Правильные семейства функций и порождаемые ими квазигруппы:

Комбинаторные и алгебраические свойства

К. Д. Царегородцев

Научные руководители:
к.ф.-м.н., Панкратьев А.Е.
к.ф.-м.н., Галатенко А.В.

МГУ им. М. В. Ломоносова

21 ноября 2025 г.

Содержание

Актуальность темы исследования

- **Симметричная криптография**[1]: совершенные шифры, хэш-функции, поточные шифры, генераторы псевдослучайных чисел.
- **Асимметричная криптография**[2]: постквантовые схемы электронной подписи, схемы выработки общего ключа, гомоморфное шифрование.
- Приложения в **теории кодирования**[3].
- **Схемы аутентификации** и многое другое[4].

[1] Dimitrova и Markovski, «On quasigroup pseudo random sequence generator»; Gligoroski, *On the S-box in GAGE and InGAGE*; Gligoroski, Markovski и Knapskog, «The stream cipher Edon80»; Gligoroski и др., «GAGE and InGAGE»; Markovski, Gligoroski и Kocarev, «Unbiased random sequences from quasigroup string transformations»; Mileva и Markovski, «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function».

[2] Gligoroski, Markovski и Knapskog, «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme»; Барышников и Катышев, «Использование неассоциативных структур для построения алгоритмов открытого распределения ключей»; Грибов, «Гомоморфность некоторых криптографических систем на основе неассоциативных структур»; Марков, Михалёв и Кислицын, «Неассоциативные структуры в гомоморфной криптографии».

[3] Markov, Mikhalev и Nechaev, «Nonassociative Algebraic Structures in Cryptography and Coding»; Гонсалес и др., «Групповые коды и их неассоциативные обобщения», «Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы».

[4] Chauhan, Gupta и Verma, «Quasigroups and their applications in cryptography»; Shcherbacov, *Elements of Quasigroup Theory and Applications*; Артамонов, «Квазигруппы и их приложения», «О применениях квазигрупп в криптографии».

Квазигруппа

Пара $(Q, \circ)$, Q — (конечное) множество, $\circ\colon Q \times Q \to Q$, для любых $a, b \in Q$ существуют единственные $x, y \in Q$, такие что: $a \circ x = b$, $y \circ a = b$.

Denes и Keedwell, *Latin squares and their applications (2nd edition)*; Белоусов, *Основы теории квазигрупп и луп*.

- В общем случае Q задается таблицей размера $|Q| \times |Q|$.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого класса[5].
- Итеративное построение из более «маленьких» (произведения)[6].
- Изотопы некоторых «хорошо изученных» групп (например, группы точек эллиптической кривой[7]).
- Функциональное задание квазигруппы:

$$x \circ y = z \leftrightarrow z_i = f_i(x_1, \ldots, x_n, y_1, \ldots, y_n).$$

[5] Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups».

[6] Gligoroski и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

[7] Марков, Михалёв и Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

Криптографически релевантные свойства квазигрупп

- Малое число ассоциативных троек, то есть троек элементов $(a, b, c) \in Q^3$

$$(a \circ b) \circ c = a \circ (b \circ c)$$

- Отсутствие подквазигрупп, т.е. подмножеств $Q' \subset Q$, которые замкнуты относительно умножения.
- Полиномиальная полнота квазигрупп (любое отображение $f \colon Q^n \to Q$ задается с помощью композиции констант и операции умножения).

Используемые обозначения

Q	квазигруппа с операцией $\circ$
k	размер множества Q, $k = \lvert Q \rvert$, значность логики
$\mathbb{E}_k$	множество $\{0, \ldots, k-1\}$ (обычно предполагаем $\mathbb{E}_k = \mathbb{Z}_k$)
$\mathcal{F}$	семейство (набор) функций $\mathcal{F} = (f_1, \ldots, f_n)$, $\mathcal{F} \colon Q^n \to Q^n$
f_i	i-я функция семейства $\mathcal{F}$
n	размер семейства
$Func(Q)$	множество функций $f \colon Q \to Q$
$Perm(Q)$	множество подстановок (биекций) на Q

Правильное семейство

Семейство функций на Q^n называется правильным, если для любых двух наборов $x \neq y$ найдется такая координата i, что $x_i \neq y_i$, но $f_i(x) = f_i(y)$.

Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

- Семейство булевых функций $\mathcal{F} = (f_1, \ldots, f_n)$ является правильным тогда и только тогда[8], когда отображение $(x, y) \to z = x \oplus y \oplus \mathcal{F}(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))$ задает квазигрупповую операцию **при любом выборе** внутренних функций $\pi_1, \ldots, \pi_n$.
- Пусть $\mathcal{F}\colon \mathbb{E}_k^n \to \mathbb{E}_k^n$ — правильное семейство, M — мощность образа отображения $x \to \mathcal{F}(x)$. Тогда[9] число различных квазигрупп, порождаемых указанной конструкцией, не менее чем M^{k^2}.

[8] Носов, «Построение классов латинских квадратов в булевой базе данных»; Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

[9] Галатенко и др., «О порождении n-квазигрупп с помощью правильных семейств функций».

Цели и задачи исследования

Цель исследования: изучение свойств правильных семейств функций, а также алгебраических свойств квазигрупп, заданных правильными семействами функций.

Задачи исследования

- Получение новых критериев правильности семейств функций, а также установление естественного соответствия между правильными семействами функций и другими комбинаторно-алгебраическими структурами.
- Исследование общих свойств правильных семейств функций, включая структуру множества неподвижных точек, а также стабилизатор относительно определенных классов преобразований.
- Нахождение новых классов правильных семейств и изучение их свойств, включая мощность класса и мощность образа представителей.
- Разработка нового способа построения квазигрупп на основе правильных семейств функций, создание шифра, сохраняющего формат, на основе этой конструкции, и анализ характеристик полученного шифра.

Содержание

Критерий в терминах регулярности, Теорема 1

Семейство $\mathcal{F}_n$ на $Q_1 \times \ldots \times Q_n$ является правильным тогда и только тогда, когда для любого набора отображений $\psi_i \colon Q_i \to Q_i$, $1 \leq i \leq n$, следующее отображение из $Q_1 \times \ldots \times Q_n$ в себя биективно:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \mathbf{x} \circ \Psi(\mathcal{F}_n(\mathbf{x})) = \begin{bmatrix} x_1 \circ_1 \psi_1(f_1(x_1, \ldots, x_n)) \\ \vdots \\ x_n \circ_n \psi_n(f_n(x_1, \ldots, x_n)) \end{bmatrix}, \; x_i \in Q_i.$$

Критерий обобщает известный результат[10] для абелевых групп.

[10] Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

Один способ задания квазигруппы

Пусть $\mathcal{F}$, $\mathcal{G}$ — два правильных семейства функций размера n над группой $(G^n, +)$. Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию $\circ$ следующим образом:

$$\mathbf{x} \circ \mathbf{y} = \mathbf{x} + \mathcal{F}(\mathbf{x}) + \mathbf{y} + \mathcal{G}(\mathbf{y}).$$

- Операция $\circ$ является квазигрупповой (**Теорема** 1).
- Индексы ассоциативности квазигрупп, построенных по паре $(\mathcal{F}, \mathcal{G})$ и по паре $(\mathcal{G}, \mathcal{F})$, совпадают (**Теорема** 5).
- Для $G = \mathbb{Z}_2$ индексы ассоциативности квазигрупп, построенных по паре $(\mathcal{F}, \mathcal{G})$ и по паре $(\mathcal{F} \oplus \alpha, \mathcal{G} \oplus \alpha)$, совпадают (**Теорема** 7).
- Для $G = \mathbb{Z}_2$ количество ассоциативных троек в квазигруппе, построенной по паре правильных булевых семейств $(\mathcal{F}, \mathcal{G})$, четно (**Теорема** 8).

