Правильные семейства функций и порождаемые ими квазигруппы

Комбинаторные и алгебраические свойства

К. Царегородцев[1, 2]

[1]МГУ им. М. В. Ломоносова

[2]АО «Актив-софт»
Москва, Россия

16 октября 2025 г.

Содержание доклада

1. Введение: квазигруппы в криптографии

2. Правильные семейства функций и квазигруппы

3. Свойства правильных семейств функций

Содержание

Технический момент: используемые обозначения

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

«Обычная» криптография

- Часто используемые алгебраические структуры в криптографии: поля, кольца (коммутативные, ассоциативные, с единицей), коммутативные группы, коды, решетки.
- В исследовательской литературе предлагаются к рассмотрению и более «экзотические» структуры: **некоммутативные** группы и алгебры (например, группы кос, алгебры матриц, алгебра кватернионов и так далее)[1], **неассоциативные структуры**: квазигруппы, квазигрупповые кольца и т.д[2].
- В докладе будет рассматриваться один способ построения квазигрупп на основе т.н. «правильных семейств функций», а также свойства этих семейств самих по себе.

[1] Myasnikov, 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*.

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

«Обычная» криптография

- Часто используемые алгебраические структуры в криптографии: поля, кольца (коммутативные, ассоциативные, с единицей), коммутативные группы, коды, решетки.
- В исследовательской литературе предлагаются к рассмотрению и более «экзотические» структуры: **некоммутативные** группы и алгебры (например, группы кос, алгебры матриц, алгебра кватернионов и так далее)[1], **неассоциативные структуры**: квазигруппы, квазигрупповые кольца и т.д[2].
- В докладе будет рассматриваться один способ построения квазигрупп на основе т.н. «правильных семейств функций», а также свойства этих семейств самих по себе.

[1] Myasnikov, 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*.

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

«Обычная» криптография

- Часто используемые алгебраические структуры в криптографии: поля, кольца (коммутативные, ассоциативные, с единицей), коммутативные группы, коды, решетки.
- В исследовательской литературе предлагаются к рассмотрению и более «экзотические» структуры: **некоммутативные** группы и алгебры (например, группы кос, алгебры матриц, алгебра кватернионов и так далее)[1], **неассоциативные структуры**: квазигруппы, квазигрупповые кольца и т.д[2].
- В докладе будет рассматриваться один способ построения квазигрупп на основе т.н. «правильных семейств функций», а также свойства этих семейств самих по себе.

[1] Myasnikov, 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*.

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

Квазигруппа

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

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

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)

$$L_a\colon Q \to Q,\ L_a(x) = a \circ x,\ \ R_a\colon Q \to Q,\ R_a(y) = y \circ a,$$

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

Квазигруппа

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

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

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)

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

являются биекциями на Q.

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

Квазигруппа

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

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

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)

$$L_a\colon Q \to Q,\ L_a(x) = a \circ x,\ R_a\colon Q \to Q,\ R_a(y) = y \circ a,$$

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 **изотоп**[3]:

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

[3] Denes 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 $\{0, \dots, k-1\}$, каждое элемент появляется **только один раз** в каждом столбце и каждой строке таблицы.
- 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.

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

Квазигруппы: симметричные механизмы

- ГПСЧ[4], блочные шифры[5], поточные шифры[6], хэш-функции[7].
- Низкоресурсные (lightweight) хэш-функция и AEAD-алгоритм[8].
- Основным нелинейным компонентом в упомянутых алгоритмах является квазигрупповое умножение.
- Приложения в теории кодирования[9].

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

[5] Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

[6] Gligoroski, Markovski и Knapskog, «The stream cipher Edon80».

[7] Gligoroski, «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'»; Mileva и Markovski, «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function».

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

[9] Couselo 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».

Квазигруппы: симметричные механизмы

- ГПСЧ[4], блочные шифры[5], поточные шифры[6], хэш-функции[7].
- Низкоресурсные (lightweight) хэш-функция и AEAD-алгоритм[8].
- Основным нелинейным компонентом в упомянутых алгоритмах является квазигрупповое умножение.
- Приложения в теории кодирования[9].

