lines for receiving suspicious content) allow for early detection of viral messages and reconstruction of cross-platform flows, while open social networks only partially reflect what is happening in end-to-end (E2E) environments [191,192].

In the multicultural and multilingual context of Kazakhstan, resilience relies on institutional measures of cybersecurity and information policy. The basic framework is set by the Cybersecurity Concept "Cyber Shield of Kazakhstan" (Government Resolution No. 407 of 30 June 2017) and subsequent initiatives; ITU confirms the launch and implementation of the concept. Academic publications analyze vulnerabilities and lessons from the pandemic period for information security. Practice shows that during crises, the share of disinformation through social networks and instant messengers increases—both technical monitoring measures and media literacy programs are required [193–195]. Taiwan demonstrates a model of "civic digital resilience": a collaborative effort between the state, the civic tech community, and fact-checking. Research documents persistent attacks from the Chinese side, especially during electoral periods; at the same time, academic and applied works describe institutional and civic responses, ranging from co-fact-checking to preventive communication and educational programs [185,196,197].

Thus, the forms of information warfare are already very diverse. However, there is every reason to believe that they will evolve further. As shown in the next section, there are tools that allow influencing the basis of the mentality of the population of any state—its sociocultural code.

5. Impact on the Sociocultural Code: Theory and Practice

The sociocultural code (in the literature, similar concepts such as "mentality", "civilizational code", etc., were also often used earlier) is a set of values, norms, symbols, historical narratives, and collective ideas that shape the identity of a society. In the context of an information war, attacks on this code become a strategic tool that can weaken internal cohesion,

undermine trust in historical heritage and transform the system of value orientations. Such influences can be direct—through the distortion of historical facts and the imposition of alternative interpretations of events—or indirect, including the gradual erosion of cultural constants through mass culture, media, and educational practices. Modern information campaigns, based on the achievements of cognitive psychology, linguistics, and digital technologies, are capable of deliberately modifying the symbolic space of a nation, altering both external image perception and internal self-identification processes. This section is devoted to the theoretical understanding of the phenomenon of the sociocultural code, the analysis of the mechanisms of its undermining and the consideration of practical examples of both successful attacks and effective defense strategies.

In studies of information security and cultural studies, the term "sociocultural code" is used to denote a set of stable symbols, values, norms, and narratives that structure the perception of the world by a particular community [198]. These elements act as a kind of "matrix" of collective identity, ensuring the continuity of historical experience and certain behavioral patterns. The structure of the sociocultural code includes linguistic forms, myths and historical narratives, cultural rituals, symbols, and value orientations, which together create the basis for social interaction and political mobilization [199]. Information warfare, considered as a set of targeted impacts on the cognitive, emotional and behavioral spheres of society, is increasingly focused on attacks on the sociocultural code, and not just on operational disinformation. This approach is associated with the understanding that the destruction or modification of cultural meanings has more long-term consequences than short-term manipulation of facts [200]. The impact on the cultural code can be direct, for example, by substituting historical interpretations or the discrediting of national symbols, or indirect—through the gradual introduction of alternative value models and changes in the usual linguistic field [201].

The mechanisms of identity fragmentation used in information operations are often built on opposing groups within a single society. Segmentation of the cultural field along ethnic, religious, regional, or political lines leads to a weakening of the common identity and an increase in the potential for conflict [202]. This process actively uses emotional triggers associated with traumatic historical events or social injustices, which allows operators of information attacks to activate "latent" lines of cleavage [203].

One of the key areas of cultural demobilization is the undermining of trust in national history and memory. Through the systematic dissemination of revisionist interpretations and selective coverage of historical facts, a feeling is formed that the past is subject to manipulation and cannot serve as a source of collective meaning [204]. Similar strategies are observed, for example, in a number of post-Soviet countries, where media content deliberately downplayed the role of national figures or, by contrast, focused on collaborationist episodes, creating a sense of "historical guilt" [205].

The cognitive and symbolic aspects of the transformation of the cultural code manifest in changing the meanings of established symbols and concepts. This process is often accompanied by a semiotic "reversal" of symbols—in which positive cultural markers are redefined as negative, and vice versa. Visual images traditionally associated with national pride or spiritual values can be reinterpreted in a satirical or derogatory way, which reduces their mobilization potential [206]. Similar processes occur in language: keywords and phrases acquire new connotations that can transform public discourse without an obvious change in the facts [207]. The protection of cultural constants in the context of information warfare presupposes a set of measures that include both institutional and public initiatives. Key elements include the support and development of the national language, the preservation and popularization of historical memory, and the formation of positive narratives reflecting the values and traditions of society [208]. Educational

programs that promote critical perception of information and strengthen cultural identity among young people play an important role [209]. At the same time, modern approaches require a synthesis of humanistic and technological solutions: from digital archives and interactive museum exhibits to automated systems to monitor and analyze information attacks on the cultural space [210]. Practice shows that an attack on the sociocultural code is as dangerous as physical intervention or economic pressure. Changing basic cultural guidelines can radically transform the political behavior of the population, change the perception of the legitimacy of power, and even influence international alliances. Therefore, the protection of cultural constants should be treated as a national-security priority in the context of a globalized information space [211].

5.1. The Concept and Structure of the Sociocultural Code

In the humanities and social sciences, the concept of a "sociocultural code" is used to denote a set of symbolic systems, norms, values, customs, and semiotic structures that ensure the reproduction of the cultural identity of a society and the integration of its members into a common system of meanings [212]. This code acts as a kind of "matrix" of collective thinking and behavior, determining how individuals interpret the surrounding reality, react to external events, and interact with each other. In cultural studies and semiotics, a sociocultural code is interpreted as a multilevel semiotic system that includes linguistic, visual, behavioral, and institutional elements [213]. Yu. M. Lotman, in his theory of the semiosphere, described culture as a "mechanism that creates and transmits texts," in which codes are the rules for generating and interpreting these texts [214]. In the anthropological perspective (Clifford Geertz, Pierre Bourdieu), the cultural code is considered a set of "perceptual patterns" and "fields of practice" that structure social interaction [215,216].

Modern studies (Hofstede; Schwartz) clarify that the sociocultural code includes both explicit components (language, official symbols, laws) and latent ones (deep values, myths, collective memory) [217,218]. This makes it a complex and stable object, yet vulnerable to systemic influences.

According to Hofstede and Schwartz, the sociocultural code can be considered an integration of several interconnected subsystems:

1. Language code—a system of natural language, including vocabulary, syntax, idioms, speech practices. Language not only conveys information but also structures thinking (Sapir-Whorf hypothesis) [219].
2. Value-normative code—a set of moral and ethical principles, norms of behavior and social expectations that define what is acceptable and unacceptable [220].
3. Symbolic code—national and cultural symbols (flag, coat of arms, rituals, architecture) that serve as markers of identity [221].
4. Historical-narrative code—collective ideas about the past, historical myths, heroic figures, traumatic events that shape national memory [222].
5. Social-institutional code—the structure of social institutions (family, education, religion, state), which consolidates and transmits cultural norms [223].

Each of these elements has its own system of protection against changes but can be modified by targeted information impact.

In the context of information warfare, the sociocultural code is considered both a strategic resource and a vulnerability. Changes in its individual elements can lead to a transformation of collective identity, political loyalty, and even to readiness for mobilization [224]. For example, the substitution of a historical narrative or redefinition of symbolic meanings can provoke a split in society or a decrease in resistance to external pressure [225].

An analysis of conflicts of the last decade (Ukraine, Syria, Hong Kong) shows that the impact on the sociocultural code is often carried out through media campaigns, educational programs, cultural products, and social networks [226,227]. These channels enable the combination of soft forms of influence (soft power) with elements of cognitive operations (see Section 3.5), creating the effect of "long-term penetration" into the cultural fabric of society.

One of the key characteristics of the sociocultural code is its dynamic stability. Research shows that codes can adapt to external challenges while maintaining their core values [228]. However, under a massive and multichannel attack—especially using digital technologies and algorithmic targeting—this resilience declines [229]. The platform architecture of social media, operating on the basis of the "attention economy" (see Section 3.4), facilitates the consolidation of new meanings through repetition and emotional reinforcement [230]. Thus, understanding the structure and functions of the sociocultural code is a prerequisite for developing strategies to protect it in the context of modern information warfare.

Note that the above interpretations of the sociocultural code are primarily descriptive. In [231,232], a neural network theory of the noosphere proposes, which allows us to reveal the mechanisms of formation of the sociocultural code at a level that allows for the interpretation of its evolution. Note that according to Vernadsky, the noosphere is understood as the Earth's shell, arising because of the collective activity of Homo sapience [233].

This interpretation of the sociocultural code is based on the following considerations. It is generally accepted that as a result of communicating with each other, people exchange information. This, however, is a rather rough approximation. In reality, any communication between people de facto comes down to the exchange of signals between the neurons that make up their brains. Thus, a collective neural network arises, which at the global level, can be identified with the noosphere, as understood by V.I. Vernadsky. Qualitative differences in such a global network from the totality of its individual fragments are demonstrated in rigorous mathematical models.

It is appropriate to emphasize that recent theories have been proposed based on arguments from the field of physics, which in a similar way consider the Universe by analogy with a neural network [234]. The conclusions made in the cited report are based on the results obtained in the field of the general theory of evolution [235,236]. Vanchurin's concept [234] clearly is consistent with the conclusions obtained in other fields of knowledge, where it was shown that complex systems of the most diverse nature can be modeled as neural networks, and it is this factor that determines their behavior [237–239].

The neural network interpretation of the noosphere allows us to assert that, along with the personal level, there is also a suprapersonal level of information processing [240,241]. Indeed, as shown, in particular, in [242] at the level of a correct mathematical model, the ability of a neural network to store and process information nonlinearly depends on the number of its elements. This conclusion is confirmed by current practice—otherwise, it would not make sense to create increasingly larger artificial neural networks, as is the case in practice [243,244]. Consequently, if interpersonal communications generate a global (albeit fragmented) neural network, its properties cannot be reduced to the properties of individual elements, i.e., relatively independent fragments of such a network, localized within individual brains. In philosophical literature, a similar conclusion has long been formulated: "social consciousness cannot be reduced to the consciousness of individuals". The conclusion about the existence of the suprapersonal level also allows us to reveal the essence of the collective unconscious, the existence of which was previously confirmed only on an empirical basis [245,246].

From the perspective of the neural network interpretation of the noosphere, the collective unconscious is formed by objects developing precisely at the suprapersonal

level of information processing. Information objects formed at the suprapersonal level of information processing can have a very different nature, and a significant part of them are obviously associated with the category of fashion. This can be most clearly traced based on the conclusions made in the famous monograph by Baudrillard [247]. In the cited monograph, it was convincingly shown that the cost of many goods presented on the market actually consists of two components. One of them is associated with the satisfaction of current human needs (including physiological ones). The other is symbolic and therefore, informational in nature. An obvious example: clothes should protect a person from the cold, but there are also branded clothes, the main purpose of which is to demonstrate the social status of the owner. The same can be said in relation to goods of many other groups (branded watches, cars, etc.)

As shown in [248], mature scientific theories, natural languages, and other systems. are also considered suprapersonal information objects. A sociocultural code, which is a set of supra-personal information objects that determine the characteristics of the collective behavior of the population of a certain country, ethnic group, is also formed by a similar mechanism.

5.2. Information Warfare as an Attack on Cultural and Historical Meanings

Cultural and historical meanings form the foundation of collective identity, ensuring continuity between the past, present, and future of society. In the humanities, cultural meanings are understood as a set of symbolic contents encoded in language, art, religious, and social rituals, as well as in collective narratives that form images of the desirable and the unacceptable [249]. Historical meanings, in turn, represent interpretations of key events of the past, anchored in the memory of society through official chronicles, educational programs, commemorative dates, and material artifacts [250]. Information warfare in their modern understanding consider these meanings not merely as a context in which the struggle is waged, but as targets of influence. Since a change in the interpretation of the past or a redefinition of cultural markers can transform the value orientations of the population and thereby change its political and social behavior [251]. In political communication and conflict studies, scholars argue that the struggle for meaning is a struggle for power over the perception of reality [252]. M. Foucault pointed out that power operates through control over discourse, which determines what is considered truth and what is subject to oblivion [253]. In the context of information warfare, this means that strategic influence is aimed not so much at facts as at their interpretation and symbolic framing.

Modern doctrines of cognitive operations (see Section 3.5) consider cultural and historical meanings as key points of application of efforts, since they underlie “frames”—cognitive structures through which people comprehend information [254]. Altering frames can radically change social attitudes without direct coercion, which makes this approach extremely attractive to strategic actors.

One of the most common methods of attack is rewriting history, in which an alternative version of key events is promoted through textbooks, documentaries, popular media, and Internet resources [255]. This may involve both emphasizing certain aspects and completely excluding inconvenient facts from public discourse.

Another method is the redefinition of symbols. Flags, monuments, and national heroes can be reinterpreted—from the glorification of previously marginalized figures to the demonization of historical leaders [256]. This strategy is often accompanied by visual campaigns on social media, memetic content, and hashtag actions aimed at mass user engagement [257].

Discursive inversion is also used, in which key concepts of national identity (e.g., “freedom”, “independence”, “tradition”) are filled with opposite or distorted content [258].

A study by Ross shows how a new historical narrative was formed in post-revolutionary France through educational reforms and popular culture [259]. In more modern examples, the analysis of the Ukrainian crisis of 2014–2022 demonstrates that both sides in the conflict actively use the media to reinforce their own interpretations of events and discredit the opposing ones [260]. In the Baltic countries, over the past three decades, programs have been implemented to reinterpret the Soviet period, which have been accompanied by the dismantling of monuments and the changing of street names [261]. In Syria and Iraq, the actions of terrorist organizations such as ISIS have included the targeted destruction of cultural artifacts, which was aimed at breaking cultural continuity and undermining the identity of local communities [262].

The digitalization of the information space has radically increased the scale and speed of attacks on cultural and historical meanings. Social media and video-hosting sites allow instant distribution of content in which cultural symbols are reinterpreted through visual and auditory forms [263]. Algorithmic recommendation mechanisms amplify the impact by creating a selective reality for users, in which certain versions of the past become dominant [264].

In addition, an analysis of algorithmic campaigns on Twitter and Facebook (2016–2020) shows that a significant portion of the coordinated operations include culturally loaded messages—from nationalist slogans to posts about controversial historical dates [265].

Effective protection of cultural and historical meanings requires the integration of measures into educational, cultural, and information policies. This includes transparency of historical sources, multidisciplinary examination of educational materials, the development of digital media literacy, and the involvement of society in the discussion of cultural heritage [266]. Of particular importance is the creation of positive narratives that strengthen identity and not just respond to external attacks [267].

Thus, information warfare in the 21st century is increasingly taking place on the battlefield of cultural and historical meanings. Success in this struggle depends not only on control over information channels, but also on the ability to protect and develop the system of meanings that underlies the collective “we”.

5.3. Mechanisms of Identity Fragmentation and Cultural Demobilization

Identity fragmentation in the context of information warfare is a process of blurring, splitting, and redefining collective ideas about belonging to a particular social, cultural or national group. This process is not limited to the diversity of cultural forms that naturally arises in a globalized world. It involves targeted information- and communication-based efforts aimed at undermining shared value orientations, symbols, and narratives that ensure the unity of society [268].

Cultural demobilization is a closely related phenomenon in which a community loses its willingness to protect and reproduce its cultural codes and becomes passive in maintaining and transmitting them. As Castells notes, the modern communications network creates opportunities for the atomization of groups and individuals, which in a political context reduces the ability of society to consolidate around common goals [269].

One of the key psychological mechanisms of identity fragmentation is cognitive dissonance, which occurs as a result of exposure to contradictory and mutually exclusive narratives [270]. When an individual is confronted with competing interpretations of events, he or she may lose confidence in the validity of any of them, which undermines the sense of belonging to a group with a clearly articulated position.

Another factor is social categorization [271]. In the context of information warfare, the boundaries between “us” and “them” are deliberately blurred or redrawn, which leads to the formation of new subgroups with competing identities within the formerly single community.

Framing and priming effects have an additional impact: the constant repetition of certain associations and interpretations of cultural symbols changes how the audience perceives their cultural and historical belonging [272].

From a sociological perspective, identity fragmentation is based on network segmentation—a process in which digital platforms form closed communication clusters ("echo chambers") where messages of homogeneous content circulate [273]. This leads to a decrease in mutual understanding between groups and an increase in intergroup hostility [274].

Platform algorithms optimized to maximize engagement contribute to the fact that the user sees predominantly content that corresponds to his already established beliefs, which accelerates the polarization and fragmentation of the cultural space [275].

Media also play a role in the creation of competing narrative centers. In conditions of media pluralism, these centers can exist naturally, but in a situation of information confrontation, their emergence is often the result of targeted work by external actors seeking to weaken the dominant identity [276].

Modern technologies enable personalized propaganda in which messages are individually selected based on analysis of a user's digital footprint [277]. This enhances the fragmentation effect, as different groups receive fundamentally different versions of reality.

Additionally, memetic campaigns become a tool for "infiltrating" alternative meanings into popular culture. Memes, images, and slogans, often devoid of obvious political overtones, can eventually become markers of subcultural identities opposed to the official one [278–281].

Cultural demobilization often becomes the target result of information operations. This state is characterized by a decrease in participation in cultural practices, a refusal to protect cultural symbols, and a passive attitude towards their transformation. As the analysis of Qureshi (2021) shows, such effects arise not only due to direct pressure, but also due to "fatigue" from constant conflicts in the media space [282].

Information campaigns that create a constant feeling of uncertainty and mistrust contribute to apathy and loss of interest in collective action, which weakens society's resilience to external challenges [283].

Modern research suggests using a comprehensive approach to monitoring identity fragmentation, including analysis of discursive fields in social media, tracking changes in the popularity of cultural symbols, and assessment the level of trust in national institutions [284].

Psychometric methods make it possible to identify a decrease in the sense of belonging to a national community, while sociotechnical indicators record an increase in the number of information clusters that are inconsistent with each other [285].

Taken together, these methods make it possible not only to diagnose identity fragmentation, but also to assess the effectiveness of counteraction strategies.

6. Methods of Countering Information Attacks

The growing scale and complexity of information threats require the development of comprehensive and multilevel countermeasure strategies. Unlike reactive measures of the past, modern approaches rely on preventive preparation of society, algorithmic tools to detect and block malicious content, and the formation of sustainable cognitive and cultural barriers to manipulation. Effective protection is based on a combination of media literacy, independent fact-checking, the implementation of architectural and algorithmic solutions at the level of digital platforms, international regulation, and the use of specialized technical tools for authentication and tracking the origin of information. Of particular importance are interdisciplinary approaches that combine the capabilities of computer science, psychology, linguistics, law, and international relations. This section systematizes key practices and

technological approaches that prove effective in the context of modern information warfare and considers prospects for their further improvement.

6.1. Fact-Checking and De-Banking

Fact-checking is a systematic activity aimed at identifying, verifying, and refuting false information in public discourse. It was initially developed in journalistic practice as a tool for improving the quality of news content and ensuring audience trust in the media [286]. However, in the context of modern information warfare, fact-checking has acquired strategic importance, becoming one of the key forms of information defense. Along with it, debunking is actively used—the process of exposing false statements by providing contextual data and evidence of inconsistency [287]. Historically, fact-checking practices are rooted in the editorial standards of print journalism of the 20th century. However, their institutionalization as a separate direction began in the early 21st century against the backdrop of the growth of Internet journalism and social networks, which accelerated the circulation of unverified information [288]. Some of the pioneers in this area were the organizations FactCheck.org (founded in 2003) and PolitiFact (2007), which set standards for the transparency of sources, verification procedures, and public presentation of results [289].

In the context of information warfare, fact-checking performs a dual function: on the one hand, it is a tool for protecting public discourse from disinformation, and on the other, it serves as a mechanism for strengthening critical thinking and media literacy of the population [290]. Research shows that systematic fact-checking helps reduce trust in false narratives and curb their dissemination on social media [291].

In the modern media space, there are two dominant models of organizing fact-checking: institutional and independent. The first is integrated into large media outlets, government agencies, or international organizations that have the resources to conduct large-scale investigations [292]. Some examples include BBC Reality Check and AFP Fact Check, which operate globally. The independent model is represented by nonprofit organizations and civic initiatives financed by grants, donations, and crowdfunding [293]. These include Bellingcat, StopFake, The Poynter Institute, which specialize in specific topics—from military conflicts to environmental information. Such organizations often have greater flexibility and can respond quickly to local information attacks. Both models face the problem of trust: critics argue that institutional projects can be subject to political or corporate interests, while independent initiatives run the risk of limited resources and a possible lack of formalized methodological standards [294].

The development of digital technologies has led to the emergence of automated fact-checking systems that use natural language processing (NLP), machine learning, and computer vision [295]. Platforms such as ClaimReview and Full Fact integrate algorithms for verifying claims in real time, which help reduce the time lag between the emergence of false information and its refutation [296].

In the context of an information warfare, OSINT (Open Source Intelligence) tools play an important role, allow analysis of open sources, verify photos and videos, identify manipulations with images, and determine the geolocation of events [297]. Such methods are actively used in investigations of war crimes and information operations, as shown by cases in Syria and Ukraine [298].

Debunking differs from simple fact-checking in that it involves not only identifying the unreliability of a claim but also explaining the mechanisms of manipulation underlying it [299]. Psychological research shows that simple refutation often does not lead to a change in beliefs, especially if the false information corresponds to the value orientations of the au-

dience [300]. Therefore, effective debunking includes an emotionally neutral presentation, the use of authoritative sources, and the demonstration of logical contradictions [301].

One promising approach is prebunking—a preventive refutation in which the audience is familiarized with typical disinformation techniques in advance, which form cognitive "immunity" [302]. Experiments conducted within the framework of the "Inoculation Theory" project (van der Linden et al.) show that prior information about the manipulative techniques used reduces their effectiveness [303].

Despite its effectiveness, fact-checking faces a number of limitations. First, a significant portion of false messages are distributed in closed digital ecosystems that are inaccessible to public monitoring [304]. Second, debunking often spreads more slowly than misinformation and has a smaller viral effect [305]. Third, there is a backfire effect, whereby audiences exposed to debunking becomes more convinced of their beliefs [306].

Furthermore, in polarized societies, fact-checking can be interpreted as political censorship, undermining trust in the fact-checking organizations themselves [307]. This necessitates high transparency in methodology and sources, as well as independent auditing of the work of fact-checking organizations [308].

Research on the effectiveness of fact-checking shows mixed results. A meta-analysis by Nyhan and Reifler (2020) shows that short-term reductions in belief in falsehoods are relatively easy to achieve, but long-term effects require repeated and systematic interventions [309]. The "CrossCheck" initiative, launched during the 2017 French elections, shows that coordinated work between media and technology companies can significantly reduce the level of disinformation in the public space [310]. Thus, fact-checking and debunking are important elements of the system for countering information warfare, but require constant improvement of methodology, implementation of technological innovations and strengthening of public trust.

6.2. Prebunking (Inoculation) and Cognitive Defense

Prebunking, also called cognitive inoculation, is a strategy for countering disinformation in which audiences are provided with advanced information about potential manipulative techniques and false narratives before they are exposed to them in real-world contexts [311]. This approach borrows metaphorically from the principles of biological vaccination: just as a vaccine introduces a weakened pathogen to build immunity, cognitive inoculation "inoculates" a person with knowledge of manipulation, building resistance to it [312]. Inoculation theory was proposed by William McGuire in the early 1960s [313] and was originally used in social psychology to study resistance to persuasion. It suggests that pre-exposure to weak versions of an argument, together with their refutation, stimulates the development of cognitive "defense" mechanisms. Later studies adapt this approach to the contemporary media environment and show its high effectiveness in combating online disinformation [314].

In the context of information warfare, prebunking plays a special role, as it shifts the focus from reactive measures (debunking) to proactive ones, reducing the vulnerability of the target audience even before an information attack begins [315].

Modern prebunking programs are implemented in several formats:

1. Educational campaigns—short-term courses, videos, and infographics that introduce users to manipulation techniques such as emotional triggers, false dichotomy, substitution of sources, fabrication of evidence [316].
2. Game simulations—interactive games such as "Bad News Game" or "Go Viral!", developed at the University of Cambridge, which allow users to "be in the role" of the creator of disinformation, thereby mastering the mechanisms of its production and protection from it [317].

3. Integration into platforms—social networks and search engines now integrate prebunking elements into their interfaces, e.g., through notifications about checking sources or warnings about manipulative content [318].

Empirical studies demonstrate that even short-term interaction with prebunking materials increases users' ability to recognize manipulative techniques by 20–30%, and the effect can persist for several weeks [319].

The effectiveness of prebunking relies on several key cognitive mechanisms:

- Metacognition—increased awareness of one's own processes of information perception and critical analysis [320].
- Epistemic vigilance—the ability to assess the reliability of an information source and the internal consistency of argumentation [321].
- Cognitive load—the ability to distribute attention between several information streams, reducing susceptibility to manipulative messages [322].

It is important that the "information vaccine" be dosed: an excessive number of examples of false information can cause the opposite effect—an increase in cynicism and distrust toward all sources [323].

Despite the obvious advantages, prebunking has several limitations. First, it requires an accurate prediction of which narratives will be used by the enemy, which is not always possible [324]. Second, its effectiveness decreases if the audience has already been subjected to deep cognitive polarization [325]. Third, in multicultural societies, it is necessary to adapt prebunking materials to cultural codes and local contexts to avoid misunderstanding or rejection [326].

In strategic terms, prebunking can be considered an element of a broader concept of cognitive resilience, which includes media literacy, critical thinking, and social trust [327]. Its integration into national educational systems, as well as into mechanisms of international cooperation through NATO, the EU, and the UN, is seen as a promising avenue for protection against transnational information threats [328].

6.3. Algorithmic and Architectural Measures of Platforms

Algorithmic and architectural measures are a key layer of defense for digital platforms against the spread of disinformation and other forms of information attacks. These measures cover both the design of the platform itself—its interfaces, data structures, content moderation, and ranking mechanisms—and the use of algorithmic systems, including machine learning and artificial intelligence, to automatically detect and neutralize malicious information flows [329].

The architecture of a digital platform largely determines the speed and scale at which disinformation spreads. Research shows that the presence of instant repost functions, personalized recommendation algorithms, and weak integration of source verification mechanisms amplify the effect of "information cascades" [330]. Platforms whose architecture focuses on maximizing engagement (engagement-driven design) often inadvertently create an environment favorable for the viral spread of false narratives [331]. In response, major social media platforms implement architectural restrictions to slow the spread of unverified content. For example, Twitter (now X) tested a limit on retweets without comments, and WhatsApp tested a limit on forwarding messages to groups [332]. These measures demonstrate that architectural design can be used as a tool to deter information attacks.

Machine learning has become a central element in the fight against disinformation. Modern algorithms can analyze millions of pieces of content in real time, classifying them by their credibility, sentiment, source, and style [333]. The most common approaches include:

- Natural language processing (NLP) models trained on labeled corpora of fake and credible news [334].

- Graph models to detect coordinated networks and anomalous account activity [335].
- Computer vision to detect deepfakes and manipulations in images and videos [336].

The effectiveness of algorithms largely depends on the quality of the training data. Having multicultural and multilingual datasets are critical for global platforms, as localized disinformation often uses unique cultural and linguistic codes [337].

A recent trend is to integrate algorithmic solutions directly into the architecture of platforms. For example, automatic fact-checking algorithms can be built into the post-publishing interface, warning the author about potentially inaccurate information before publication [338]. YouTube has integrated algorithms for recognizing and removing malicious videos into the content upload chain, which allows them to be blocked before they become publicly available [339].

Despite their obvious advantages, algorithmic and architectural measures have limitations. First, they are prone to errors—both false positives and false negatives [340]. Second, the closed nature of algorithms and the lack of transparency in platform architectures have drawn criticism from researchers and human rights organizations, pointing to the risks of censorship and manipulation of algorithms for political purposes [341]. Third, attackers adapt to algorithms using content obfuscation, memetic forms, and coded messages [342].