Примеры правильных семейств

- Константные семейства[11] $f_i \equiv const_i$.
- Треугольные семейства $f_i = f_i(x_1, \ldots, x_{i-1})$.
- Класс квадратичных семейств (**Теорема** 2):

$$\mathcal{F}(x_1, \ldots, x_n) = \begin{bmatrix} 0 \\ x_1 \\ x_1 \oplus x_2 \\ \vdots \\ x_1 \oplus x_2 \oplus \ldots \oplus x_{n-1} \end{bmatrix} \bigoplus \begin{bmatrix} \bigoplus_{i<j,\ i,j\neq 1}^{n} x_i x_j \\ \bigoplus_{i<j,\ i,j\neq 2}^{n} x_i x_j \\ \bigoplus_{i<j,\ i,j\neq 3}^{n} x_i x_j \\ \vdots \\ \bigoplus_{i<j,\ i,j\neq n}^{n} x_i x_j \end{bmatrix}.$$

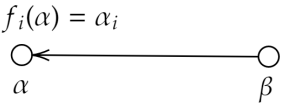
[11] Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

Содержание

Пусть $\mathcal{F}$ — правильное семейство.

- **Булев куб $\mathbf{B}_n$**: вершины $V = \{\alpha \in \mathbb{E}_2^n\}$; ребра $\{\alpha, \beta\} \in E \Leftrightarrow \rho(\alpha, \beta) = 1$ (расстояние Хэмминга).
- **Граф семейства $\Gamma_{\mathcal{F}}$:** Ориентируем ребро в графе $\mathbb{E}_2^n$ следующим образом: добавим ориентированное ребро $(\beta, \alpha) \in E$ тогда и только тогда, когда $f_i(\alpha) = \alpha_i$.

Неподвижная точка α
отображения $x \to \mathcal{F}(x)$
соответствует стоку в графе $\Gamma_{\mathcal{F}}$



Лемма 1, Следствие 1

Булево семейство $\mathcal{F}$ является правильным тогда и только тогда, когда семейство $\mathcal{F}$ и каждая из его проекций имеет единственную неподвижную точку.

Критерий может быть обобщен на k-значную логику[12].

[12] Галатенко, Носов и Панкратьев, «Об одном критерии правильности семейства функций».

Ориентация с единственным стоком (unique sink orientation, USO) куба $\mathbf{B}_n$ — ориентированный граф, построенный по $\mathbf{B}_n$ со следующим характеристическим свойством: в каждом подкубе $\mathbf{B}_n$ существует единственный сток.

Schurr, «Unique sink orientations of cubes»; Szabó и Welzl, «Unique sink orientations of cubes».

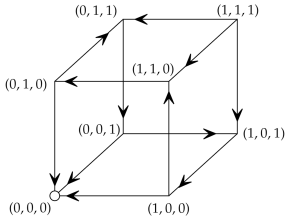


Рис. 1: Одностоковая ориентация трехмерного булева куба $\mathbf{B}_3$

Взаимно-однозначное соответствие, Теорема 9

Граф $\Gamma_{\mathcal{F}}$ семейства булевых функций $\mathcal{F}$ является одностоковой ориентацией (USO) тогда и только тогда, когда $\mathcal{F}$ — правильное семейство.

Булевы сети с наследственно единственной неподвижной точкой

HUFP-сеть (сеть с наследственно единственной неподвижной точкой, hereditarily unique fixed point network) — булево семейство $\mathcal{F}$ со следующим свойством: $\mathcal{F}$ и все его проекции имеют единственную неподвижную точку (как отображения $\mathbb{E}_2^n \to \mathbb{E}_2^n$).

Richard, «Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks»; Ruet, «Asynchronous Boolean networks and hereditarily bijective maps», «Local cycles and dynamical properties of Boolean networks»; Thomas, «Regulatory networks seen as asynchronous automata: a logical description».

Правильные семейства ↔ HUFP-сети, Теорема 12

Булево семейство $\mathcal{F}$ является правильным $\Leftrightarrow$ $\mathcal{F}$ задает HUFP-сеть.

