

Правильные семейства функций и порождаемые ими квазигруппы

Комбинаторные и алгебраические свойства

Содержание доклада

1. Введение: зачем исследуем?
2. Глава 1: основные определения и примеры
3. Глава 2: эквивалентные условия правильности семейств
4. Глава 3: свойства правильных семейств
5. Глава 4: алгоритмические и вычислительные аспекты

Технический момент: используемые обозначения

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

Еще технический момент

Примеры/определения

Как правило, НЕ мои.

Утверждения

Тоже не мои.

Леммы-теоремы-утверждения

Мои.

Где не мои — приводятся ссылки на работы. Если в тексте есть упоминание Теоремы X, то номер X взят из диссертации.

Содержание

- 1 Введение: зачем исследуем?
- 2 Глава 1: основные определения и примеры
- 3 Глава 2: эквивалентные условия правильности семейств
- 4 Глава 3: свойства правильных семейств
- 5 Глава 4: алгоритмические и вычислительные аспекты

«Обычная» криптография

В криптографии широко используются различные алгебраические структуры:

- поля: \mathbb{F}_q ;
- коммутативные группы: \mathbb{F}_q^* , $\mathbb{E}(\mathbb{F}_q)$;
- кольца (коммутативные, ассоциативные, с единицей): \mathbb{Z} , \mathbb{Z}_n ;
- коды (векторные подпространства над конечными полями), решетки¹, ...

¹Bernstein, Buchmann и Dahmen, *Post-quantum cryptography*.

«Необычная» криптография

При этом в исследовательской литературе предлагаются к рассмотрению и более «экзотические» структуры, например:

- модули более общего вида²;
- **некоммутативные** группы и алгебры (например, группы кос, алгебры матриц, алгебра кватернионов и так далее)³;
- **неассоциативные структуры**: квазигруппы, квазигрупповые кольца и т.д.⁴.

Именно на последние мы и посмотрим чуть подробнее.

²Нечаев, «Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам».

³Myasnikov, Shpilrain и Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*; Молдовян, Молдовян и Молдовян, «Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах»; Романьков, *Алгебраическая криптология: монография*.

⁴Markov, Mikhalev и Nechaev, «Nonassociative Algebraic Structures in Cryptography and Coding»; Артамонов, «Квазигруппы и их приложения», «О применениях квазигрупп в криптографии».

Квазигруппа

Квазигруппа, Определение 1

Множество Q с заданной на нём бинарной операцией $\circ: Q \times Q \rightarrow Q$, со следующим свойством: для любых $a, b \in Q$ существуют единственные $x, y \in Q$, такие что:

$$a \circ x = b, \quad y \circ a = b.$$

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

Другими словами, операции **левого** L_a и **правого** R_a умножения (сдвиги)

$$L_a: Q \rightarrow Q, L_a(x) = a \circ x, R_a: Q \rightarrow Q, R_a(y) = y \circ a,$$

являются биекциями на Q .

По сути = группа без ассоциативности и единицы, но с **сокращением** как слева, так и справа.

Квазигруппа

Квазигруппа, Определение 1

Множество Q с заданной на нём бинарной операцией $\circ: Q \times Q \rightarrow Q$, со следующим свойством: для любых $a, b \in Q$ существуют единственные $x, y \in Q$, такие что:

$$a \circ x = b, \quad y \circ a = b.$$

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

Другими словами, операции **левого** L_a и **правого** R_a умножения (сдвиги)

$$L_a: Q \rightarrow Q, L_a(x) = a \circ x, R_a: Q \rightarrow Q, R_a(y) = y \circ a,$$

являются биекциями на Q .

По сути = группа без ассоциативности и единицы, но с сокращением как слева, так и справа.

Квазигруппа

Квазигруппа, Определение 1

Множество Q с заданной на нём бинарной операцией $\circ: Q \times Q \rightarrow Q$, со следующим свойством: для любых $a, b \in Q$ существуют единственные $x, y \in Q$, такие что:

$$a \circ x = b, \quad y \circ a = b.$$

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

Другими словами, операции **левого** L_a и **правого** R_a умножения (сдвиги)

$$L_a: Q \rightarrow Q, L_a(x) = a \circ x, R_a: Q \rightarrow Q, R_a(y) = y \circ a,$$

являются биекциями на Q .

По сути = группа без ассоциативности и единицы, но с **сокращением** как слева, так и справа.

Несколько примеров

- Q — любая группа, например $Q = \mathbb{Z}_k$, $\circ = +$;
- $Q = \mathbb{Z}_k$, $\circ = -$ (не группа, т.к. $a - (b - c) \neq (a - b) - c$);
- (G, \cdot) — группа, π, σ, τ — подстановки на G , тогда можно рассмотреть изотоп⁵
(Определение 5):

$$x \circ y = \tau(\pi(x) \cdot \sigma(y)).$$

⁵Denes и Keedwell, *Latin squares and their applications (2nd edition)*; Белоусов, *Основы теории квазигрупп и луп*.

Несколько примеров

- Q — любая группа, например $Q = \mathbb{Z}_k$, $\circ = +$;
- $Q = \mathbb{Z}_k$, $\circ = -$ (не группа, т.к. $a - (b - c) \neq (a - b) - c$);
- (G, \cdot) — группа, π, σ, τ — подстановки на G , тогда можно рассмотреть изотоп⁵
(Определение 5):

$$x \circ y = \tau(\pi(x) \cdot \sigma(y)).$$

⁵Denes и Keedwell, *Latin squares and their applications (2nd edition)*; Белоусов, *Основы теории квазигрупп и луп*.

Несколько примеров

- Q — любая группа, например $Q = \mathbb{Z}_k$, $\circ = +$;
- $Q = \mathbb{Z}_k$, $\circ = -$ (не группа, т.к. $a - (b - c) \neq (a - b) - c$);
- (G, \cdot) — группа, π, σ, τ — подстановки на G , тогда можно рассмотреть **изотоп**⁵
(Определение 5):

$$x \circ y = \tau(\pi(x) \cdot \sigma(y)).$$

⁵Denes и Keedwell, *Latin squares and their applications (2nd edition)*; Белоусов, *Основы теории квазигрупп и луп*.

Латинский квадрат

- Квадратная таблица размера $k \times k$, заполнена элементами множества $\{0, \dots, k-1\}$, каждый элемент появляется **только один раз** в каждом столбце и каждой строке таблицы (**Определение 2**).
- Таблица умножения квазигруппы $Q = \{q_1, \dots, q_k\}$ (на пересечении i -й строки и j -го столбца пишем $(q_i \circ q_j) \in Q$) является латинским квадратом.

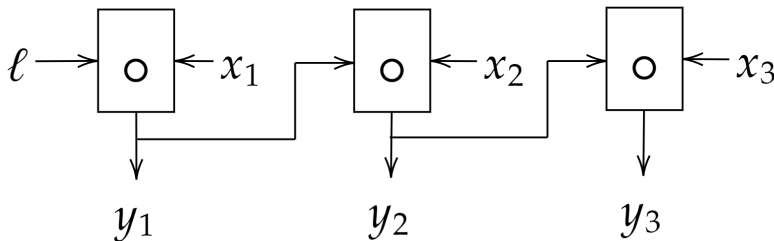
$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 3 & 4 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 1 & 2 & 0 \\ 4 & 2 & 0 & 1 & 3 \end{bmatrix}$$


Пример: E -преобразование

Пусть $x_1, \dots, x_k, \ell \in Q$. Определим⁶ преобразование E_ℓ :

$$E_\ell(x_1 \dots x_k) = y_1 \dots y_k,$$

$$y_1 = \ell \circ x_1, \quad y_{i+1} = y_i \circ x_{i+1}.$$



⁶Markovski и Bakeva, «Quasigroup string processing: Part 4».

Пример: итерации E -преобразований

- Можем ввести кратное E -преобразование:

$$E_{\ell_1, \dots, \ell_n}(x) = E_{\ell_1}(\dots(E_{\ell_n}(x))\dots),$$

- Отображение E_a обладает набором «хороших» криптографических свойств⁷.

⁷Bakeva и Dimitrova, «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis»; Markovski и Bakeva, «Quasigroup string processing: Part 4»; Markovski, Gligoroski и Bakeva, «Quasigroup String Processing: Part 1»; Яшунский, «О преобразованиях распределений вероятностей бесповторными квазигрупповыми формулами», «О скорости сходимости квазигрупповых сверток вероятностных распределений», «Уточнение скорости сходимости распределений квазигрупповых «сумм» конечных случайных величин».

Механизмы

- ГПСЧ на основе итерации E -преобразований⁸.
- Блочный шифр **INRU**⁹, E -преобразование используется в качестве нелинейного элемента.
- «Односторонняя функция»¹⁰ и основанные на ней хэш-функции:

$$R(a_1 \dots a_n) = E_{a_1} (\dots E_{a_n} (a_1 \dots a_n) \dots).$$

⁸Dimitrova и Markovski, «On quasigroup pseudo random sequence generator»; Markovski, Gligoroski и Kocarev, «Unbiased random sequences from quasigroup string transformations».

⁹Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

¹⁰Gligoroski, «On a family of minimal candidate one-way functions and one-way permutations»; Gligoroski и Knapskog, «Edon-R (256,384,512)—an efficient implementation of Edon-R family of cryptographic hash functions»; Gligoroski, Markovski и Kocarev, «Edon-R, An Infinite Family of Cryptographic Hash Functions»; Gligoroski и др., «Cryptographic hash function Edon-R'».

Другие предложения (кратко)

Основная идея: использовать в качестве нелинейного компонента примитива некоторое квазигрупповое преобразование.

- Низкоресурсная (легковесная/lightweight) хэш-функция **GAGE** и AEAD-алгоритм **InGAGE** (см. <http://gageingage.org/>, также¹¹).
- Поточный шифр **Edon80**¹².
- Хэш-функция **NaSHA**¹³.

¹¹Gligoroski, *On the S-box in GAGE and InGAGE*; Gligoroski и др., «GAGE and InGAGE».

¹²Gligoroski, Markovski и Knapskog, «The stream cipher Edon80».

¹³Mileva и Markovski, «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function».