Empirical evidence suggests that a combination of architectural constraints and algorithmic moderation can significantly reduce the rate at which disinformation spreads. For example, a study by Mosseri et al. (2022) finds that algorithmic deactivation of the top 0.1% of disinformation nodes in a network reduces the overall volume of false content by 25% within one week [343]. However, long-term sustainability of such measures requires continuous algorithmic updates and adaptation of architectural solutions [344].

The future of algorithmic and architectural measures lies in the development of explainable AI (XAI), which will increase the transparency of decisions to block or flag content [345], and the introduction of decentralized architectures that provide information verification based on blockchain technologies [346]. In addition, platforms are increasingly considering the integration of "information encryption layers"—systems that allow the verification of the origin of content using metadata and digital signatures [347].

6.4. Identifying and Neutralizing Coordinated Networks

Coordinated Inauthentic Behavior (CIB) is the concerted action of a group of interconnected accounts or digital entities aimed at manipulating public opinion, undermining trust in institutions, and spreading particular narratives [348]. Such networks can include fully automated bots, "semi-automated" accounts operated by humans (cyborg accounts), and real user profiles engaged in a campaign through covert coordination [349]. The nature of CIB is that each individual node in the network may appear legitimate, but the overall pattern of interactions indicates artificial and directed behavior. The network approach to studying CIB relies on social graph models, in which nodes represent accounts and edges represent interactions between them (likes, reposts, mentions, and replies) [350]. In the theory of complex networks, such structures often have characteristic topological features: increased clustering, abnormally high density of connections within subgroups, synchronicity of activity, and similarity of content patterns [351]. Research on the dynamics of information flows shows that coordinated networks form "information resonances"—periods of synchronous publications timed to certain events or news items [352].

Modern methods for detecting CIB can be divided into several categories:

1. Social network analysis. This approach uses centrality metrics (degree centrality, betweenness centrality), community detection and graph density analysis to identify abnormally connected clusters [353].

2. Temporal activity analysis. Coordinated campaigns are often characterized by synchronous publications, so detection algorithms use correlation of time series of account activity [354].
3. Content analysis. Natural language processing (NLP) methods can detect high lexical and syntactic similarities between posts, which may indicate the use of templates or a centralized script [355].
4. Multimodal analysis. Combining behavioral, network, and content features yields the highest accuracy in detecting CIB, especially when using deep neural network architectures [356].

Many platforms and research groups are implementing machine learning algorithms to automatically detect instances of CIB. Popular architectures include Graph Neural Networks (GNNs), which can model complex dependencies between nodes and reveal hidden coordination structures [357]. Additionally, temporal clustering methods and anomaly detectors based on autoencoder models are used [358]. An interesting example is the "Hamilton 68" project (Alliance for Securing Democracy), which tracked Russian-language bot farms on Twitter, identifying synchronous bursts of activity and characteristic content markers [359].

In 2018, Facebook publicly disclosed for the first time a large-scale CIB network linked to the Internet Research Agency in Russia [360]. Analysis shows that the network of hundreds of pages and accounts operated in multiple language segments and was coordinated through closed admin groups.

In 2020, Twitter and Facebook jointly blocked a network allegedly linked to Iran that used fake media brands to advance political narratives in the US and Europe [361].

During the COVID-19 pandemic, coordinated anti-vaccine campaigns have been recorded, using bots and real accounts to amplify narratives about the "dangers of vaccination" [362].

Neutralization of CIB includes both technical and organizational measures [363]:

- removal or blocking of identified network nodes;
- deactivation of the management infrastructure (e.g., closed admin groups);
- notification of users who interacted with malicious content;
- cooperation with government and international structures to exchange threat data.

An important area is preventive detection, when algorithms record early signs of coordination, allowing intervention before the campaign reaches its maximum reach [364].

Despite the successes in detecting CIB, serious problems remain: the high adaptability of networks that can change activity patterns to bypass algorithms; the difficulty of attributing campaigns to specific state or non-state actors; legal and ethical restrictions on mass monitoring of online activity [365].

In addition, there is a risk of false positives, in which active but legitimate communities are mistakenly classified as CIB, which can lead to a violation of freedom of expression [366].

The development of CIB detection methods is moving toward complex multilevel systems that combine behavioral analysis, NLP, computer vision, and network algorithms into a single architecture. A promising direction is the introduction of interactive platforms for OSINT analysis, where researchers and platforms can jointly track suspicious campaigns in real time [367].

6.5. Supporting Media Literacy and Digital Critical Thinking

Media literacy and digital critical thinking are increasingly considered in the scientific and political agenda as key elements of society's resilience to modern forms of information warfare. In conditions where the information environment is saturated with both reliable and manipulative messages, it is the individual's ability to critically evaluate sources, check

facts, and understand the mechanisms of disinformation and manipulation that becomes a barrier against information attacks [368]. In academic terms, media literacy includes not only technical skills to search and process information, but also cognitive skills for analyzing, interpreting, and critical understanding media messages [369]. According to UNESCO (2018), media literacy is "a set of competencies that enable citizens to receive, evaluate, use, create, and disseminate information and media content in various forms" [370]. Digital critical thinking, in turn, focuses on the ability to identify logical errors, cognitive distortions, and hidden narratives in digital communications. It is related to the concept of cognitive resilience, which implies the ability to resist information manipulation even in conditions of high emotional or social engagement [371].

Empirical studies in recent years have demonstrated a direct link between the level of media literacy and the likelihood of spreading fake news [372]. Thus, Gaillard et al. (2020) show that participants with a high level of source verification skills and knowledge of the basic principles of journalism are less likely to share disinformation materials on social media [373]. Similarly, a study by Roozenbeek and van der Linden (2019) show that short-term online games simulating strategies for spreading disinformation can increase users' resilience to fakes by activating the so-called "inoculation effect" [374].

Media literacy support can be implemented in several forms:

1. Formal education. Incorporating media literacy into school and university curricula is one of the most effective ways to develop critical thinking in the long term [375]. Finland and Estonia are often cited as examples of successful integration of media literacy into the national education system, which correlates with low levels of trust in disinformation sources [376].
2. Informal learning. Massive online courses (MOOCs), seminars and trainings run by NGOs, universities and media organizations make it possible to reach adult audiences who are not always involved in formal education [377].
3. Gaming and simulation methods. Projects such as the Bad News Game [374] and Harmony Square [378] show that interactive formats increase engagement and retention of material and also help participants better recognize manipulative techniques.

At the global level, an important coordinator of efforts to develop media literacy is UNESCO, which promotes the concept of "Media and Information Literacy" (MIL) [370]. Since 2018, the European Commission has implemented the "Digital Education Action Plan", which includes the development of media literacy and digital critical thinking as a priority for EU member states [379]. In the United States, Stanford History Education Group (SHEG) projects are underway aimed at developing critical assessment skills for digital content in schoolchildren and students [380].

Since 2020, pilot projects to introduce media literacy into the school curriculum have been implemented in Kazakhstan, with the support of the OSCE and local NGOs [381]. The main focus is on the ability to verify sources, recognize fake images, and analyze the context of publications.

A meta-analysis by Burkhardt [382] shows that most media literacy programs lead to a statistically significant improvement in information assessment skills, but the effect may be short-lived if knowledge is not constantly reinforced. Roozenbeek et al. [383] note that regular, recurring training provides higher resistance to manipulation than one-time educational events.

Key barriers to media literacy development include:

- Information overload—users may experience "fact-checking fatigue" in the face of a large information flow [384].
- Low level of digital infrastructure in some countries, which limits access to online learning resources [385].

- Cultural and language barriers that affect the adaptation of educational materials [386].
- Polarization of society, in which even factually accurate information may be rejected due to political identity [387].

In the future, approaches to media literacy will increasingly integrate with AI technologies. A possible direction is the creation of personalized training systems that adapt materials to a user's cognitive profile, thereby increasing the effectiveness of assimilation [388]. Another promising direction is the introduction of media literacy skills into corporate cybersecurity programs, which protect both personal and organizational information assets [389].

6.6. Technical Measures (Authentication, Traceability)

Technical measures for authentication and tracking the origin of digital content are one of the key areas in countering modern forms of information warfare, especially in the context of the rapid growth of synthetic media and deepfakes. Unlike cognitive or educational approaches, these methods rely on cryptographic, network, and infrastructure solutions that provide the ability to verify the authenticity of the source and the immutability of the content [390].

The classic mechanism for ensuring authenticity is the use of public key infrastructure (PKI) and digital signatures. In the PKI model, each entity (user, server, or content) receives a unique pair of keys—private and public. The private key is used to create a digital signature, and the public key is used to verify it [391]. These technologies are widely used in protecting email (S/MIME, PGP), web communications (TLS/SSL), and can be adapted to verify multimedia content.

In the context of the fight against disinformation, digital signatures allow:

- confirm authorship;
- guarantee post-creation integrity;
- integrate verification into browsers, social networks, and news platforms.

For example, the Content Authenticity Initiative (CAI) project, initiated by Adobe, Twitter and The New York Times, develops standards for embedding metadata and cryptographic signatures directly into multimedia files [392].

Blockchain, as an immutable and decentralized ledger, provides the ability to record the moment of content creation, the chain of its changes and owners. This is especially relevant for photo and video materials that can be modified during distribution. The Truepic platform uses blockchain to verify images, storing their hashes and metadata in a public blockchain [393].

The advantages of blockchain include:

- decentralization, excluding the control of a single organization;
- immutability of records;
- transparency and verifiability.

The limitations include the high cost of transactions in some networks and the difficulty of scaling when working with a large volume of media files [394].

Provenance tracking involves recording the entire "lifecycle" of a digital object, from its creation to its current state. Modern provenance tracking systems include:

- metadata embedding (EXIF, IPTC);
- digital watermarks—hidden markers that are resistant to transformations [395];
- trusted chain standards (e.g., C2PA—"Coalition for Content Provenance and Authenticity") that combine cryptographic signatures and secure metadata [396].

C2PA, developed with the participation of Microsoft, Adobe, and the BBC, provides for the creation of a "provenance manifest" that can be automatically verified before displaying content on the platform.

With the development of generative models capable of creating photorealistic images and audio recordings, the need for automated counterfeit detection tools has increased. Deep learning algorithms are now used not only to recognize deepfakes [397], but also to automatically validate cryptographic attributes of content.

The combination of artificial intelligence with authentication systems allows:

- identify metadata inconsistencies;
- analyze pixel and spectral characteristics;
- check consistency between the declared source and the content's style.

Meanwhile, there are already examples of implementation:

- BBC Project Origin—an initiative to mark original news materials using C2PA and verify chains of trust before publication [398].
- Starling Lab (Stanford University)—a project using blockchain and cryptographic methods to protect digital evidence, including photo and video materials from conflict zones [399].
- Microsoft Video Authenticator—a tool that analyzes photo and video content to identify possible manipulations [400].

Despite technological advances, the implementation of technical measures faces a number of problems [401]:

- the lack of a global content verification standard;
- potential vulnerability of metadata to deletion or substitution;
- the need for a scalable infrastructure;
- ethical issues related to privacy and anonymity.

An important aspect remains the balance between ensuring the authenticity of information and preserving the right to anonymous expression, especially in authoritarian regimes where anonymity protects activists [402].

6.7. Regulatory Initiatives and International Agreements

In recent years, the European Union has built a multilayered regulatory framework to combat disinformation and related risks—from obligations for platforms and advertising intermediaries to requirements for AI transparency and the protection of media pluralism. This architecture is important not only as a "legal background" for technical and organizational measures (see Sections 6.1–6.6), but also as a mechanism for aligning incentives: the regulator forces participants in the digital ecosystem to take into account the social costs of information attacks, which are underestimated in purely market logic.

The basic "framework" is set by the Digital Services Regulation (DSA). It extends to intermediaries and platforms, and introduces a new set of responsibilities for "very large online platforms" (VLOPs) and "very large online search engines" (VLOSEs). Including systemic risk assessments (disinformation, manipulation of the information environment), mitigation measures (adjustment of recommendations, design interventions, and increased moderation) and data access obligations for researchers, as well as expanded transparency of advertising and recommendation systems [403,404]. These mechanisms institutionalize cooperation between academia and platforms and make possible the verification of "anti-fake news" claims (see Sections 6.3 and 6.4). The Commission explicitly links the DSA to the need to "prevent illegal and harmful online activity and the spread of disinformation" and strengthens co-regulatory tools. At the "soft" (but de facto mandatory for VLOPs under the DSA) level, the Enhanced Code of Practice on Disinformation (2022) is in effect:

44 commitments, from demonetization of lies to libraries of political advertising, tools for users and increased transparency, with the Code conceived as a recognized "code of conduct" in the logic of the DSA (co-regulation) [405,406]. The practice of 2023–2025 has shown that the withdrawal of individual companies from the Code does not exempt them from the strict requirements of the DSA. Supervision and sanctions are transferred to the plane of "hard" law (fines, investigations into systemic risks)—a line that the European Commission has consistently pursued in public communications and reports [407]. From October 2025, Regulation (EU) 2024/900 on transparency and targeting political advertising will come into force. It introduces mandatory labeling of political ads, public libraries (archives), disclosure of the source of funding and strict restrictions on microtargeting, especially based on sensitive data and in relation to minors. The regulation is directly linked to the objectives of countering information manipulation and foreign interference in electoral processes and complements the DSA requirements for advertising transparency [408].

Practical consequence: large platforms are restructuring their product and advertising policies in the EU in advance, and in some cases are announcing their refusal to carry out political advertising, citing the difficulty of complying with the new rules—an indicator of the "rigidity" of the regime and its ability to change market behavior [409–411]. The European Media Freedom Act (EMFA) entered into force on 7 May 2024, with key provisions applying from 8 August 2025. It strengthens guarantees of editorial independence, transparency of media ownership, allocation of public advertising budgets, and introduces procedures to reduce the arbitrary risks of media platforms "taking down" content (including requirements for notification, justification, and appeals). In the context of the IW, this is the "second leg" of the balance: while increasing the responsibility of platforms under the DSA, the EU protects media pluralism and the procedural rights of media players, so that the fight against disinformation does not transform into an unjustified suppression of legitimate journalism [412,413].

At the sectoral level, the EMFA is coupled with the updated Audiovisual Media Services Directive (AVMSD, 2018/1808), which extended duties on protection against incitement to hatred, violence and terrorism, as well as protection measures for minors, to video sharing platforms (VSPs). For IW, this is an important "bridge" from classic broadcast regulation to platform regulation: VSPs are required to have report-and-takedown mechanisms, measures against inflammatory/terrorist content, and media literacy efforts [414]. The AI Act enshrined transparency obligations for systems that generate or manipulate content: users must be informed that they are interacting with AI; synthetic content (including deepfakes) must be labeled; and providers of shared AI systems are required to implement detection/labeling technologies and provide a set of accompanying documentation.

The "unacceptable risk" prohibitions will apply from 2 February 2025, and the transparency obligations will be phased in over 2025–2026. These provisions are directly related to Section 6.6 on content authentication/origin, creating a legal "base" for technical initiatives (C2PA, CAI, etc.) [415,416]. Of thematic importance is Regulation (EU) 2021/784 on countering the dissemination of terrorist content online (TERREG): it requires platforms to remove material identified by competent authorities within one hour, introduces mechanisms for cross-border orders, and procedural guarantees. For the architecture of countering IW, this is a precedent of the "hourly norm", which in crisis scenarios (information attacks accompanied by real threats) sets the bar for "default responsiveness" and pushes towards pre-prepared procedures and interfaces for interaction with authorities and researchers [417,418].

Although NIS2 is not about "content", it strengthens the cybersecurity of digital service providers and critical infrastructure, minimizing the condition under which IW is accompanied by sabotage and attacks on the availability of platforms and media. In the

circuit of communication networks, NIS2 increases the requirements for risk management, incident reporting and supply chains—this is the "cyber foundation" for the resilience of the information environment, especially in the phase of escalations and hybrid operations [419].

The updated eIDAS 2.0 (Regulation (EU) 2024/1183) forms the European Digital Identity Wallet—the basis for trusted attributes and electronic signatures on the user side. For countering IW, this opens the way for the mass availability of verifiable attributes (e.g., verified "author" or "organizational" labels that are semi-transparent to privacy), which can be used in conjunction with content origin standards (see Section 6.6) and "signed media content" policies on platforms [420,421]. The Data Act (Regulation (EU) 2023/2854) is not about disinformation per se but is important for the data ecosystem: it introduces rules on fair access/reuse of data and will come into force on 12 September 2025. For research and regulatory reporting, it strengthens the "right to know", especially where platforms and intermediaries act as "data holders", which can facilitate risk audits and assessments of DSA measures. As well as support for independent research into the spread of malicious narratives (in combination with the DSA researcher access regime) [422–424].

What does this all mean in practice:

1. The DSA-AI Act-EMFA legal "triangle" simultaneously sets obligations to reduce systemic risks (including disinformation), transparency of AI/synthetics, and procedural guarantees for the media. In terms of the operational policy of platforms, this means the need for built-in risk interventions (ranking adjustments, cascade slowdowns, and ad repository), default synthetic labeling, and procedural transparency in the moderation of editorial content.
2. Political advertising is separated into its own "high transparency and responsible targeting mode," which closes the main "force multiplier" of AI in electoral cycles—microtargeting based on sensitive data and opaque sponsorship.
3. Crisis and priority content categories (terrorism, violence, national security incidents) receive a procedural "fast track" in the TERREG style; combined with DSA crisis response protocols, this creates operational readiness for surges in coordinated attacks.
4. Researcher access and reporting are no longer a "goodwill" option: DSA/EMFA/Data Act and code regimes make "evidence-based" control a permanent norm—a critical condition for external validation of the effectiveness of measures.

7. IoT/IIoT Threats and Mitigation Patterns in the Context of Information Warfare

The Internet of Things (IoT) and the Industrial Internet of Things (IIoT) significantly expand the attack surface: billions of low-cost, and heterogeneous devices form a distributed fabric of sensors and actuators that serves both information functions (data collection and routing) and cyber-physical processes (production, transportation, and energy management). Recent reviews identify a triad of risks: (i) limited computing and energy resources, leading to simplified cryptographic stacks; (ii) a fragmented ecosystem of standards and unstable supply chains; (iii) long device lifecycles with rare updates [425–428]. In the case of IIoT, these vulnerabilities are exacerbated by requirements for high fault tolerance and deterministic latency, which make traditional information security tools (scanning, patch management, service restarts) difficult to apply [429,430].

IoT acts as both a tool and an object of information warfare. First, IoT botnets (Mirai is a typical example) allow DDoS attacks to be scaled up to the level of strategic pressure on communications platforms and content delivery infrastructure, disrupting access to media resources [431,432]. Second, compromising sensors and telemetry channels opens up the possibility of data substitution and undermining trust—especially critical in the energy and transportation sectors [428,433]. European reports record an increase in "hacktivist" cam-

paigns using DDoS, where IoT devices are used as tools, and attacks serve as a diversionary maneuver before data theft [434]. Incidents in the energy sector of Ukraine show that even if the targets of attacks are physical infrastructure, the information effects (disorientation of operators, overload of support lines, loss of trust in monitoring) are achieved faster than material damage [435]. Threats, information effects and defense patterns are given in Table 3.

Table 3. Threats, information effects and defense patterns.

Threat	Information Effect in IW	Counteraction Pattern
IoT Botnet (DDoS)	Violation of access to platforms, diversionary maneuver	MUD whitelists, ingress filtering, scrubbing
Telemetry substitution	Loss of trust in data, disorientation of operators	OSCORE/EDHOC, OT segmentation, alternative communication channels
Traffic analysis	Behavioral Patterns Leak, Privacy Weakened	Behavioral analytics, encryption, MUD
Firmware vulnerabilities	Mass mobilization of devices in IW campaigns	Security-by-design (NISTIR 8259/8259A, ETSI 303 645), safe OTA
SCADA attacks	Disruption of processes, resonance in the media and public perception	Hard OT segmentation, anomaly detection, communication playbooks

Typical threat profile

- mass botnet campaigns (scanning open services, dictionary attacks on weak passwords, exploitation of firmware update vulnerabilities);
- privacy attacks (analysis of encrypted traffic and metadata to reconstruct behavioral scenarios in “smart homes”);
- CPS/IIoT integrity attacks (injection of false data, substitution of time and synchronization, compromise of protected subsystems).

Counteraction patterns

1. **Security-by-design**. The NISTIR 8259/8259A baselines require: unique identification, secure updating, configuration protection, logging, component transparency (SBOM), managed passwords, and cryptography. ETSI EN 303 645 sets out similar minimum requirements for consumer devices [436–438].
2. **Network whitelisting and profiling**. RFC 8520 (MUD) translates the manufacturer’s intent into network policy: the device publishes allowed interactions, and the controller applies a “default deny” ACL. This dramatically reduces the attack surface; the method is complemented by behavioral analytics (e.g., N-BaIoT) [439].
3. **Easy cryptography**. For limited protocols (CoAP/UDP, 6LoWPAN), OSCORE (RFC 8613) and EDHOC (RFC 9528) are used, providing authentication and integrity with minimal overhead [440,441].
4. **Segmentation and Zero Trust**. NIST SP 800-82 Rev.2 recommends tight isolation of OT segments, DMZs, one-way gateways, and restricted protocols [442]. This reduces the likelihood of lateral movement by attackers and minimizes IW effects.
5. **Vulnerability and Supply Chain Management.** Component transparency (SBOM), firmware signing, secure OTA updates and periodic key rotation are mandatory practices [443].
6. **DDoS counteraction**. Ingress filtering (BCP-38), scrubbing centers, quarantine VLANs and MUD profiles are used. This increases the cost of mobilizing IoT botnets for IoT campaigns [444].

8. Evolution of Information Processing Systems from the Point of View of Information Warfare Issues

The development of digital signal processing technologies and computing architectures opens up fundamentally new opportunities for identifying, filtering, and neutralizing

information threats. In the context of rapidly growing data volumes and increasingly complex manipulation patterns, traditional methods of information analysis are becoming insufficient. They are replaced or supplemented by high-performance algorithms capable of operating in real time, analyzing both obvious and hidden signs of information attacks.

Furthermore, the development of computing technology has an increasingly noticeable impact on society, which is increasingly evident. As noted above, the "society—information technology" system is currently at a bifurcation point. The variability of the development vectors of computing systems (and, consequently, AI) implies several plausible scenarios for this transformation in the foreseeable future. Due to the growing geopolitical turbulence, these transformations are likely to be associated with one or another form of information warfare.

As emphasized in [8], the transformation of computing technology is due to objective reasons. In particular, the possibilities for further improvement of computing technology built on semiconductors, the von Neumann architecture and binary logic have been largely exhausted. In the last decade, there has been an increasingly active search for alternatives. In addition to the above-mentioned works devoted to neuromorphic materials [10,11], one can mention quantum computing [445,446], attempts to implement optical computers [447,448], computing systems based on DNA [449,450], etc. It is permissible to assert that the issue of creating computing systems on a quasi-biological basis [451,452] is already on the agenda, an obvious prerequisite for which is work in the field of electronics based on polymer hydrogels [453,454], biocompatible electronics [455,456], and related areas.

Research in the field of creating neuromorphic materials is closely related to improving the algorithms for the functioning of neural networks, specifically, with work in the field of explainable neural networks [457], which are becoming increasingly relevant. Indeed, neural network training algorithms are currently well developed [458], but the result of such training cannot always be predicted, nor can the specific algorithms used by the neural network be established. In conditions where neural networks (and AI built on their basis) are increasingly used in critically important areas of activity, it is necessary to ensure their predictability, which leads to the need to create explainable neural networks.

This raises the question of deciphering the network's internal code, which can be addressed using methods proposed in [459,460]. The algorithmic/operational transparency of neural-network operation, as emphasized in [461], in turn, is of great importance for the synthesis of neuromorphic materials, since from a chemical point of view it is convenient to implement their tuning/training directly in the synthesis process.

Different types of advanced computing technology correspond to different vectors of development of the system "society—information technology" (global information and communication environment). Thus, quasi-biological computing, which may interface with the human brain, aligns most closely with transhumanist concepts [462,463] tracing back to Huxley [464].

Ideas connected to transhumanism are diverse. In particular, the literature presents works that defend the concept of 'digital immortality,' i.e., transferring human consciousness to a non-biological information carrier [465,466]. From a formal point of view, such an approach obviously has a right to exist: the operational capabilities of existing computing systems are approaching those possessed by the human brain.

However, there is an important nuance. As emphasized in [467], the existing definitions of intelligence are purely descriptive. The essence of intelligence—and especially human consciousness—remains unresolved. Consequently, at the level of research that can be achieved in the foreseeable future, it will likely remain unclear what information should be "written into a computer" in order to obtain a "copy" of a real person.

This example clearly highlights one of the main problems of a methodological (if not philosophical) nature that arises when trying to implement "strong" AI. The question of its

algorithmic basis is of fundamental importance. This returns us to the above-mentioned range of problems related to the creation of neuromorphic materials. The brief overview in this area presented above, as well as the overview presented in [14], allows us to state that such an algorithmic basis can be variable. Existing AI and the computing tools implementing them are built on binary logic, which, however, is not mandatory. Thus, in the 1970s, not unsuccessful attempts were made to implement computers operating with ternary logic [468,469]. Moreover, there is no reason to assume that binary logic is organically inherent in human thinking. As emphasized in [3], Aristotle's logic covers the simplest—from the point of view of formalization—type of reasoning. Human thinking cannot be reduced to it.

Consequently, it is permissible to speak not only about the variability of scenarios for the development of computer technology, but also about the variability of the algorithms that underlie it. This returns to the question of the neural network theory of society (more broadly, the noosphere) and its role in the information warfare. If society is an analog of a neural network, then from general methodological considerations it follows that there must be algorithms for processing information that are complementary to its structure. Note that AI is increasingly integrated with telecommunication networks. This means that the emergence of algorithms of the above type will turn AI into a kind of "mediator" between the ordinary (personal) and suprapersonal levels of information processing. Thus, a methodological basis arises for creating nontrivial tools for influencing various components of the sociocultural code, in particular, the collective unconscious.

This section first examines the most obvious problems associated with the development of new algorithms for information processing as they relate to the problems of information warfare (the task of filtering information noise). Then, from the same perspective, the possibilities of practical use of transformations like the Fourier transform but built on the use of finite algebraic structures (Galois fields, etc.) are considered. Next, new approaches to the construction of convolutional neural networks are considered, which are of significant interest from the point of view of explainable AI, which are closely related to the Fourier–Galois transforms and similar ones. It is further proved that finite algebraic structures (a special case of which underlies modular arithmetic) are indeed of significant interest from the point of view of creating nontrivial computing systems. The section concludes with a consideration of some humanitarian aspects of the issues raised.

8.1. Digital Signal Processing in Problems of Filtering Information Noise

Digital signal processing (DSP) is one of the key tools in modern systems for countering information attacks, especially in cases where the information flow is multimodal—including text, audiovisual, and metadata. Initially, DSP developed as a field focused on processing physical signals (speech, radio-frequency, images), but in the last two decades its methods have been adapted to work with "information noise"—chaotic or specially generated data that complicates the extraction of relevant information [470,471]. In the context of information warfare, information noise is defined as a set of messages that do not carry a useful semantic load or intentionally distort the signals necessary for decision-making. A classic example is the "pollution" of the information space by coordinated botnets, creating the illusion of public consensus or, conversely, mass discontent [472]. DSP provides tools for detecting such anomalies through spectral analysis, filtering, correlation methods, and signal decomposition into basis functions.

One of the fundamental approaches is the use of linear and nonlinear filters to extract the useful signal from the stream. Linear filtering (e.g., using low-pass or high-pass filters) suppresses high-frequency bursts of activity characteristic of coordinated injections.

Nonlinear methods, including median filtering and morphological operations, are effective in suppressing impulse noise and identifying stable patterns [473,474].

The use of frequency analysis, in particular, the fast Fourier transform (FFT) and wavelet transforms, enables translation of the information stream into the spectral domain, where it is easier to detect hidden periodicities or characteristic attack signatures. Studies show that even in text data (e.g., in tweet sequences), spectral characteristics can be identified that indicate the artificial origin of messages [475].