Полученное соответствие (правильность $\Leftrightarrow$ USO-ориентации, HUFP-сети) позволяет переводить результаты с одного «языка» на другой.

Примеры переноса

- Вероятностный алгоритм порождения правильных семейств с помощью процедуры MCMC[13].
- Оценка на число $T(n)$ булевых правильных семейств

$$\log_2(T(n)) = \Theta\left(2^n \cdot \log_2(n)\right),$$

оценка на долю треугольных правильных семейств среди всех правильных семейств (треугольных семейств экспоненциально мало, **Теорема** 10).
- Новые классы правильных семейств: рекурсивно треугольные семейства (**Лемма** 9), локально треугольные семейства (**Теорема** 13).
- Характеризация через несамодвойственные проекции (**Теорема** 14).

[13] Schurr, «Unique sink orientations of cubes»; Галатенко и др., «Порождение правильных семейств функций».

Кликовое представление правильных семейств

- Правильные семейства находятся во взаимно-однозначном соответствии с кликами некоторым образом построенного графа («обобщенный граф Келлера»).
- Для $k = 2$ перенос из теории USO-ориентаций[14], для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n)$: $V = \mathbb{E}_{k^2}^n$,

$$\{v, w\} \in E \leftrightarrow \exists i,\ 1 \leq i \leq n\colon v_i \equiv w_i \bmod k,\ v_i \neq w_i.$$

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами[15].

Теорема 15

Каждой клике на k^n вершинах в графе $G(k, n)$ можно поставить в биективное соответствие некоторое правильное семейство $\mathcal{F}_n$ размера n на $\mathbb{E}_k^n$.

[14] Borzechowski, Doolittle и Weber, «A Universal Construction for Unique Sink Orientations».

[15] Mathew, Östergård и Popa, «Enumerating cube tilings»; Sikirić, Itoh и Poyarkov, «Cube packings, second moment and holes».

Содержание

Преобразование перекодировки

Пусть $\Phi, \Psi \in Perm(Q)^n$, $\Psi(x) = (\psi_1(x_1), \ldots, \psi_n(x_n))$ для $x \in Q^n$. Если $\mathcal{F}$ — правильное семейство, то $\Phi(\mathcal{F}(\Psi(x)))$ также правильно.

Галатенко, Носов и Панкратьев, «Об одном критерии правильности семейства функций».

Согласованная перенумерация

Пусть $\sigma \in Perm(n)$, зададим преобразование $\mathcal{F} \to \sigma(\mathcal{F})$ согласованной перенумерации следующим образом:

$$f_i(x_1, \ldots, x_n) \to f_{\sigma(i)}(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Если $\mathcal{F}(x)$ — правильное, то $\sigma(\mathcal{F})$ также правильно.

Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

- Согласованные перенумерации и перекодировки биективны, сохраняют правильность семейства, являются изометриями $\mathbb{E}_k^n$ (в метрике Хэмминга).
- Общая постановка задачи: пусть Φ, Ψ — биекции на Q^n: $\Phi, \Psi \in Perm(Q^n)$. Описать структуру стабилизатора множества всех правильных семейств, заданных на Q^n:

$\{(\Phi, \Psi) \in Perm(Q^n) \mid \Phi(\mathcal{F}(\Psi(x)))$ правильно для любого правильного $\mathcal{F}\colon Q^n \to Q^n\}$.

Стабилизатор правильных семейств, Теорема 19

Пусть семейства $\mathcal{G}(\mathbf{x})$ вида $\mathcal{G}(\mathbf{x}) = \Phi(\mathcal{F}(\Psi(\mathbf{x})))$ являются правильным для всех правильных семейств $\mathcal{F}$, заданных на $\mathbb{E}_k^n$, Φ и Ψ — биекции множества $\mathbb{E}_k^n$. Тогда Φ и Ψ имеют вид

$$\Phi = \sigma \circ A, \Psi = \sigma \circ B,$$

где $\sigma \in \mathcal{S}_n$ — перенумерация, $A, B \in (\mathcal{S}_{\mathbb{E}_k})^n$ — перекодировка.