Другие предложения (кратко)-2

- Асимметричные криптопримитивы — аналоги пост-квантовых схем (**multivariate cryptography**¹⁴).
- Основная идея: подобрать такое нелинейное преобразование \mathcal{P} , что вычисление \mathcal{P} и \mathcal{P}^{-1} сделать «легко», а затем «скрыть» структуру \mathcal{P} , взяв обратимые линейные преобразования \mathcal{S} и \mathcal{T} и рассмотрев композицию $\mathcal{F}(x) = \mathcal{S}(\mathcal{P}(\mathcal{T}(x)))$.
- В работах¹⁵ предлагалось рассматривать в качестве нелинейной компоненты \mathcal{P} композицию E -преобразований.
- В работах¹⁶ предлагаемая система и её модификации были успешно атакованы (решение задачи **MinRank** с помощью базисов Грёбнера).

¹⁴Wolf и Preneel, *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*.

¹⁵Chen, 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», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».

¹⁶Faugère и др., «A polynomial-time key-recovery attack on MQQ cryptosystems»; Mohamed и др., «Algebraic attack on the MQQ public key cryptosystem».

Другие предложения (кратко)-2

- Асимметричные криптопримитивы — аналоги пост-квантовых схем (**multivariate cryptography**¹⁴).
- Основная идея: подобрать такое нелинейное преобразование \mathcal{P} , что вычисление \mathcal{P} и \mathcal{P}^{-1} сделать «легко», а затем «скрыть» структуру \mathcal{P} , взяв обратимые линейные преобразования \mathcal{S} и \mathcal{T} и рассмотрев композицию $\mathcal{F}(x) = \mathcal{S}(\mathcal{P}(\mathcal{T}(x)))$.
- В работах¹⁵ предлагалось рассматривать в качестве нелинейной компоненты \mathcal{P} композицию E -преобразований.
- В работах¹⁶ предлагаемая система и её модификации были успешно атакованы (решение задачи **MinRank** с помощью базисов Грёбнера).

¹⁴Wolf и Preneel, *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*.

¹⁵Chen, 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», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».

¹⁶Faugère и др., «A polynomial-time key-recovery attack on MQQ cryptosystems»; Mohamed и др., «Algebraic attack on the MQQ public key cryptosystem».

Другие предложения (кратко)-2

- Асимметричные криптопримитивы — аналоги пост-квантовых схем (**multivariate cryptography**¹⁴).
- Основная идея: подобрать такое нелинейное преобразование \mathcal{P} , что вычисление \mathcal{P} и \mathcal{P}^{-1} сделать «легко», а затем «скрыть» структуру \mathcal{P} , взяв обратимые линейные преобразования \mathcal{S} и \mathcal{T} и рассмотрев композицию $\mathcal{F}(x) = \mathcal{S}(\mathcal{P}(\mathcal{T}(x)))$.
- В работах¹⁵ предлагалось рассматривать в качестве нелинейной компоненты \mathcal{P} композицию E -преобразований.
- В работах¹⁶ предлагаемая система и её модификации были успешно атакованы (решение задачи **MinRank** с помощью базисов Грёбнера).

¹⁴Wolf и Preneel, *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*.

¹⁵Chen, 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», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».

¹⁶Faugère и др., «A polynomial-time key-recovery attack on MQQ cryptosystems»; Mohamed и др., «Algebraic attack on the MQQ public key cryptosystem».

Другие предложения (кратко)-2

- Асимметричные криптопримитивы — аналоги пост-квантовых схем (**multivariate cryptography**¹⁴).
- Основная идея: подобрать такое нелинейное преобразование \mathcal{P} , что вычисление \mathcal{P} и \mathcal{P}^{-1} сделать «легко», а затем «скрыть» структуру \mathcal{P} , взяв обратимые линейные преобразования \mathcal{S} и \mathcal{T} и рассмотрев композицию $\mathcal{F}(x) = \mathcal{S}(\mathcal{P}(\mathcal{T}(x)))$.
- В работах¹⁵ предлагалось рассматривать в качестве нелинейной компоненты \mathcal{P} композицию E -преобразований.
- В работах¹⁶ предлагаемая система и её модификации были успешно атакованы (решение задачи **MinRank** с помощью базисов Грёбнера).

¹⁴Wolf и Preneel, *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*.

¹⁵Chen, 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», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».

¹⁶Faugère и др., «A polynomial-time key-recovery attack on MQQ cryptosystems»; Mohamed и др., «Algebraic attack on the MQQ public key cryptosystem».

Другие предложения (кратко)-3

- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа¹⁷, гомоморфное шифрование¹⁸: используются **ППС/ПЛС-группоиды**, **луповые кольца** над медиальными квазигруппами (изотопы абелевых групп с коммутирующими автоморфизмами).
- Приложения в теории кодирования¹⁹...
- и многое другое²⁰.

¹⁷Барышников и Катышев, «Использование неассоциативных структур для построения алгоритмов открытого распределения ключей»; Катышев, Марков и Нечаев, «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей».

¹⁸Gribov, Zolotykh и Mikhalev, «A construction of algebraic cryptosystem over the quasigroup ring»; Грибов, «Гомоморфность некоторых криптографических систем на основе неассоциативных структур»; Марков, Михалёв и Кислицын, «Неассоциативные структуры в гомоморфной криптографии».

¹⁹Couselo и др., «Loop codes»; 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»; Марков и др., «Квазигруппы и кольца в кодировании и построении криптосхем».

²⁰Chauhan, 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».

Другие предложения (кратко)-3

- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа¹⁷, гомоморфное шифрование¹⁸: используются **ППС/ПЛС-группоиды**, **луповые кольца** над медиальными квазигруппами (изотопы абелевых групп с коммутирующими автоморфизмами).
- Приложения в теории кодирования¹⁹...
- и многое другое²⁰.

¹⁷Барышников и Катышев, «Использование неассоциативных структур для построения алгоритмов открытого распределения ключей»; Катышев, Марков и Нечаев, «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей».

¹⁸Gribov, Zolotykh и Mikhalev, «A construction of algebraic cryptosystem over the quasigroup ring»; Грибов, «Гомоморфность некоторых криптографических систем на основе неассоциативных структур»; Марков, Михалёв и Кислицын, «Неассоциативные структуры в гомоморфной криптографии».

¹⁹Couselo и др., «Loop codes»; 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»; Марков и др., «Квазигруппы и кольца в кодировании и построении криптосхем».

²⁰Chauhan, 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».

Другие предложения (кратко)-3

- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа¹⁷, гомоморфное шифрование¹⁸: используются **ППС/ПЛС-группоиды**, **луповые кольца** над медиальными квазигруппами (изотопы абелевых групп с коммутирующими автоморфизмами).
- Приложения в теории кодирования¹⁹...
- и многое другое²⁰.

¹⁷Барышников и Катышев, «Использование неассоциативных структур для построения алгоритмов открытого распределения ключей»; Катышев, Марков и Нечаев, «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей».

¹⁸Gribov, Zolotikh и Mikhalev, «A construction of algebraic cryptosystem over the quasigroup ring»; Грибов, «Гомоморфность некоторых криптографических систем на основе неассоциативных структур»; Марков, Михалёв и Кислицын, «Неассоциативные структуры в гомоморфной криптографии».

¹⁹Couselo и др., «Loop codes»; 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»; Марков и др., «Квазигруппы и кольца в кодировании и построении криптосхем».

²⁰Chauhan, 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».

Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого класса²¹.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)²².
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой²³, модульное вычитание²⁴).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

²¹Chen, 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».

²²Gligoroski и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

²³Марков, Михалёв и Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

²⁴Snášel и др., «Hash functions based on large quasigroups».

Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого класса²¹.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)²².
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой²³, модульное вычитание²⁴).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

²¹Chen, 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».

²²Gligoroski и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

²³Марков, Михалёв и Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

²⁴Snášel и др., «Hash functions based on large quasigroups».

Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого класса²¹.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)²².
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой²³, модульное вычитание²⁴).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

²¹Chen, 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».

²²Gligoroski и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

²³Марков, Михалёв и Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

²⁴Snášel и др., «Hash functions based on large quasigroups».

Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого класса²¹.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)²².
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой²³, модульное вычитание²⁴).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

²¹Chen, 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».

²²Gligoroski и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

²³Марков, Михалёв и Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

²⁴Snášel и др., «Hash functions based on large quasigroups».

Как задать квазигруппу?

- В общем случае квазигруппа над множеством Q задается таблицей умножения размера $|Q| \times |Q|$; это много.
- Случайная генерация (поиск + отсев) квазигрупп из некоторого узкого класса²¹.
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)²².
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой²³, модульное вычитание²⁴).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

²¹Chen, 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».

²²Gligoroski и др., «Cryptographic hash function Edon-R'»; Грибов, «Алгебраические неассоциативные структуры и их приложения в криптографии».

²³Марков, Михалёв и Нечаев, «Неассоциативные алгебраические структуры в криптографии и кодировании».

²⁴Snášel и др., «Hash functions based on large quasigroups».

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному²⁵:

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

- Для краткости набор функций $\mathcal{F} = (f_1, \dots, f_n)$

$$f_i: Q_1 \times \dots \times Q_n \rightarrow Q_i, \quad i = 1, \dots, n,$$

будем называть семейством функций (**Определение 17**); семейство задает отображение множества $Q = Q_1 \times \dots \times Q_n$ в себя.

- Рассмотрим для простоты случай $Q_i = \{0, 1\}$: какие условия надо наложить на функции f_i , чтобы операция $x \circ y$ задавала **структуру квазигруппы** на $\{0, 1\}^n$?

²⁵Носов и Панкратьев, «О функциональном задании латинских квадратов».

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному²⁵:

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

- Для краткости набор функций $\mathcal{F} = (f_1, \dots, f_n)$

$$f_i: Q_1 \times \dots \times Q_n \rightarrow Q_i, \quad i = 1, \dots, n,$$

будем называть семейством функций (**Определение 17**); семейство задает отображение множества $Q = Q_1 \times \dots \times Q_n$ в себя.

- Рассмотрим для простоты случай $Q_i = \{0, 1\}$: какие условия надо наложить на функции f_i , чтобы операция $x \circ y$ задавала **структуру квазигруппы** на $\{0, 1\}^n$?

²⁵Носов и Панкратьев, «О функциональном задании латинских квадратов».

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному²⁵:

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

- Для краткости набор функций $\mathcal{F} = (f_1, \dots, f_n)$

$$f_i: Q_1 \times \dots \times Q_n \rightarrow Q_i, \quad i = 1, \dots, n,$$

будем называть семейством функций (**Определение 17**); семейство задает отображение множества $Q = Q_1 \times \dots \times Q_n$ в себя.