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

[5] Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

[6] Gligoroski, Markovski и Knapskog, «The stream cipher Edon80».

[7] Gligoroski, «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'»; Mileva и Markovski, «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function».

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

[9] Couselo 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».

Квазигруппы: симметричные механизмы

- ГПСЧ[4], блочные шифры[5], поточные шифры[6], хэш-функции[7].
- Низкоресурсные (lightweight) хэш-функция и AEAD-алгоритм[8].
- Основным нелинейным компонентом в упомянутых алгоритмах является квазигрупповое умножение.
- Приложения в теории кодирования[9].

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

[5] Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

[6] Gligoroski, Markovski и Knapskog, «The stream cipher Edon80».

[7] Gligoroski, «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'»; Mileva и Markovski, «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function».

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

[9] Couselo 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».

Квазигруппы: симметричные механизмы

- ГПСЧ[4], блочные шифры[5], поточные шифры[6], хэш-функции[7].
- Низкоресурсные (lightweight) хэш-функция и AEAD-алгоритм[8].
- Основным нелинейным компонентом в упомянутых алгоритмах является квазигрупповое умножение.
- Приложения в теории кодирования[9].

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

[5] Tiwari и др., «INRU: A Quasigroup Based Lightweight Block Cipher».

[6] Gligoroski, Markovski и Knapskog, «The stream cipher Edon80».

[7] Gligoroski, «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'»; Mileva и Markovski, «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function».

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

[9] Couselo 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».

Квазигруппы: асимметричные механизмы

- Асимметричные схемы подписи[10] — аналоги пост-квантовых схем многомерной криптографии (multivariate cryptography).
- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа[11], гомоморфное шифрование[12]: используются **ППС/ПЛС-группоиды**, **луповые кольца** над медиальными квазигруппами (изотопы абелевых групп с коммутирующими автоморфизмами).
- Более подробно вопрос освещен в[13].

[10] Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».

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

[12] Gribov, 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».

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

Квазигруппы: асимметричные механизмы

- Асимметричные схемы подписи[10] — аналоги пост-квантовых схем многомерной криптографии (multivariate cryptography).
- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа[11], гомоморфное шифрование[12]: используются **ППС/ПЛС-группоиды**, **луповые кольца** над медиальными квазигруппами (изотопы абелевых групп с коммутирующими автоморфизмами).
- Более подробно вопрос освещен в[13].

[10] Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».

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

[12] Gribov, 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».

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

Квазигруппы: асимметричные механизмы

- Асимметричные схемы подписи[10] — аналоги пост-квантовых схем многомерной криптографии (multivariate cryptography).
- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа[11], гомоморфное шифрование[12]: используются **ППС/ПЛС-группоиды**, **луповые кольца** над медиальными квазигруппами (изотопы абелевых групп с коммутирующими автоморфизмами).
- Более подробно вопрос освещен в[13].

[10] Chen, Knapskog и Gligoroski, «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity»; Gligoroski, Markovski и Knapskog, «A public key block cipher based on multivariate quadratic quasigroups», «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups»; Gligoroski и др., «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme».

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

[12] Gribov, 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».

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

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 класса с компактно задаваемыми представителями[14].
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)[15].
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой[16], модульное вычитание[17]).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

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

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

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

[17] Snášel 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 класса с компактно задаваемыми представителями[14].
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)[15].
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой[16], модульное вычитание[17]).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

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

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

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

[17] Snášel 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 класса с компактно задаваемыми представителями[14].
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)[15].
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой[16], модульное вычитание[17]).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

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

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

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

[17] Snášel 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 класса с компактно задаваемыми представителями[14].
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)[15].
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой[16], модульное вычитание[17]).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

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

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

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

[17] Snášel 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 класса с компактно задаваемыми представителями[14].
- Итеративное построение из более «маленьких» (конструкции наподобие прямых произведений)[15].
- Изотопы некоторых «хорошо изученных» групп (например, изотоп группы точек эллиптической кривой[16], модульное вычитание[17]).
- Функциональное задание квазигруппы: поговорим о нём подробнее.

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

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

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

[17] Snášel и др., «Hash functions based on large quasigroups».