Ограниченность мощности образа, Утверждение 29

Число значений, принимаемых правильным семейством порядка n в k-значной логике, не превосходит k^{n-1}.

Галатенко и др., «О порождении n-квазигрупп с помощью правильных семейств функций».

Мощность образа квадратичного семейства, Теорема 21

$$\begin{bmatrix} 0 \\ x_1 \\ \vdots \\ x_1 \oplus x_2 \oplus \ldots \oplus x_{n-1} \end{bmatrix} \oplus \begin{bmatrix} \bigoplus_{i<j,\ i,j\neq 1}^{n} x_i x_j \\ \bigoplus_{i<j,\ i,j\neq 2}^{n} x_i x_j \\ \vdots \\ \bigoplus_{i<j,\ i,j\neq n}^{n} x_i x_j \end{bmatrix}$$

Семейство имеет максимальную мощность образа 2^{n-1}.

$$\mathcal{F}_n(x) = \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ f_2(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix} = \begin{bmatrix} \overline{x}_2 \cdot x_3 \\ \overline{x}_3 \cdot x_4 \\ \vdots \\ \overline{x}_1 \cdot x_2 \end{bmatrix}.$$

Семейство $\mathcal{F}_n$ является правильным[16] при нечетных n.

Мощность образа семейства, Теорема 22

Мощность образа семейства $\mathcal{F}_n$ равна Lucas_n (n-е число Люка):

$$\mathsf{Lucas}_n = \mathsf{Lucas}_{n-1} + \mathsf{Lucas}_{n-2}, \quad \mathsf{Lucas}_0 = 2, \quad \mathsf{Lucas}_1 = 1.$$

[16] Галатенко, Носов и Панкратьев, «Порождение квадратичных квазигрупп с помощью правильных семейств булевых функций».

Пусть $\mathcal{F}\colon Q^n \to Q^n$ — правильное, $(Q, \circ)$ — квазигруппа. Тогда отображение

$$\sigma_{\mathcal{F}}(x)\colon x \to x \circ \mathcal{F}(x), \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \begin{bmatrix} x_1 \circ f_1(x_1, \ldots, x_n) \\ \vdots \\ x_n \circ f_n(x_1, \ldots, x_n) \end{bmatrix}$$

является подстановкой: $\sigma_{\mathcal{F}} \in Perm(Q^n)$.

Обратимость «правильных подстановок», Теорема 23

Если $(Q, +)$ — группа (т.е., операция $+$ ассоциативна), то семейство $\mathcal{G}\colon Q^n \to Q^n$, определенное равенством

$$\mathcal{G}(x) = (-x) + \sigma_{\mathcal{F}}^{-1}(x)$$

также является правильным.

Подстановки, порождаемые правильными семействами

- Множество «правильных подстановок» $\mathcal{S}^{\mathsf{prop}}$ замкнуто относительно взятия обратного элемента.
- $\mathcal{S}^{\mathsf{prop}}$ **не является** подгруппой $Perm(Q^n)$.
- $\langle \mathcal{S}^{\mathsf{prop}} \rangle$ действует транзитивно на Q^n (любой элемент из Q^n можно перевести в любой другой с помощью композиции некоторого количества σ_F).
- Если $Q = \mathbb{E}_2$, то[17] $\langle \mathcal{S}^{\mathsf{prop}} \rangle = Perm(\mathbb{E}_2^n)$.
- Если $\mathcal{F}$ — правильное семейство булевых функций, то число решений уравнения $\mathcal{F}(x) = \alpha$ четно для любого $\alpha \in \{0,1\}^n$ (**Теорема** 20); у подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек (**Теорема** 24).

[17] Schurr, «Unique sink orientations of cubes».