- Рассмотрим для простоты случай $Q_i = \{0, 1\}$: какие условия надо наложить на функции f_i , чтобы операция $x \circ y$ задавала **структуру квазигруппы** на $\{0, 1\}^n$?

²⁵Носов и Панкратьев, «О функциональном задании латинских квадратов».

Содержание

- 1 Введение: зачем исследуем?
- 2 Глава 1: основные определения и примеры
- 3 Глава 2: эквивалентные условия правильности семейств
- 4 Глава 3: свойства правильных семейств
- 5 Глава 4: алгоритмические и вычислительные аспекты

Правильные семейства булевых функций

Правильное семейство, Определение 27

Семейство булевых функций $f_i: \mathbb{E}_2^n \rightarrow \mathbb{E}_2^n$ 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», «Построение классов латинских квадратов в булевой базе данных».

Правильные семейства можно задавать над логикой любой значности k^{26} , над произвольными группами²⁷; над прямыми произведениями других квазигрупп²⁸ и d -квазигрупп²⁹.

²⁶ Носов, «Построение параметрического семейства латинских квадратов в векторной базе данных».

²⁷ Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

²⁸ Galatenko, Nosov и Pankratiev, «Latin squares over quasigroups».

²⁹ Плаксина, «Построение параметрического семейства многомерных латинских квадратов».

Правильные семейства булевых функций

Правильное семейство, Определение 27

Семейство булевых функций $f_i: \mathbb{E}_2^n \rightarrow \mathbb{E}_2^n$ 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», «Построение классов латинских квадратов в булевой базе данных».

Правильные семейства можно задавать над логикой любой значности k^{26} , над произвольными группами²⁷; над прямыми произведениями других квазигрупп²⁸ и d -квазигрупп²⁹.

²⁶ Носов, «Построение параметрического семейства латинских квадратов в векторной базе данных».

²⁷ Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

²⁸ Galatenko, Nosov и Pankratiev, «Latin squares over quasigroups».

²⁹ Плаксина, «Построение параметрического семейства многомерных латинских квадратов».

Связь правильных семейств и квазигрупп, Утверждение 1

Семейство булевых функций $F = (f_1, \dots, f_n)$ является правильным тогда и только тогда, когда отображение вида

$$(x, y) \rightarrow z = x \oplus y \oplus F(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n))$$

задает квазигрупповую операцию **при любом выборе** внутренних функций π_1, \dots, π_n .

Носов, «Построение классов латинских квадратов в булевой базе данных».

Существенная (не)зависимость, Замечание 13

Из определения правильности следует, что f_i не зависит существенно от x_i .

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

Связь правильных семейств и квазигрупп, Утверждение 1

Семейство булевых функций $F = (f_1, \dots, f_n)$ является правильным тогда и только тогда, когда отображение вида

$$(x, y) \rightarrow z = x \oplus y \oplus F(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n))$$

задает квазигрупповую операцию **при любом выборе** внутренних функций π_1, \dots, π_n .

Носов, «Построение классов латинских квадратов в булевой базе данных».

Существенная (не)зависимость, Замечание 13

Из определения правильности следует, что f_i не зависит существенно от x_i .

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

Правильные семейства и квазигруппы-2

Критерий в терминах регулярности, Теорема 1

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

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

Критерий обобщает известный результат³⁰ для абелевых групп.

³⁰Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

Константные семейства, Пример 2

$f_i \equiv \text{const}_i$ является правильным.

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

Треугольные семейства, Пример 3

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} \text{const} \\ f_2(x_1) \\ f_3(x_1, x_2) \\ \vdots \\ f_n(x_1, \dots, x_{n-1}) \end{bmatrix}$$

является правильным.

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

Константные семейства, Пример 2

$f_i \equiv \text{const}_i$ является правильным.

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

Треугольные семейства, Пример 3

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} \text{const} \\ f_2(x_1) \\ f_3(x_1, x_2) \\ \vdots \\ f_n(x_1, \dots, x_{n-1}) \end{bmatrix}$$

является правильным.

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

Класс квадратичных семейств, Теорема 2

Семейство \mathcal{F} является правильным для любого $n \geq 1$:

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

Преобразование сдвига, Утверждение 9, Теорема 4

Для любого $\alpha = (a_1, \dots, a_n) \in Q^n$ определим преобразование сдвига:

$$x \in Q^n \rightarrow L_\alpha(x) = (a_1 \circ x_1, \dots, a_n \circ x_n),$$

$$x \in Q^n \rightarrow R_\alpha(x) = (x_1 \circ a_1, \dots, x_n \circ a_n).$$

Если $\mathcal{F}: Q^n \rightarrow Q^n$ правильное, то $T_\alpha(\mathcal{F}(T_\beta(x)))$ также правильное, где $T \in \{L, R\}$, $\alpha, \beta \in Q^n$.

Обобщение результата³¹ для абелевых групп.

³¹Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

Преобразование перекодировки, Определение 58, Определение 59

Для любого набора $\Psi = (\psi_1, \dots, \psi_n) \in \text{Func}(Q)^n$ определим преобразование перекодировки:

$$x \in Q^n \rightarrow \Psi(x) = (\psi_1(x_1), \dots, \psi_n(x_n)).$$

Пусть $\Phi \in \text{Func}(Q)^n$, $\Psi \in \text{Perm}(Q)^n$. Если $\mathcal{F}(x) = (f_1(x), \dots, f_n(x))$ правильное, то $\Phi(\mathcal{F}(\Psi(x)))$ также правильное.

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

Если $\Phi, \Psi \in \text{Perm}(Q)^n$, то подобные преобразования будем называть преобразованиями перекодировки.

Сдвиги являются частными случаями преобразования перекодировки.

Преобразование перекодировки, Определение 58, Определение 59

Для любого набора $\Psi = (\psi_1, \dots, \psi_n) \in \text{Func}(Q)^n$ определим преобразование перекодировки:

$$x \in Q^n \rightarrow \Psi(x) = (\psi_1(x_1), \dots, \psi_n(x_n)).$$

Пусть $\Phi \in \text{Func}(Q)^n$, $\Psi \in \text{Perm}(Q)^n$. Если $\mathcal{F}(x) = (f_1(x), \dots, f_n(x))$ правильное, то $\Phi(\mathcal{F}(\Psi(x)))$ также правильное.

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

Если $\Phi, \Psi \in \text{Perm}(Q)^n$, то подобные преобразования будем называть преобразованиями перекодировки.

Сдвиги являются частными случаями преобразования перекодировки.

Преобразование перекодировки, Определение 58, Определение 59

Для любого набора $\Psi = (\psi_1, \dots, \psi_n) \in \text{Func}(Q)^n$ определим преобразование перекодировки:

$$x \in Q^n \rightarrow \Psi(x) = (\psi_1(x_1), \dots, \psi_n(x_n)).$$

Пусть $\Phi \in \text{Func}(Q)^n$, $\Psi \in \text{Perm}(Q)^n$. Если $\mathcal{F}(x) = (f_1(x), \dots, f_n(x))$ правильное, то $\Phi(\mathcal{F}(\Psi(x)))$ также правильное.

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

Если $\Phi, \Psi \in \text{Perm}(Q)^n$, то подобные преобразования будем называть преобразованиями перекодировки.

Сдвиги являются частными случаями преобразования перекодировки.

Согласованная перенумерация, Утверждение 10

Пусть $\sigma \in Perm(n)$, определим преобразование согласованной перенумерации:

$$\begin{aligned}\mathcal{F} &\rightarrow \sigma(\mathcal{F}), \\ f_i(x_1, \dots, x_n) &\rightarrow f_{\sigma(i)}(x_{\sigma(1)}, \dots, x_{\sigma(n)}).\end{aligned}$$

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

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

Проекция, Утверждение 11

Подставим значение $a \in Q$ вместо переменной x_i и исключим функцию f_i , $1 \leq i \leq n$.

$$F'(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = \Pi_a^i(F) = \begin{bmatrix} f_1(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ \vdots \\ f_{i-1}(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ f_{i+1}(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ \vdots \\ f_n(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \end{bmatrix}.$$

Полученное семейство является правильным.

Galatenko, Nosov и Pankratiev, «Latin squares over quasigroups».

Криптографические 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 $f: Q^n \rightarrow Q$ задается с помощью композиции констант и операции умножения).

Криптографические 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 $f: Q^n \rightarrow Q$ задается с помощью композиции констант и операции умножения).

Криптографические 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 $f: Q^n \rightarrow Q$ задается с помощью композиции констант и операции умножения).

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:

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

Об индексах ассоциативности

- 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).

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:

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

Об индексах ассоциативности

- 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 $(\mathcal{F}, \mathcal{G})$, чётно (**Теорема 8**).

Содержание

- 1 Введение: зачем исследуем?
- 2 Глава 1: основные определения и примеры
- 3 Глава 2: эквивалентные условия правильности семейств**
- 4 Глава 3: свойства правильных семейств
- 5 Глава 4: алгоритмические и вычислительные аспекты

Одностоковые ориентации (USO)

Булев куб B_n

- вершины: $V = \{\alpha \in \mathbb{E}_2^n\}$;
- ребра: $\{\alpha, \beta\} \in E \Leftrightarrow \rho(\alpha, \beta) = 1$ (расстояние Хэмминга).

Яблонский, *Введение в дискретную математику*.

Ориентация с единственным стоком USO, Определение 45

Ориентация с единственным стоком (unique sink orientation, USO) куба B_n — ориентированный граф, построенный по B_n со следующим характеристическим свойством: в каждом подкубе B_n существует единственный сток.

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

USO: один пример

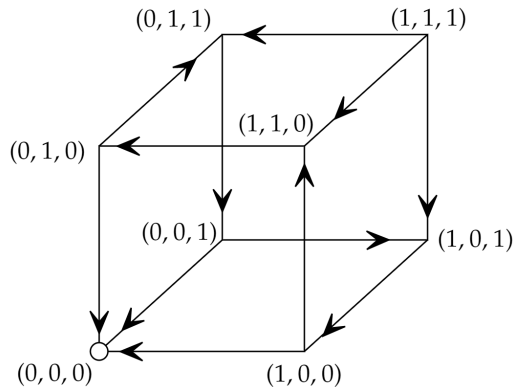
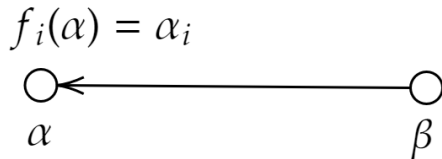


Рис. 1: Одностокковая ориентация трехмерного булева куба B_3

Пусть \mathcal{F} — семейство булевых функций.