For complex multimodal signals, singular value decomposition (SVD) and principal component analysis (PCA) methods are relevant, which allow one to identify basic data structures and discard random or artificially created variations [476]. This is especially effective in detecting fake images and videos, where signs of manipulation can be masked by noise.

An important area is the use of adaptive filters that change their parameters depending on the statistics of the input signal. Such filters, based on the LMS (Least Mean Squares) and RLS (Recursive Least Squares) algorithms, are used in real-time systems that analyze social media dynamics and network traffic [477].

Modern research in this area increasingly turns to hybrid methods that combine DSP with machine learning. For example, spectral features identified at the stage of digital processing used as inputs to neural networks to classify information sources or identify anomalies [478,479]. Thus, DSP serves as a "first-stage" filter, preparing data for more complex analytical models.

Many of these methods have already been adapted to the tasks of countering information warfare. Thus, publications on digital filtering of news streams propose algorithms that allow reducing the level of information noise by 40–60% without losing relevant messages [480]. In combination with computing architectures optimized for parallel processing, this opens up opportunities for large-scale monitoring of the information space in real time.

Thus, the DSP provides a basic technological basis for combating information noise, acting not only as a data "cleaning" tool, but also as a means of early detection of attacks disguised as a natural information flow. Its further development in conjunction with new computing architectures described in the following sections is key to increasing the resilience of the information infrastructure to impacts.

The examples above support this assessment. Even in such a field as filtering information noise, the use of finite algebraic structures, in particular, Galois fields, shows clear promise.

8.2. Using Fourier–Galois Transforms to Reveal Hidden Patterns

The Fourier–Galois Transform (FGT) is an extension of the classical Discrete Fourier Transform (DFT) over finite fields and rings, allowing discrete data to be processed under modular arithmetic [481,482]. Unlike the traditional DFT, which operates in the field of complex numbers (i.e., continuously changing quantities), the FGT is defined for elements of finite algebraic structures, making it particularly suitable for digital computers implementing operations in residue number systems (RNS) or modular arithmetic [483]. In the context of information warfare, the FGT opens up unique opportunities for analyzing large and noisy data sets. The fact is that many types of manipulative information attacks manifest themselves as weak but persistent patterns in time series or network activity that can be masked by noise. When working in complex arithmetic, extracting such patterns is difficult due to round-off errors and high computational costs, while using FGT in finite fields allows one to preserve accuracy and reduce the load on computational resources [484].

The study by Kadyrzhan et al. (2024) on partial digital convolutions [485] and the work by Suleimenov & Bakirov (2025) on finite rings [486] show that integrating FGT into logical-algebraic models allows one to effectively decompose an information flow

into orthogonal components even under conditions of incomplete data. This property is critically important, for example, when analyzing botnet activity, when observations capture only a fragment of the interaction graph.

From a theoretical point of view, FGT is based on the properties of multiplicative subgroups of finite fields GF(p^n) or rings Z_m. Let p be a prime number, then the field GF(p^n) contains a multiplicative group of order $p^n - 1$, on which discrete harmonics can be constructed, similar to complex exponentials in DFT [487]. This allows one to determine the frequency components of data encoded in modular form, which is especially useful in architectures operating on the principle of residual arithmetic.

Practical applications of FGT in countering information attacks include:

- Detection of coordinated activity: modular analysis of time sequences of publications in social networks reveals hidden cycles and synchronization of actions between anonymous accounts.
- Detection of hidden periodicity: FGT can find repeating structures even in highly fragmented data, which is difficult in classical spectral analysis.
- Data compression and filtering: due to operation in modular arithmetic systems, FGT allows one to implement efficient algorithms for compression and rejection of noise components without losing critical signals [488,489].

In addition, the computational efficiency of FGT is enhanced by using RNS, where calculations in different modules are performed in parallel and the result is combined using the Chinese Remainder Theorem [490]. This makes it possible to process large amounts of information in real time, which is essential for monitoring information flows in the face of rapidly evolving attacks.

The combined use of FGT with partial convolution methods (see Section 6.2) enables building hybrid analysis systems, where selected data segments are subjected to high-precision spectral decomposition, and the analysis results are used to detect and localize attack sources.

Additional prospects for using FGT in spatial analysis problems are demonstrated in the work by Suleimenov et al. [491] on mosaic structures in discrete coordinate systems. In this study, a method for forming two-dimensional and three-dimensional discrete spaces based on finite algebraic rings using mosaic (tiling) partitions is proposed. Such structures allow representing large data arrays as regular fragments with orthogonal properties, which simplifies their processing and analysis of frequency characteristics. In the context of countering information threats, this makes it possible to effectively identify spatio-temporal correlations between different segments of the information flow, for example, when analyzing the geographic distribution of disinformation sources or visualizing clusters of synchronous activity in social media. The use of mosaic coordinate systems together with FGT provides an additional level of detail for spectral analysis, allowing not only to detect hidden patterns, but also to localize them in the data space, which is especially important for complex monitoring systems. Thus, FGT is not just a mathematical tool, but a fundamental element of computing architectures aimed at ensuring resistance to information threats. Its development within the framework of finite algebraic structures opens up prospects for building high-performance and energy-efficient systems integrated into both specialized processors and data analysis software packages.

This example is primarily illustrative, but it demonstrates that relatively simple patterns can underlie very complex structures. An important task is to develop tools that establish such patterns in a verifiable manner.

This brings us back to the question of methods for constructing explainable neural networks, since such networks are among the main tools for image analysis, including from the point of view of establishing their quantitative parameters [492,493].

8.3. Methodology of Partial Convolutions and Discrete Logical-Algebraic Models

Modern electronics (which, among other things, is the basis of computing technology) is largely based on the theory of linear electrical circuits [494]. The main advantage of this theory is that it allows us to reduce the analysis of any processes occurring in such networks to an examination of their amplitude-frequency characteristics. The mathematical basis for this is the convolution theorem, which states that the Fourier transform of the convolution of two functions is the product of their Fourier transforms [495].

In the classical theory of linear electric circuits, signal models are functions that take real or complex values. When moving to digital signals, i.e., signals that correspond to a certain set of discrete levels, it is natural to use functions that take values in any suitable finite algebraic structure (Galois field, finite algebraic ring, etc. [496]). We emphasize that a signal is a physical process, and a function that serves as its model is a mathematical object. The choice of the latter is therefore no more than a matter of convenience and convention [497].

This conclusion is applicable, in particular, to problems of digital image processing [498]. A digitized image can be represented as a function that takes discrete values in a finite range of amplitudes. Consequently, its model can be a function that takes values, for example, in a Galois field.

For such fields, an analog of the convolution theorem has been formulated, a visual proof of which is given, for example, in the work [499]. However, an important caveat applies. Direct application of the analog of the convolution theorem, formulated in terms of Galois fields, does not correspond in physical meaning to convolution calculated in terms of continuity (real or complex values). This difficulty is overcome in [500], in which the concept of partial digital convolution was introduced.

Partial Digital Convolution (PDC) is a method for processing discrete signals in which convolution operations are performed not over the entire domain of a function, but over selected subsets of it, which allows for a significant reduction in computational complexity and adaptation of algorithms to specific features of the input data [501]. This approach aligns the ranges of input and output variables. This makes it possible to construct orthogonal bases for convolution over various finite fields and eliminates the occurrence of inconsistencies in the ranges of input and output variables that arise during direct calculations of digital convolution. Due to this, the algebraic properties of convolution are preserved while reducing computational complexity.

Kadyrzhan et al. (2024) reported [485] a formalization of the partial digital convolution method based on algebraic extensions and construction of orthogonal bases. The authors show that the use of algebraic ring theory and modular arithmetic enables PDC implementation in computing systems with a high degree of parallelism, while ensuring minimal accuracy loss. This approach is especially promising when integrated into specialized processor architectures focused on processing streams in real time. One of the key advantages of PDC is its compatibility with discrete logical-algebraic models—formal structures that describe data not as real numbers but as elements of finite sets (rings, fields, or lattices). Such models allow processing information signals in a more compact and error-resistant form, which is critical for problems where data can be distorted or fragmented [502,503]. The logical-algebraic approach to convolutions is based on operations in finite algebraic structures, which opens up opportunities for optimization for specific hardware platforms. For example, the use of operations modulo a prime or composite number makes it possible to use highly efficient computation methods in RNS, which in turn enable computation without intermediate carries [486]. This is directly related to research in the field of finite ring computing architectures and RNS [504,505].

The practical value of this approach is evident in the problems of filtering information noise and detecting hidden correlations. For example, in the analysis of social networks, partial convolutions can be applied to time-series "windows" reflecting the activity of individual user groups, and logical-algebraic models enable robust comparison of such patterns even with a high degree of data noise. In combination with the DSP methods described in Section 6.1, PDC and logical-algebraic models enable the construction of a multilevel filtering architecture: at the first level, selecting priority flow segments, at the second, high-precision processing of selected segments using error-resistant algebraic methods.

In the context of information warfare, the methodology in question is of particular importance when analyzing massive data streams, such as social media or network logs, where full processing of all messages in real time is not always technically possible. enables focusing computational resources on segments flagged as potentially anomalous by preliminary (e.g., spectral or statistical) analysis, thus accelerating response to threats [506].

Thus, the methodology of partial convolutions and its integration with discrete logical-algebraic models form the basis for creating new-generation computing systems capable of effectively combating information attacks in the context of big data and limited resources. Their further development, including in the direction of optimization for FPGAs and specialized processors, enables scalable real-time monitoring and filtering systems.

However, the prospects for its use are not limited to this. Unlike the analog of the convolution theorem, as discussed in [498], the method of partial convolutions allows us to consider digital convolutions with full preservation of the physical meaning of the transformations performed. Consequently, this method can be considered as a certain step forward in relation to the methods of creating explainable neural networks. Indeed, in accordance with the classical theory of linear electrical circuits, it is possible to obtain a circuit with specified characteristics, starting from its transfer function (in other terminology—amplitude-frequency characteristic). Similarly, a convolutional neural network can be built starting from an analog of the transfer function (more precisely, a set of such functions, each defined over its own Galois field), constructed using the method in [485].

Methodologically, this corresponds to the problem considered in Section 8.2. A complex image represented in digital form must be reduced to simpler characteristics. Establishing the transfer function of a convolutional neural network allows us to solve this problem for many important applications that use neural networks of this type, e.g., [507]. A similar approach can be used for relatively small images, and in this case the analog of the transfer function is not only found explicitly but also serves as a basis for constructing electrical circuits that solve a specific problem [508].

This approach, among other things, creates the prerequisites for deciphering the true algorithms of the functioning of neural networks and their naturally arising analogs. In particular, in the future, it is possible to set the task of deciphering the sociocultural code. This, in turn, creates prerequisites for optimizing the impact on such a code, which is directly related to the problems of information warfare. Consequently, the analysis of the prospects for the development of computing tools using finite algebraic structures is of interest from this point of view as well.

8.4. Finite Ring and Residual System Computer Architectures

Finite ring and RNS based architectures are a special class of digital computing systems in which operations are performed modulo one or more integers. Their key feature is the ability to perform arithmetic operations in parallel without the need to carry propagation, which leads to a significant increase in the computational speed [490,509].

In the context of countering information warfare, such architectures have a number of advantages:

- high throughput—the ability to process large amounts of data in real time;
- energy efficiency—due to the elimination of complex carry operations;
- fault tolerance—due to modular redundancy and the ability to detect/correct errors;
- built-in data protection—modular arithmetic complicates direct recovery of the original data when intercepting intermediate results [510].

Suleimenov et al. (2023) [504] show that the use of multivalued logic based on algebraic rings significantly expands the capabilities of such architectures in signal processing. The use of finite rings (for example, Zm, where m is a composite number) allows one to implement calculators capable of working not only with binary but also with multivalued logical variables, which is especially useful when modeling complex systems with a large number of states, including social networks and communication platforms.

Suleimenov & Bakirov (2025) [486] propose a method for constructing discrete coordinate systems based on finite algebraic rings. This solution has direct practical significance for spatiotemporal data analysis systems in problems of monitoring information flows.

From the point of view of computational theory, RNS is based on the decomposition of integers into a set of residues in mutually prime moduli {m$_1$, m$_2$, . . ., m_k}. Arithmetic operations are performed in each modulus independently, which enables full parallelism. The result is reconstructed using the Chinese Remainder Theorem (CRT) [511]. This approach is ideally suited for FPGA and ASIC architectures, where each modular branch can be implemented as a separate computing unit.

A notable case is a multiplication-modulo-7 method developed and patented in Kazakhstan [512]. This method optimizes one of the key operations in RNS and ring arithmetic systems, reducing cycle count and increasing performance of specialized processors. For information security and information noise filtering tasks, such optimizations are critical, since multiplication is a basic operation in most spectral analysis methods (including Fourier–Galois transforms, see Section 8.3).

Modern research [513,514] shows that architectures based on finite rings and RNS are successfully used in cryptography, digital filtering systems, and even in machine learning. For example, in botnet detection and filtering tasks, RNS architectures allow implementing fast and error-resistant correlation analysis algorithms without losing performance as the data volume grows. A significant contribution to the development of computing architectures based on modular arithmetic was made by Kadyrzhan et al. (2025) [515], dedicated to the prospects of using quasi-Mersenne numbers in the design of parallel-serial processors. The work shows that such modules make it possible to simplify the hardware implementation of multiplication and addition due to the features of the representation that are close to Mersenne numbers, but with a more flexible choice of parameters. This provides a compromise between performance, hardware costs, and the versatility of the architecture, which is especially important for systems that perform digital filtering and identify manipulative patterns in data streams in real time.

Research conducted in this direction also made it possible to create fairly simple means for calculating discrete logarithms [516]. Calculating such logarithms was considered a very difficult task for a long time. As noted in [517], the first practical public-key cryptosystem, the Diffie-Hellman key exchange algorithm, relies on the assumption that discrete logarithms are computationally hard. This assumption, characterized as a hypothesis, underpins the presumed security of various other public-key schemes [517]. At the time of the cited publication, this hypothesis was the subject of extensive debate, and this situation persisted until recently [518].

Furthermore, even problems that were previously considered and solved purely in terms of continuous functions admit a transition to a discrete description. In particular, in [519] it is shown that the description of the propagation of electromagnetic waves in

space can be reduced to a discrete form. On this basis, in [520] it is shown that arbitrary converters of electromagnetic radiation can also be reduced to an equivalent circuit that contains only discrete elements. This potentially creates the prerequisites for the use of algebraic methods, including in problems of this type.

For clarity, we will also provide a small numerical illustration based on the materials of the works [500,505].

As a simple illustration of modular processing in a Residue Number System, consider the integer N = 73 represented under the modulus set {5, 7, 11}. The residues are (73 mod 5, 73 mod 7, 73 mod 11) = (3, 3, 7). An arithmetic operation can then be performed independently in each modulus. For instance, let us add M = 52, which is represented as (2, 3, 8). Their sum in RNS is (3 + 2 mod 5, 3 + 3 mod 7, 7 + 8 mod 11) = (0, 6, 4). Using the Chinese Remainder Theorem, this corresponds to the integer 125 in the original domain. The modular decomposition allows the operation to be carried out fully in parallel, without carry propagation, and then efficiently reconstructed.

A toy example of the Fourier–Galois Transform can be given over the finite field GF(7). Consider the input vector f = [2–5]. Let ω be a primitive element of GF(7), for instance $\omega = 3$, which has order 6. The transform is computed as F(k) = Σ f(n) ω^(kn) mod 7. For k = 0, F(0) = 1 + 2 + 3 + 4 = 10 $\equiv$ 3 (mod 7). For k = 1, F(1) = 1·3^0 + 2·3^1 + 3·3^2 + 4·3^3 $\equiv$ 1 + 6 + 5 + 6 $\equiv$ 18 $\equiv$ 4 (mod 7). Proceeding analogously for other k yields the transformed sequence. This simple example demonstrates how algebraic periodicities in finite fields can be exploited to perform convolution-like operations with full determinism and reduced complexity.

To illustrate the practical benefits of modular architectures, consider the example of a residue number system (RNS) processor configured with the moduli set {2, 3, 5, 17, 257}. The dynamic range of this configuration is approximately 2^{17}, which is equivalent to a 16-bit integer processor. Importantly, the critical path is determined solely by the largest modulus (257), corresponding to the complexity of an 8-bit adder or multiplier, while all smaller channels operate in parallel. Assuming a conservative clock frequency of 200 MHz for such an 8-bit modular unit, the throughput of vector additions in RNS reaches around 200 million "16-bit equivalent" additions per second. By comparison, a conventional 16-bit binary adder under the same technology assumptions typically operates at about 150 MHz, yielding approximately 150 million additions per second; thus, the RNS scheme achieves a $\approx$1.3$\times$ gain for addition. The advantage becomes even clearer for multiplication: while classical 16-bit binary multipliers often require multiple cycles or reduced frequency (50–150 million multiplications per second effective throughput), RNS multipliers remain one-cycle operations per modulus, sustaining $\approx$200 million per second, i.e., up to 2–3$\times$ faster. Moreover, scaling to higher dynamic ranges is achieved by simply adding new moduli without extending the critical path, thereby maintaining frequency while increasing representable precision. This carry-free parallelism highlights why RNS-based processors are particularly attractive for real-time and high-throughput applications. In a complementary manner, Fourier–Galois Transforms (FGT) preserve consistency of value domains by ensuring that both inputs and outputs remain strictly within GF(p^n), thereby avoiding fractional results inherent in classical convolution. This modular consistency across both RNS and FGT reinforces their practical value as efficient and deterministic alternatives to conventional arithmetic.

Thus, the combination of finite rings, RNS and specialized modular algorithms, including optimized multiplication schemes, forms the basis of high-performance computing systems capable of effectively countering modern threats in the information environment. Their use in complex monitoring and filtering systems allows for prompt analysis of information flows and rapid detection of anomalies even in conditions of massive attacks.

8.5. Intelligent Filters for Resistance to Manipulative Patterns

Intelligent filters for resilience against manipulative patterns are a class of digital information processing systems that use machine learning algorithms, signal theory, and mathematical models based on finite algebraic structures to identify and suppress malicious or manipulative information influences. Their key task is to automatically distinguish relevant information from distorted or intentionally modified information in the conditions of intense information noise [74,521].

In the context of information warfare, manipulative patterns can take various forms—from the mass publication of similar messages (astroturfing) and the targeted dissemination of false narratives to the synchronous activity of botnets and the use of deepfakes [522]. Classical filtering methods based on static rules or heuristics are not flexible enough, since attackers quickly adapt their tactics. In contrast, intelligent filters are capable of online learning and self-adaptation, enabling long-term resilience [523]. The mathematical basis of such filters often combines:

- spectral analysis methods (including Fourier–Galois transforms, see Section 8.3) to identify hidden periodicities;
- partial digital convolutions to isolate characteristic spatio-temporal structures;
- residual number systems and finite ring arithmetic for high-speed parallel data processing;
- multivalued logic to model uncertainty and make decisions under incomplete information [524].

From an architectural point of view, an intelligent filter usually includes several processing levels:

1. Data preprocessing and normalization—removing noise components, restoring gaps, modular data decomposition.
2. Feature extraction—spectral, statistical, and topological features of the information flow.
3. Pattern classification—using neural networks (including graph networks), Bayesian models, or hybrid logical-algebraic schemes.
4. Dynamic adaptation—adjusting filter thresholds and a set of features based on the attacker's current tactics.

Real-world studies in the field of applying intelligent filters to countering IW problems demonstrate high effectiveness. For example, the work of Song et al. (2019) [489] show that integrating spectral methods with trainable models can achieve up to 95% accuracy in detecting coordinated attacks on Twitter. Other studies [525] describe the use of algorithms based on residue arithmetic for video-streams processing and detecting anomalous image manipulations, which is relevant for detecting deepfakes.

An important area is resistance to adaptive attacks. Here, a special role is played by algorithms that can generate "counter-patterns"—information noise that distorts the attacker's data and reduces the effectiveness of his learning algorithms. This approach is close to the concept of "adversarial machine learning" but is applied in the opposite direction—for defense, not for attack [526].

The practical implementation of intelligent filters is often based on hybrid architectures that combine FPGA/ASIC modules for high-speed signal processing and CPU/GPU blocks for high-level analysis. Such integration enables high throughput and complex analytical functionality at the same time, which is critical for real-time monitoring of social networks during massive information attacks. Thus, intelligent filters for resistance to manipulative patterns are one of the key technological components of the modern arsenal of protection against information threats. Their development is directly related to progress in the field of digital signal processing, algebraic calculators and machine learning, and

their implementation in content monitoring and moderation systems allows not only to identify, but also to neutralize malicious effects before they reach a critical mass.

Thus, traditional ML/NLP detectors demonstrate significant achievements in recognizing manipulated content, but have limitations in the context of noisy data, high load, and the need for predictable behavior. Alternative computational approaches, in particular, methods based on the RNS, Fourier–Galois transform (FGT), and partial digital convolutions, open up opportunities for deterministic processing and efficient parallelization, while maintaining robustness to noise and reducing resource intensity. A comparative analysis of the presented directions is summarized in Table 4. An extended version of the analysis, including additional criteria and more detailed characteristics, is given in Appendix A (Table A1).

Table 4. Comparative analysis of mainstream ML/NLP detectors and DSP-based approaches.

Approach	Advantages	Limitations	Typical Application Scenarios
Text ML/NLP classifiers (LogReg/SVM/Transformer)	High accuracy on annotated corpora; adaptability to new patterns	Sensitive to noise and concept drift; stochastic outputs	Disinformation detection in texts and social media
Graph-based network anomaly detection (CIB/botnets)	Captures structural relations; resilient to manipulation of individual nodes	Requires large-scale graph data; computationally intensive	Botnet detection, coordinated inauthentic behavior
Multimodal deep detectors (CV/audio for deepfakes)	Integrates text, audio, video; high performance for deepfakes	Resource-hungry; large training datasets needed	Synthetic video/audio detection
Rule-based/OSINT + knowledge graphs	Transparent and interpretable; expert control possible	Limited scalability; fails on novel attack patterns	Monitoring known campaigns, fact-checking
DSP—Residue Number System (RNS) pipelines	High-speed, parallelism, determinism	Complex reconstruction, careful modulus choice needed	Real-time systems, cryptography
DSP—Fourier–Galois Transform (FGT) over GF(p)	Algebraic rigor, noise resilience, parallelizable	Requires specialized support, niche adoption	Signal processing, cryptography
DSP—Partial digital convolution (modular)	Reduces computational complexity; subset operations possible	Requires correct domain alignment	Incomplete data processing, modular systems
DSP—Finite-field algebraic checksums/hashes	Deterministic, lightweight, fast integrity checks	Restricted to finite-field tasks	Integrity verification, fast screening
Hybrid ML + DSP (ensemble/cascaded)	Combines ML flexibility with DSP robustness	Integration complexity; balancing trade-offs	Critical infrastructures, high-load systems

9. Ethical and Legal Aspects of Combating Disinformation

Countering disinformation inevitably involves a complex balance between protecting information security and preserving fundamental rights and freedoms, primarily freedom of speech. Strengthening controls and content filtering can help reduce the spread of false information, but carry the risk of censorship, restrictions on political pluralism, and abuses by government or corporate actors.

In international practice, approaches to regulating the information space range from soft forms of self-regulation and codes of conduct to tough legislative initiatives with administrative and criminal sanctions. At the same time, the key challenge remains the development of universal norms that account for both the cultural and legal characteristics of different countries and the cross-border nature of digital communications.

This section analyzes the main ethical dilemmas and legal mechanisms in the field of combating disinformation and assesses how different regulatory models affect democratic resilience and human rights.

9.1. Freedom of Speech vs. Information Security

The issue of the relationship between freedom of expression and information security is one of the central ethical and legal challenges in countering disinformation. Freedom of speech is enshrined in key international legal acts, including Article 19 of the Universal Declaration of Human Rights (1948) [527] and Article 19 of the International Covenant on Civil and Political Rights (1966) [528]. This emphasize the right of every person to freely

express their opinion, including "freedom to seek, receive and impart information and ideas of all kinds." However, the same documents stipulate that this right may be limited "in the interests of national security, public order, public health or morals." Thus, at the normative level, there is recognition of the need for a balance between individual freedom of expression and the collective security of the information space. In the context of an information warfare, this balance is especially fragile. Mass disinformation campaigns aimed at undermining democratic institutions can threaten not only political stability, but also human rights, including the right to reliable information [529,530].

Academic literature identifies two key approaches to resolving this dilemma. The first is liberal-absolutist, according to which any form of restriction of freedom of speech is unacceptable, and disinformation threats should be neutralized exclusively through counter-narratives and increased media literacy [531]. The second is pragmatic-regulatory, allowing for restrictions on certain types of content in the presence of a proven threat to national or public security [532].

In practice, most states adhere to a mixed approach. For example, the European Union in its "Code of Practice on Disinformation" (2022) [533] sets out voluntary commitments of online platforms to remove harmful content, while introducing transparency and accountability requirements to avoid unjustified censorship. At the same time, some countries (for example, Singapore with its POFMA law—"Protection from Online Falsehoods and Manipulation Act") [534] apply strict centralized control over information, which has drawn criticism from human rights organizations [535].

Research shows that excessive restrictions on freedom of speech under the pretext of information security can have the opposite effect—a decrease in trust in government institutions and an increase in activity in shadow communication channels [536]. In turn, the complete lack of regulation in the context of digital platforms with algorithmic personalization creates conditions for the rapid spread of false narratives and manipulative patterns [64].

The issue of proportionality of interference deserves special attention. The European Court of Human Rights (case "Handyside v. United Kingdom", 1976) established that freedom of expression extends not only to information that is perceived positively or neutrally, but also to that which "offends, shocks or disturbs" [537]. This means that measures aimed at combating disinformation must be strictly proportionate to the threat and avoid creating an excessive chilling effect on legitimate public discourse [538].

In modern conditions, the principle of minimum necessary restriction has become a key ethical guideline, suggesting that any restrictions on freedom of speech must be [539]:

- enshrined in law;
- necessary to achieve a legitimate goal;
- proportionate to the potential damage;
- subject to independent judicial or public control.

Thus, finding a balance between freedom of speech and information security requires fine-tuning of the law, an interdisciplinary approach, and transparent accountability mechanisms. Only under these conditions can the risk of abuse be minimized and, at the same time, the threats of information warfare be effectively countered.

9.2. Platform Responsibility and Moderation

The debate over platform responsibility for content has evolved from "soft" self-regulation to hybrid models with strict legal obligations. In the 2010s, voluntary norms formed the basis—internal community rules, public reports on compliance with standards, industry "principles". However, by the early 2020s, the center of gravity had shifted to

co-regulation: states set the frameworks and procedures, and private platforms ensure their operational implementation.

In the United States, §230 Communications Decency Act (47 U.S.C. §230) preserves immunity for intermediaries for editorial decisions, which contributed to the early stage of "moderation by own rules" and mass automation. In the EU, the logic of positive duties is enshrined: the Digital Services Act (DSA) established a detailed system of procedures and accountability, especially for "very large online platforms" (VLOPs): regular assessments of systemic risks, mitigation measures, independent audits, access to data for researchers and supervisory powers of regulators [540].

Thus, moderation is no longer solely a matter of private discretion and is integrated into a risk-management legal regime. This applies not only to obviously illegal content (terrorism, exploitation of children, calls for violence), but also to the "gray zone"—borderline legal materials that may pose a public danger: disinformation campaigns, intimidation, coordinated inauthentic behavior, manipulative recommendations.

The DSA has institutionalized a risk-based approach: platforms are required to regularly assess risks (election interference, threats to security and human rights, the impact of recommendation systems), publish reports, take proportionate measures (adjusting algorithms, strengthening advertising verification, setting up moderation rules), undergo independent audits, and provide researchers with standardized access to data [540].