Содержание

Алгоритм шифрования, сохраняющего формат (FPE-схема)

- FPE-схема[18]: алгоритм, позволяющий зашифровывать сообщения из произвольного конечного множества M таким образом, что результат зашифрования также лежит в множестве M.
- Преобразуем $m \in M$, где $(M, \circ)$ — квазигруппа, в $c \in M$ по правилу:

$$m \to c = L_{k_1,\ldots,k_\ell}(m) = k_1 \circ (k_2 \circ (\ldots (k_\ell \circ m) \ldots)) .$$

- Элементы k_i и последовательность сдвигов выбирается на основе мастер-ключа и настройки (tweak) псевдослучайным образом.
- Необходимо специфицировать конкретную квазигруппу.

[18] Bellare и др., «Format-preserving encryption».

- Пусть $\mathcal{F}$, $\mathcal{G}$ — правильные семейства на $(H^n, +)$.
- Рассмотрим квазигруппу

$$(x, y) \to x \circ y = x + \mathcal{F}(x) + y + \mathcal{G}(y),$$

- Если $\mathcal{F}$ — правильное семейство на группе H^n, то семейство $\widetilde{\mathcal{F}}$

$$\widetilde{\mathcal{F}}(x) = (-x) + \pi_{\mathcal{F}}^{-1}(x), \quad \pi_{\mathcal{F}}(x) = x + \mathcal{F}(x), \quad x \in H^n,$$

  также является правильным на H^n.
- Таким образом, операция $x \circ y$ **обращается справа** следующим образом:

$$x = \pi_{\widetilde{F}}\left((x \circ y) - \pi_G(y)\right).$$

- Обращение слева также возможно. Обращение $\Leftrightarrow$ алгоритм расшифрования $\Leftrightarrow$ FPE-схема.

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна[19].
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости[20].
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма[21] со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma_{\mathcal{F}}$, задаваемая семейством $\mathcal{F}$, является одностоковой.
- Алгоритм опирается на характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

[19] Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

[20] Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

[21] Bosshard и Gärtner, «Pseudo unique sink orientations».

Численные эксперименты

- Найдено точное число правильных, треугольных, рекурсивно/локально треугольных булевых семейств для малых значений $n \leq 5$.
- Найдены индексы ассоциативности квазигрупп порядка $|Q| \in \{4, 8\}$, задаваемых парами правильных семейств, для $n = 16$ проведен статистический эксперимент; изучены свойства афинности и простоты.

Содержание

Положения, выносимые на защиту

- Между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентациями), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-сетями) существует естественное соответствие. Между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера также существует естественное соответствие.
- Стабилизатор множества правильных семейств функций представляет собой множество пар согласованных изометрий пространства Хэмминга (согласованных перенумераций и перекодировок).
- Отображения, задаваемые правильными семействами булевых функций, всегда имеют четное число неподвижных точек.

Положения, выносимые на защиту

- Мощность множества правильных семейств булевых функций размера n $T(n)$ удовлетворяет отношению $\log_2(T(n)) = \Theta\left(2^n \cdot \log_2(n)\right)$. Треугольные семейства составляют бесконечно малую долю среди всех правильных семейств булевых функций.
- Локально треугольные, рекурсивно треугольные и сильно квадратичное семейства являются правильными. Мощность образов рассмотренных в работе квадратичных булевых правильных семейств близка к максимально возможной.
- Предложенная в работе конструкция позволяет порождать квазигруппы с помощью правильных семейств функций. Алгоритм шифрования, построенный на основе этой конструкции, сохраняет формат исходных сообщений (является FPE-схемой). Ряд утверждений о числе ассоциативных троек в квазигруппах, построенных на основе предложенной конструкции, позволяет свести вопрос об изучении индексов ассоциативности от всех пар правильных семейств к классам эквивалентности пар правильных семейств.