Граф семейства $\Gamma_{\mathcal{F}}$, Определение 47

- Вершины: $V = \{\alpha \in \mathbb{E}_2^n\}$.
- Пусть $\alpha \neq \beta$, $\rho(\alpha, \beta) = 1$, $\alpha_i \neq \beta_i$, добавим ориентированное ребро $(\beta, \alpha) \in E$ тогда и только тогда, когда $f_i(\alpha) = \alpha_i$.



Стоки графа $\Gamma_{\mathcal{F}}$

Неподвижные точки булевых семейств, Лемма 1

У правильного семейства булевых функций всегда существует единственная неподвижная точка.

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

$$f_i(\alpha) = \alpha_i, \quad 1 \leq i \leq n.$$

- Ориентации подкубов в $\Gamma_{\mathcal{F}}$ задаются проекциями \mathcal{F}' семейства \mathcal{F} .

Взаимно-однозначное соответствие, Теорема 9

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

Стоки графа $\Gamma_{\mathcal{F}}$

Неподвижные точки булевых семейств, Лемма 1

У правильного семейства булевых функций всегда существует единственная неподвижная точка.

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

$$f_i(\alpha) = \alpha_i, \quad 1 \leq i \leq n.$$

- Ориентации подкубов в $\Gamma_{\mathcal{F}}$ задаются проекциями \mathcal{F}' семейства \mathcal{F} .

Взаимно-однозначное соответствие, Теорема 9

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

USO и правильность: два описания одного объекта

- Существует взаимно-однозначное соответствие между «алгебраическим» (определение правильности) и «геометрическим» (USO) описаниями.
- Это позволяет переводить результаты с одного «языка» на другой.
- Некоторые примеры переноса: вероятностный алгоритм порождения правильных семейств с помощью процедуры MCS³², оценка на число булевых правильных семейств³³, новые классы правильных семейств.

³²Schurr, «Unique sink orientations of cubes»; Галатенко и др., «Порождение правильных семейств функций».

³³Царегородцев, «О свойствах правильных семейств булевых функций».

Пусть $T(n)$ ($\Delta(n)$) — число **булевых** правильных (треугольных) семейств размера n .

Оценка на число булевых правильных семейств, Утверждение 23

$$n^{A \cdot 2^n} \leq T(n) \leq n^{B \cdot 2^n},$$

где A, B — некоторые положительные константы.

Matousek, «The Number Of Unique-Sink Orientations of the Hypercube».

Булевых треугольных семейств экспоненциально мало, Теорема 10

$$\frac{\Delta(n)}{T(n)} = o\left(\frac{1}{n^{D \cdot 2^n}}\right) \text{ при } n \rightarrow \infty,$$

для некоторого $D > 0$. Почти все булевы правильные семейства не являются треугольными.

Пусть $T(n)$ ($\Delta(n)$) — число **булевых** правильных (треугольных) семейств размера n .

Оценка на число булевых правильных семейств, Утверждение 23

$$n^{A \cdot 2^n} \leq T(n) \leq n^{B \cdot 2^n},$$

где A, B — некоторые положительные константы.

Matousek, «The Number Of Unique-Sink Orientations of the Hypercube».

Булевых треугольных семейств экспоненциально мало, Теорема 10

$$\frac{\Delta(n)}{T(n)} = o\left(\frac{1}{n^{D \cdot 2^n}}\right) \text{ при } n \rightarrow \infty,$$

для некоторого $D > 0$. Почти все булевы правильные семейства не являются треугольными.

Рекурсивная треугольность

Рекурсивно треугольное семейство, Определение 48

Семейство $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ со свойством: существует i , такое что $f_i \equiv \text{const}_i$, и $\Pi_a^i(\mathcal{F})$ рекурсивно треугольны для всех $a \in \mathbb{E}_k$.

Обобщение понятия рекурсивной ориентации булева куба ³⁴. Треугольные семейства являются рекурсивно треугольными.

О правильности рекурсивно треугольных семейств, Лемма 9

Рекурсивно треугольные семейства являются правильными.

Теорема доказывается через локально треугольные семейства, о них позднее.

³⁴OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, A141770

Рекурсивная треугольность

Рекурсивно треугольное семейство, Определение 48

Семейство $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ со свойством: существует i , такое что $f_i \equiv \text{const}_i$, и $\Pi_a^i(\mathcal{F})$ рекурсивно треугольны для всех $a \in \mathbb{E}_k$.

Обобщение понятия рекурсивной ориентации булева куба ³⁴. Треугольные семейства являются рекурсивно треугольными.

О правильности рекурсивно треугольных семейств, Лемма 9

Рекурсивно треугольные семейства являются правильными.

Теорема доказывается через локально треугольные семейства, о них позднее.

³⁴OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, A141770

Рекурсивная треугольность

Рекурсивно треугольное семейство, Определение 48

Семейство $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ со свойством: существует i , такое что $f_i \equiv \text{const}_i$, и $\Pi_a^i(\mathcal{F})$ рекурсивно треугольны для всех $a \in \mathbb{E}_k$.

Обобщение понятия рекурсивной ориентации булева куба ³⁴. Треугольные семейства являются рекурсивно треугольными.

О правильности рекурсивно треугольных семейств, Лемма 9

Рекурсивно треугольные семейства являются правильными.

Теорема доказывается через локально треугольные семейства, о них позднее.

³⁴OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, A141770

Рекурсивная треугольность

Рекурсивно треугольное семейство, Определение 48

Семейство $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ со свойством: существует i , такое что $f_i \equiv \text{const}_i$, и $\Pi_a^i(\mathcal{F})$ рекурсивно треугольны для всех $a \in \mathbb{E}_k$.

Обобщение понятия рекурсивной ориентации булева куба ³⁴. Треугольные семейства являются рекурсивно треугольными.

О правильности рекурсивно треугольных семейств, Лемма 9

Рекурсивно треугольные семейства являются правильными.

Теорема доказывается через локально треугольные семейства, о них позднее.

³⁴OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, A141770

Рекуррентное соотношение

Рекурсивно треугольных семейств мало, Лемма 5, Теорема 11

Пусть $\Delta_k^{\text{rec}}(n)$ — число рекурсивно треугольных семейств размера n над k -значной логикой. Тогда выполняется равенство:

$$\Delta_k^{\text{rec}}(n) = \sum_{j=1}^n (-1)^{j+1} \cdot k^j \cdot \binom{n}{j} \Delta_k^{\text{rec}}(n-j)^{k^j}.$$

Доля булевых рекурсивно треугольных семейств размера n в классе всех булевых правильных семейств размера n стремится к 0 при $n \rightarrow \infty$.

Обобщение результата для рекурсивной ориентации булева куба ³⁵.

³⁵OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, A141770

Неподвижные точки правильного семейства

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.

В общем случае: семейство $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки \mathcal{F} все её проекции имеют единственную неподвижную точку³⁶.

В булевом случае свойство единственности неподвижной точки даёт ещё одно характеристическое свойство правильных семейств, которое изучалось в контексте математической биологии (экспрессия генов³⁷).

³⁶Галатенко, Носов и Панкратьев, «Об одном критерии правильности семейства функций».

³⁷Richard, «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».

Неподвижные точки правильного семейства

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.

В общем случае: семейство $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки \mathcal{F} все её проекции имеют единственную неподвижную точку³⁶.

В булевом случае свойство единственности неподвижной точки даёт ещё одно характеристическое свойство правильных семейств, которое изучалось в контексте математической биологии (экспрессия генов³⁷).

³⁶Галатенко, Носов и Панкратьев, «Об одном критерии правильности семейства функций».

³⁷Richard, «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».

Неподвижные точки правильного семейства

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.

В общем случае: семейство $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки \mathcal{F} все её проекции имеют единственную неподвижную точку³⁶.

В булевом случае свойство единственности неподвижной точки даёт ещё одно характеристическое свойство правильных семейств, которое изучалось в контексте математической биологии (экспрессия генов³⁷).

³⁶Галатенко, Носов и Панкратьев, «Об одном критерии правильности семейства функций».

³⁷Richard, «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».

Булевы сети с наследственно единственной неподвижной точкой, Определение

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 $\mathbb{E}_2^n \rightarrow \mathbb{E}_2^n$).

Richard, «Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks».

Правильные семейства \leftrightarrow HUFP-сети, Теорема 12

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

Соответствие между булевыми правильными семействами и HUFP-сетями позволяет перенести (и обобщить) часть результатов, полученных в контексте изучения динамики таких сетей, на правильные семейства.

Булевы сети с наследственно единственной неподвижной точкой, Определение

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 $\mathbb{E}_2^n \rightarrow \mathbb{E}_2^n$).

Richard, «Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks».

Правильные семейства \leftrightarrow HUFP-сети, Теорема 12

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

Соответствие между булевыми правильными семействами и HUFP-сетями позволяет перенести (и обобщить) часть результатов, полученных в контексте изучения динамики таких сетей, на правильные семейства.

Пусть \mathcal{F} — семейство размера n .

Локальный граф взаимодействий $G(\mathcal{F}, \alpha)$

- Вершины: $V = \{1, \dots, n\}$.
- Ребра: $i \rightarrow j$ тогда и только тогда, когда f_j существенно зависит от x_i «локально» в точке a :

$$f_j(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \neq f_j(\alpha_1, \dots, \alpha_i \oplus 1, \dots, \alpha_n).$$

Ациклические локальные графы

Пусть $G(\mathcal{F}, \alpha)$ — ациклический для каждой точки $\alpha \in \mathbb{E}_2^n$, тогда \mathcal{F} — HUFP-сеть.

Shih и Dong, «A combinatorial analogue of the Jacobian problem in automata networks».

Пусть \mathcal{F} — семейство размера n .

Локальный граф взаимодействий $G(\mathcal{F}, \alpha)$

- Вершины: $V = \{1, \dots, n\}$.
- Ребра: $i \rightarrow j$ тогда и только тогда, когда f_j существенно зависит от x_i «локально» в точке a :

$$f_j(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \neq f_j(\alpha_1, \dots, \alpha_i \oplus 1, \dots, \alpha_n).$$

Ациклические локальные графы

Пусть $G(\mathcal{F}, \alpha)$ — ациклический для каждой точки $\alpha \in \mathbb{E}_2^n$, тогда \mathcal{F} — HUFP-сеть.