At the national level, Germany implements the NetzDG with a notice-and-action procedure and complaint reporting [541], and the UK implements the Online Safety Act with a duty of care framework, which obliges platforms to systematically prevent the risks of harmful content through risk assessment, safety-by-design, and Ofcom supervision [542]. Similar processes are underway across Asia, where states are creating their own regulatory frameworks to counter disinformation. In Singapore, the key instrument is the Protection from Online Falsehoods and Manipulation Act (POFMA, 2019), which empowers authorities to issue mandatory directions (correction directions) to correct false claims. The law focuses on factual distortions, and failure to comply with the directions entails administrative and criminal liability [543].

In China, the regulatory complex includes the Cybersecurity Law (2017), the Data Law (2021), and the Personal Information Law (2021), as well as specialized acts such as the Deep Synthesis Regulations (2022), which regulate the use of algorithms and synthetic content: it introduces deepfake labeling requirements and imposes obligations on providers to prevent the manipulative use of technologies [544]. Taiwan passed the Anti-Infiltration Act in 2020, which limits external funding and coordination of information campaigns, complementing it with measures by the National Communications Commission (NCC) aimed at countering disinformation in the media environment [545].

In South Asia, India has implemented the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which strengthened the responsibilities of intermediaries in content moderation, the introduction of grievance officers, and the transparency of algorithms. An attempt to supplement the regulation with the creation of a state Fact-Check Unit was stayed by the Supreme Court in March 2024 as raising issues of proportionality and freedom of expression [546]. In addition, the Digital Personal Data Protection Act, 2023 is in force, forming rules for the processing and targeting of personal data in political communication [547].

In Southeast Asia, Vietnam, through the Cybersecurity Law (2019) and Decree No. 53/2022, has established mechanisms for the removal of false information and data localization requirements for global platforms [548]. In 2021, Hong Kong amended the Personal Data (Privacy) Ordinance, criminalizing doxxing and empowering the PCPD to issue takedown orders [549]. In 2022, the Philippines adopted the SIM Registration

Act, aimed at curbing anonymous dissemination of disinformation on instant messaging apps [550]. In Indonesia, amendments to the ITE Law clarified the concept of defamation and simultaneously criminalized the "dissemination of false statements causing public concern" [551].

At the "soft law" level, the Recommendation of the Committee of Ministers of the Council of Europe on the roles of Internet intermediaries (CM/Rec(2018)2) and the updated Santa Clara Principles on transparency and procedural guarantees (user notifications, clear reasons for blocking, the possibility of appeal, the publication of metrics) are enshrined [552,553].

The main operational problem is scale and reliance on automation. The moderation system of large platforms combines rules, tools, and people: filters and classifiers (hash matching, machine-learning (ML) models), manual review queues, appeals, escalations to policy teams, interaction with "trusted flaggers" and law enforcement agencies. Even with high accuracy metrics, algorithmic decisions systematically make mistakes: false positives affecting minority content, cross-cultural contexts, irony, and memes. Therefore, the institution of procedural guarantees—notifications, accessible appeals, independent reviews (including the Oversight Board Meta)—has become a central element of "moderation ethics" [554–556].

Research shows that the "right to explanation" and traceability of decisions reduce the "chilling effect" and strengthen user trust, even when content is not reinstated [557]. The accountability system faces dilemmas. First, "over-removal vs. under-enforcement": strict NetzDG deadlines and threats of fines push platforms to premature takedowns, which is criticized by NGOs and the Council of Europe [541,552]. Second, transparency and access to researchers' data (DSA, Art. 40) conflict with privacy, commercial confidentiality, and security; the solution is standardized access interfaces, independent verification of projects, and audit of datasets [540]. Third, the problem of interoperability and encryption: extending moderation to closed channels undermines cryptographic protection. Therefore, regulators increasingly limit themselves to metadata, reporting, and "safety by design" instead of mass content scanning [542,543].

At the governance level, the institutionalization of the "procedural constitutionalism" of platforms is taking shape: codes, registries and libraries of political advertising, labeling of state media; transparency of recommendation systems and user choice "switches" (DSA); external experts, auditors, academic partnerships, public councils and independent dispute resolution bodies (Oversight Board). In the literature, this is described as a "new administrative system of online speech," where private rules and state requirements form a regime closer to administrative law than to editorial discretion [554,558,559]. Finally, the platform becomes not only a "moderator," but also an "architect of the environment." Responsibility shifts "up the stack": from deleting posts to managing systemic risks through feed design, notification cadence, labeling and virality controls, advertiser vetting, and researcher access. Empirical evidence shows that resilience to disinformation depends more on the properties of recommendation systems and advertising infrastructure than on targeted removals. Therefore, the DSA, the Santa Clara Principles and the Council of Europe recommendations agree on one thing: platform accountability is measured not by "removed/not removed" acts, but by processes—risk assessments, explainability of algorithms, access to data, the possibility of appeal and independent oversight [543,552,553]. A summary table of regulatory acts is provided in Appendix B, Table A2.

Despite these limitations, several jurisdictions have already accumulated evidence of successful countermeasures against information operations. Initiatives such as the DSA, POFMA, the Anti-Infiltration Act, the SIM Registration Act, as well as NATO initiatives and Ukraine case studies, demonstrate measurable outcomes ranging from reductions

in cybercrime to increased transparency of political advertising. A summary of these successful practices and their outcomes is provided in Appendix B Table A3.

9.3. Risks of Censorship and Abuse by Government Agencies

Countering disinformation inevitably creates the temptation to interpret state powers broadly: the more "elastic" the legal basis and the broader the discretion of the authorities, the higher the likelihood that measures intended to protect the public interest will turn into a tool for suppressing criticism and controlling the public sphere. This is manifested in three interrelated practices: overly vague offenses, accelerated "emergency" procedures without due guarantees, and opaque administrative moderation delegated to platforms. International standards proceed from the opposite: any restrictions on freedom of expression are permissible only if they meet the test of legality, legitimacy of the goal, and necessity/proportionality of the intervention; otherwise, a "chilling effect" occurs, when citizens refrain from legitimate speech for fear of sanctions [560,561]. The risks of vagueness are most often associated with laws aimed at "false information", "fakes", or "undermining public order".

The joint declaration of the UN, OSCE, OAS and African Commission special rapporteurs (2017) explicitly recommended abandoning criminal law provisions based on vague categories of "falsehood" and instead strengthening government transparency and media literacy [562]. Similar conclusions are contained in the reports of the UN Special Rapporteurs on freedom of opinion and expression (D. Kaye; I. Khan): regulation of disinformation should be "a scalpel, not a sledgehammer," exclude criminal prosecution for honest misconceptions and protect investigative journalism and scientific debate [563,564]. When vague norms are backed up by high fines and accelerated blocking procedures, in practice it is critical and opposition speech that suffers the most—this is recorded in the annual reviews "Freedom on the Net" (Freedom House), which notes an increase in arbitrary blocking of media outlets, NGO pages and individual journalists under the pretext of combating "fakes" and "extremism" [565]. Emergency regimes and "fast" content-removal mechanisms pose a separate threat to procedural guarantees.

The European Court of Human Rights has consistently emphasized that the protection of freedom of expression also extends to information that "offends, shocks or disturbs" (Handyside v. the United Kingdom (1976)) and that interference must be justified by a "pressing social need," with sanctions and procedures proportionate to the aim [538]. The practice of instant blocking without judicial review, mass seizures of editorial equipment, long-term "temporary" bans on the dissemination of information—all this entails disproportionate damage to public discourse. The case of Delfi AS v. Estonia (2015) is also indicative, where the Court simultaneously recognized the admissibility of certain liability of intermediaries and pointed out the need for a delicate balance between the effectiveness of law enforcement and the prevention of excessive deletion of lawful speech [566]. If such regimes lack notifications to the addressee, reasoned decisions, prompt and effective means of appeal, independent review and statistical reporting, the risk of abuse increases sharply—this is indicated by both the Council of Europe recommendations on the roles of internet intermediaries (CM/Rec(2018)2) and the updated Santa Clara Principles on transparency and due process [552,553].

Another layer of abuse is structural measures affecting the communications infrastructure: targeted Internet shutdowns, traffic slowdowns, blocking of messaging apps and platforms during protests and elections. From the perspective of international law, such shutdowns are considered a "last resort" and, as a general rule, disproportionate, since they affect the rights of millions and paralyze access to vital information. This is how they are qualified in the reports of the Access Now ("KeepItOn") campaign and the

resolutions of the UN Human Rights Council calling on states to refrain from "deliberately disrupting access to information online" [567,568]. In practice, "blocks" are often used preventively, outside of a state of emergency and without clear legal argumentation, which makes them more compatible with the policy of control than with legitimate security protection. Finally, delegating moderation to platforms without a clear legal framework ("soft censorship") allows governments to influence the dissemination of content through "informal" channels—sending out "recommendations," closed work with "trusted informants" that is not subject to judicial review.

ARTICLE 19 and the OECD emphasize that such practices undermine accountability and turn platforms into quasi-governmental regulators without democratic constraints; a minimum set of guarantees includes public registers of government requests, user notifications, statistics on removed content, independent audits, and researchers' access to data [557,569]. Thus, the ethical and legal risks of combating disinformation stem not from the idea of regulation itself, but from the lack of legal precision, procedural guarantees, and independent control. These risks are mitigated by narrow and clearly defined legal frameworks (with priority given to civil and administrative remedies over criminal ones), judicial and quasi-judicial oversight, transparent notice-reason-appeal procedures, auditing of algorithms and risk assessments, and international principles that enshrine the priority of proportionality and necessity. Without these conditions, the fight against disinformation too easily turns into a fight against dissent—and thereby undermines the very resilience of societies that it is intended to protect.

10. Higher Education in the Context of Information Warfare: Crisis and the Need for a Paradigm Shift

The main target of the use of information warfare tools has apparently been and remains the higher education system. This is natural: it is here that highly qualified personnel and the worldview of the political, economic and scientific elite are formed, which subsequently influences the behavior of society as a whole. The most politically and economically active social groups become conduits of external influences, including influence on the sociocultural code of a particular country and ethnic group.

Consequently, the analysis of the influence of information warfare on the university sector requires an assessment of the current state of higher education. This is also important from the point of view of the basic thesis of this review: modern civilization is at a bifurcation point, and this logic fully applies to higher education. The initial question, therefore, is the nature of the modern interaction of higher education with society.

Without delving too deeply into history, let us begin in the early 19th century, when Wilhelm von Humboldt formulated the principles underlying the classical university, which flourished at the turn of the 19th and 20th centuries. These principles assumed that genuine higher education was possible only with the active involvement of students in scientific activities. This approach became one of the cornerstones of the second industrial revolution, which led to a radical transformation of lifestyle: electricity became a mass industrial commodity, the metro and tram networks of European cities developed, and industry grew rapidly.

However, at that time, higher education remained predominantly elite. Thus, in the Russian Empire, access was limited to certain social strata., As evidenced by the high cost of book collections: a private library could cost as much as a noble estate.

In the 20th century, the situation changed: higher education became mass. Today, universities everywhere face the "mass challenge": the need to train a large number of teachers, significant costs for teaching and infrastructure borne by families and the state. The impact of the higher education system on collective consciousness is growing, while

the tools that were effective at the turn of the 19th and 20th centuries are gradually losing their effectiveness. Professors are no longer the undisputed leaders of public opinion (especially noticeable in post-Soviet states); students increasingly draw their ideological guidelines from the Internet and social networks. Nevertheless, under certain conditions, higher education is capable of regaining its original positions.

The crises in higher education are caused, among other things, by objective factors previously considered in our works [570–572]. In particular, the curricula of most universities largely reproduce the disciplinary structure of science. By the beginning of the 21st century, this structure has become excessively differentiated, which now acts as a brake on scientific and technological progress [3]. In the sphere of higher education, the negative effect is even more pronounced, which is clearly seen in the example of Kazakhstan. A simple count of specialties and specializations demonstrates the staffing shortfalls in many areas, which prevents development of a full-fledged competitive environment. With a population of about 20 million people, it is objectively impossible to ensure the implementation of educational programs corresponding to such a ramified disciplinary grid.

This brings us back to the thesis stated at the beginning of the review—about the need for convergence of natural science, technical and humanitarian knowledge. If in traditional engineering fields (urban planning, civil engineering, etc.) the system oriented towards the paradigms of the early 20th century still functions largely by inertia, then in relation to the problems of information warfare, such an approach is clearly untenable.

This review shows that a specialist in the field of information warfare must master significant amounts of knowledge in both the humanities and technical fields. Moreover, when training strategists in this field, it is necessary to consider the development trajectories of computer technology and possible "black swans" caused by its non-trivial evolution. Today, most countries lack dedicated degree programs in this field; within the Humboldt paradigm, their creation is conceptually difficult.

The classical model assumed the sequence "first knowledge—then practice": a student must master a significant amount of theory, after which he or she can move on to practical activities. When prerequisite knowledge becomes excessive, this linear logic fails. The training of specialists must be based on other principles.

The problems of information warfare, therefore, require a transition to a new paradigm of higher education that better corresponds to the massification of higher education. Here, various issues are closely intertwined—from the influence of generative artificial intelligence already transforming higher education to the training of personnel for the education system itself. Both areas, as well as intermediate tasks, are at the forefront of information confrontation. Generative models influence collective consciousness, including via the university sector; the teaching corps, in turn, broadcast to society the narratives that they have learned in the process of professionalization. A fundamental task arises: is it possible to overcome them in the conditions of the historically established "capture" of the teaching corps by certain sets of narratives? A similar question arises regarding the use of GenAI.

Historical experience shows that overcoming such limitations is possible. The new most often matures within the old, overcoming it. However, in the context of information warfare, waiting for the "natural" course of change, as was the case in previous eras, seems an unacceptable luxury. Given the tasks of higher education, these processes require targeted acceleration. The post-industrial paradigm of continuous education, based on step-by-step training, where each subsequent step is closely related to practice, is increasingly relevant. A simple example is the training of FPV drone operators, for both civilian and military tasks. Having mastered the basic skills and demonstrated the results, the student moves on to the next level. In such a model, the key element is not examinations but motivation.

Today, access to high-quality educational resources is practically unlimited: there are high-level open courses, including courses from teachers at the Massachusetts Institute of Technology (MIT) and other universities. It is critical that the student sees the personal usefulness of knowledge at each stage. In practical terms, this means the possibility of starting at an early stage (for example, at the school level), developing basic skills in using technologies, and then selecting motivated participants for more advanced training. At the same time, there is no need to strictly reproduce traditional classroom practices; the educational process can be designed as a trajectory in which the content and level of requirements increase as practical effectiveness is proven.

In this regard, the role of broad humanities education of technical specialists increases. It is impossible to work effectively in the field of information warfare without mastering basic socio-political doctrines and the corresponding cultural and philosophical foundations. Modern society and the higher education system derived from it (especially in the field of technology, computer technology, etc.) often marginalize the general humanitarian component. However, the problems of information warfare demonstrate that this position is unstable: a professional in this field must combine the competencies of a technical specialist and a humanist.

The solution to this problem should be sought in integrative, step-by-step models of training: first, a demonstration of the practical necessity of training (not for the sake of a diploma, but for solving specific problems), then an awareness of the inevitability of the humanitarian component as a condition of professional competence. Step by step, a specialist is formed for whom training becomes a continuous process of a lifetime, and life experience is a source of strategic thinking. Such a trajectory should be organically woven into the system of higher education: there is no point in long-term accumulation of abstract information outside of practice. It is important that the practical significance of knowledge is manifested and realized at each stage of professional development.

11. Future Directions and Research Agenda

The rapid development of technologies, including artificial intelligence, neural interfaces, and automatic content-generation systems, is creating fundamentally new horizons for information warfare. If today the main focus is on social networks, recommendation algorithms, and manipulation of collective consciousness through digital media. Then in the near future we expect a shift to a deeper integration of influences at the cognitive and neurophysiological levels.

The scientific community increasingly explores the synthesis of approaches from various disciplines—from sociology and political science to neuroscience and computer modeling—which opens up opportunities for developing more accurate and personalized methods of protection. At the same time, there is a growing need for international collaborations to develop global standards for countering information threats and ensure adaptation to local conditions.

This section outlines promising areas of research, analyzes potential scenarios for the evolution of information warfare and identifies key challenges facing the academic and expert community in the coming years.

11.1. Interdisciplinary Syntheses: AI + Sociology + Law

The development of methods for countering modern forms of information warfare requires the integration of approaches from various scientific disciplines. New methodological frameworks are emerging at the intersection of artificial intelligence, sociology and law, allowing for the simultaneous consideration of technical, social, and regulatory aspects of information security.

Since the late 2010s, artificial intelligence (AI) has become the main technical engine in detecting and neutralizing disinformation. Deep learning algorithms are used to automatically identify fake content, recognize deepfakes, and analyze network structures for the dissemination of false narratives [573].

For example, studies by Ghorbanpour et al. [574] demonstrate the successful application of transformer architectures (BERT, RoBERTa) to automatically detect disinformation on polysemantic political topics. Yet, the researchers emphasize that purely algorithmic filtering does not take into account the sociocultural context and therefore requires supplementation with social-scientific approaches.

The sociological component helps explain how people perceive and disseminate information in the context of digital platforms. The work of Cinelli et al. (2021) [575] shows that even with the same content presentation, the perception of messages varies significantly depending on the structure of social connections and the algorithmic recommendations of platforms.

In this context, AI can be used to model information flows and filter bubbles, which makes it possible to predict which segments of society are most vulnerable to certain types of cognitive operations. However, correct interpretation requires sociological expertise to explain the cultural and political factors shaping media behavior.

The legal aspect forms the regulatory framework that defines the boundaries of the permissible use of AI in the fight against disinformation. The European "Digital Services Act" (2022) [576] and the draft "AI Act" (expected to be adopted in 2025) [577] introduce mandatory requirements for the transparency of algorithms and the risk assessment of automated systems. The interaction of AI with law here is two-way: on the one hand, legislation limits the use of technologies to avoid censorship and discrimination; on the other hand, it stimulates the development of more transparent and accountable algorithms. An example is the research by Gorwa et al. [578], which analyzes the legal liability of platforms for automatic content moderation.

Effective integration of AI, sociology and law requires the creation of interdisciplinary research platforms where algorithm developers work closely with social researchers and lawyers. Such projects are already being implemented in the EU within the framework of the Horizon Europe program, for example, the MediaResist project (2022–2025) [579], which develops tools to assess the information resilience of society considering both technological and socio-cultural and legal factors. Thus, interdisciplinary synthesis enables more precise and ethically justified technologies for countering information warfare, minimizing the risks of excessive interference and simultaneously increasing the effectiveness of protection.

11.2. Scenarios of the Information War of the Future: From Cyber Operations to Neural Interfaces

The future of information warfare forms at the intersection of cyber operations, cognitive technologies, and neural interfaces. If in the 2010s the key tools were social media, botnets, and cyberattacks on infrastructure. Then in the 2030s and 2040s a transition to complex hybrid operations is predicted that combine the management of information flows, direct influence on cognitive processes, and integration with brain–computer interface (BCI) technology [580,581]. Classic cyber operations of the future include not only hacking and data leaks, but also their instant transformation into disinformation campaigns using generative AI. Automation of the creation of falsified content (deepfake 2.0) allows messages to be adapted in real time to the psychological profiles of the target audience [582]. Such capabilities are already being demonstrated in experiments on "personalized propaganda," where algorithms select arguments based on behavioral data [81].

The most radical direction will be the development of BCI and neurostimulation technologies that allow direct recording and, in the future, modification of brain activity

patterns. Research in DARPA (N3 program) [583] and Chinese military projects on "intellectual warfare" (Intelligentized Warfare) [584] already indicate the possibility of integrating neural interfaces into military and intelligence systems. Such technologies can potentially be used to transmit information, train, or manipulate the operator's emotional states in combat or political missions [585].

Next-generation AI systems will be able to act as autonomous "information agents" that conduct long-term communications with target subjects, simulating social connections and forming long-term influence. Research in the field of social bots and conversational AI shows that people can form trust in autonomous digital agents [586], which in the context of future IW could become critically dangerous. In parallel, the field of neuromarketing and applied cognitive technologies is developing, where incentives are selected based on biometric and psychophysiological indicators [587]. The use of these methods in a military context will allow for "targeted" cognitive attacks that affect decision-making in crisis situations [588].

Future IW scenarios suggest the emergence of "personalized information bubbles" created based on continuous analysis of user data in combination with access to their neuroprofile. This will lead to the need to develop fundamentally new security measures, including "cognitive firewalls"—systems that filter incoming information at the level of sensory perception [589].

The shift in emphasis from mass information campaigns to individualized neurocommunications creates a legal vacuum. International humanitarian law and cybersecurity norms do not yet include provisions directly regulating the use of BCI in military or propaganda operations [590]. In 2021, the European Parliament adopted a resolution on human rights in the era of neurotechnology [591], but it is advisory in nature. By the middle of the 21st century, information warfare may transform into an integrated system of "info-neuro-cyber operations," where the key target will be not just the information field, but the human cognitive architecture. This requires the accelerated development of interdisciplinary defense strategies that include technical, legal, cultural, and neuropsychological measures.

12. Conclusions

In conclusion, modern forms of information warfare are a multilayered phenomenon, where traditional manipulation methods are enhanced by digital technologies, from personalization algorithms to generative AI. The review shows that effective counteraction requires a comprehensive approach: from understanding cognitive and social mechanisms to applying advanced computational methods (FGT, RNS) and to implementing legal frameworks. Despite progress in identifying threats, challenges remain—ethical dilemmas, censorship risks, and the evolution of attacks toward the neurocognitive level. Further research should focus on interdisciplinary syntheses, international standards, and adaptive defense systems to ensure the resilience of society in the era of information dominance.

Materials presented in the review confirm once again that the problems of information warfare are multifaceted, covering both humanitarian and technical aspects. In the technical dimension, the development of new computing systems aimed at gradually approaching the biological prototype—the human brain—is of particular importance. The study of such problems can serve as a tool for waging information warfare, since the attitude towards various versions of the concept of transhumanism remains extremely ambiguous. At the same time, the identification of certain prospects for the further development of humanity inevitably affects public consciousness, forming corresponding research directions and setting new vectors of scientific research.

One of the main conclusions that follows from the analysis is the need to move to a different paradigm of higher education based on the principle of convergence of natural

science, technical, and humanitarian knowledge. This principle is of universal importance for the education system as a whole, but the inertia of social structures, especially such a conservative system as the university, makes the transformation of paradigms an extremely slow and difficult process. The problems of information warfare in this context play a special role, since they clearly demonstrate that the existing disciplinary structure of science creates critically important obstacles, including those affecting the development of higher education. Consequently, this area can become the driver of the practical implementation of new educational models.

At the same time, the problems of information warfare are not limited to the sphere of higher education, although the latter occupies a key place in the formation of the sociocultural code. Of significant importance is also the development of new computing systems that are capable of being complementary to the structure of society to a certain extent. No less important is the provision of forms of interaction with the suprapersonal level of information processing. It can be assumed that many key contradictions associated with information warfare will be determined precisely by the struggle for influence on this level, since artificial intelligence, as shown in the review, already performs the function of an intermediary between the individual and suprapersonal levels of information processing.

Author Contributions: Conceptualization, A.B.; methodology, A.B. and I.S.; formal analysis, A.B.; writing—original draft preparation, A.B.; writing—review and editing, A.B. and I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan: AP26104635.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Extended comparison of ML/NLP and DSP-based approaches across technical dimensions.

Approach	Noise Resilience	Parallelism	Determinism	Resource Footprint	Interpretability	Key Limitations
Text ML/NLP	Medium (sensitive to noisy inputs)	Limited (GPU/TPU acceleration)	Stochastic	High (large-scale clusters)	Low	Requires large corpora, prone to overfitting
Graph-based	Medium	Medium–high	Stochastic	High	Medium	Quality of graph construction critical
Multimodal deep	Medium	Limited	Stochastic	Very high	Low	Needs multimodal datasets, high training cost
Rule-based	High	Low	Full	Low	High	Limited scalability, rigid to novel patterns
DSP—RNS	High	Very high	Full	Low–medium	Medium	Complex reconstruction (CRT), modulus choice
DSP—FGT	High	High	Full	Low	Medium	Limited adoption, specialized expertise needed
DSP—Partial conv.	High	Medium	Full	Low	Medium	Requires domain consistency, niche visibility
DSP—Finite-field	High	High	Full	Very low	Medium	Restricted to GF(p) tasks
Hybrid ML + DSP	High	Medium	Partial	Medium	Medium	Integration overhead, trade-off management

Appendix B

Table A2. Regulatory Measures to Counter Disinformation: Europe, Asia and National Practices.

Document/Act	Region/Country	Year	Key Points	Connection with Information Warfare	Status
Law on Online Platforms and Online Advertising	Kazakhstan	2023	Requires large social media platforms and messengers to appoint a local legal representative, enforce removal of prohibited content (including “false information”), ensure transparency of advertising revenues, and cooperate with state authorities on content moderation	Used to counter disinformation campaigns and foreign information influence, though raising concerns on freedom of expression	In force
Digital Services Act (DSA)	EU	2022	Mandatory risk assessments for VLOPs, audits, researcher access to data, crisis protocols	Reduces the risks of disinformation, election interference and erosion of trust	Comes into full effect 2024–2025

Table A2. *Cont.*

Document/Act	Region/Country	Year	Key Points	Connection with Information Warfare	Status
NetzDG	Germany	2017	«Notice-and-action», reporting of complaints, penalties for failure to meet deadlines	Rapid response to disinformation and extremist content	In force
Online Safety Act	United Kingdom	2023	«Duty of care», systematic risk assessment, Ofcom supervision, "safety by design"	Combating malicious and disinformation content	In force
Santa Clara Principles	Global (civil society initiative)	2018/updated 2021	Moderation transparency, user notifications, right of appeal	Increases trust, reduces chilling effect	Voluntary (soft law)
Council of Europe Recommendation CM/Rec(2018)2	EU	2018	Roles of Internet intermediaries, transparency, responsibility	Conceptual Framework for Countering IW	Soft law
POFMA	Singapore	2019	Mandatory correction directions, liability for refusal	Quickly correct false claims on the web	In force
Cybersecurity Act	China	2017	Control of critical infrastructure and platforms	Strengthening supervision of the digital environment	In force
Data Law	China	2021	Regulation of data circulation, state control	Used in cyber and information operations	In force
Personal Information Law	China	2021	Rules for processing and protecting user data	Control over targeting and disinformation	In force
Regulation on Deep Synthesis	China	2022	Deepfakes labeling requirements, prohibition of manipulative use	Direct protection against deepfake usage in IW	In force
Anti-Infiltration Act	Taiwan	2020	Limiting External Campaign Funding, NCC Measures Against Disinformation	Countering foreign information operations	In force
IT Rules (Intermediary Guidelines)	India	2021	Increased responsibilities of intermediaries, grievance officers, transparency of algorithms	Controlling the digital environment, limiting IW campaigns	In force
Digital Personal Data Protection Act	India	2023	Rules for processing personal data, restrictions on targeting	Reducing manipulation through advertising and data	In force
Cybersecurity Law + Decree 53	Vietnam	2019/2022	Removal of false information, data localization	Control of global platforms, limitation of IW	In force
Personal Data (Privacy) Ordinance (Amendment)	Hong Kong	2021	Criminalization of doxxing, PCPD orders	Counteracting manipulative distortions and attacks on personalities	In force
SIM Registration Act	Philippines	2022	Mandatory SIM registration, limitation of anonymity	Reducing the scope of anonymous disinformation	In force
ITE Law Amendments	Indonesia	2008 (amendments 2020s)	Clarification of the concept of slander, criminalization of "false statements"	Used to control discourse, sometimes criticized for censorship	In force

Table A3. Successful cases of counteracting IW and related online risks: measures and results.