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному[18]:

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

- Для краткости набор функций $\mathcal{F} = (f_1, \dots, f_n)$, $f_i \colon Q^n \to Q, \quad i = 1, \dots, n$, будем называть семейством функций; семейство задает отображение множества 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 $\{0, 1\}^n$?

[18] Носов и Панкратьев, «О функциональном задании латинских квадратов».

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному[18]:

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

- Для краткости набор функций $\mathcal{F} = (f_1, \ldots, f_n)$, $f_i \colon Q^n \to Q, \quad i = 1, \ldots, n$, будем называть семейством функций; семейство задает отображение множества 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 $\{0, 1\}^n$?

[18] Носов и Панкратьев, «О функциональном задании латинских квадратов».

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному[18]:

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

- Для краткости набор функций $\mathcal{F} = (f_1, \ldots, f_n)$, $f_i \colon Q^n \to Q, \quad i = 1, \ldots, n$, будем называть семейством функций; семейство задает отображение множества 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 $\{0, 1\}^n$?

[18] Носов и Панкратьев, «О функциональном задании латинских квадратов».

Содержание

Правильные семейства булевых функций

Правильное семейство

Семейство булевых функций $f_i \colon \mathbb{E}_2^n \to \mathbb{E}_2^n$ 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[19], над произвольными группами[20]; над прямыми произведениями других квазигрупп[21] и d-квазигрупп[22].

[19] Носов, «Построение параметрического семейства латинских квадратов в векторной базе данных».

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

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

[22] Плаксина, «Построение параметрического семейства многомерных латинских квадратов».

Правильные семейства булевых функций

Правильное семейство

Семейство булевых функций $f_i\colon \mathbb{E}_2^n \to \mathbb{E}_2^n$ 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[19], над произвольными группами[20]; над прямыми произведениями других квазигрупп[21] и d-квазигрупп[22].

[19] Носов, «Построение параметрического семейства латинских квадратов в векторной базе данных».

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

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

[22] Плаксина, «Построение параметрического семейства многомерных латинских квадратов».

Примеры правильных семейств

- Константные семейства $f_i \equiv const_i$ являются правильными.
- Треугольные семейства являются правильными

$$\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} f_1() \\ f_2(x_1) \\ \vdots \\ f_n(x_1, \ldots, x_{n-1}) \end{bmatrix}.$$

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

[22] Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом»; Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

Примеры правильных семейств

- Константные семейства $f_i \equiv const_i$ являются правильными.
- Треугольные семейства являются правильными

$$\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} f_1() \\ f_2(x_1) \\ \vdots \\ f_n(x_1, \ldots, x_{n-1}) \end{bmatrix}.$$

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

[22] Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом»; Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

Примеры правильных семейств

- Константные семейства $f_i \equiv const_i$ являются правильными.
- Треугольные семейства являются правильными

$$\begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} f_1(\,) \\ f_2(x_1) \\ \vdots \\ f_n(x_1, \ldots, x_{n-1}) \end{bmatrix}.$$

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

[22] Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом»; Носов и Панкратьев, «Латинские квадраты над абелевыми группами».

Класс квадратичных семейств

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

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

Число правильных булевых семейств $T(n)$

Размер n	$T(n)$
$n = 1$	2
$n = 2$	12
$n = 3$	744
$n = 4$	5541744
$n = 5$	638560878292512

Оценка на число булевых правильных семейств

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

где A, B — некоторые положительные константы.

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

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна[23].
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости[24].
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).

[23] Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».
[24] Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна[23].
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости[24].
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).

[23] Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».
[24] Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна[23].
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости[24].
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).

[23] Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».
[24] Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

Один способ задания квазигруппы

- Есть несколько способов задать структуру квазигруппы на множестве Q^n с помощью правильных семейств, в докладе рассмотрим одно из них.
- Пусть $\mathcal{F}, \mathcal{G}$ — два правильных семейства функций размера n над группой $(G^n, +)$. Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию $\circ$ следующим образом:

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

- Операция $\circ$ является квазигрупповой.
- Это следует из более общей теоремы об эквивалентности свойства правильности семейства и регулярности некоторого семейства отображений.