Shih и Dong, «A combinatorial analogue of the Jacobian problem in automata networks».

Локальный граф взаимодействий-2

Локально треугольные семейства, Определение 51

$\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ локально треугольно, если $G(\mathcal{F}, \alpha)$ ацикличесен для каждой точки $\alpha \in \mathbb{E}_k^n$, где локальная зависимость f от x_i в точке α определяется неравенством:

$$\exists b: f(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \neq f(\alpha_1, \dots, b, \dots, \alpha_n).$$

Теорема 13

Локально треугольные семейства являются правильными.

Обобщение результата³⁸ на k -значную логику.

Лемма 9

Всякое рекурсивно треугольное семейство является локально треугольным.

³⁸Shih и Dong, «A combinatorial analogue of the Jacobian problem in automata networks».

Локальный граф взаимодействий-2

Локально треугольные семейства, Определение 51

$\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ локально треугольно, если $G(\mathcal{F}, \alpha)$ ацикличесен для каждой точки $\alpha \in \mathbb{E}_k^n$, где локальная зависимость f от x_i в точке α определяется неравенством:

$$\exists b: f(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \neq f(\alpha_1, \dots, b, \dots, \alpha_n).$$

Теорема 13

Локально треугольные семейства являются правильными.

Обобщение результата³⁸ на k -значную логику.

Лемма 9

Всякое рекурсивно треугольное семейство является локально треугольным.

³⁸Shih и Dong, «A combinatorial analogue of the Jacobian problem in automata networks».

Локальный граф взаимодействий-2

Локально треугольные семейства, Определение 51

$\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ локально треугольно, если $G(\mathcal{F}, \alpha)$ ацикличесен для каждой точки $\alpha \in \mathbb{E}_k^n$, где локальная зависимость f от x_i в точке α определяется неравенством:

$$\exists b: f(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \neq f(\alpha_1, \dots, b, \dots, \alpha_n).$$

Теорема 13

Локально треугольные семейства являются правильными.

Обобщение результата³⁸ на k -значную логику.

Лемма 9

Всякое рекурсивно треугольное семейство является локально треугольным.

³⁸Shih и Dong, «A combinatorial analogue of the Jacobian problem in automata networks».

Характеризация через несамодвойственные проекции

Самодвойственное семейство

Отображение $\mathcal{F}: \mathbb{E}_2^n \rightarrow \mathbb{E}_2^k$ самодвойственно, если для любого набора $x \in \mathbb{E}_2^n$ выполняется свойство $\mathcal{F}(\bar{x}) = \overline{\mathcal{F}(x)}$.

О несамодвойственности проекций, Теорема 14

Семейство \mathcal{F} булевых функций правильно тогда и только тогда, когда каждая из его проекций

$$\Pi_{i_1, \dots, i_k}^{a_1, \dots, a_k}(\mathcal{F})$$

не является самодвойственным булевым отображением.

По сути — следствие результата из Richard, «Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks».

Характеризация через несамодвойственные проекции

Самодвойственное семейство

Отображение $\mathcal{F}: \mathbb{E}_2^n \rightarrow \mathbb{E}_2^k$ самодвойственно, если для любого набора $x \in \mathbb{E}_2^n$ выполняется свойство $\mathcal{F}(\bar{x}) = \overline{\mathcal{F}(x)}$.

О несамодвойственности проекций, Теорема 14

Семейство \mathcal{F} булевых функций правильно тогда и только тогда, когда каждая из его проекций

$$\Pi_{i_1, \dots, i_k}^{a_1, \dots, a_k}(\mathcal{F})$$

не является самодвойственным булевым отображением.

По сути — следствие результата из Richard, «Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks».

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-ориентаций³⁹, для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n): V = \mathbb{E}_{k^2}^n$,

$$\{v, w\} \in E \leftrightarrow \exists i, 1 \leq i \leq n: v_i \equiv w_i \pmod k, v_i \neq w_i.$$
- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами⁴⁰.

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 .

³⁹Borzechowski, Doolittle и Weber, «A Universal Construction for Unique Sink Orientations».

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-ориентаций³⁹, для $k > 2$ — авторское обобщение.

■ Обобщенный граф Келлера $G(k, n): V = \mathbb{E}_{k^2}^n$,

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

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами⁴⁰.

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 .

³⁹Borzechowski, Doolittle и Weber, «A Universal Construction for Unique Sink Orientations».

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-ориентаций³⁹, для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n): V = \mathbb{E}_{k^2}^n$,

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

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами⁴⁰.

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 .

³⁹Borzechowski, Doolittle и Weber, «A Universal Construction for Unique Sink Orientations».

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-ориентаций³⁹, для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n): V = \mathbb{E}_{k^2}^n$,

$$\{v, w\} \in E \leftrightarrow \exists i, 1 \leq i \leq n: v_i \equiv w_i \pmod k, v_i \neq w_i.$$
- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами⁴⁰.

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 .

³⁹Borzechowski, Doolittle и Weber, «A Universal Construction for Unique Sink Orientations».

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-ориентаций³⁹, для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n): V = \mathbb{E}_{k^2}^n$,

$$\{v, w\} \in E \leftrightarrow \exists i, 1 \leq i \leq n: v_i \equiv w_i \pmod k, v_i \neq w_i.$$
- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами⁴⁰.

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 .

³⁹Borzechowski, Doolittle и Weber, «A Universal Construction for Unique Sink Orientations».

Содержание

- 1 Введение: зачем исследуем?
- 2 Глава 1: основные определения и примеры
- 3 Глава 2: эквивалентные условия правильности семейств
- 4 Глава 3: свойства правильных семейств**
- 5 Глава 4: алгоритмические и вычислительные аспекты

Общий вид биекций, сохраняющих правильность

Сдвиги, согласованные перенумерации, перекодировки — все эти преобразования:

- биективны,
- сохраняют правильность семейства,
- являются изометриями \mathbb{E}_k^n (в метрике Хэмминга).

Общая постановка задачи: пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in \text{Perm}(Q^n)$.

Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

$$\{(\Phi, \Psi) \in \text{Perm}(Q^n) \mid \Phi(F(\Psi(x))) \text{ правильно для любого правильного } F: Q^n \rightarrow Q^n\}.$$

Описать структуру этого множества.

Общий вид биекций, сохраняющих правильность

Сдвиги, согласованные перенумерации, перекодировки — все эти преобразования:

- биективны,
- сохраняют правильность семейства,
- являются изометриями \mathbb{E}_k^n (в метрике Хэмминга).

Общая постановка задачи: пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in Perm(Q^n)$.

Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

$$\{(\Phi, \Psi) \in Perm(Q^n) \mid \Phi(F(\Psi(x))) \text{ правильно для любого правильного } F: Q^n \rightarrow Q^n\}.$$

Описать структуру этого множества.

Общий вид биекций, сохраняющих правильность

Сдвиги, согласованные перенумерации, перекодировки — все эти преобразования:

- биективны,
- сохраняют правильность семейства,
- являются изометриями \mathbb{E}_k^n (в метрике Хэмминга).

Общая постановка задачи: пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in \text{Perm}(Q^n)$.

Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

$$\{(\Phi, \Psi) \in \text{Perm}(Q^n) \mid \Phi(F(\Psi(x))) \text{ правильно для любого правильного } F: Q^n \rightarrow Q^n\}.$$

Описать структуру этого множества.

Общий вид биекций, сохраняющих правильность

Сдвиги, согласованные перенумерации, перекодировки — все эти преобразования:

- биективны,
- сохраняют правильность семейства,
- являются изометриями \mathbb{E}_k^n (в метрике Хэмминга).

Общая постановка задачи: пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in Perm(Q^n)$.

Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

$$\{(\Phi, \Psi) \in Perm(Q^n) \mid \Phi(F(\Psi(x))) \text{ правильно для любого правильного } F: Q^n \rightarrow Q^n\}.$$

Описать структуру этого множества.

Общий вид биекций, сохраняющих правильность

Сдвиги, согласованные перенумерации, перекодировки — все эти преобразования:

- биективны,
- сохраняют правильность семейства,
- являются изометриями \mathbb{E}_k^n (в метрике Хэмминга).

Общая постановка задачи: пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in Perm(Q^n)$.

Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

$$\{(\Phi, \Psi) \in Perm(Q^n) \mid \Phi(F(\Psi(x))) \text{ правильно для любого правильного } F: Q^n \rightarrow Q^n\}.$$

Описать структуру этого множества.

Общий вид биекций, сохраняющих правильность

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 использованы следующие обозначения:

$\sigma \in \mathcal{S}_n$: перенумерация координат вектора,

$A, B \in (\mathcal{S}_{\mathbb{E}_k})^n$: перекодировки вектора.

Связь мощности образа и числа порождаемых квазигрупп

Пусть $\mathcal{F} = (f_1, \dots, f_n)$ — правильное, тогда отображение вида

$$(x, y) \rightarrow z = x \oplus y \oplus f(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n))$$

задает квазигрупповую операцию **при любом выборе** π_1, \dots, π_n .

- Сколько может получиться **различных** квазигрупп при разных π_1, \dots, π_n ?
- Плохой пример: если все $f_i \equiv \text{const}_i$, то смена π_i ничего не даст.

Утверждение 2

Пусть $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ — правильное семейство, M — мощность образа отображения $x \rightarrow \mathcal{F}(x)$. Тогда число различных квазигрупп, порождаемых указанной конструкцией, не менее чем M^{k^2} .

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

Связь мощности образа и числа порождаемых квазигрупп

Пусть $\mathcal{F} = (f_1, \dots, f_n)$ — правильное, тогда отображение вида

$$(x, y) \rightarrow z = x \oplus y \oplus f(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n))$$

задает квазигрупповую операцию **при любом выборе** π_1, \dots, π_n .

- Сколько может получиться **различных** квазигрупп при разных π_1, \dots, π_n ?
- Плохой пример: если все $f_i \equiv \text{const}_i$, то смена π_i ничего не даст.

Утверждение 2

Пусть $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ — правильное семейство, M — мощность образа отображения $x \rightarrow \mathcal{F}(x)$. Тогда число различных квазигрупп, порождаемых указанной конструкцией, не менее чем M^{k^2} .