Jurisdiction/Program	Key Measures	Period/Case	Result/Metric
EU—Digital Services Act (DSA) Transparency Database	Mandatory publication of "statements of reasons" for moderation; publicly accessible dashboard and API	2024–2025	Hundreds of millions/billions of records in the database; research access and comparability of moderation practices between VLOP/VLOSE
EU—DSA: Ensuring election integrity	Risk assessments and mitigating measures for elections; European Commission supervision	2023 (parliamentary elections in Slovakia) → 2024–2025 scaling	EC notes change in VLOPs approaches to electoral integrity within DSA; development of transparency procedures
EU—Strengthened Code of Practice on Disinformation	Voluntary-mandatory reporting of platforms (Google, Meta, Microsoft, TikTok): demonetization, political advertising, metrics	2023 (second reporting wave)	Regular semi-annual reports on the implementation of commitments; launch of a transparency center
Singapore—POFMA	Mandatory Correction Directions, blocking if not followed	2019–2022	Recorded: 69 CD, 13 TCD, 5 GCD and other measures by 30 June 2022; formalized and prompt corrections of false statements
Taiwan: Countering Election Disinformation	Coordination of government agencies, fact-checking, civil society involvement, rapid refutations	Presidential elections 2024	The integrity of the vote was preserved; large-scale ballot stuffing was quickly eliminated (example with a "cut" video)
Hong Kong—Anti-doxxing (PDPO Amendments 2021)	PCPD's authority to issue cessation notices, criminal prosecution	2021–2023	>17,700 doxxing posts to remove, >90–95% compliance; hundreds of investigations, dozens of arrests
Philippines—SIM Registration Act	Mandatory SIM registration to reduce anonymous abuse	2023–2024	Police recorded −42.9% of cybercrimes after full implementation; (in parallel—blocking billions of spam SMS)
Meta—Oversight Board (procedural guarantees)	Independent review of moderation decisions; public decisions and recommendations	2023	53 decisions; ~90%—cancelation of original Meta decisions; expansion of areas (PoW, hate speech, etc.)
Google—Ads Safety/Ads Transparency	Filtering/blocking "bad" ads with ML systems; political advertising transparency centers	2023	Large-scale preventive blocking of "bad" ads (ML/GenAI support); centralized access to political advertising
Ukraine—blackout prevention	CERT-UA, ESET, etc.: early detection, interdepartmental coordination, OT protection	2022	Sandworm attack on power grid thwarted before widespread blackout; cyber resilience gains confirmed

References

1. Hilbert, M. Digital technology and social change: The digital transformation of society from a historical perspective. *Dialogues Clin. Neurosci.* **2020**, *22*, 189–194. [CrossRef] [PubMed]
2. Van Veldhoven, Z.; Vanthienen, J. Digital transformation as an interaction-driven perspective between business, society, and technology. *Electron. Mark.* **2022**, *32*, 629–644. [CrossRef]
3. Suleimenov, I.; Gabrielyan, O.; Matrassulova, D. Philosophical foundations of sciences and prospects of multivalued logic in describing thinking. *Sci. Educ.* **2025**, 1–19. [CrossRef]
4. O'dEa, X. Generative AI: Is it a paradigm shift for higher education? *Stud. High. Educ.* **2024**, *49*, 811–816. [CrossRef]
5. Lim, W.M.; Gunasekara, A.; Pallant, J.L.; Pallant, J.I.; Pechenkina, E. Generative AI and the future of education: Ragnarök or reformation? A paradoxical perspective from management educators. *Int. J. Manag. Educ.* **2023**, *21*, 100790. [CrossRef]
6. Wach, K.; Duong, C.D.; Ejdys, J.; Kazlauskaitė, R.; Korzynski, P.; Mazurek, G.; Paliszkiewicz, J.; Ziemba, E. The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. *Entrep. Bus. Econ. Rev.* **2023**, *11*, 7–30. [CrossRef]
7. Michel-Villarreal, R.; Vilalta-Perdomo, E.; Salinas-Navarro, D.E.; Thierry-Aguilera, R.; Gerardou, F.S. Challenges and opportunities of generative AI for higher education as explained by ChatGPT. *Educ. Sci.* **2023**, *13*, 856. [CrossRef]
8. Kalimoldayev, M.N.; Pak, I.T.; Baipakbayeva, S.T.; Mun, G.A.; Shaltykova, D.B.; Suleimenov, I.E. Methodological basis for the development strategy of artificial intelligence systems in the Republic of Kazakhstan in the message of the president of the Republic of Kazakhstan dated October 5, 2018. *News Natl. Acad. Sci. Repub. Kazakhstan–Ser. Geol. Tech. Sci.* **2018**, *6*, 47–54. [CrossRef]
9. Gumyusenge, A.; Melianas, A.; Keene, S.T.; Salleo, A. Materials strategies for organic neuromorphic devices. *Annu. Rev. Mater. Res.* **2021**, *51*, 47–71. [CrossRef]
10. Krauhausen, I.; Koutsouras, D.A.; Melianas, A.; Keene, S.T.; Lieberth, K.; Ledanseur, H.; Sheelamanthula, R.; Giovannitti, A.; Torricelli, F.; Mcculloch, I.; et al. Organic neuromorphic electronics for sensorimotor integration and learning in robotics. *Sci. Adv.* **2021**, *7*, eabl5068. [CrossRef]
11. Li, J.; Fan, F.; Fu, X.; Liu, M.; Chen, Y.; Zhang, B. Building uniformly structured polymer memristors via a 2D conjugation strategy for neuromorphic computing. *Macromol. Rapid Commun.* **2024**, *46*, e2400172. [CrossRef]
12. Niu, X.; Tian, B.; Zhu, Q.; Dkhil, B.; Duan, C. Ferroelectric polymers for neuromorphic computing. *Appl. Phys. Rev.* **2022**, *9*, 021309. [CrossRef]
13. Suleimenov, I.; Gabrielyan, O.; Kopishev, E.; Kadyrzhan, A.; Bakirov, A.; Vitulyova, Y. Advanced Applications of Polymer Hydrogels in Electronics and Signal Processing. *Gels* **2024**, *10*, 715. [CrossRef] [PubMed]
14. Seo, D.-G.; Lee, Y.; Go, G.-T.; Pei, M.; Jung, S.; Jeong, Y.H.; Lee, W.; Park, H.-L.; Kim, S.-W.; Yang, H.; et al. Versatile neuromorphic electronics by modulating synaptic decay of single organic synaptic transistor: From artificial neural networks to neuro-prosthetics. *Nano Energy* **2019**, *65*, 104035. [CrossRef]
15. Erokhin, V.; Karabulatova, I.S. Neuromorphic Elements as a First Step Towards Sociomorphic Systems. *BioNanoScience* **2025**, *15*, 1–10. [CrossRef]
16. Kahneman, D. *Thinking, Fast and Slow*; Farrar, Straus and Giroux: New York, NY, USA, 2011.
17. Stanovich, K.E.; West, R.F. Individual differences in reasoning: Implications for the rationality debate? *Behav. Brain Sci.* **2000**, *23*, 645–665. [CrossRef]
18. Lewandowsky, S.; Ecker, U.K.H.; Cook, J. Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. *J. Appl. Res. Mem. Cogn.* **2017**, *6*, 353–369. [CrossRef]
19. Nickerson, R.S. Confirmation bias: A ubiquitous phenomenon in many guises. *Rev. Gen. Psychol.* **1998**, *2*, 175–220. [CrossRef]
20. Pariser, E. *The Filter Bubble: What the Internet Is Hiding from You*; Penguin Press: New York, NY, USA, 2011.
21. Flaxman, S.; Goel, S.; Rao, J.M. Filter bubbles, echo chambers, and online news consumption. *Public Opin. Q.* **2016**, *80*, 298–320. [CrossRef]
22. Fazio, L.K.; Brashier, N.M.; Payne, B.K.; Marsh, E.J. Knowledge does not protect against illusory truth. *J. Exp. Psychol. Gen.* **2015**, *144*, 993–1002. [CrossRef]
23. Lewandowsky, S.; Ecker, U.; Seifert, C.; Schwarz, N.; Cook, J. Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychol. Sci. Public Interest* **2012**, *13*, 106–131. [CrossRef] [PubMed]
24. Dechêne, A.; Stahl, C.; Hansen, J.; Wänke, M. The Truth About the Truth: A Meta-Analytic Review of the Truth Effect. *Pers. Soc. Psychol. Rev.* **2009**, *14*, 238–257. [CrossRef] [PubMed]
25. Tversky, A.; Kahneman, D. Judgment under Uncertainty: Heuristics and Biases. *Science* **1974**, *185*, 1124–1131. [CrossRef]
26. Furnham, A.; Boo, H.C. A literature review of the anchoring effect. *J. Socio-Econ.* **2011**, *40*, 35–42. [CrossRef]
27. Thorndike, E. A constant error in psychological ratings. *J. Appl. Psychol.* **1920**, *4*, 25–29. [CrossRef]
28. Murdock, B.B. The serial position effect of free recall. *J. Exp. Psychol.* **1962**, *64*, 482–488. [CrossRef]

29. Lord, C.G.; Ross, L.; Lepper, M.R. Biased assimilation and attitude polarization: The effects of prior theories on subsequently considered evidence. *J. Pers. Soc. Psychol.* **1979**, *37*, 2098–2109. [CrossRef]
30. Entman, R.M. Framing: Toward clarification of a fractured paradigm. *J. Commun.* **1993**, *43*, 51–58. [CrossRef]
31. Marcus, G.E.; Neuman, W.R.; MacKuen, M. *Affective Intelligence and Political Judgment*; University of Chicago Press: Chicago, IL, USA, 2000.
32. Lerner, J.S.; Li, Y.; Valdesolo, P.; Kassam, K.S. Emotion and decision making. *Annu. Rev. Psychol.* **2015**, *66*, 799–823. [CrossRef]
33. Brady, W.J.; Wills, J.A.; Jost, J.T.; Tucker, J.A.; Van Bavel, J.J. Emotion shapes the diffusion of moralized content in social networks. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 7313–7318. [CrossRef]
34. Ross, L.; Greene, D.; House, P. The false consensus effect. *J. Exp. Soc. Psychol.* **1977**, *13*, 279–301. [CrossRef]
35. Murray, S.C. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*; Houghton Mifflin: New York, NY, USA, 1983.
36. Harris, L.T.; Fiske, S.T. Social groups that elicit disgust are differentially processed in mPFC. *Soc. Cogn. Affect. Neurosci.* **2007**, *2*, 45–51. [CrossRef] [PubMed]
37. Westen, D.; Blagov, P.S.; Harenski, K.; Kilts, C.; Hamann, S. Neural bases of motivated reasoning: An fMRI study of emotional constraints on partisan political judgment in the 2004 US presidential election. *J. Cogn. Neurosci.* **2006**, *18*, 1947–1958. [CrossRef] [PubMed]
38. Craig, R.T. Communication theory as a field. *Commun. Theory* **1999**, *9*, 119–161. [CrossRef]
39. McQuail, D.; Windahl, S. *Communication Models for the Study of Mass Communications*; Routledge: London, UK, 2015.
40. Lasswell, H.D. The structure and function of communication in society. In *The Communication of Ideas*; Bryson, L., Ed.; Harper: New York, NY, USA, 1948; pp. 37–51.
41. Severin, W.J.; Tankard, J.W. *Communication Theories: Origins, Methods, and Uses in the Mass Media*; Longman: New York, NY, USA, 1992; pp. 265–266.
42. Katz, E.; Lazarsfeld, P.F.; Roper, E. *Personal Influence: The Part Played by People in the Flow of Mass Communications*; Routledge: London, UK, 2017.
43. Dubois, E.; Gaffney, D. The multiple facets of influence: Identifying political influentials and opinion leaders on Twitter. *Am. Behav. Sci.* **2014**, *58*, 1260–1277. [CrossRef]
44. Bakshy, E.; Rosenn, I.; Marlow, C.; Adamic, L. The role of social networks in information diffusion. In Proceedings of the WWW 2012: 21st World Wide Web Conference, Lyon, France, 16–20 April 2012; pp. 519–528.
45. Arnaboldi, V.; Conti, M.; Passarella, A.; Dunbar, R.I. Online social networks and information diffusion: The role of ego networks. *Online Soc. Netw. Media* **2017**, *1*, 44–55. [CrossRef]
46. Tandoc, E.C., Jr.; Lim, Z.W.; Ling, R. Defining "fake news" A typology of scholarly definitions. *Digit. J.* **2018**, *6*, 137–153.
47. Goldman, A.I. A guide to social epistemology. In *Social Epistemology: Essential Readings*; Oxford University Press: Oxford, UK, 2011; pp. 11–37.
48. Resnik, D. Social epistemology and the ethics of research. *Stud. Hist. Philos. Sci. Part A* **1996**, *27*, 565–586. [CrossRef]
49. Lewandowsky, S.; Smillie, L.; Garcia, D.; Hertwig, R.; Weatherall, J.; Egidy, S.; Robertson, R.E.; O'connor, C.; Kozyreva, A.; Lorenz-Spreen, P.; et al. Technology and democracy: Understanding the influence of online technologies on political behaviour and decision-making. *Phil. Trans. R. Soc. A* **2020**, *378*, 20190317.
50. Levy, N. In trust we trust: Epistemic vigilance and responsibility. *Soc. Epistem.* **2022**, *36*, 283–298. [CrossRef]
51. Farkas, J.; Schou, J. *Post-Truth, Fake News and Democracy: Mapping the Politics of Falsehood*; Routledge: London, UK, 2023.
52. Douglas, K.M.; Uscinski, J.E.; Sutton, R.M.; Cichocka, A.; Nefes, T.; Ang, C.S.; Deravi, F. Understanding conspiracy theories. *Politics Psychol.* **2019**, *40*, 3–35. [CrossRef]
53. Borgatti, S.P.; Mehra, A.; Brass, D.J.; Labianca, G. Network analysis in the social sciences. *Science* **2009**, *323*, 892–895. [CrossRef]
54. Freeman, L.C. A Set of measures of centrality based on betweenness. *Sociometry* **1977**, *40*, 35–41. [CrossRef]
55. Pastor-Satorras, R.; Castellano, C.; Van Mieghem, P.; Vespignani, A. Epidemic processes in complex networks. *Rev. Mod. Phys.* **2015**, *87*, 925–979. [CrossRef]
56. Roozenbeek, J.; van der Linden, S. The fake news game: Actively inoculating against the risk of misinformation. *J. Risk Res.* **2018**, *22*, 570–580. [CrossRef]
57. Jamieson, K.H. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know*; Oxford University Press: Oxford, UK, 2020.
58. McCombs, M.E.; Shaw, D.L. The agenda-setting function of mass media. *Public Opin. Q.* **1972**, *36*, 176–187. [CrossRef]
59. Entman, R.M. Framing media power. *Inf. Commun. Soc.* **2010**, *13*, 163–183.
60. Highfield, T.; Leaver, T. Instagrammatics and digital methods: Studying visual social media, from selfies and GIFs to memes and emoji. *Commun. Res. Pract.* **2016**, *2*, 47–62. [CrossRef]
61. Yang, S. *Networks: An Introduction by MEJ Newman*; Oxford University Press: Oxford, UK, 2013; 720p.
62. Watts, D.J.; Strogatz, S.H. Collective dynamics of 'small-world' networks. *Nature* **1998**, *393*, 440–442. [CrossRef]
63. Barabási, A.-L.; Albert, R. Emergence of scaling in random networks. *Science* **1999**, *286*, 509–512. [CrossRef]

64. Vziatysheva, V. How fake news spreads online? *Int. J. Media Inf. Lit.* **2020**, *5*, 217. [CrossRef]
65. Kermack, W.O.; McKendrick, A.G. A contribution to the mathematical theory of epidemics. *Proc. R. Soc. Lond. Ser. A Contain. Pap. Math. Phys. Character* **1927**, *115*, 700–721. [CrossRef]
66. Daley, D.J.; Kendall, D.G. Stochastic rumours. *IMA J. Appl. Math.* **1965**, *1*, 42–55. [CrossRef]
67. Granovetter, M. Threshold models of collective behavior. *Am. J. Sociol.* **1978**, *83*, 1420–1443. [CrossRef]
68. Borge-Holthoefer, J.; Perra, N.; Gonçalves, B.; González-Bailón, S.; Arenas, A.; Moreno, Y.; Vespignani, A. The dynamics of information-driven coordination phenomena: A transfer entropy analysis. *Sci. Adv.* **2016**, *2*, e1501158. [CrossRef]
69. Macal, C.; North, M. Tutorial on agent-based modelling and simulation. *J. Simul.* **2010**, *4*, 151–162. [CrossRef]
70. Islam, S.; Sarkar, T.; Khan, S.H.; Kamal, A.-H.M.; Hasan, S.M.M.; Kabir, A.; Yeasmin, D.; Islam, M.A.; Chowdhury, K.I.A.; Anwar, K.S.; et al. COVID-19–related infodemic and its impact on public health. *Am. J. Trop. Med. Hyg.* **2020**, *103*, 1621–1629. [CrossRef]
71. Lerman, K.; Ghosh, R. Information contagion: An empirical study of the spread of news on digg and twitter social networks. In Proceedings of the International AAAI Conference on Web and Social Media, Washington, DC, USA, 23–26 May 2010; Volume 4, pp. 90–97. [CrossRef]
72. Ferrara, E.; Yang, Z. Measuring emotional contagion in social media. *PLoS ONE* **2015**, *10*, e0142390. [CrossRef]
73. Kenah, E.; Robins, J.M. Second look at the spread of epidemics on networks. *Phys. Rev. E* **2007**, *76*, 036113. [CrossRef]
74. Allen, J.; Howland, B.; Mobius, M.; Rothschild, D.; Watts, D.J. Evaluating the fake news problem at the scale of the information ecosystem. *Sci. Adv.* **2020**, *6*, eaay3539. [CrossRef]
75. Howard, P.N.; Kollanyi, B. Bots, #StrongerIn, and #Brexit: Computational propaganda during the UK-EU referendum. *arXiv* **2016**, arXiv:1606.06356. [CrossRef]
76. Kivelä, M.; Arenas, A.; Barthelemy, M.; Gleeson, J.P.; Moreno, Y.; Porter, M.A. Multilayer networks. *J. Complex Netw.* **2014**, *2*, 203–271. [CrossRef]
77. Simon, H.A. Designing organizations for an information-rich world. *Int. Libr. Crit. Writ. Econ.* **1996**, *70*, 187–202.
78. Davenport, T.H.; Beck, J.C. The attention economy. *Ubiquity* **2001**, *2001*, 1-es. [CrossRef]
79. Wu, T. *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*; Vintage: New York, NY, USA, 2017.
80. Ricci, F.; Rokach, L.; Shapira, B. Recommender systems: Techniques, applications, and challenges. In *Recommender Systems Handbook*; Springer Nature: New York, NY, USA, 2021; pp. 1–35.
81. Bakshy, E.; Messing, S.; Adamic, L.A. Exposure to ideologically diverse news and opinion on Facebook. *Science* **2015**, *348*, 1130–1132. [CrossRef]
82. Ribeiro, M.H.; Ottoni, R.; West, R.; Almeida, V.A.F.; Meira, W. Auditing radicalization pathways on YouTube. In Proceedings of the FAT* '20: Conference on Fairness, Accountability, and Transparency, Barcelona, Spain, 27–30 January 2020; pp. 131–141.
83. Tufekci, Z. Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Technol. Law J.* **2015**, *13*, 203–218.
84. Pennycook, G.; Rand, D.G. Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. *Cognition* **2019**, *188*, 39–50. [CrossRef]
85. Sen, A.; Sengupta, S. Digital revolution and information age: Emergence of economies of attention. *Technology* **2021**, *6*, 89–95.
86. Starbird, K. Disinformation's spread: Bots, trolls and all of us. *Nature* **2019**, *571*, 449. [CrossRef]
87. NATO StratCom COE. *Social Media as a Tool of Hybrid Warfare*; NATO StratCom Centre of Excellence: Riga, Latvia, 2016. Available online: https://stratcomcoe.org (accessed on 8 August 2025).
88. EUvsDisinfo. Disinformation and Digital Platforms: The EU Response; European External Action Service. Available online: https://euvsdisinfo.eu (accessed on 8 August 2025).
89. Starbird, K.; Wilson, T. Cross-platform disinformation campaigns: Lessons learned and next steps. *Harv. Kennedy Sch. Misinf. Rev.* **2020**, *1*, 10171226. [CrossRef]
90. Alonso-Muñoz, L.; Tirado-García, A.; Casero-Ripollés, A. Telegram in campaign: The use of mobile instant messaging services in electoral political communication. *Commun. Soc.* **2022**, *35*, 71–88. [CrossRef]
91. Libicki, M.C. *Conquest in Cyberspace: National Security and Information Warfare*; Cambridge University Press: Cambridge, UK, 2007.
92. Pomerantsev, P. *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia*; Public Affairs: New York, NY, USA, 2014.
93. Paul, C.; Matthews, M. The Russian "firehose of falsehood" propaganda model. *Rand Corp.* **2016**, *2*, 1–10.
94. Sacilotto, M.S.G. Allied joint doctrine for strategic communications. *NRDC-GR Her.* **2023**.
95. US SOCOM. *Special Operations Forces Vision & Strategy 2030*; United States Special Operations Command: Tampa, FL, USA, 2020.
96. US Army. *The U.S. Army in Multi-Domain Operations 2028*; TRADOC Pamphlet 525-3-1; U.S. Army Training and Doctrine Command: Fort Eustis, VA, USA, 2018.
97. Russian Federation. *Doctrine of Information Security of the Russian Federation*; Russian Federation: Moscow, Russia, 2016.
98. NATO StratCom COE. *Russia's Footprint in the Nordic-Baltic Information Environment*; NATO StratCom COE: Riga, Latvia, 2020.
99. Mulvenon, J.C. Chinese Cyber Espionage. Hearing on Chinese Hacking: Impact on Human Rights and Commercial Rule of Law. *Congr.-Exec. Comm. China* **2013**, *25*, 2013.

100. State Council of the PRC. *China's National Defense in the New Era*; PRC: Beijing, China, 2019.
101. Hoffman, F.G. *Conflict in the 21st Century: The Rise of Hybrid Wars*; Potomac Institute: Arlington, VA, USA, 2007.
102. Fridman, O. *Russian "Hybrid Warfare": Resurgence and Politicization*; Oxford University Press: Oxford, UK, 2018.
103. Chesney, B.; Citron, D. Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. Law Rev.* **2019**, *107*, 1753–1820. [CrossRef]
104. Tufekci, Z. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*; Yale University Press: Yale, CT, USA, 2017.
105. Helmus, T.C.; Bodine-Baron, E.; Radin, A.; Magnuson, M.; Mendelsohn, J.; Marcellino, W.; Bega, A.; Winkelman, Z. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*; RAND Corporation: Santa Monica, CA, USA, 2018. [CrossRef]
106. NATO Innovation Hub. Cognitive Warfare; NATO. Available online: https://innovationhub-act.org (accessed on 8 August 2025).
107. US Army Cyber Institute. *Cognitive Domain Training Scenarios*; US Army Cyber Institute: New York, NY, USA, 2022.
108. Singer, P.W.; Brooking, E.T. *LikeWar: The Weaponization of Social Media*; Houghton Mifflin Harcourt: Boston, MA, USA, 2018.
109. Floridi, L. On human dignity as a foundation for the right to privacy. *Philos. Technol.* **2016**, *29*, 307–312. [CrossRef]
110. Wardle, C.; Derakhshan, H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*; Council of Europe: Strasbourg, France, 2017.
111. Fallis, D. What is disinformation? *Libr. Trends* **2015**, *63*, 401–426. [CrossRef]
112. Anderau, G. Defining fake news. *Kriter. J. Philos.* **2021**, *35*, 197–215. [CrossRef]
113. Lazer, D.M.J.; Baum, M.A.; Benkler, Y.; Berinsky, A.J.; Greenhill, K.M.; Menczer, F.; Metzger, M.J.; Nyhan, B.; Pennycook, G.; Rothschild, D.; et al. The science of fake news. *Science* **2018**, *359*, 1094–1096. [CrossRef]
114. Howard, P.N.; Ganesh, B.; Liotsiou, D.; Kelly, J.; François, C. *The IRA, Social Media and Political Polarization in the United States 2012–2018*; Oxford Internet Institute: Oxford, UK, 2018.
115. Frame, A.; Brachotte, G. Engineering victory and defeat: The role of social bots on Twitter during the French Presidential Elections. In *Comparing Two Outsiders' 2016–17 Wins: Trump & Macron's Campaigns*; Presses Universitaires de France: Paris, France, 2018.
116. Bastos, M.T.; Mercea, D. The Brexit botnet and user-generated hyperpartisan news. *Soc. Sci. Comput. Rev.* **2017**, *37*, 38–54. [CrossRef]
117. Guess, A.M.; Nyhan, B.; Reifler, J. Exposure to untrustworthy websites in the 2016 US election. *Nat. Hum. Behav.* **2020**, *4*, 472–480. [CrossRef]
118. Klayman, J. Varieties of confirmation bias. *Psychol. Learn. Motiv.* **1995**, *32*, 385–418.
119. Hassan, A.; Barber, S.J. The effects of repetition frequency on the illusory truth effect. *Cogn. Res. Princ. Implic.* **2021**, *6*, 1–12. [CrossRef]
120. Sismondo, S. Post-truth? *Soc. Stud. Sci.* **2017**, *47*, 3–6. [CrossRef]
121. Paul, C.; Matthews, M. *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*; RAND Corporation: Santa Monica, CA, USA, 2016.
122. Zarocostas, J. How to fight an infodemic. *Lancet* **2020**, *395*, 676. [CrossRef]
123. Bennett, W.L.; Livingston, S. The disinformation order: Disruptive communication and the decline of democratic institutions. *Eur. J. Commun.* **2018**, *33*, 122–139. [CrossRef]
124. Brantner, C.; Geise, S.; Lobinger, K. Fractured Paradigm? Theories, concepts and methodology of visual framing research: A systematic review. In Proceedings of the Annual Conference of the International Communication Association (ICA)—Visual Communication Studies Division, Phoenix, AZ, USA, 24–28 May 2012; pp. 1–40.
125. Starbird, K.; Arif, A.; Wilson, T. Disinformation as collaborative work. *Proc. ACM Hum.-Comput. Interact.* **2019**, *3*, 1–26. [CrossRef]
126. Woolley, S.C.; Howard, P.N. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*; Oxford University Press: Oxford, UK, 2018. [CrossRef]
127. Thomas, K.; Grier, C.; Song, D.; Paxson, V. Suspended accounts in retrospect. In Proceedings of the IMC '11: Internet Measurement Conference, Berlin, Germany, 2–4 November 2011; pp. 243–258.
128. Chen, A. The agency. *N. Y. Times Mag.* **2015**, *2*, 1–14.
129. Gleicher, N. Removing Coordinated Inauthentic Behavior from Facebook and Instagram. Meta Newsroom. Available online: https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/ (accessed on 8 August 2025).
130. Ferrara, E.; Varol, O.; Davis, C.; Menczer, F.; Flammini, A. The rise of social bots. *Commun. ACM* **2016**, *59*, 96–104. [CrossRef]
131. Davis, C.A.; Varol, O.; Ferrara, E.; Flammini, A.; Menczer, F. BotOrNot. In Proceedings of the 25th International Conference Companion, Montreal, QC, Canada, 11–15 April 2016; pp. 273–274.
132. Bell, J.B. *The Secret Army: The IRA*; Routledge: Abingdon, UK, 2017.
133. Bourdas, A.M.A. *Disinformation in France: A Strategy of Information Warfare in the Digital Age*; Charles University: Praha, Czech Republic, 2023.
134. Caldarelli, G.; De Nicola, R.; Del Vigna, F.; Petrocchi, M.; Saracco, F. The role of bot squads in the political propaganda on Twitter. *Commun. Phys.* **2020**, *3*, 81. [CrossRef]