Апробация работы

- XXVI Международная конференция студентов, аспирантов и молодых учёных «Ломоносов», Москва, Россия, с 8 по 12 апреля 2019 г.;
- X симпозиум «Современные тенденции в криптографии» (CTCrypt 2021), Дорохово, Россия, с 1 по 4 июня 2021 г.;
- XI симпозиум «Современные тенденции в криптографии» (CTCrypt 2022), Новосибирск, Россия, с 6 по 9 июня 2022 г.;
- Четырнадцатый международный семинар «Дискретная математика и ее приложения» имени академика О.Б. Лупанова под руководством В. В. Кочергина, Э. Э. Гасанова, С. А. Ложкина, А. В. Чашкина, с 20 по 25 июня 2022 г.;
- 11-я Международная конференция «Дискретные модели в теории управляющих систем», Красновидово, Россия, с 26 по 29 мая 2023 г.;
- Третья Международная конференция “MATHEMATICS IN ARMENIA: ADVANCES AND PERSPECTIVES”, Ереван, Армения, со 2 по 8 июля 2023 г.;

Апробация работы

- 22-я Международная конференция «Сибирская научная школа-семинар “Компьютерная безопасность и криптография” имени Геннадия Петровича Агибалова», Барнаул, Россия, с 4 по 9 сентября 2023 г.;
- Международная конференция «Математика в созвездии наук», Москва, Россия, с 1 по 2 апреля 2024 г.;
- Международная конференция «Алгебра и математическая логика: теория и приложения», Казань, Россия, с 27 июня по 1 июля 2024 г.;
- XX Международная научная конференция «Проблемы теоретической кибернетики», Москва, Россия, с 5 по 8 декабря 2024 г.

Апробация работы

- Научно-исследовательский семинар по алгебре механико-математического факультета МГУ под руководством Д. О. Орлова, М. В. Зайцева, 2023 г.
- Научно-исследовательский семинар «Математические вопросы кибернетики» кафедр дискретной математики и математической теории интеллектуальных систем механико-математического факультета и математической кибернетики факультета вычислительной математики и кибернетики МГУ под руководством Э. Э. Гасанова, В. В. Кочергина, С. А. Ложкина, 2023 г.
- Семинар «Компьютерная алгебра» факультета ВМК МГУ и ВЦ РАН под руководством профессора С. А. Абрамова, 2023 г.
- Семинар «Теория автоматов» механико-математического факультета МГУ под руководством профессора Э. Э. Гасанова, 2023 г.
- Семинар «Современные проблемы криптографии» под руководством ведущего научного сотрудника В. А. Носова и доцента А. Е. Панкратьева, механико-математический факультет МГУ, неоднократно.

Основные результаты по теме диссертации изложены в **9** печатных изданиях, **8** из которых опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика, из них **6** — в рецензируемых научных изданиях, входящих в ядро РИНЦ и международные базы цитирования (Web of Science / Scopus), RSCI, **2** — в рецензируемых научных изданиях из дополнительного списка МГУ, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика и входящих в список ВАК.

Публикации по теме диссертации

- «О соответствии между правильными семействами и реберными ориентациями булевых кубов», Интеллектуальные системы. Теория и приложения, 24:1 (2020), 97–100.
- «О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов», ПДМ, 2020, 48, 16–21 (2020).
- «О свойствах правильных семейств булевых функций», Дискрет. матем., 33:1 (2021), 91–102.
- “Format-preserving encryption: a survey”, Матем. вопр. криптогр., 13:2 (2022), 133–153.
- «Об одном квазигрупповом алгоритме шифрования, сохраняющего формат», ПДМ. Приложение, 2023, 16, 102–104.
- «Об индексе ассоциативности конечных квазигрупп», Интеллектуальные системы. Теория и приложения, 28:3 (2024), 80–101.

Публикации автора (в соавторстве)

- A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev, “Proper families of functions and their applications”, Матем. вопр. криптогр., 14:2 (2023), 43–58.
- А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, К. Д. Царегородцев, «О порождении n-квазигрупп с помощью правильных семейств функций», Дискрет. матем., 35:1 (2023), 35–53.
- A. V. Galatenko, A. E. Pankratiev, K. D. Tsaregorodtsev,“A Criterion of Properness for a Family of Functions”, Journal of Mathematical Sciences, 284:4 (2024), 451–459.