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

Связь мощности образа и числа порождаемых квазигрупп

Пусть $\mathcal{F} = (f_1, \dots, f_n)$ — правильное, тогда отображение вида

$$(x, y) \rightarrow z = x \oplus y \oplus f(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n))$$

задает квазигрупповую операцию **при любом выборе** π_1, \dots, π_n .

- Сколько может получиться **различных** квазигрупп при разных π_1, \dots, π_n ?
- Плохой пример: если все $f_i \equiv \text{const}_i$, то смена π_i ничего не даст.

Утверждение 2

Пусть $\mathcal{F}: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ — правильное семейство, M — мощность образа отображения $x \rightarrow \mathcal{F}(x)$. Тогда число различных квазигрупп, порождаемых указанной конструкцией, не менее чем M^{k^2} .

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

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

Семейство

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

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

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

Семейство

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

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

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

Правильность семейства, Замечание 17

Семейство \mathcal{F}_n является правильным при нечетных n .

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

Мощность образа семейства, Теорема 22

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

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

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

Правильность семейства, Замечание 17

Семейство \mathcal{F}_n является правильным при нечетных n .

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

Мощность образа семейства, Теорема 22

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

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

Подстановки, порождаемые правильными семействами

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

$$\sigma_{\mathcal{F}}(x): x \rightarrow x \circ \mathcal{F}(x), \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \rightarrow \begin{bmatrix} x_1 \circ f_1(x_1, \dots, x_n) \\ \vdots \\ x_n \circ f_n(x_1, \dots, x_n) \end{bmatrix}$$

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

Пусть $\mathcal{F}: Q^n \rightarrow Q^n$ — правильное. Рассмотрим $\sigma_{\mathcal{F}}^{-1} \in \text{Perm}(Q^n)$.

Обратимость «правильных подстановок», Теорема 23

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

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

также является правильным.

Т.е., если \mathcal{F} — правильное, то существует правильное семейство \mathcal{G} со свойством

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

Таким образом, множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).

Пусть $\mathcal{F}: Q^n \rightarrow Q^n$ — правильное. Рассмотрим $\sigma_{\mathcal{F}}^{-1} \in \text{Perm}(Q^n)$.

Обратимость «правильных подстановок», Теорема 23

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

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

также является правильным.

Т.е., если \mathcal{F} — правильное, то существует правильное семейство \mathcal{G} со свойством

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

Таким образом, множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).

Пусть $\mathcal{F}: Q^n \rightarrow Q^n$ — правильное. Рассмотрим $\sigma_{\mathcal{F}}^{-1} \in \text{Perm}(Q^n)$.

Обратимость «правильных подстановок», Теорема 23

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

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

также является правильным.

Т.е., если \mathcal{F} — правильное, то существует правильное семейство \mathcal{G} со свойством

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

Таким образом, множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).

О подстановках, порождаемых правильными семействами-2

Множество «правильных подстановок» $\mathcal{S}^{\text{prop}}$ не является подгруппой $\text{Perm}(Q^n)$.

Транзитивность действия, Теорема 25

Замыкание $\mathcal{S}^{\text{prop}}$ действует транзитивно на Q^n (любой элемент из Q^n можно перевести в любой другой с помощью композиции некоторого количества σ_F).

Булев случай

При $Q = \mathbb{E}_2$ замыкание σ_F порождает все множество подстановок $\text{Perm}(\mathbb{E}_2^n)$.

Schurr, «Unique sink orientations of cubes».

О подстановках, порождаемых правильными семействами-2

Множество «правильных подстановок» $\mathcal{S}^{\text{prop}}$ не является подгруппой $\text{Perm}(Q^n)$.

Транзитивность действия, Теорема 25

Замыкание $\mathcal{S}^{\text{prop}}$ действует транзитивно на Q^n (любой элемент из Q^n можно перевести в любой другой с помощью композиции некоторого количества σ_F).

Булев случай

При $Q = \mathbb{E}_2$ замыкание σ_F порождает все множество подстановок $\text{Perm}(\mathbb{E}_2^n)$.

Schurr, «Unique sink orientations of cubes».

О подстановках, порождаемых правильными семействами-2

Множество «правильных подстановок» $\mathcal{S}^{\text{prop}}$ не является подгруппой $\text{Perm}(Q^n)$.

Транзитивность действия, Теорема 25

Замыкание $\mathcal{S}^{\text{prop}}$ действует транзитивно на Q^n (любой элемент из Q^n можно перевести в любой другой с помощью композиции некоторого количества σ_F).

Булев случай

При $Q = \mathbb{E}_2$ замыкание $\sigma_{\mathcal{F}}$ порождает все множество подстановок $\text{Perm}(\mathbb{E}_2^n)$.

Schurr, «Unique sink orientations of cubes».

О подстановках, порождаемых правильными семействами-3

Пусть \mathcal{F} — правильное семейство булевых функций.

Четность числа элементов в прообразе, Теорема 20

Для любого $\alpha \in \{0, 1\}^n$ число решений уравнения $\mathcal{F}(x) = \alpha$ всегда четно.

Количество неподвижных точек $\sigma_{\mathcal{F}}$, Теорема 24

У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.

О подстановках, порождаемых правильными семействами-3

Пусть \mathcal{F} — правильное семейство булевых функций.

Четность числа элементов в прообразе, Теорема 20

Для любого $\alpha \in \{0, 1\}^n$ число решений уравнения $\mathcal{F}(x) = \alpha$ всегда четно.

Количество неподвижных точек $\sigma_{\mathcal{F}}$, Теорема 24

У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.

Содержание

- 1 Введение: зачем исследуем?
- 2 Глава 1: основные определения и примеры
- 3 Глава 2: эквивалентные условия правильности семейств
- 4 Глава 3: свойства правильных семейств
- 5 Глава 4: алгоритмические и вычислительные аспекты

Алгоритм шифрования, сохраняющего формат (FPE-схема)

- FPE-схема⁴¹: алгоритм, позволяющий зашифровывать сообщения из произвольного конечного множества M таким образом, что результат зашифрования также лежит в множестве M .
- Преобразуем $t \in M$, где (M, \circ) — квазигруппа, в $c \in M$ по правилу:

$$t \rightarrow c = L_{k_1, \dots, k_\ell}(t) = k_1 \circ (k_2 \circ (\dots (k_\ell \circ t) \dots)).$$

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

⁴¹Bellare и др., «Format-preserving encryption».

Алгоритм шифрования, сохраняющего формат (FPE-схема)

- FPE-схема⁴¹: алгоритм, позволяющий зашифровывать сообщения из произвольного конечного множества M таким образом, что результат зашифрования также лежит в множестве M .
- Преобразуем $t \in M$, где (M, \circ) — квазигруппа, в $c \in M$ по правилу:

$$t \rightarrow c = L_{k_1, \dots, k_\ell}(t) = k_1 \circ (k_2 \circ (\dots (k_\ell \circ t) \dots)).$$

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

⁴¹Bellare и др., «Format-preserving encryption».

Алгоритм шифрования, сохраняющего формат (FPE-схема)

- FPE-схема⁴¹: алгоритм, позволяющий зашифровывать сообщения из произвольного конечного множества M таким образом, что результат зашифрования также лежит в множестве M .
- Преобразуем $t \in M$, где (M, \circ) — квазигруппа, в $c \in M$ по правилу:

$$t \rightarrow c = L_{k_1, \dots, k_\ell}(t) = k_1 \circ (k_2 \circ (\dots (k_\ell \circ t) \dots)).$$

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

⁴¹Bellare и др., «Format-preserving encryption».

Алгоритм шифрования, сохраняющего формат (FPE-схема)

- FPE-схема⁴¹: алгоритм, позволяющий зашифровывать сообщения из произвольного конечного множества M таким образом, что результат зашифрования также лежит в множестве M .
- Преобразуем $t \in M$, где (M, \circ) — квазигруппа, в $c \in M$ по правилу:

$$t \rightarrow c = L_{k_1, \dots, k_\ell}(t) = k_1 \circ (k_2 \circ (\dots (k_\ell \circ t) \dots)).$$

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

⁴¹Bellare и др., «Format-preserving encryption».

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

■ Рассмотрим квазигруппу

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

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

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

также является правильным на H^n .

■ Таким образом, операция $x \circ y$ **обращается справа** следующим образом:

$$x = \pi_{\tilde{\mathcal{F}}}((x \circ y) - \pi_{\mathcal{G}}(y)).$$

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

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

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

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

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

также является правильным на H^n .

- Таким образом, операция $x \circ y$ **обращается справа** следующим образом:

$$x = \pi_{\tilde{\mathcal{F}}}((x \circ y) - \pi_{\mathcal{G}}(y)).$$

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

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

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

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

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

также является правильным на H^n .

- Таким образом, операция $x \circ y$ **обращается справа** следующим образом:

$$x = \pi_{\tilde{\mathcal{F}}}((x \circ y) - \pi_{\mathcal{G}}(y)).$$

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

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

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

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

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

также является правильным на H^n .

- Таким образом, операция $x \circ y$ **обращается справа** следующим образом:

$$x = \pi_{\tilde{\mathcal{F}}}((x \circ y) - \pi_{\mathcal{G}}(y)).$$

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

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

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

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

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

также является правильным на H^n .

- Таким образом, операция $x \circ y$ **обращается справа** следующим образом:

$$x = \pi_{\tilde{\mathcal{F}}}((x \circ y) - \pi_{\mathcal{G}}(y)).$$

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

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

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

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

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

также является правильным на H^n .

- Таким образом, операция $x \circ y$ **обращается справа** следующим образом:

$$x = \pi_{\tilde{\mathcal{F}}}((x \circ y) - \pi_{\mathcal{G}}(y)).$$

- 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-полна⁴².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости⁴³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма⁴⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma_{\mathcal{F}}$, задаваемая семейством \mathcal{F} , является одностокковой.
- Алгоритм опирается на характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

⁴²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

⁴³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

⁴⁴Bosshard и Gärtner, «Pseudo unique sink orientations».

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна⁴².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости⁴³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма⁴⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma_{\mathcal{F}}$, задаваемая семейством \mathcal{F} , является одностокковой.
- Алгоритм опирается на характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

⁴²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

⁴³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

⁴⁴Bosshard и Gärtner, «Pseudo unique sink orientations».