135. Chan, C.-H.; Fu, K.-W. The relationship between cyberbalkanization and opinion polarization: Time-series analysis on Facebook pages and opinion polls during the Hong Kong occupy movement. *J. Comput. Commun.* **2017**, *22*, 266–283. [CrossRef]
136. Ratkiewicz, J.; Conover, M.; Meiss, M.; Goncalves, B.; Flammini, A.; Menczer, F. Detecting and tracking political abuse in social media. In Proceedings of the International AAAI Conference on Web and Social Media, Barcelona, Spain, 17–21 July 2011; Volume 5, pp. 297–304. [CrossRef]
137. Vosoughi, S.; Roy, D.; Aral, S. The spread of true and false news online. *Science* **2018**, *359*, 1146–1151. [CrossRef] [PubMed]
138. Cresci, S.; Di Pietro, R.; Petrocchi, M.; Spognardi, A.; Tesconi, M. The paradigm-shift of social spambots. In Proceedings of the 26th International Conference on World Wide Web Companion—WWW '17 Companion, Perth, Australia, 3–7 April 2017; pp. 963–972.
139. Keller, T.R.; Klinger, U. Social bots in election campaigns: Theoretical, empirical, and methodological implications. *Politics Commun.* **2018**, *36*, 171–189. [CrossRef]
140. NATO StratCom COE. *Robotrolling 2022/2*; NATO Strategic Communications Centre of Excellence: Riga, Latvia, 2022.
141. EEAS. *European External Action Service Special Report: Disinformation on COVID-19*; EEAS East StratCom Task Force: Brussels, Belgium, 2020.
142. Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial nets. *Adv. Neural Inf. Process. Syst.* **2014**, *27*, 2672–2680.
143. Karras, T.; Laine, S.; Aila, T. A style-based generator architecture for generative adversarial networks. *IEEE Trans. Pattern Anal. Mach. Intell.* **2020**, *43*, 4217–4228. [CrossRef]
144. Jia, J.; Zhang, W.; Weiss, R.J.; Wang, Y.; Shen, J.; Jia, Y.; Chen, Z.; Ren, F. Transfer learning from speaker verification to multispeaker text-to-speech synthesis. *Adv. Neural Inf. Process. Syst.* **2018**, *31*, 4485–4495.
145. Saharia, C.; Chan, W.; Saxena, S.; Li, L.; Whang, J.; Denton, E.; Ghasemipour, S.K.; Lopes, R.G.; Salimans, T.; Ho, J.; et al. Photorealistic text-to-image diffusion models with deep language understanding. *Adv. Neural Inf. Process. Syst.* **2022**, *35*, 36479–36494.
146. Vaccari, C.; Chadwick, A. Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Soc. Media + Soc.* **2020**, *6*, 2056305120903408. [CrossRef]
147. Halbryt, A.; Kalidindi, K.; Staab, L.; Novitsky, M. *A Deep Dive into Deepfakes*; University of Twente: Enschede, The Netherlands, 2022.
148. Paris, B.; Donovan, J. *Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence*; Data & Society Research Institute: New York, NY, USA, 2019.
149. Westerlund, M. The emergence of deepfake technology: A review. *Technol. Innov. Manag. Rev.* **2019**, *9*, 39–52. [CrossRef]
150. Korshunov, P.; Marcel, S. Deepfakes: A new threat to face recognition? Assessment and detection. *arXiv* **2018**, arXiv:1812.08685. [CrossRef]
151. Tolosana, R.; Vera-Rodriguez, R.; Fierrez, J.; Morales, A.; Ortega-Garcia, J. Deepfakes and beyond: A Survey of face manipulation and fake detection. *Inf. Fusion* **2020**, *64*, 131–148. [CrossRef]
152. Matern, F.; Riess, C.; Stamminger, M. Exploiting visual artifacts to expose deepfakes and face manipulations. In Proceedings of the 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), Waikoloa Village, HI, USA, 7–11 June 2019; pp. 83–92.
153. Verdoliva, L. Media forensics and deepfakes: An overview. *IEEE J. Sel. Top. Signal Process.* **2020**, *14*, 910–932. [CrossRef]
154. Korshunov, P.; Marcel, S. Improving generalization of deepfake detection with data farming and few-shot learning. *IEEE Trans. Biom. Behav. Identity Sci.* **2022**, *4*, 386–397. [CrossRef]
155. Europol. *Facing Reality? Law Enforcement and the Challenge of Deepfakes*; European Union Agency for Law Enforcement Cooperation: The Hague, The Netherlands, 2022.
156. European Parliament. *Artificial Intelligence Act—Text Adopted*; European Parliament: Strasbourg, France, 2022.
157. Dawkins, R. *The Extended Selfish Gene*; Oxford University Press: Oxford, UK, 2016.
158. Ross, A.S.; Rivers, D.J. Digital cultures of political participation: Internet memes and the discursive delegitimization of the 2016 U.S Presidential candidates. *Discourse Context Media* **2017**, *16*, 1–11. [CrossRef]
159. Shifman, L. *Memes in Digital Culture*; MIT Press: Cambridge, MA, USA, 2013.
160. Milner, R.M. *The World Made Meme: Public Conversations and Participatory Media*; MIT Press: Cambridge, MA, USA, 2018.
161. Wiggins, B.E.; Bowers, G.B. Memes as genre: A structurational analysis of the memescape. *New Media Soc.* **2014**, *17*, 1886–1906. [CrossRef]
162. Johnson, N.F.; Leahy, R.; Restrepo, N.J.; Velasquez, N.; Zheng, M.; Manrique, P.; Devkota, P.; Wuchty, S. Hidden resilience and adaptive dynamics of the global online hate ecology. *Nature* **2019**, *573*, 261–265. [CrossRef]
163. Hunting, K.O. The role of popular media in 2016 US presidential election memes. *Transform. Work. Cult.* **2019**, *32*. [CrossRef]
164. Golovchenko, Y.; Hartmann, M.; Adler-Nissen, R. State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation. *Int. Aff.* **2018**, *94*, 975–994. [CrossRef]

165. Ylä-Anttila, T. Populist knowledge: 'Post-truth' repertoires of contesting epistemic authorities. *Eur. J. Cult. Politi-Sociol.* **2018**, *5*, 356–388. [CrossRef]
166. Lonnberg, A.; Xiao, P.; Wolfinger, K. The growth, spread, and mutation of internet phenomena: A study of memes. *Results Appl. Math.* **2020**, *6*, 100092. [CrossRef]
167. Sharma, S.; Alam, F.; Akhtar, S.; Dimitrov, D.; Martino, G.D.S.; Firooz, H.; Halevy, A.; Silvestri, F.; Nakov, P.; Chakraborty, T. Detecting and understanding harmful memes: A survey. In Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence {IJCAI-22}, Vienna, Austria, 23–29 July 2022; pp. 5597–5606.
168. Aguilera-Carnerero, C.; Becker, M.J.; Scheiber, M. *5. Same Tools, Different Target: Countering Hate Speech with Memes*; OpenBook Publishers: Cambridge, UK, 2025.
169. Mihailidis, P.; Viotty, S. Spreadable spectacle in digital culture: Civic expression, fake news, and the role of media literacies in "post-fact" society. *Am. Behav. Sci.* **2017**, *61*, 441–454. [CrossRef]
170. Phillips, W. *This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream Culture*; MIT Press: Cambridge, MA, USA, 2015.
171. Howard, P.N.; Woolley, S.; Calo, R. Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *J. Inf. Technol. Politics* **2018**, *15*, 81–93. [CrossRef]
172. DiResta, R.; Shaffer, K.; Ruppel, B.; Sullivan, D.; Matney, R.; Fox, R.; Albright, J.; Johnson, B. *The Tactics & Tropes of the Internet Research Agency*; U.S. Senate (SSCI): Washington, DC, USA, 2019.
173. Senate Intelligence Select Committee. *Russian Active Measures Campaigns and Interference in the 2016 US Election*; Senate Intelligence Select Committee; U.S. Government Publishing Office: Washington, DC, USA, 2020; Volume 2, pp. 11–20.
174. Bell, J.B. *The IRA, 1968–2000: An Analysis of a Secret Army*; Routledge: Abingdon, UK, 2013.
175. Guess, A.; Nagler, J.; Tucker, J. Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Sci. Adv.* **2019**, *5*, eaau4586. [CrossRef] [PubMed]
176. European External Action Service. *EUvsDisinfo*; EEAS East StratCom Task Force: Brussels, Belgium, 2018.
177. European Commission. *Tackling COVID-19 Disinformation—Getting the Facts Right (JOIN/2020/8 Final)*; European Commission: Brussels, Belgium, 2020.
178. Bjola, C.; Pamment, J. (Eds.) *Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy*; Routledge: London, UK, 2018.
179. Jacobs, R.N. Media, Culture, and Civil Society. *Quest. Commun.* **2016**, *29*, 379–393. [CrossRef]
180. Giles, K. *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*; Chatham House: London, UK, 2023.
181. Atlantic Council/DFRLab. *Undermining Ukraine: How Russia Widened Its Global Information War in 2023*; Atlantic Council: Washington, DC, USA, 2024.
182. Freedom House. *Freedom on the Net 2023: Ukraine*; Freedom House: Washington, DC, USA, 2023.
183. Hung, T.C.; Hung, T.W. How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation warfare. *J. Glob. Secur. Stud.* **2022**, *7*, ogac016. [CrossRef]
184. Quirk, S. Lawfare in the disinformation age: Chinese interference in Taiwan's 2020 elections. *Harv. Int'l LJ* **2021**, *62*, 525.
185. Rauchfleisch, A.; Tseng, T.H.; Kao, J.J.; Liu, Y.T. Taiwan's public discourse about disinformation: The role of journalism, academia, and politics. *J. Pract.* **2023**, *17*, 2197–2217. [CrossRef]
186. Lee, F.L. Social media and the spread of fake news during a social movement: The 2019 Anti-ELAB protests in Hong Kong. *Commun. Public* **2020**, *5*, 122–125. [CrossRef]
187. Schissler, M. Beyond hate speech and misinformation: Facebook and the Rohingya genocide in Myanmar. *J. Genocide Res.* **2024**, *27*, 445–470. [CrossRef]
188. Ansar, A.; Maitra, J. Digital diaspora activism at the margins: Unfolding Rohingya diaspora interactions on facebook (2017–2022). *Soc. Media + Soc.* **2024**, *10*, 20563051241228603. [CrossRef]
189. Sinpeng, A.; Gueorguiev, D.; Arugay, A.A. Strong fans, weak campaigns: Social media and Duterte in the 2016 Philippine election. *J. East Asian Stud.* **2020**, *20*, 353–374. [CrossRef]
190. Arugay, A.A.; Baquisal, J.K.A. Mobilized and polarized: Social media and disinformation narratives in the 2022 Philippine elections. *Pac. Aff.* **2022**, *95*, 549–573. [CrossRef]
191. Kazemi, A.; Garimella, K.; Shahi, G.K.; Gaffney, D.; Hale, S.A. Research note: Tiplines to uncover misinformation on encrypted platforms: A case study of the 2019 Indian general election on WhatsApp. *Harv. Kennedy Sch. Misinf. Rev.* **2022**, *3*. [CrossRef]
192. Basavaraj, K.A. Misinformation in India's 2019 national election. *J. Quant. Descr. Digit. Media* **2022**, *2*. [CrossRef]
193. Government of the Republic of Kazakhstan. *Resolution of 30.06.2017 No. 407 "On Approval of the Cybersecurity Concept ("Cyber Shield of Kazakhstan")"*; Government of the Republic of Kazakhstan: Astana, Kazakhstan, 2017.
194. International Telecommunication Union. *Implementing Kazakhstan's Cybersecurity Concept*; ITU News: Geneva, Switzerland, 2022.

195. Nussipova, A.; Aliyarov, E.; Kabilova, R.; Karymsakova, K.; Nuralina, B. Pandemic, hoaxes and information security of Kazakhstan. *J. Inf. Policy* **2023**, *13*, 140–158. [CrossRef]
196. National Bureau of Asian Research. *Taiwan's Response to Disinformation (Special Report № 93)*; NBR: Seattle, WA, USA, 2021.
197. Köckritz, A. *In a Savvy Disinformation Offensive, China Takes Aim at Taiwan Elections*; Mercator Institute for China Studies: Berlin, Germany, 2023.
198. Torop, P. Cultural semiotics and culture. *Sign. Syst. Stud.* **1999**, *27*, 9–23. [CrossRef]
199. Smith, A.D. *National Identity*; University of Nevada Press: Reno, NV, USA, 1991.
200. Pomerantsev, P.; Weiss, M. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*; Institute of Modern Russia: New York, NY, USA, 2014. Available online: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf (accessed on 8 August 2025).
201. Castells, M. *Communication Power*; OUP Oxford: Oxford, UK, 2013.
202. Hale, H.E. *The Foundations of Ethnic Politics*; Cambridge University Press: Cambridge, UK, 2008. [CrossRef]
203. Wodak, R. *The Politics of Fear: What Right-Wing Populist Discourses Mean*; Sage: London, UK, 2015. [CrossRef]
204. Assmann, J. *Cultural Memory and Early Civilization*; Cambridge University Press: Cambridge, UK, 2011. [CrossRef]
205. Sunstein, C.R.; Vermeule, A. *Conspiracy Theories*; The University of Chicago: Chicago, IL, USA, 2008.
206. Barthes, R. *Mythologies*; Hill and Wang: New York, NY, USA, 1972.
207. van Dijk, T.A. Discourse and manipulation. *Discourse Soc.* **2006**, *17*, 359–383. [CrossRef]
208. Norris, P.; Inglehart, R. *Cultural Backlash*; Cambridge University Press: Cambridge, UK, 2019. [CrossRef]
209. Jenkins, H.; Ford, S.; Green, J.; Booth, P.; Busse, K.; Click, M.; Li, X.; Ross, S.; Stein, L. Spreadable media: Creating value and meaning in a networked culture. *Ciné. J.* **2014**, *53*, 152–177. [CrossRef]
210. UNESCO. *Operational Guidelines for the Implementation of the Convention for the Safeguarding of the Intangible Cultural Heritage*; UNESCO: New York, NY, USA, 2021. Available online: https://ich.unesco.org/en/directives (accessed on 8 August 2025).
211. Nye, J.S. *The Future of Power*; PublicAffairs: New York, NY, USA, 2011.
212. Hall, S.; Evans, J.; Nixon, S. *Representation: Cultural Representations and Signifying Practices*; Sage: London, UK, 2024.
213. Eco, U. *A Theory of Semiotics*; Indiana University Press: Bloomington, IN, USA, 1979; Volume 217.
214. Mandelker, A.; Lotman, Y.M.; Shukman, A.; Eco, U. Universe of the mind: A semiotic theory of culture. *Russ. Rev.* **1993**, *52*, 552. [CrossRef]
215. Susen, S. The interpretation of cultures: Geertz is still in town. *Sociol. Int. J. Sociol. Debate* **2024**, *18*, 25–63. [CrossRef]
216. Bourdieu, P. Outline of a Theory of Practice. In *The New Social Theory Reader*; Routledge: London, UK, 2020; pp. 80–86.
217. Hofstede, G.; Hofstede, G.J.; Minkov, M. *Cultures and Organizations: Software of the Mind*, 3rd ed.; McGraw-Hill: Columbus, OH, USA, 2010.
218. Schwartz, S.H. The refined theory of basic values. In *Values and Behavior*; Roccas, S., Sagiv, L., Eds.; Springer: Heidelberg, Germany, 2017; pp. 51–72. [CrossRef]
219. Lucy, J.A. Linguistic relativity. *Annu. Rev. Anthr.* **1997**, *26*, 291–312. [CrossRef]
220. Parsons, T. *The Structure of Social Action*; Free Press: New York, NY, USA, 1968.
221. McCrone, D.; Bechhofer, F. *Understanding National Identity*; Cambridge University Press: Cambridge, UK, 2015.
222. Assmann, J. Cultural memory: Script, recollection, and political identity in early civilizations. *Hist. East West* **2003**, *1*, 154–177. [CrossRef]
223. North, D.C. *Institutions, Institutional Change and Economic Performance*; Cambridge University Press: Cambridge, UK, 1990. [CrossRef]
224. Nye, J.S. *Soft Power: The Means to Success in World Politics*; PublicAffairs: New York, NY, USA, 2004.
225. Snow, N.; Taylor, P.M. (Eds.) *The Persuasion Handbook: Developments in Theory and Practice*; Routledge: London, UK, 2008.
226. Pomerantsev, P. *This Is Not Propaganda: Adventures in the War Against Reality*; Faber & Faber: London, UK, 2019.
227. Wilson, A. *Ukraine Crisis: What It Means for the West*; Yale University Press: Yale, CT, USA, 2014.
228. Inglehart, R.; Welzel, C. *Modernization, Cultural Change, and Democracy*; Cambridge University Press: Cambridge, UK, 2001. [CrossRef]
229. Fallis, D. The varieties of disinformation. In *The Philosophy of Information Quality*; Springer: Cham, Switzerland, 2014; pp. 135–161.
230. Buchanan, T.; Zhao, J. Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation. *PLoS ONE* **2020**, *15*, e0239666. [CrossRef] [PubMed]
231. Gabrielyan, O.; Suleimenov, I. Objective Foundations of Ethics and Prospects for Its Development: Information and Communication Approach. *Conatus* **2025**, *10*, 111–125. [CrossRef]
232. Suleimenov, I.E.; Gabrielyan, O.A.; Bakirov, A.S. Neural network approach to the interpretation of ancient Chinese geomancy feng shui practices. *Eur. J. Sci. Theol.* **2023**, *19*, 39–51.
233. Jasečková, G.; Konvit, M.; Vartiak, L. Vernadsky's concept of the noosphere and its reflection in ethical and moral values of society. *Hist. Sci. Technol.* **2022**, *12*, 231–248. [CrossRef]

234. Vanchurin, V. The world as a neural network. *Entropy* **2020**, *22*, 1210. [CrossRef]
235. Vanchurin, V.; Wolf, Y.I.; Katsnelson, M.I.; Koonin, E.V. Toward a theory of evolution as multilevel learning. *Proc. Natl. Acad. Sci. USA* **2022**, *119*, e2120037119. [CrossRef]
236. Vanchurin, V.; Wolf, Y.I.; Koonin, E.V.; Katsnelson, M.I. Thermodynamics of evolution and the origin of life. *Proc. Natl. Acad. Sci. USA* **2022**, *119*, e2120042119. [CrossRef]
237. Suleimenov, I.; Panchenko, S.; Gabrielyan, O.; Pak, I. Voting procedures from the perspective of theory of neural networks. *Open Eng.* **2016**, *6*. [CrossRef]
238. Kabdushev, S.; Gabrielyan, O.; Kopishev, E.; Suleimenov, I. Neural network properties of hydrophilic polymers as a key for development of the general theory of evolution. *R. Soc. Open Sci.* **2025**, *12*, 242149. [CrossRef]
239. Shaikhutdinov, R.; Mun, G.; Kopishev, E.; Bakirov, A.; Kabdushev, S.; Baipakbaeva, S.; Suleimenov, I. Effect of the formation of hydrophilic and hydrophobic–hydrophilic associates on the behavior of copolymers of N-vinylpyrrolidone with methyl acrylate in aqueous solutions. *Polymers* **2024**, *16*, 584. [CrossRef]
240. Ibragim, S.; Oleg, G.; Vitulyova, Y. Problems of many-valued logic from the point of view of the theory of sociocultural code. *J. Ecohumanism* **2024**, *3*, 236–248. [CrossRef]
241. Suleimenov, I.E.; Gabrielyan, O.A.; Bakirov, A.S. Initial study of general theory of complex systems: Physical basis and philosophical understanding. *Bull. Electr. Eng. Inform.* **2025**, *14*, 774–789. [CrossRef]
242. Suleimenov, I.E.; Matrassulova, D.K.; Moldakhan, I.; Vitulyova, Y.S.; Kabdushev, S.B.; Bakirov, A.S. Distributed memory of neural networks and the problem of the intelligence's essence. *Bull. Electr. Eng. Inform.* **2022**, *11*, 510–520. [CrossRef]
243. Chen, T.; Zhang, S.; Liu, S.; Du, Z.; Luo, T.; Gao, Y.; Liu, J.; Wang, D.; Wu, C.; Sun, N.; et al. A small-footprint accelerator for large-scale neural networks. *ACM Trans. Comput. Syst.* **2015**, *33*, 6. [CrossRef]
244. Burr, G.W.; Shelby, R.M.; Sidler, S.; di Nolfo, C.; Jang, J.; Boybat, I.; Shenoy, R.S.; Narayanan, P.; Virwani, K.; Giacometti, E.U.; et al. Experimental demonstration and tolerancing of a large-scale neural network (165 000 Synapses) using phase-change memory as the synaptic weight element. *IEEE Trans. Electron Devices* **2015**, *62*, 3498–3507. [CrossRef]
245. Hauke, C. The unconscious: Personal and collective. In *The Handbook of Jungian Psychology*; Routledge: London, UK, 2012; pp. 54–73.
246. Sandner, D. The Psychological Foundations of the Collective Unconscious. In *Society and the Unconscious: Cultural Psychological Insights*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 91–101.
247. Baudrillard, J.; Lovitt, C.R.; Klopsch, D. Toward a Critique of the Political Economy of the Sign. *SubStance* **1976**, *5*, 111. [CrossRef]
248. Suleimenov, I.; Gabrielyan, O.; Vitulyova, Y. Dialectics of Scientific Revolutions from the Point of View of Innovations Theory. *Wisdom* **2022**, *24*, 25–35. [CrossRef]
249. Beauvais, C. Fake news: Why do we believe it? *Jt. Bone Spine* **2022**, *89*, 105371. [CrossRef]
250. Wykes, M. *Representation: Cultural Representations and Signifying Practices*; Raymond Williams Society: Manchester, UK, 1998.
251. Assmann, A. *Cultural Memory and Western Civilization: Functions, Media, Archives*; Cambridge University Press: Cambridge, UK, 2011.
252. Brennan, J. Propaganda about propaganda. *Crit. Rev.* **2017**, *29*, 34–48. [CrossRef]
253. Scheufele, B. Framing-effects approach: A theoretical and methodological critique. *Communications* **2004**, *29*, 401–428. [CrossRef]
254. Foucault, M. *Power/Knowledge: Selected Interviews and Other Writings*; Pantheon: New York, NY, USA, 1980.
255. Corman, S.R.; Trethewey, A.; Goodall, H.L., Jr. *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*; Peter Lang: Lausanne, Switzerland, 2008.
256. Apple, M.; Apple, M.W. *Ideology and Curriculum*; Routledge: London, UK, 2004.
257. Forest, B.; Johnson, J. Monumental politics: Regime type and public memory in post-communist states. *Post-Sov. Aff.* **2011**, *27*, 269–288. [CrossRef]
258. Highfield, T. *Social Media and Everyday Politics*; John Wiley & Sons: Hoboken, NJ, USA, 2017.
259. Ross, S. Don't Think of an Elephant: Know Your Values and Frame the Debate. *Melb. J. Politics* **2006**, *31*, 145–149.
260. Darnton, R. *A Literary Tour de France*; Oxford University Press: Oxford, UK, 2018.
261. Yablokov, I. Conspiracy theories as a Russian public diplomacy tool: The case of Russia Today (RT). *Politics* **2015**, *35*, 301–315. [CrossRef]
262. Ehala, M. *Signs of Identity: The Anatomy of Belonging*; Routledge: London, UK, 2017.
263. Harmanşah, Ö. ISIS, heritage, and the spectacles of destruction in the global media. *Near East. Archaeol.* **2015**, *78*, 170–177. [CrossRef]
264. Boyd, D. *It's Complicated: The Social Lives of Networked Teens*; Yale University Press: Yale, CT, USA, 2014.
265. Bozdag, E.; Hoven, J.v.D. Breaking the filter bubble: Democracy and design. *Ethics Inf. Technol.* **2015**, *17*, 249–265. [CrossRef]
266. Bradshaw, S.; Howard, P.N. The global organization of social media disinformation campaigns. *J. Int. Aff.* **2018**, *71*, 23–32.
267. Gere, C. *Digital Culture*; Reaktion Books: London, UK, 2009.
268. Szostek, J. The Power and Limits of Russia's Strategic Narrative in Ukraine: The Role of Linkage. *Perspect. Politics* **2017**, *15*, 379–395. [CrossRef]

269. Alvesson, M. *Communication, Power and Organization (No. 72)*; Walter de Gruyter: Berlin, Germany, 1996.
270. Morvan, C.; O'Connor, A. *An Analysis of Leon Festinger's a Theory of Cognitive Dissonance*; Macat Library: London, UK, 2017.
271. Böhm, R.; Rusch, H.; Baron, J. The psychology of intergroup conflict: A review of theories and measures. *J. Econ. Behav. Organ.* **2020**, *178*, 947–962. [CrossRef]
272. Entman, R.M. Framing bias: Media in the distribution of power. *J. Commun.* **2007**, *57*, 163–173. [CrossRef]
273. Sunstein, C.R. *#Republic: Divided Democracy in the Age of Social Media*; Princeton University Press: Princeton, NJ, USA, 2018.
274. Barberá, P. How social media reduces mass political polarization. Evidence from Germany, Spain, and the US. *Job Mark. Pap. N. Y. Univ.* **2014**, *46*, 1–46.
275. Simons, J.; Ghosh, D. *Utilities for Democracy: Why and How the Algorithmic Infrastructure of Facebook and Google Must Be Regulated*; Brookings Institute: Washington, DC, USA, 2020.
276. Chadwick, A.; Stromer-Galley, J. Digital media, power, and democracy in parties and election campaigns. *Int. J. Press/Politics* **2016**, *21*, 283–293. [CrossRef]
277. Kreiss, D.; Mcgregor, S.C. Technology firms shape political communication: The work of Microsoft, Facebook, Twitter, and Google with campaigns during the 2016 US presidential cycle. *Politics Commun.* **2017**, *35*, 155–177. [CrossRef]
278. Wiggins, B.E. *The Discursive Power of Memes in Digital Culture: Ideology, Semiotics, and Intertextuality*; Routledge: London, UK, 2019.
279. Guess, A.M.; Lyons, B.A. Misinformation, disinformation, and online propaganda. *Soc. Media Democr. State Field Prospect. Reform* **2020**, *10*, 10–33.
280. Kuzio, T. Competing Nationalisms, Euromaidan, and the Russian-Ukrainian Conflict. *Stud. Ethn. Natl.* **2015**, *15*, 157–169. [CrossRef]
281. Howard, P.N.; Hussain, M.M. *Democracy's Fourth Wave?: Digital Media and the Arab Spring*; Oxford University Press: Oxford, UK, 2013. [CrossRef]
282. Qureshi, W.A. The rise of hybrid warfare. *Notre Dame J. Int'l Comp. L.* **2020**, *10*, 173.
283. Waisbord, S. Truth is what happens to news. *J. Stud.* **2018**, *19*, 1866–1878. [CrossRef]
284. Qasmi, A.U. Identity formation through national calendar: Holidays and commemorations in Pakistan. *Nations Natl.* **2017**, *23*, 620–641. [CrossRef]
285. Bail, C.A. Combining natural language processing and network analysis to examine how advocacy organizations stimulate conversation on social media. *Proc. Natl. Acad. Sci. USA* **2016**, *113*, 11823–11828. [CrossRef] [PubMed]
286. Kalsnes, B. Deciding what's true: The rise of political fact-checking in American journalism. *Digit. J.* **2017**, *6*, 670–672. [CrossRef]
287. Kandel, N. Information disorder syndrome and its management. *J. Nepal Med. Assoc.* **2020**, *58*, 280–285. [CrossRef]
288. Brandtzaeg, P.B.; Følstad, A. Trust and distrust in online fact-checking services. *Commun. ACM* **2017**, *60*, 65–71. [CrossRef]
289. Amazeen, M.A. Revisiting the epistemology of fact-checking. *Crit. Rev.* **2015**, *27*, 1–22. [CrossRef]
290. Nyhan, B.; Reifler, J. Displacing misinformation about events: An experimental test of causal corrections. *J. Exp. Politics Sci.* **2015**, *2*, 81–93. [CrossRef]
291. Friggeri, A.; Adamic, L.; Eckles, D.; Cheng, J. Rumor cascades. In Proceedings of the Eighth International Conference on Weblogs and Social Media, Ann Arbor, MI, USA, 1–4 June 2014.
292. Graves, L.; Cherubini, F. *The Rise of Fact-Checking Sites in Europe*; Reuters Institute for the Study of Journalism: Oxford, UK, 2016.
293. Spivak, C. The fact-checking explosion: In a bitter political landscape marked by rampant allegations of questionable credibility, more and more news outlets are launching truth-squad operations. *Am. J. Rev.* **2010**, *32*, 38–44.
294. Primig, F. The influence of media trust and normative role expectations on the credibility of fact checkers. *J. Pract.* **2022**, *18*, 1137–1157. [CrossRef]
295. Hassan, N.; Arslan, F.; Li, C.; Tremayne, M. Toward automated fact-checking. In Proceedings of the KDD '17: The 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, NS, Canada, 13–17 August 2017; pp. 1803–1812.
296. Full Fact. Annual Report. 2022. Available online: https://fullfact.org/ (accessed on 8 August 2025).
297. Bellingcat. Investigative Methodology. 2023. Available online: https://www.bellingcat.com/resources/how-tos/ (accessed on 8 August 2025).
298. Higgins, E. *We Are Bellingcat*; Bloomsbury: London, UK, 2019.
299. Visvizi, A.; Lytras, M.D. (Eds.) *Politics and Technology in the Post-Truth Era*; Emerald Publishing Limited: Leeds, UK, 2019.
300. Nyhan, B.; Reifler, J. When corrections fail: The persistence of political misperceptions. *Politics Behav.* **2010**, *32*, 303–330. [CrossRef]
301. Lewandowsky, S.; Cook, J.; Ecker, U.; Albarracin, D.; Amazeen, M.A.; Kendou, P.; Lombardi, D.; Newman, E.; Pennycook, G.; Porter, E.; et al. *The Debunking Handbook 2020*; OpenBU: Boston, MA, USA, 2020. [CrossRef]
302. Herting, K.K.Y.Y. Building Psychological Resistance Against False Information in Middle School through Digital Games. Master's Thesis, The University of Bergen, Bergen, Norway, 2024.
303. van der Linden, S.; Leiserowitz, A.; Rosenthal, S.; Maibach, E. Inoculating the public against misinformation about climate change. *Glob. Chall.* **2017**, *1*, 1600008. [CrossRef]