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна⁴².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости⁴³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма⁴⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma_{\mathcal{F}}$, задаваемая семейством \mathcal{F} , является одностокковой.
- Алгоритм опирается на характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

⁴²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

⁴³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

⁴⁴Bosshard и Gärtner, «Pseudo unique sink orientations».

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна⁴².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости⁴³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма⁴⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma_{\mathcal{F}}$, задаваемая семейством \mathcal{F} , является одностокковой.
- Алгоритм опирается на характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

⁴²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

⁴³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

⁴⁴Bosshard и Gärtner, «Pseudo unique sink orientations».

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна⁴².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости⁴³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма⁴⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma_{\mathcal{F}}$, задаваемая семейством \mathcal{F} , является одностокковой.
- Алгоритм опирается на характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

⁴²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

⁴³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

⁴⁴Bosshard и Gärtner, «Pseudo unique sink orientations».

Численные эксперименты

Размер n	$\Delta(n)$	$\Delta^{\text{rec}}(n)$	$\Delta^{\text{loc}}(n)$	$T(n)$
$n = 1$	2	2	2	2
$n = 2$	12	12	12	12
$n = 3$	488	680	680	744
$n = 4$	481776	3209712	3349488	5541744
$n = 5$	157549032992	94504354122272	—	638560878292512

$\Delta(n)$: число булевых треугольных семейств размера n ; $\Delta^{\text{loc}}(n)$: число булевых локально-треугольных семейств размера n ; $\Delta^{\text{rec}}(n)$: число булевых рекурсивно-треугольных семейств размера n ; $T(n)$: число булевых правильных семейств размера n .

Число классов эквивалентности

Размер n	Число классов 1	Число классов 2
$n = 1$	1	1
$n = 2$	2	2
$n = 3$	19	10
$n = 4$	14614	1291

Классы 1 (2): классы отношения эквивалентности, заданного согласованными подстановками совместно с (внутренними и) внешними сдвигами.

Индексы ассоциативности, $n = 2$

$a(Q)$	Кол-во Q
16	32
32	96
64	16

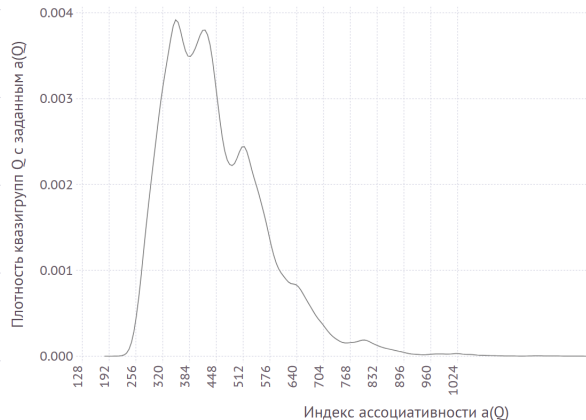
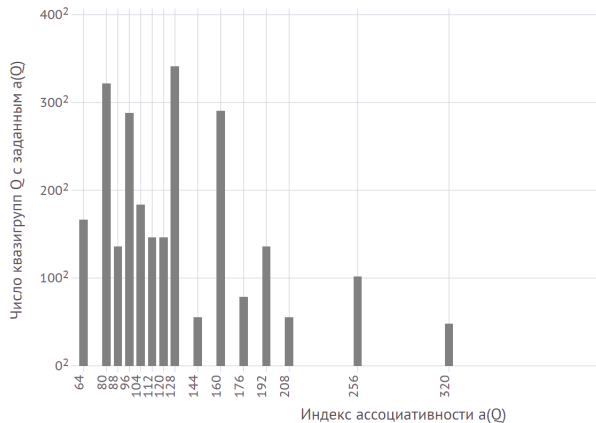
Квазигруппа $Q = (\mathbb{E}_2^n, \circ)$ задается по паре правильных булевых семейств \mathcal{F}, \mathcal{G} с помощью операции

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

Индексы ассоциативности, $n = 3$

$a(Q)$	Кол-во Q	$a(Q)$	Кол-во Q
64	27648	144	3072
80	103424	160	84480
88	18432	176	6144
96	82944	192	18432
104	33792	208	3072
112	21504	256	10368
120	21504	320	2304
128	116352	512	64

Индексы ассоциативности, $n = 4$



Основные результаты диссертации

- Установлено естественное соответствие между булевыми правильными семействами и одностоковыми ориентациями графов булевых кубов (USO-ориентации), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFР-сети); установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера.
- Доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга (согласованные перенумерации и перекодировки); показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек; получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций.

Основные результаты диссертации

- Установлено естественное соответствие между булевыми правильными семействами и одностокowymi ориентациями графов булевых кубов (USO-ориентации), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFР-сети); установлено естественное соответствие между правильными семействами в логике произвольной значности и кликами в обобщенных графах Келлера.
- Доказано, что стабилизатором множества правильных семейств функций являются изометрии пространства Хэмминга (согласованные перенумерации и перекодировки); показано, что отображения, задаваемые с помощью правильных семейств булевых функций, всегда имеют четное число неподвижных точек; получена оценка на число правильных семейств булевых функций, предложены оценки доли треугольных семейств среди всех правильных семейств булевых функций.

Основные результаты диссертации-2

- Построены новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство); получены оценки на число рекурсивно треугольных семейств; для некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами.
- Предложен новый способ порождения квазигрупп на основе правильных семейств функций; доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах; предложен новый алгоритм шифрования, сохраняющего формат (FPE-схема), основанный на квазигрупповых операциях.

Основные результаты диссертации-2

- Построены новые классы правильных семейств функций (рекурсивно треугольные, локально треугольные, сильно квадратичное семейство); получены оценки на число рекурсивно треугольных семейств; для некоторых правильных семейств булевых функций получены точные значения мощности образа отображений, задаваемых этими правильными семействами.
- Предложен новый способ порождения квазигрупп на основе правильных семейств функций; доказан ряд утверждений о числе ассоциативных троек в порождаемых квазигруппах; предложен новый алгоритм шифрования, сохраняющего формат (FPE-схема), основанный на квазигрупповых операциях.

Публикации автора (личные)

- «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.

Спасибо за внимание!



info@rutoken.ru








www.rutoken.ru
www.aktiv-company.ru









+7 495 925-77-90









Список литературы I

-  Bakeva, V. и V. Dimitrova. «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis». Англ. В: *ICT Innovations 2010: Second International Conference, ICT Innovations 2010, Ohrid Macedonia, September 12-15, 2010. Revised Selected Papers 2*. Springer. 2011, с. 61—70.
-  Bellare, М. и др. «Format-preserving encryption». Англ. В: *Selected Areas in Cryptography: 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada*. Springer. 2009, с. 295—312.
-  Bernstein, Daniel J., Johannes Buchmann и Erik Dahmen. *Post-quantum cryptography*. Springer Berlin, Heidelberg, 2009. DOI: <https://doi.org/10.1007/978-3-540-88702-7>.
-  Borzechowski, М., J Doolittle и S. Weber. «A Universal Construction for Unique Sink Orientations». Англ. В: *arXiv preprint arXiv:2211.06072* (2022).
-  Bosshard, V. и B. Gärtner. «Pseudo unique sink orientations». Англ. В: *arXiv preprint arXiv:1704.08481* (2017).






Список литературы II

-  Chauhan, D., I. Gupta и R. Verma. «Quasigroups and their applications in cryptography». Англ. В: *Cryptologia* 45.3 (2021), с. 227—265.
-  Chen, Y., S. J. Knapskog и D. Gligoroski. «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity». Англ. В: *Submitted to ISIT 2010* (2010), с. 14.
-  Couselo, E. и др. «Loop codes». Англ. В: *Discrete Mathematics and Applications* 14.2 (2004), с. 163—172.
-  Denes, J. и A. Keedwell. *Latin squares and their applications (2nd edition)*. Англ. Elsevier, 2015.
-  Dimitrova, V. и J. Markovski. «On quasigroup pseudo random sequence generator». Англ. В: *Proceedings of the 1st Balkan Conference in Informatics, Thessaloniki*. 2004.
-  Faugère, J.-C. и др. «A polynomial-time key-recovery attack on MQQ cryptosystems». Англ. В: *IACR International Workshop on Public Key Cryptography*. Springer. 2015, с. 150—174.

Список литературы III

-  Galatenko, A. V., V. A. Nosov и A. E. Pankratiev. «Latin squares over quasigroups». Англ. В: *Lobachevskii Journal of Mathematics* 41.2 (2020), с. 194—203.
-  Gligoroski, D. «On a family of minimal candidate one-way functions and one-way permutations». Англ. В: *Int. J. Netw. Secur.* 8.3 (2009), с. 211—220.
-  — . *On the S-box in GAGE and InGAGE*. Англ.
<http://gageingage.org/upload/LWC2019NISTWorkshop.pdf>. 2019.
-  Gligoroski, D. и S. J. Knapskog. «Edon-R (256,384,512)—an efficient implementation of Edon-R family of cryptographic hash functions». Англ. В: *Commentationes Mathematicae Universitatis Carolinae* 49.2 (2008), с. 219—239.
-  Gligoroski, D., S. Markovski и S. J. Knapskog. «A public key block cipher based on multivariate quadratic quasigroups». Англ. В: *arXiv preprint arXiv:0808.0247* (2008).
-  — . «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups». Англ. В: *Proceedings of the American Conference on Applied Mathematics*. 2008, с. 44—49.

Список литературы IV

-  Gligoroski, D., S. Markovski и S. J. Knapskog. «The stream cipher Edon80». Англ. В: *New stream cipher designs*. Springer, 2008, с. 152—169.
-  Gligoroski, D., S. Markovski и L. Kocarev. «Edon-R, An Infinite Family of Cryptographic Hash Functions». Англ. В: *International Journal of Security and Networks* 8.3 (2009), с. 293—300.
-  Gligoroski, D. и др. «Cryptographic hash function Edon-R'». Англ. В: *2009 Proceedings of the 1st International Workshop on Security and Communication Networks*. IEEE. 2009, с. 1—9.
-  Gligoroski, D. и др. «GAGE and InGAGE». Англ. В: *A Submission to the NIST Lightweight Cryptography Standardization Process* (2019).
-  Gligoroski, D. и др. «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme». Англ. В: *International Conference on Trusted Systems*. Springer. 2011, с. 184—203.