304. Zhang, Y.; Sharma, K.; Liu, Y. Capturing cross-platform interaction for identifying coordinated accounts of misinformation campaigns. In Proceedings of the European Conference on Information Retrieval, Dublin, Ireland, 2–6 April 2023; Springer Nature: Cham, Switzerland, 2023; pp. 694–702.
305. Pierri, F.; Ceri, S. False news on social media: A data-driven survey. *ACM Sigmod Rec.* **2019**, *48*, 18–27. [CrossRef]
306. Wood, T.; Porter, E. The elusive backfire effect: Mass attitudes' steadfast factual adherence. *Political Behav.* **2019**, *41*, 135–163. [CrossRef]
307. Pennycook, G.; Rand, D.G. Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proc. Natl. Acad. Sci. USA* **2019**, *116*, 2521–2526. [CrossRef]
308. Graves, L. Anatomy of a fact check: Objective practice and the contested epistemology of fact checking. *Commun. Cult. Crit.* **2016**, *10*, 518–537. [CrossRef]
309. Nyhan, B.; Reifler, B. *Misinformation and Fact-Checking: Research Findings from Social Science*; New America Foundation: Washington, DC, USA, 2012.
310. Wardle, C. First Draft's CrossCheck Initiative. First Draft News. 2019. Available online: https://firstdraftnews.org/ (accessed on 8 August 2025).
311. van der Linden, S.; Roozenbeek, J.; Compton, J. Inoculating against fake news about COVID-19. *Front. Psychol.* **2020**, *11*, 566790. [CrossRef]
312. Compton, J. Prophylactic versus therapeutic inoculation treatments for resistance to influence. *Commun. Theory* **2019**, *30*, 330–343. [CrossRef]
313. McGuire, W.J. Some Contemporary Approaches. *Adv. Exp. Soc. Psychol.* **1964**, *1*, 191–229. [CrossRef]
314. Banas, J.A.; Rains, S.A. A meta-analysis of research on inoculation theory. *Commun. Monogr.* **2010**, *77*, 281–311. [CrossRef]
315. Van der Linden, S.; Roozenbeek, J. Psychological inoculation against fake news. In *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation*; Routledge/Taylor & Francis Group: Abingdon, UK, 2020; pp. 147–169.
316. Vernon, J.L. Science in the post-truth era. *Am. Sci.* **2017**, *105*, 2–3. [CrossRef]
317. Roozenbeek, J.; van der Linden, S.; Nygren, T. Prebunking interventions based on the inoculation theory. *Harv. Kennedy Sch. Misinf. Rev.* **2020**. [CrossRef]
318. Google Jigsaw. Prebunking: Building Resilience Against Misinformation. 2022. Available online: https://jigsaw.google.com/ (accessed on 8 August 2025).
319. Kiili, K.; Siuko, J.; Ninaus, M. Tackling misinformation with games: A systematic literature review. *Interact. Learn. Environ.* **2024**, *32*, 7086–7101. [CrossRef]
320. Kahan, D.M. Misconceptions, misinformation, and the logic of identity-protective cognition. In *Cultural Cognition Project Working Paper*; Yale Law School: New Haven, CT, USA, 2017.
321. Sperber, D.; Clément, F.; Heintz, C.; Mascaro, O.; Mercier, H.; Origgi, G.; Wilson, D. Epistemic vigilance. *Mind Lang.* **2010**, *25*, 359–393. [CrossRef]
322. Sweller, J. Cognitive load theory. *Psychol. Learn. Motiv.* **2011**, *55*, 37–76. [CrossRef]
323. Maertens, R.; Roozenbeek, J.; Basol, M.; van der Linden, S. Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments. *J. Exp. Psychol. Appl.* **2021**, *27*, 1. [CrossRef]
324. Basol, M.; Roozenbeek, J.; Van der Linden, S. Good news about bad news: Gamified inoculation boosts confidence and cognitive immunity against fake news. *J. Cogn.* **2020**, *3*, 2. [CrossRef]
325. Guess, A.M.; Lerner, M.; Lyons, B.; Montgomery, J.M.; Nyhan, B.; Reifler, J.; Sircar, N. A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proc. Natl. Acad. Sci. USA* **2020**, *117*, 15536–15545. [CrossRef] [PubMed]
326. UNESCO. *Media and Information Literacy: A Critical Necessity in the Post-COVID World*; UNESCO: Paris, France, 2021.
327. NATO StratCom COE. *Cognitive Resilience in the Information Environment*; NATO Strategic Communications Centre of Excellence: Riga, Latvia, 2020.
328. Monti, M. The EU Code of Practice on Disinformation and the Risk of the Privatisation of Censorship. In *Democracy and Fake News*; Routledge: London, UK, 2020; pp. 214–225.
329. Gillespie, T. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*; Yale University Press: Yale, CT, USA, 2018. [CrossRef]
330. Jalili, M.; Perc, M. Information cascades in complex networks. *J. Complex Netw.* **2017**, *5*, 665–693. [CrossRef]
331. Saurwein, F.; Spencer-Smith, C. Automated trouble: The role of algorithmic selection in harms on social media platforms. *Media Commun.* **2021**, *9*, 222–233. [CrossRef]
332. Garimella, K.; Tyson, G. WhatApp, doc? A first look at WhatsApp public group data. In Proceedings of the International AAAI Conference on Web and Social Media, Palo Alto, CA, USA, 25–28 June 2018; Volume 12. [CrossRef]
333. Shu, K.; Sliva, A.; Wang, S.; Tang, J.; Liu, H. Fake news detection on social media: A data mining perspective. *ACM SIGKDD Explor. Newsl.* **2017**, *19*, 22–36. [CrossRef]

334. Zhou, X.; Zafarani, R. A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Comput. Surv.* **2020**, *53*, 109. [CrossRef]
335. Gallwitz, F.; Kreil, M. The Rise and Fall of 'Social Bot' Research. 2021. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3814191 (accessed on 8 August 2025).
336. Amerini, I.; Barni, M.; Battiato, S.; Bestagini, P.; Boato, G.; Bonaventura, T.S.; Bruni, V.; Caldelli, R.; De Natale, F.; De Nicola, R.; et al. Deepfake media forensics: State of the art and challenges ahead. In Proceedings of the International Conference on Advances in Social Networks Analysis and Mining, Rende, Italy, 2–5 September 2024; Springer Nature: Cham, Switzerland, 2024; pp. 33–48.
337. Alam, F.; Shaar, S.; Dalvi, F.; Sajjad, H.; Nikolov, A.; Mubarak, H.; Martino, G.D.S.; Abdelali, A.; Durrani, N.; Darwish, K.; et al. Fighting the COVID-19 infodemic: Modeling the perspective of journalists, fact-checkers, social media platforms, policy makers, and the society. *arXiv* **2020**, arXiv:2005.00033.
338. Pennycook, G.; Rand, D.G. Accuracy prompts are a replicable and generalizable approach for reducing the spread of misinformation. *Nat. Commun.* **2022**, *13*, 2333. [CrossRef]
339. YouTube Official Blog. Our Ongoing Work to Tackle Misinformation. 2021. Available online: https://blog.google/around-the-globe/google-europe/our-ongoing-work-to-fight-misinformation-online/ (accessed on 8 August 2025).
340. Narayanan, A.; Vallor, S. Why software engineering courses should include ethics coverage. *Commun. ACM* **2014**, *57*, 23–25. [CrossRef]
341. Abokhodair, N.; Skop, Y.; Rüller, S.; Aal, K.; Elmimouni, H. Opaque algorithms, transparent biases: Automated content moderation during the Sheikh Jarrah Crisis. *First Monday* **2024**, *29*. [CrossRef]
342. Nazar, S.; Pieters, T. Plandemic revisited: A product of planned disinformation amplifying the COVID-19 "infodemic". *Front. Public Health* **2021**, *9*, 649930. [CrossRef] [PubMed]
343. Bak-Coleman, J.B.; Kennedy, I.; Wack, M.; Beers, A.; Schafer, J.S.; Spiro, E.S.; Starbird, K.; West, J.D. Combining interventions to reduce the spread of viral misinformation. *Nat. Hum. Behav.* **2022**, *6*, 1372–1380. [CrossRef]
344. Figueira, Á.; Oliveira, L. The current state of fake news: Challenges and opportunities. *Procedia Comput. Sci.* **2017**, *121*, 817–825. [CrossRef]
345. Arrieta, A.B.; Díaz-Rodríguez, N.; Del Ser, J.; Bennetot, A.; Tabik, S.; Barbado, A.; Garcia, S.; Gil-Lopez, S.; Molina, D.; Benjamins, R.; et al. Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Inf. Fusion* **2020**, *58*, 82–115. [CrossRef]
346. Wang, X.; Xie, H.; Ji, S.; Liu, L.; Huang, D. Blockchain-based fake news traceability and verification mechanism. *Heliyon* **2023**, *9*, e17084. [CrossRef]
347. Adobe. BBC. The New York Times. Content Authenticity Initiative. 2022. Available online: https://contentauthenticity.org/ (accessed on 8 August 2025).
348. Benkler, Y.; Faris, R.; Roberts, H. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*; Oxford University Press: Oxford, UK, 2018.
349. Bienvenue, E. Computational propaganda: Political parties, politicians, and political manipulation on social media. *Int. Aff.* **2020**, *96*, 525–527. [CrossRef]
350. Newman, M.E.J. *Networks*; Oxford University Press: Oxford, UK, 2018.
351. Barabási, A.-L. *Network Science*; Cambridge University Press: Cambridge, UK, 2016.
352. Ramašauskaitė, O. The Role of Collaborative Networks in Combating Digital Disinformation. In *2. International Conference on Economics" Regional Development-Digital Economy": Proceedings Book, 21–23 December 2023*; Liberty Academic Publishers: New York, NY, USA, 2023; pp. 432–437.
353. Tangherlini, T.R.; Shahsavari, S.; Shahbazi, B.; Ebrahimzadeh, E.; Roychowdhury, V.; Lin, Y.-R. An automated pipeline for the discovery of conspiracy and conspiracy theory narrative frameworks: Bridgegate, Pizzagate and storytelling on the web. *PLoS ONE* **2020**, *15*, e0233879. [CrossRef]
354. Pacheco, D.; Hui, P.-M.; Torres-Lugo, C.; Truong, B.T.; Flammini, A.; Menczer, F. Uncovering coordinated networks on social media: Methods and case studies. In Proceedings of the International AAAI Conference on Web and Social Media, Online, 7–10 June 2021.
355. Zannettou, S.; Caulfield, T.; De Cristofaro, E.; Sirivianos, M.; Stringhini, G.; Blackburn, J. Disinformation warfare: Understanding state-sponsored trolls on twitter and their influence on the web. In Proceedings of the WWW '19: The Web Conference, San Francisco, CA, USA, 13–17 May 2019; pp. 218–226.
356. Kumar, S.; Shah, N. False information on the web and social media: A survey. *Proc. VLDB Endow.* **2018**, *11*, 2134–2147.
357. Wu, L.; Morstatter, F.; Carley, K.M.; Liu, H. Misinformation in social media: Definition, manipulation, and detection. *ACM SIGKDD Explor. Newsl.* **2019**, *21*, 80–90. [CrossRef]
358. Monti, F.; Frasca, F.; Eynard, D.; Mannion, D.; Bronstein, M.M. Fake news detection on social media using geometric deep learning. *arXiv* **2019**, arXiv:1902.06673. [CrossRef]

359. Alliance for Securing Democracy. Hamilton 68 Dashboard. 2018. Available online: https://securingdemocracy.gmfus.org/fact-sheet-hamilton-68-dashboard-2017-2018/ (accessed on 8 August 2025).
360. Facebook. Removing Bad Actors from Facebook. 2018. Available online: https://about.fb.com/news/2018/06/removing-bad-actors-from-facebook/ (accessed on 8 August 2025).
361. Twitter Safety. Information Operations Directed at Political Discourse in the United States. 2020. Available online: https://blog.x.com/en_us/topics/company/2020/information-operations-june-2020 (accessed on 8 August 2025).
362. Wilson, S.L.; Wiysonge, C. Social media and vaccine hesitancy. *BMJ Glob. Health* **2020**, *5*, e004206. [CrossRef]
363. EUvsDisinfo. Disinformation Review. 2021. Available online: https://euvsdisinfo.eu/ (accessed on 8 August 2025).
364. Magelinski, T.; Ng, L.; Carley, K. A Synchronized action framework for detection of coordination on social media. *J. Online Trust. Saf.* **2022**, *1*. [CrossRef]
365. Bradshaw, S.; Bailey, H.; Howard, P.N. *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*; Oxford Internet Institute: Oxford, UK, 2021.
366. Campbell, L. Freedom of Expression in the Platform Age: Between Moderation and Censorship. 2025. Available online: https://www.researchgate.net/publication/393786792_Freedom_of_Expression_in_the_Platform_Age_Between_Moderation_and_Censorship (accessed on 8 August 2025).
367. Kriel, C.; Pavliuc, A. Reverse engineering Russian Internet Research Agency tactics through network analysis. *Def. Strateg. Commun.* **2019**, *6*, 199–227. [CrossRef]
368. Mihailidis, P.; Thevenin, B. Media literacy as a core competency for engaged citizenship in participatory democracy. *Am. Behav. Sci.* **2013**, *57*, 1611–1622. [CrossRef]
369. Potter, W.J. *Media Literacy*; SAGE Publications: London, UK, 2019.
370. UNESCO. *Media and Information Literacy: Policy and Strategy Guidelines*; UNESCO: Paris, France, 2018.
371. Paul, R.; Elder, L. *The Miniature Guide to Critical Thinking Concepts and Tools*; Foundation for Critical Thinking: Santa Barbara, CA, USA, 2019.
372. Ciampaglia, G.L. Fighting fake news: A role for computational social science in the fight against digital misinformation. *J. Comput. Soc. Sci.* **2017**, *1*, 147–153. [CrossRef]
373. Gaillard, S.; Oláh, Z.A.; Venmans, S.; Burke, M. Countering the cognitive, linguistic, and psychological underpinnings behind susceptibility to fake news: A review of current literature with special focus on the role of age and digital literacy. *Front. Commun.* **2021**, *6*, 661801. [CrossRef]
374. Roozenbeek, J.; van der Linden, S. Fake news game confers psychological resistance against online misinformation. *Palgrave Commun.* **2019**, *5*, 12. [CrossRef]
375. Hobbs, R. Teaching and learning in a post-truth world. *Educ. Leadersh.* **2017**, *75*, 26–31.
376. Salminen, J.; Tornberg, L.; Venäläinen, P. Public institutions as learning environments in Finland. In *Miracle of Education: The Principles and Practices of Teaching and Learning in Finnish Schools (Second Revised Edition)*; SensePublishers: Rotterdam, The Netherlands, 2016; pp. 253–266.
377. Livingstone, S.; Helsper, E. Gradations in digital inclusion: Children, young people and the digital divide. *New Media Soc.* **2007**, *9*, 671–696. [CrossRef]
378. Afghahi, E. Newsgame vs. Fake News: A Case Study of Breaking Harmony Square. *News Sci. Q.* **2024**, *13*, e203739.
379. European Commission. *Digital Education Action Plan*; EU Publications: Brussels, Belgium, 2018.
380. Wineburg, S.; McGrew, S.; Breakstone, J.; Ortega, T. *Evaluating Information: The Cornerstone of Civic Online Reasoning*; Stanford History Education Group: Stanford, CA, USA, 2016.
381. OSCE Programme Office in Nur-Sultan. *Media Literacy in Kazakhstan: Pilot Projects*; OSCE Programme Office in Nur-Sultan: Astana, Kazakhstan, 2020.
382. Burkhardt, J.M. *Combating Fake News in the Digital Age*; American Library Association: Chicago, IL, USA, 2017; Volume 53, pp. 5–9.
383. Roozenbeek, J.; Van Der Linden, S.; Goldberg, B.; Rathje, S.; Lewandowsky, S. Psychological inoculation improves resilience against misinformation across cultures. *Sci. Adv.* **2022**, *8*, eabo0063. [CrossRef]
384. Liu, X.; Qi, L.; Wang, L.; Metzger, M.J. Checking the fact-checkers: The role of source type, perceived credibility, and individual differences in fact-checking effectiveness. *Commun. Res.* **2023**, *52*, 719–746. [CrossRef]
385. UNESCO Institute for Statistics. *Measuring Digital Literacy*; UNESCO: Paris, France, 2019.
386. Tornero, J.M.P.; Sánchez, M.O.P.; Baena, G.; Luque, S.G.; Tejedor, S.; Fernández, N. Trends and models of Media literacy in Europe: Between digital competence and critical understanding. *Anàl. Quad. Comun. Cult.* **2010**, *40*, 85–100.
387. Iyengar, S.; Sood, G.; Lelkes, Y. Affect, not ideology: A social identity perspective on polarization. *Public Opin. Q.* **2012**, *76*, 405–431. [CrossRef]

388. Yaseen, H.; Mohammad, A.S.; Ashal, N.; Abusaimeh, H.; Ali, A.; Sharabati, A.A.A. The impact of adaptive learning technologies, personalized feedback, and interactive AI tools on student engagement: The moderating role of digital literacy. *Sustainability* **2025**, *17*, 1133. [CrossRef]
389. Cybersecurity & Infrastructure Security Agency (CISA). *Building Resilience Through Digital Literacy*; CISA: Washington, DC, USA, 2021.
390. Revez, J.; Corujo, L. Scientists' behaviour towards information disorder: A systematic review. *J. Inf. Sci.* **2024**. [CrossRef]
391. Stallings, W. *Cryptography and Network Security: Principles and Practice*, 7th ed.; Pearson: London, UK, 2017.
392. Content Authenticity Initiative. About CAI. 2021. Available online: https://contentauthenticity.org (accessed on 8 August 2025).
393. Truepic. Truepic Vision: Authenticity for Images and Video. 2020. Available online: https://truepic.com (accessed on 8 August 2025).
394. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov. Rev.* **2016**, *2*, 6–10.
395. Shih, F.Y. *Digital Watermarking and Steganography: Fundamentals and Techniques*; CRC Press: Boca Raton, FL, USA, 2017.
396. Coalition for Content Provenance and Authenticity (C2PA). Technical Specification. 2022. Available online: https://c2pa.org (accessed on 8 August 2025).
397. Nowroozi, E.; Seyedshoari, S.; Mohammadi, M.; Jolfaei, A. Impact of media forensics and deepfake in society. In *Breakthroughs in Digital Biometrics and Forensics*; Springer International Publishing: Cham, Switzerland, 2022; pp. 387–410.
398. BBC. Project Origin; 2021. Available online: https://www.bbc.com/beyondfakenews/trusted-news-initiative/project-origin-securing-trust-in-media (accessed on 8 August 2025).
399. Starling Lab. Technology for Trust. 2022. Available online: https://starlinglab.org (accessed on 8 August 2025).
400. Microsoft. Microsoft Video Authenticator. 2020. Available online: https://news.microsoft.com (accessed on 8 August 2025).
401. Richards, N.M.; King, J.H. Big data and the future for privacy. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK; Northampton, MA, USA, 2016; pp. 272–290.
402. York, J.C.; Zuckerman, E. Moderating the public sphere. In *Human Rights in the Age of Platforms*; MIT Press: Cambridge, MA, USA, 2019.
403. European Commission. The EU's Digital Services Act. Available online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (accessed on 8 August 2025).
404. European Commission. Questions and Answers on the Digital Services Act. 2020. Available online: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (accessed on 8 August 2025).
405. Kuczerawy, A.; Terzis, G.; Kloza, D.; Kuzelewska, E.; Tottier, D. *Fighting Online Disinformation: Did the EU Code of Practice Forget About Freedom of Expression?* Intersentia: Mechelen, Belgium, 2020.
406. Chystoforova, K.; Reviglio, U. Framing the role of experts in platform governance: Negotiating the code of practice on disinformation as a case study. *Internet Policy Rev.* **2025**, *14*, 1–28. [CrossRef]
407. Associated Press. Musk's X Is the Biggest Purveyor of Disinformation, EU Official Says. 2024. Available online: https://apnews.com/article/9f7823726f812bb357ee4225b884354f (accessed on 8 August 2025).
408. European Union. Regulation (EU) 2024. 2024. Available online: https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng (accessed on 8 August 2025).
409. Dobber, T.; Fathaigh, R.Ó.; Borgesius, F.J.Z. The regulation of online political micro-targeting in Europe. *Internet Policy Rev.* **2019**, *8*, 1–20. [CrossRef]
410. Reuters. Meta to Halt Political Advertising in EU from October, Blames EU Rules. 2025. Available online: https://www.reuters.com/sustainability/meta-halt-political-advertising-eu-october-blames-eu-rules-2025-07-25/ (accessed on 8 August 2025).
411. Associated Press. Meta Will Cease Political Ads in European Union by Fall, Blaming Bloc's New Rules. 2025. Available online: https://apnews.com/article/89efeac96723308d2a0469740d24d433 (accessed on 8 August 2025).
412. European Commission. European Media Freedom Act. Available online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en (accessed on 8 August 2025).
413. European Parliament. Media Freedom Act Enters into Application to Support Democracy and Journalism. 2025. Available online: https://www.europarl.europa.eu/news/en/press-room/20250725IPR29818/media-freedom-act-enters-into-application-to-support-democracy-and-journalism (accessed on 8 August 2025).
414. European Union. Directive (EU) 2018. 2018. Available online: https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng (accessed on 8 August 2025).
415. European Parliament. EU AI Act: First Regulation on Artificial Intelligence. 2023. Available online: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (accessed on 8 August 2025).
416. Artificial Intelligence Act. Article 50: Transparency Obligations for Providers. Available online: https://artificialintelligenceact.eu/article/50/ (accessed on 8 August 2025).
417. European Union. Regulation (EU) 2021. 2021. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32021R0784 (accessed on 8 August 2025).
418. European Commission. Terrorist Content Online. Available online: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online_en (accessed on 8 August 2025).

419. European Union. Directive (EU) 2022. 2022. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed on 8 August 2025).
420. European Union. Regulation (EU) 2024. 2024. Available online: https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng (accessed on 8 August 2025).
421. European Commission. EU Digital Identity Wallet. Available online: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/European%2BCommission%2Badopts%2Bnew%2Bround%2Bof%2BEU%2BDigital%2BIdentity%2BWallet%2Bimplementing%2Bregulations (accessed on 8 August 2025).
422. European Union. Regulation (EU) 2023. 2023. Available online: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (accessed on 8 August 2025).
423. European Union. Transparency and Targeting of Political Advertising. Available online: https://eur-lex.europa.eu/EN/legal-content/summary/transparency-and-targeting-of-political-advertising.html (accessed on 8 August 2025).
424. European Union. Transparency and Targeting of Political Advertising. EUR-Lex. Available online: https://eur-lex.europa.eu/eli/C/2024/6758/oj/eng (accessed on 8 August 2025).
425. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
426. Mosenia, A.; Jha, N.K. A Comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* **2016**, *5*, 586–602. [CrossRef]
427. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
428. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
429. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the DAC '15: The 52nd Annual Design Automation Conference, San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
430. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The industrial internet of things (IIoT): An analysis framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
431. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
432. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the mirai botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp. 1093–1110.
433. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-BaIoT—Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [CrossRef]
434. Safi, M.; Dadkhah, S.; Shoeleh, F.; Mahdikhani, H.; Molyneaux, H.; Ghorbani, A.A. A survey on IoT profiling, fingerprinting, and identification. *ACM Trans. Internet Things* **2022**, *3*, 1–39. [CrossRef]
435. Case, D.U. Analysis of the cyber attack on the Ukrainian power grid. *Electr. Inf. Shar. Anal. Cent. (E-ISAC)* **2016**, *388*, 3.
436. ENISA. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. In *ENISA Report*; European Union Agency for Cybersecurity: Athens, Greece, 2017.
437. *NIST SP 800-82*; Rev.Guide to Industrial Control Systems (ICS) Security. NIST: Gaithersburg, MD, USA, 2015.
438. NISTIR. *Foundational Cybersecurity Activities for IoT Device Manufacturers*; NIST: Gaithersburg, MD, USA, 2020.
439. *NISTIR 8259A*; IoT Device Cybersecurity Capability Core Baseline. NIST: Gaithersburg, MD, USA, 2020.
440. Lear, E.; Droms, R.; Romascanu, D. *RFC 8520: Manufacturer Usage Description (MUD)*; IETF: Fremont, CA, USA, 2019.
441. Selander, G.; Mattsson, J.; Palombini, F.; Seitz, L. *RFC 8613: Object Security for Constrained RESTful Environments (OSCORE)*; IETF: Fremont, CA, USA, 2019.
442. *ETSI EN 303 645 V2.1*; Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI: Sophia-Antipolis, France, 2020.
443. Selander, G.; Mattsson, J.P.; Preuß Mattsson, C.; Russ, H. *RFC 9528: Ephemeral Diffie-Hellman Over COSE (EDHOC)*; IETF: Fremont, CA, USA, 2024.
444. ENISA. Threat Landscape 2023: Transport Sector. In *ENISA Report*; ENISA: Athens, Greece, 2023.
445. Yang, Z.; Zolanvari, M.; Jain, R. A survey of important issues in quantum computing and communications. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1059–1094. [CrossRef]
446. Preskill, J. Quantum computing 40 years later. In *Feynman Lectures on Computation*; CRC Press: Boca Raton, FL, USA, 2023; pp. 193–244.
447. McMahon, P.L. The physics of optical computing. *Nat. Rev. Phys.* **2023**, *5*, 717–734. [CrossRef]
448. Kazanskiy, N.L.; Butt, M.A.; Khonina, S.N. Optical computing: Status and perspectives. *Nanomaterials* **2022**, *12*, 2171. [CrossRef]
449. Demir, B.; Gultakti, C.A.; Koker, Z.; Anantram, M.P.; Oren, E.E. Electronic properties of DNA origami nanostructures revealed by in silico calculations. *J. Phys. Chem. B* **2024**, *128*, 4646–4654. [CrossRef]

450. Fan, D.; Wang, J.; Wang, E.; Dong, S. Propelling DNA computing with materials' power: Recent advancements in innovative DNA logic computing systems and smart bio-applications. *Adv. Sci.* **2020**, *7*, 2001766. [CrossRef]
451. Ling, H.; Koutsouras, D.A.; Kazemzadeh, S.; van de Burgt, Y.; Yan, F.; Gkoupidenis, P. Electrolyte-gated transistors for synaptic electronics, neuromorphic computing, and adaptable biointerfacing. *Appl. Phys. Rev.* **2020**, *7*, 011307. [CrossRef]
452. Kim, S.; Heo, K.; Lee, S.; Seo, S.; Kim, H.; Cho, J.; Lee, H.; Lee, K.-B.; Park, J.-H. Ferroelectric polymer-based artificial synapse for neuromorphic computing. *Nanoscale Horiz.* **2020**, *6*, 139–147. [CrossRef]
453. Zhang, Z.; Sabbagh, B.; Chen, Y.; Yossifon, G. Geometrically scalable iontronic memristors: Employing bipolar polyelectrolyte gels for neuromorphic systems. *ACS Nano* **2024**, *18*, 15025–15034. [CrossRef]
454. Zhou, T.; Yuk, H.; Hu, F.; Wu, J.; Tian, F.; Roh, H.; Shen, Z.; Gu, G.; Xu, J.; Lu, B.; et al. 3D printable high-performance conducting polymer hydrogel for all-hydrogel bioelectronic interfaces. *Nat. Mater.* **2023**, *22*, 895–902. [CrossRef]
455. Koo, J.H.; Song, J.; Yoo, S.; Sunwoo, S.; Son, D.; Kim, D. Unconventional device and material approaches for monolithic biointegration of implantable sensors and wearable electronics. *Adv. Mater. Technol.* **2020**, *5*, 2000407. [CrossRef]
456. Gong, M.; Zhang, L.; Wan, P. Polymer nanocomposite meshes for flexible electronic devices. *Prog. Polym. Sci.* **2020**, *107*, 101279. [CrossRef]
457. Ibrahim, R.; Shafiq, M.O. Explainable convolutional neural networks: A taxonomy, review, and future directions. *ACM Comput. Surv.* **2023**, *55*, 206. [CrossRef]
458. Jaiswal, P.; Gupta, N.K.; Ambikapathy, A. Comparative study of various training algorithms of artificial neural network. In Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 12–13 October 2018; pp. 1097–1101.
459. Suleimenov, I.E.; Bakirov, A.S.; Matrassulova, D.K. A technique for analyzing neural networks in terms of ternary logic. *J. Theor. Appl. Inf. Technol.* **2021**, *99*, 2537–2553.
460. Vitulyova, Y.S.; Bakirov, A.S.; Shaltykova, D.B.; Suleimenov, I.E. Prerequisites for the analysis of the neural networks functioning in terms of projective geometry. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2020; Volume 946, p. 012001.
461. Shaltykova, D.; Kadyrzhan, K.; Caiko, J.; Vitulyova, Y.; Suleimenov, I. Trigger-Based Systems as a Promising Foundation for the Development of Computing Architectures Based on Neuromorphic Materials. *Technologies* **2025**, *13*, 326. [CrossRef]
462. de Liaño, G.D.; Fernández-Götz, M. Posthumanism, new humanism and beyond. *Camb. Archaeol. J.* **2021**, *31*, 543–549. [CrossRef]
463. Bardziński, F. Between Bioconservatism and transhumanism: In search of a third way. *Ethics Prog.* **2015**, *6*, 153–163. [CrossRef]
464. Huxley, J. New bottles for new wine. *J. R. Anthr. Inst. Great Br. Irel.* **1950**, *80*. [CrossRef]
465. Savin-Baden, M.; Burden, D. Digital immortality and virtual humans. *Postdigital Sci. Educ.* **2018**, *1*, 87–103. [CrossRef]
466. Popescu, F.; Scarlat, C. Human digital immortality: Where human old dreams and new technologies meet. In *Research Paradigms and Contemporary Perspectives on Human-Technology Interaction*; IGI Global: Hershey, PA, USA, 2017; pp. 266–282.
467. Suleimenov, I.E.; Vitulyova, Y.S.; Bakirov, A.S.; Gabrielyan, O.A. Artificial Intelligence: What is it? In Proceedings of the 2020 6th International Conference on Computer and Technology Applications, Antalya, Turkey, 14–16 April 2020; pp. 22–25.
468. Brusentsov, N.P.; Alvarez, J.R. Ternary computers: The setun and the setun 70. In Proceedings of the IFIP Conference on Perspectives on Soviet and Russian Computing, Petrozavodsk, Russia, 3–7 July 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 74–80.
469. Brusentsov, N.P.; Alvarez, J.R. *IFIP Advances in Information and Communication Technology*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 357, pp. 74–80. [CrossRef]
470. Pfister, H. Discrete-Time Signal Processing. 2017. Lecture Note. Available online: http://pfister.ee.duke.edu/courses/ece485/dtsp.pdf (accessed on 8 August 2025).
471. Mitra, S.K. *Digital Signal Processing: A Computer-Based Approach*; McGraw-Hill: Columbus, OH, USA, 2011.
472. Hagen, L.; Neely, S.; Keller, T.E.; Scharf, R.; Vasquez, F.E. Rise of the machines? Examining the influence of social bots on a political discussion network. *Soc. Sci. Comput. Rev.* **2020**, *40*, 264–287. [CrossRef]
473. Gonzalez, R.C.; Woods, R.E. *Digital Image Processing*; Pearson: London, UK, 2018.
474. Bovik, A. *The Essential Guide to Image Processing*; Academic Press: New York, NY, USA, 2009.
475. Efthimion, P.G.; Payne, S.; Proferes, N. Supervised machine learning bot detection techniques to identify social twitter bots. *SMU Data Sci. Rev.* **2018**, *1*, 5.
476. Jolliffe, I.T.; Cadima, J. Principal component analysis: A review and recent developments. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2016**, *374*, 20150202. [CrossRef]
477. Haykin, S. *Adaptive Filter Theory*; Prentice Hall: Hoboken, NJ, USA, 2002.
478. Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*; MIT Press: Cambridge, MA, USA, 2016.
479. Garg, S.; Kaur, K.; Kumar, N.; Kaddoum, G.; Zomaya, A.Y.; Ranjan, R. A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 924–935. [CrossRef]

480. Sadok, Z. An Adaptive and Energy-Efficient Edge Framework for Real-Time Fake News Detection. In Proceedings of the 2025 International Wireless Communications and Mobile Computing (IWCMC), Abu Dhabi, United Arab Emirates, 12–16 May 2016; pp. 1440–1447.
481. Pollard, J.M. The fast Fourier transform in a finite field. *Math. Comput.* **1971**, *25*, 365–374. [CrossRef]
482. Reed, I.S.; Truong, T.K. The use of finite fields in the Fourier transform over a finite field. *IEEE Trans. Inf. Theory* **1975**, *21*, 208–213. [CrossRef]
483. Blahut, R.E. *Fast Algorithms for Digital Signal Processing*; Addison-Wesley: Boston, MA, USA, 2010.
484. Tolimieri, R.; An, M.; Lu, C. *Mathematics of Multidimensional Fourier Transform Algorithms*; Springer: Berlin, Germany, 1998.
485. Kadyrzhan, A.; Bakirov, A.; Shaltykova, D.; Suleimenov, I. Application of the algebraic extension method to the construction of orthogonal bases for partial digital convolutions. *Algorithms* **2024**, *17*, 496. [CrossRef]
486. Suleimenov, I.; Bakirov, A. Prospects for using finite algebraic rings for constructing discrete coordinate systems. *Symmetry* **2025**, *17*, 410. [CrossRef]
487. Mullen, G.L.; Panario, D. *Handbook of Finite Fields*; CRC Press: Boca Raton, FL, USA, 2013.
488. Hassan, Y.A.; Rahma, A.M.S. Improving Video Watermarking through Galois Field GF(24) Multiplication Tables with Diverse Irreducible Polynomials and Adaptive Techniques. *Comput. Mater. Contin.* **2024**, *78*, 1423–1442. [CrossRef]
489. Song, Z.; She, Y.; Yang, J.; Peng, J.; Gao, Y.; Tafazolli, R. Nonuniform sampling pattern design for compressed spectrum sensing in mobile cognitive radio networks. *IEEE Trans. Mob. Comput.* **2024**, *23*, 8680–8693. [CrossRef]
490. Pei, D.; Salomaa, A.; Ding, C. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*; World Scientific: Singapore, 1996.
491. Shaltykova, D.; Vitulyova, Y.; Bakirov, A.S.; Suleimenov, I. Formation of Periodic Mosaic Structures Using Operations in Galois Fields. *Symmetry* **2025**, *17*, 1415. [CrossRef]
492. Nazir, S.; Dickson, D.M.; Akram, M.U. Survey of explainable artificial intelligence techniques for biomedical imaging with deep neural networks. *Comput. Biol. Med.* **2023**, *156*, 106668. [CrossRef]
493. Haar, L.V.; Elvira, T.; Ochoa, O. An analysis of explainability methods for convolutional neural networks. *Eng. Appl. Artif. Intell.* **2022**, *117*, 105606. [CrossRef]
494. Marinov, C.A.; Neittaanmäki, P. *Mathematical Models in Electrical Circuits: Theory and Applications*; Springer Science & Business Media: Berlin, Germany, 1991; Volume 66.
495. Zhi, X.; Wei, D.; Zhang, W. A generalized convolution theorem for the special affine Fourier transform and its application to filtering. *Optik* **2016**, *127*, 2613–2616. [CrossRef]
496. Matrassulova, D.K.; Vitulyova, Y.S.; Konshin, S.V.; Suleimenov, I.E. Algebraic fields and rings as a digital signal processing tool. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, *29*, 206–216. [CrossRef]
497. Moldakhan, I.; Matrassulova, D.K.; Shaltykova, D.B.; Suleimenov, I.E. Some advantages of non-binary Galois fields for digital signal processing. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *23*, 871–878. [CrossRef]
498. Shaltykova, D.; Kadyrzhan, K.; Suleimenov, I.; Seitenova, G.; Kopishev, E. Application of Fourier-Galois Spectra Analysers for Rotating Image Analysis. *Polymers* **2025**, *17*, 1791. [CrossRef] [PubMed]
499. Vitulyova, E.S.; Matrassulova, D.K.; Suleimenov, I.E. New application of non-binary Galois fields Fourier transform: Digital analog of convolution theorem. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *23*, 1718–1726. [CrossRef]
500. Suleimenov, I.; Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y. Peculiarities of Applying Partial Convolutions to the Computation of Reduced Numerical Convolutions. *Appl. Sci.* **2024**, *14*, 6388. [CrossRef]
501. Bracewell, R.N. *The Fourier Transform and Its Applications*; McGraw-Hill: Columbus, OH, USA, 2000.
502. McEliece, R.J. *Finite Fields for Computer Scientists and Engineers*; Springer Science & Business Media: Berlin, Germany, 1987.
503. Lidl, R.; Niederreiter, H. *Finite Fields*; Cambridge University Press: Cambridge, UK, 1997.
504. Szabo, N.S.; Tanaka, R.I. *Residue Arithmetic and Its Applications to Computer Technology*; McGraw-Hill: Columbus, OH, USA, 1967.
505. Suleimenov, I.E.; Vitulyova, Y.S.; Kabdushev, S.B.; Bakirov, A.S. Improving the efficiency of using multivalued logic tools: Application of algebraic rings. *Sci. Rep.* **2023**, *13*, 22021. [CrossRef] [PubMed]
506. Mallat, S. *A Wavelet Tour of Signal Processing*, 2nd ed.; Academic Press: New York, NY, USA, 1999.
507. Wang, G.; Wang, D.; Du, C.; Li, K.; Zhang, J.; Liu, Z.; Tao, Y.; Wang, M.; Cao, Z.; Yan, X. Seizure prediction using directed transfer function and convolution neural network on intracranial EEG. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2020**, *28*, 2711–2720. [CrossRef]
508. Kadyrzhan, K.; Kaldybekov, D.; Baipakbaeva, S.; Vitulyova, Y.; Matrassulova, D.; Suleimenov, I. Electronic Fourier–Galois spectrum analyzer for the field GF (31). *Appl. Sci.* **2024**, *14*, 7770. [CrossRef]
509. Garner, H.L. The residue number system. *IRE Trans. Electron. Comput.* **1959**, *2*, 140–147. [CrossRef]
510. Omondi, A.; Premkumar, B. *Residue Number Systems—Theory and Implementation*; Imperial College Press: London, UK, 2007.
511. Ibran, Z.M.; Aljatlawi, E.A.; Awin, A.M. On continued fractions and their applications. *J. Appl. Math. Phys.* **2022**, *10*, 142–159. [CrossRef]

512. Republic of Kazakhstan. Method and Device for Multiplication Modulo Seven. Patent No. 36266, 16 June 2023. (In Russian)
513. Chang, C.-H.; Molahosseini, A.S.; Zarandi, A.A.E.; Tay, T.F. Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications. *IEEE Circuits Syst. Mag.* **2015**, *15*, 26–44. [CrossRef]
514. Marangunic, C.; Cid, F.; Rivera, A.; Uribe, J. Machine Learning Dependent Arithmetic Module Realization for High-Speed Computing. *J. VLSI Circuits Syst.* **2022**, *4*, 42–51.
515. Kadyrzhan, A.; Kadyrzhan, K.; Bakirov, A.; Suleimenov, I. Prospects for the use of quasi-Mersen numbers in the design of parallel-serial processors. *Appl. Sci.* **2025**, *15*, 741. [CrossRef]
516. Shaltykova, D.; Vitulyova, Y.; Kadyrzhan, K.; Suleimenov, I. Application of Partial Discrete Logarithms for Discrete Logarithm Computation. *Computers* **2025**, *14*, 343. [CrossRef]
517. Odlyzko, A. Discrete Logarithms: The Past and the Future. *Des. Codes Cryptogr.* **2000**, *19*, 129–145. [CrossRef]
518. Sarkar, A.; Roy, D.G.; Datta, P. An Overview of the Discrete Logarithm Problem in Cryptography. In *International Conference on Advanced Computing and Applications*; Springer Nature: Singapore, 2024; pp. 129–143. [CrossRef]
519. Vitulyova, Y.S.; Suleimenov, I.E.; Matrassulova, D.K.; Bakirov, A.S. Discrete form of the Huygens-Fresnel principle: To the multi-dimensional analog of the Nyquist–Shannon sampling theorem. *Int. J. Inf. Technol.* **2023**, *15*, 3751–3759. [CrossRef]
520. Vitulyova, Y.; Kadyrzhan, K.; Kadyrzhan, A.; Shaltykova, D.; Suleimenov, I. Reducing the description of arbitrary wave field converters to tensor form. *Int. J. Inf. Technol.* **2024**, *17*, 3275–3284. [CrossRef]
521. Tschiatschek, S.; Singla, A.; Rodriguez, M.G.; Merchant, A.; Krause, A. Fake news detection in social networks via crowd signals. In Proceedings of the Companion Proceedings of the WEB Conference 2018, Lyon, France, 23–27 April 2018; ACM: New York, NY, USA, 2018; pp. 517–524.
522. Agarwal, N.; Bandeli, K.K. Examining strategic integration of social media platforms in disinformation campaign coordination. *Def. Strat. Commun.* **2018**, *4*, 173–206. [CrossRef]
523. Zhang, X.; Ghorbani, A.A. An overview of online fake news: Characterization, detection, and discussion. *Inf. Process. Manag.* **2020**, *57*, 102025. [CrossRef]
524. Nagarathna; Jamuna, S. A brief review on multiple-valued logic-based digital circuits. In Proceedings of the ICT with Intelligent Applications, Proceedings of ICTIS 2021, Wuhan, China, 22–24 October 2021; Volume 1, pp. 329–337.
525. Mirsky, Y.; Lee, W. The creation and detection of deepfakes: A survey. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–41. [CrossRef]
526. Biggio, B.; Roli, F. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognit.* **2018**, *84*, 317–331. [CrossRef]
527. United Nations. Universal Declaration of Human Rights. 1948. Available online: https://www.un.org/en/about-us/universal-declaration-of-human-rights (accessed on 8 August 2025).
528. United Nations. International Covenant on Civil and Political Rights. 1966. Available online: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed on 8 August 2025).
529. Reavley, N.J.; Jorm, A.F. The quality of mental disorder information websites: A review. *Patient Educ. Couns.* **2011**, *85*, e16–e25. [CrossRef] [PubMed]
530. Posetti, J.; Bontcheva, K. Disinfodemic: Deciphering COVID-19 Disinformation. UNESCO. 2020. Available online: https://en.unesco.org/covid19/disinfodemic (accessed on 8 August 2025).
531. Sunstein, C.R. *A Prison of Our Own Design: Divided Democracy in the Age of Social Media*; Democratic Audit UK: London, UK, 2017.
532. Barendt, E. *Freedom of Speech*; Oxford University Press: Oxford, UK, 2005.
533. European Commission. Code of Practice on Disinformation. Brussels. 2022. Available online: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (accessed on 8 August 2025).
534. Government of Singapore. Protection from Online Falsehoods and Manipulation Act. 2019. Available online: https://sso.agc.gov.sg/Acts-Supp/18-2019 (accessed on 8 August 2025).
535. Char, S. *Scaring the Monkey by Killing the Chicken: Effectiveness of Countercriticism Coercion by China*; Columbia University: New York, NY, USA, 2025.
536. Roberts, M. *Censored: Distraction and Diversion Inside China's Great Firewall*; Princeton University Press: Princeton, NJ, USA, 2018.
537. European Court of Human Rights. Handyside v. the United Kingdom (Application No. 5493/72). 1976. Available online: https://hudoc.echr.coe.int/eng?i=001-57499 (accessed on 8 August 2025).
538. Kaye, D. *Speech Police: The Global Struggle to Govern the Internet*; Columbia Global Reports: New York, NY, USA, 2019.
539. Voorhoof, D. Freedom of expression and the right to information: Implications for copyright. In *Research Handbook on Human rights and Intellectual Property*; Edward Elgar Publishing: Cheltenham, UK; Northampton, MA, USA, 2015; pp. 331–353.
540. European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act). 2022. Available online: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (accessed on 8 August 2025).
541. Bundesministerium der Justiz. Netzwerkdurchsetzungsgesetz (NetzDG). 2017. Available online: https://www.gesetze-im-internet.de/netzdg/ (accessed on 8 August 2025).

542. UK Parliament. Online Safety Act 2023. 2023. Available online: https://www.legislation.gov.uk/ukpga/2023/50/enacted (accessed on 8 August 2025).
543. Singapore Statutes Online. Protection from Online Falsehoods and Manipulation Act 2019 (POFMA). Available online: https://sso.agc.gov.sg/Act/POFMA2019 (accessed on 8 August 2025).
544. Cyberspace Administration of China. Provisions on the Administration of Deep Synthesis Internet Information Services. Available online: http://www.cac.gov.cn/2022-11/25/c_1672222609363675.htm (accessed on 8 August 2025).
545. National Communications Commission (Taiwan). Anti-Infiltration Act. Available online: https://www.ncc.gov.tw/english/ (accessed on 8 August 2025).
546. Supreme Court of India. Order on Fact-Check Unit under IT Rules. 21 March. Available online: https://www.scobserver.in/cases/challenge-to-the-it-rules-2023/ (accessed on 8 August 2025).
547. Government of India. Digital Personal Data Protection Act, Gazette of India. Available online: https://www.meity.gov.in (accessed on 8 August 2025).
548. Government of Vietnam. Cybersecurity Law 2019; Decree No. 53/2022/ND-CP. Available online: https://english.luatvietnam.vn (accessed on 8 August 2025).
549. Hong Kong PCPD. Personal Data (Privacy) (Amendment) Ordinance 2021 (Anti-Doxxing). Available online: https://www.pcpd.org.hk (accessed on 8 August 2025).
550. Republic of the Philippines. SIM Registration Act, Republic Act No. 11934. Available online: https://www.officialgazette.gov.ph (accessed on 8 August 2025).
551. Government of Indonesia. Electronic Information and Transactions Law (ITE Law)—Amendments. Available online: https://peraturan.bpk.go.id (accessed on 8 August 2025).
552. Council of Europe. Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the Roles and Responsibilities of Internet Intermediaries. 2018. Available online: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680790e14 (accessed on 8 August 2025).
553. Santa Clara Principles. (2018, Updated 2021). Santa Clara Principles on Transparency and Accountability in Content Moderation. Available online: https://santaclaraprinciples.org/ (accessed on 8 August 2025).
554. Klonick, K. The new governors: The people, rules, and processes governing online speech. *Harv. L. Rev.* **2017**, *131*, 1598.
555. Meta Oversight Board. Charter & Bylaws. 2020. Available online: https://oversightboard.com/governance/ (accessed on 8 August 2025).
556. Nurik, C. *Book Review: Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*; Sage: London, UK, 2019.
557. Khan, I. Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. 2021. Available online: https://repository.graduateinstitute.ch/record/299517?v=pdf (accessed on 8 August 2025).
558. Douek, E. The Rise of Content Cartels. Knight First Amendment Institute at Columbia University. 2021. Available online: https://knightcolumbia.org/content/the-rise-of-content-cartels (accessed on 8 August 2025).
559. Keller, D. *Who Do You Sue? State and Platform Hybrid Power over Online Speech*; Hoover Institution: Stanford, CA, USA, 2019; p. 30.
560. UN Human Rights Committee. General Comment No. 34: Article 19—Freedoms of Opinion and Expression (CCPR/C/GC/34). United Nations. 2011. Available online: https://www.refworld.org/legal/general/hrc/2011/en/83764 (accessed on 8 August 2025).
561. European Court of Human Rights. Magyar Helsinki Bizottság v. Hungary (Application No. 18030/11). 2016. Available online: https://hudoc.echr.coe.int/eng#\{%22itemid%22:[%22001-167828%22]\} (accessed on 8 August 2025).
562. UN/OAS/OSCE/ACHPR. Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda. 2017. Available online: https://www.osce.org/fom/302796 (accessed on 8 August 2025).
563. Kaye, D. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/38/35). United Nations Human Rights Council. 2018. Available online: https://undocs.org/A/HRC/38/35 (accessed on 8 August 2025).
564. Khan, I. Disinformation and Freedom of Opinion and Expression. Report of the UN Special Rapporteur (A/77/288). United Nations General Assembly. 2022. Available online: https://undocs.org/A/77/288 (accessed on 8 August 2025).
565. Truong, M. *FREEDOM ON THE NET 2023-Methodology Questions-A. Obstacles to Access (0–25 Points)*; Freedom House: Washington, DC, USA, 2023.
566. European Court of Human Rights. Delfi AS v. Estonia (Application No. 64569/09) [GC]. Strasbourg, France, 2015. Available online: https://hudoc.echr.coe.int/eng#\{%22itemid%22:[%22001-155105%22]\} (accessed on 8 August 2025).
567. Access Now. The State of Internet Shutdowns. KeepItOn Coalition. 2024. Available online: https://www.accessnow.org/keepiton (accessed on 8 August 2025).
568. UN Human Rights Council. Resolution A/HRC/32/L.20—The Promotion, Protection and Enjoyment of Human Rights on the Internet. 2016. Available online: https://undocs.org/A/HRC/32/L.20 (accessed on 8 August 2025).

569. Sloane, C.A. The Sub Rosa Plan of Reorganization: Side-Stepping Creditor Protections in Chapter 11. *Bankr. Dev. J.* **1999**, *16*, 37.
570. Suleimenova, K.; Obukhova, P.; Shaltykova, D.; Suleimenov, I. Post-transition period and quality of higher education: Ways to overcome the crisis phenomena. *Int. Lett. Soc. Humanist. Sci.* **2013**, *8*, 49–56. [CrossRef]
571. Obukhova, P.; Guichard, J.-P.; Baikenov, A.; Suleimenov, I. Influence of collective consciousness on quality of the higher education in Kazakhstan. *Procedia Soc. Behav. Sci.* **2015**, *185*, 172–178. [CrossRef]
572. Suleimenov, I.; Guichard, J.P.; Baikenov, A.; Obukhova, P.; Suleimenova, K. Degradation of Higher Education in Kazakhstan as an example of post-transitional crisis. *Int. Lett. Soc. Humanist. Sci.* **2015**, *54*, 26–33. [CrossRef]
573. Shu, K.; Bhattacharjee, A.; Alatawi, F.; Nazer, T.H.; Ding, K.; Karami, M.; Liu, H. Combating disinformation in a social media age. *WIREs Data Min. Knowl. Discov.* **2020**, *10*, e1385. [CrossRef]
574. Ghorbanpour, F.; Ramezani, M.; Fazli, M.A.; Rabiee, H.R. FNR: A similarity and transformer-based approach to detect multi-modal fake news in social media. *Soc. Netw. Anal. Min.* **2023**, *13*, 56. [CrossRef]
575. Cinelli, M.; Morales, G.D.F.; Galeazzi, A.; Quattrociocchi, W.; Starnini, M. The echo chamber effect on social media. *Proc. Natl. Acad. Sci. USA* **2021**, *118*, e2023301118. [CrossRef]
576. European Commission. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union. 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065 (accessed on 8 August 2025).
577. European Commission. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (Draft). Official Journal of the European Union. 2024. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (accessed on 8 August 2025).
578. Gorwa, R.; Binns, R.; Katzenbach, C. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data Soc.* **2020**, *7*, 2053951719897945. [CrossRef]
579. Horizon Europe. MediaResist Project. In *European Union Research and Innovation Programme*; Horizon Europe: Brussels, Belgium, 2022. Available online: https://resilientmedia.eu/?utm_source=chatgpt.com (accessed on 8 August 2025).
580. Coin, A.; Mulder, M.; Dubljević, V. Ethical aspects of BCI technology: What is the state of the art? *Philosophies* **2020**, *5*, 31. [CrossRef]
581. Rid, T. *Active Measures: The Secret History of Disinformation and Political Warfare*; Farrar, Straus and Giroux: New York, NY, USA, 2020.
582. Chesney, R.; Citron, D. Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Aff.* **2019**, *98*, 147.
583. Defense Advanced Research Projects Agency (DARPA). *Next Generation Nonsurgical Neurotechnology (N3)*; DARPA: Arlington, VA, USA, 2019.
584. Kania, E.B. In Military Civil Fusion, China Is Learning Lessons from the United States and Starting to Innovate. In *The Strategy Bridge*; 2019. Available online: https://www.cnas.org/publications/commentary/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate (accessed on 8 August 2025).
585. Kotchetkov, I.S.; Hwang, B.Y.; Appelboom, G.; Kellner, C.P.; Connolly, E.S. Brain-computer interfaces: Military, neurosurgical, and ethical perspective. *Neurosurg. Focus* **2010**, *28*, E25. [CrossRef] [PubMed]
586. Ng, L.H.X.; Carley, K.M. What is a Social Media Bot? A Global Comparison of Bot and Human Characteristics. *arXiv* **2025**, arXiv:2501.00855. [CrossRef]
587. Penrod, J. Consumer neuroscience, neuromarketing, and foucault. In *Ethics and Biopower in Neuromarketing: A Framework for an Ethical Approach to Marketing*; Springer International Publishing: Cham, Switzerland, 2022; pp. 1–26.
588. Giordano, J. *Neurotechnology in National Security and Defense*; CRC Press: Boca Raton, FL, USA, 2014.
589. Horwitz, J. *Broken Code: Inside Facebook and the Fight to Expose Its Harmful Secrets*; Doubleday: New York, NY, USA, 2023.
590. Dubljević, V.; McCall, I.C.; Illes, J. Neuroenhancement at work: Addressing the ethical, legal, and social implications. In *Organizational Neuroethics: Reflections on the Contributions of Neuroscience to Management Theories and Business Practices*; Springer International Publishing: Cham, Switzerland, 2019; pp. 87–103.
591. Ienca, M.; Andorno, R. Towards new human rights in the age of neuroscience and neurotechnology. *Life Sci. Soc. Policy* **2017**, *13*, 5. [CrossRef] [PubMed]