Список литературы V



Gribov, Aleksei Viktorovich, Pavel Andreevich Zolotykh и Aleksandr Vasil'evich Mikhalev. «A construction of algebraic cryptosystem over the quasigroup ring». В: *Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]* 1.4 (2010), с. 23—32.



Markov, V. T., A. V. Mikhalev и A. A. Nechaev. «Nonassociative Algebraic Structures in Cryptography and Coding». АНГЛ. В: *Journal of Mathematical Sciences* 245.2 (2020).








Markovski, S. и V. Bakeva. «Quasigroup string processing: Part 4». АНГЛ. В: *Contributions, Section of Natural, Mathematical and Biotechnical Sciences* 27.1-2 (2017).










Markovski, S., D. Gligoroski и V. Bakeva. «Quasigroup String Processing: Part 1». АНГЛ. В: *Proc. of Maked. Academ. of Sci. and Arts for Math. And Tect. Sci. XX* (1999), с. 157—162.







Список литературы VI

-  Markovski, S., D. Gligoroski и L. Kocarev. «Unbiased random sequences from quasigroup string transformations». Англ. В: *International workshop on fast software encryption*. Springer. 2005, с. 163—180.
-  Mathew, K. A., P. Östergård и A. Popa. «Enumerating cube tilings». Англ. В: *Discrete & Computational Geometry* 50.4 (2013), с. 1112—1122.
-  Matousek, J. «The Number Of Unique-Sink Orientations of the Hypercube». Англ. В: *Combinatorica* 26 (февр. 2006), с. 91—99.
-  Mileva, A. и S. Markovski. «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function». Англ. В: *International Conference on ICT Innovations*. Springer. 2009, с. 367—376.
-  Mohamed, S. E. и др. «Algebraic attack on the MQQ public key cryptosystem». Англ. В: *Cryptology and Network Security: 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings* 8. Springer. 2009, с. 392—401.






Список литературы VII

-  Myasnikov, Alexei, Vladimir Shpilrain и Alexander Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*. American Mathematical Soc., 2011.
-  OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences*. Англ. Published electronically at <http://oeis.org>. 2008.
-  Richard, A. «Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks». Англ. В: *Theoretical Computer Science* 583 (2015), с. 1—26.
-  Ruet, P. «Asynchronous Boolean networks and hereditarily bijective maps». Англ. В: *Natural Computing* 14 (2015), с. 545—553.
-  — . «Local cycles and dynamical properties of Boolean networks». Англ. В: *Mathematical Structures in Computer Science* 26.4 (2016), с. 702—718.
-  Schurr, I. «Unique sink orientations of cubes». Англ. Дис. . . . док. ETH Zurich, 2004.
-  Shcherbacov, V. *Elements of Quasigroup Theory and Applications*. Англ. Chapman и Hall/CRC, 2017.

Список литературы VIII

-  Shih, М.-Н. и J.-L. Dong. «A combinatorial analogue of the Jacobian problem in automata networks». Англ. В: *Advances in Applied Mathematics* 34.1 (2005), с. 30—46.
-  Sikirić, М. D., Y. Itoh и A. Poyarkov. «Cube packings, second moment and holes». Англ. В: *European Journal of Combinatorics* 28.3 (2007), с. 715—725.
-  Snášel, V. и др. «Hash functions based on large quasigroups». Англ. В: *Computational Science—ICCS 2009: 9th International Conference Baton Rouge, LA, USA, May 25-27, 2009 Proceedings, Part I* 9. Springer. 2009, с. 521—529.
-  Szabó, T. и E. Welzl. «Unique sink orientations of cubes». Англ. В: *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*. IEEE. 2001, с. 547—555.
-  Thomas, R. «Regulatory networks seen as asynchronous automata: a logical description». Англ. В: *Journal of theoretical biology* 153.1 (1991), с. 1—23.
-  Tiwari, S. K. и др. «INRU: A Quasigroup Based Lightweight Block Cipher». Англ. В: *arXiv preprint arXiv:2112.07411* (2021).

Список литературы IX

-  Wolf, Christopher и Bart Preneel. *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations*. Cryptology ePrint Archive, Paper 2005/077. <https://eprint.iacr.org/2005/077>. 2005. URL: <https://eprint.iacr.org/2005/077>.
-  Артамонов, В. А. «Квазигруппы и их приложения». В: *Чебышевский сборник* 19.2 (66) (2018), с. 111—122.
-  Барышников, Андрей Владимирович и Сергей Юрьевич Катышев. «Использование неассоциативных структур для построения алгоритмов открытого распределения ключей». В: *Математические вопросы криптографии* 9.4 (2018), с. 5—30.
-  Белоусов, В. Д. *Основы теории квазигрупп и луп*. М.: Наука, 1967.
-  Галатенко, А. В. и др. «Порождение правильных семейств функций». В: *Интеллектуальные системы. Теория и приложения* 25.4 (2021), с. 100—103.

Список литературы X



Галатенко, А. В., В. А. Носов и А. Е. Панкратьев. «Об одном критерии правильности семейства функций». В: *Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории*. Материалы XIX Международной конференции, посвященной двухсотлетию со дня рождения академика П. Л. Чебышёва. Тульский государственный педагогический университет им. Л.Н. Толстого. 2021.








— . «Порождение квадратичных квазигрупп с помощью правильных семейств булевых функций». В: *Фундаментальная и прикладная математика 23.2* (2020), с. 57—73.



Галатенко, А.В. и др. «О порождении n -квазигрупп с помощью правильных семейств функций». В: *Дискретная математика 35.1* (2023), с. 35—53. (EDN: WWYSEG; RSCI, WOS, Scopus, ИФ РИНЦ: 0.220; общий объем 1.18 п.л., Царегородцеву К. Д. принадлежат формулировка и доказательство теоремы 1 и результаты раздела 6, 29 %, 0.34 п. л.)

Список литературы XI

-  Глухов, М. М. «О применениях квазигрупп в криптографии». В: *Прикладная дискретная математика* 2 (2) (2008), с. 28—32.
-  Гонсалес, С. и др. «Групповые коды и их неассоциативные обобщения». В: *Дискретная математика* 16.1 (2004), с. 146—156.
-  — . «Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы». В: *Дискретная математика* 10.2 (1998), с. 3—29.
-  Грибов, А. В. «Алгебраические неассоциативные структуры и их приложения в криптографии». Дис. ... док. Московский государственный университет им. М. В. Ломоносова, 2015.
-  Грибов, Алексей Викторович. «Гомоморфность некоторых криптографических систем на основе неассоциативных структур». В: *Фундаментальная и прикладная математика* 20.1 (2015), с. 135—143.

Список литературы XII



Катышев, Сергей Юрьевич, Виктор Тимофеевич Марков и Александр Александрович Нечаев. «Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей». В: *Дискретная математика* 26.3 (2014), с. 45—64.



Марков, В. Т. и др. «Квазигруппы и кольца в кодировании и построении криптосхем». В: *Прикладная дискретная математика* 4 (2012).



Марков, В. Т., А. В. Михалёв и Е. С. Кислицын. «Неассоциативные структуры в гомоморфной криптографии». В: *Фундаментальная и прикладная математика* 23.2 (2020), с. 209—215.



Марков, В. Т., А. В. Михалёв и А. А. Нечаев. «Неассоциативные алгебраические структуры в криптографии и кодировании». В: *Фундаментальная и прикладная математика* 21.4 (2016), с. 99—124.

Список литературы XIII



Молдовян, Дмитрий Николаевич, Александр Андреевич Молдовян и Николай Андреевич Молдовян. «Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах». В: *Вопросы кибербезопасности* 1 (47) (2022), с. 18—25.



Нечаев, Александр Александрович. «Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам». В: *Фундаментальная и прикладная математика* 1.1 (1995), с. 229—254.








Носов, В. А. «Критерий регулярности булевского неавтономного автомата с разделенным входом». В: *Интеллектуальные системы. Теория и приложения* 3.3-4 (1998), с. 269—280.



— . «Построение классов латинских квадратов в булевой базе данных». В: *Интеллектуальные системы. Теория и приложения* 4.3-4 (1999), с. 307—320. ISSN: 2075-9460; 2411-4448.

Список литературы XIV

-  Носов, В. А. «Построение параметрического семейства латинских квадратов в векторной базе данных». В: *Интеллектуальные системы. Теория и приложения* 8.1-4 (2006), с. 517—529. ISSN: 2075-9460; 2411-4448.
-  Носов, В. А. и А. Е. Панкратьев. «Латинские квадраты над абелевыми группами». В: *Фундаментальная и прикладная математика* 12.3 (2006), с. 65—71.
-  — . «О функциональном задании латинских квадратов». В: *Интеллектуальные системы. Теория и приложения* 12.1-4 (2008), с. 317—332. ISSN: 2075-9460; 2411-4448.
-  Плаксина, И. А. «Построение параметрического семейства многомерных латинских квадратов». В: *Интеллектуальные системы. Теория и приложения* 18.2 (2014), с. 323—330.
-  Романьков, Виталий Анатольевич. *Алгебраическая криптология: монография*. ОмГУ им. Ф. М. Достоевского, 2020.

Список литературы XV



Рыков, Д. О. «О правильных семействах функций, используемых для задания латинских квадратов». В: *Интеллектуальные системы. Теория и приложения* 18.1 (2014), с. 141—152.



Царегородцев, К.Д. «О свойствах правильных семейств булевых функций». В: *Дискретная математика* 33.1 (2021). (EDN: JTVVAY; RSCI, WOS, Scopus, ИФ РИНЦ: 0.220; 100 %, 0.75 п. л.)




Перевод:

Properties of proper families of Boolean functions, *Discrete Mathematics and Applications*, 32.5 (2022), pp. 369–378; EDN: INXYMW; ИФ JCI 2023: 0.15; 100 %, 0.75 п. л., с. 91—102.



Яблонский, С. В. *Введение в дискретную математику*. 2-е изд., перераб. и доп. М.: Наука, 1986.

Список литературы XVI

-  Яшунский, А. Д. «О преобразованиях распределений вероятностей бесповторными квазигрупповыми формулами». В: *Дискретная математика* 25.2 (2013), с. 149—159.
-  — . «О скорости сходимости квазигрупповых сверток вероятностных распределений». В: *Дискретная математика* 34.3 (2022), с. 160—171.
-  — . «Уточнение скорости сходимости распределений квазигрупповых «сумм» конечных случайных величин». В: *Дискретная математика и ее приложения*. Т. 14. 2022, с. 300—302.