Один способ задания квазигруппы

- Есть несколько способов задать структуру квазигруппы на множестве Q^n с помощью правильных семейств, в докладе рассмотрим одно из них.
- Пусть $\mathcal{F}$, $\mathcal{G}$ — два правильных семейства функций размера n над группой $(G^n, +)$. Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию $\circ$ следующим образом:

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

- Операция $\circ$ является квазигрупповой.
- Это следует из более общей теоремы об эквивалентности свойства правильности семейства и регулярности некоторого семейства отображений.

Один способ задания квазигруппы

- Есть несколько способов задать структуру квазигруппы на множестве Q^n с помощью правильных семейств, в докладе рассмотрим одно из них.
- Пусть $\mathcal{F}, \mathcal{G}$ — два правильных семейства функций размера n над группой $(G^n, +)$. Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию $\circ$ следующим образом:

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

- Операция $\circ$ является квазигрупповой.
- Это следует из более общей теоремы об эквивалентности свойства правильности семейства и регулярности некоторого семейства отображений.

Один способ задания квазигруппы

- Есть несколько способов задать структуру квазигруппы на множестве Q^n с помощью правильных семейств, в докладе рассмотрим одно из них.
- Пусть $\mathcal{F}$, $\mathcal{G}$ — два правильных семейства функций размера n над группой $(G^n, +)$. Для $\mathbf{x}, \mathbf{y} \in G^n$ зададим операцию $\circ$ следующим образом:

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

- Операция $\circ$ является квазигрупповой.
- Это следует из более общей теоремы об эквивалентности свойства правильности семейства и регулярности некоторого семейства отображений.

Криптографические свойства квазигрупп

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

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

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

Криптографические свойства квазигрупп

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

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

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

Криптографические свойства квазигрупп

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

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

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

Индекс ассоциативности, теория

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

Об индексах ассоциативности

- Индексы ассоциативности квазигрупп, построенных по паре $(\mathcal{F}, \mathcal{G})$ и по паре $(\mathcal{G}, \mathcal{F})$, совпадают.
- 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.
- Для $G = \mathbb{Z}_2$ количество ассоциативных троек в квазигруппе, построенной по паре правильных булевых семейств $(\mathcal{F}, \mathcal{G})$, четно.

Индекс ассоциативности, эксперимент $n = 2$

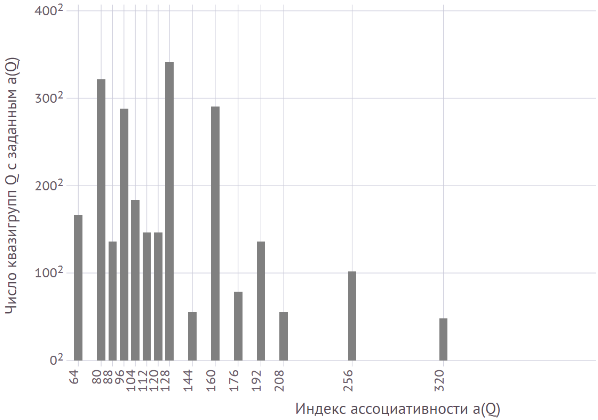
$$(x, y) \to x \circ y = x + \mathcal{F}(x) + y + \mathcal{G}(y).$$

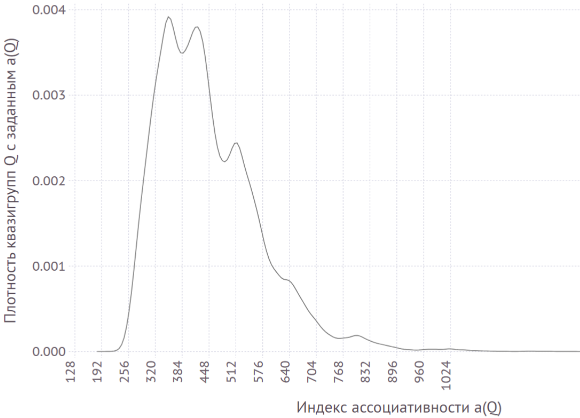
$a(Q)$	Кол-во Q
16	32
32	96
64	16

Индекс ассоциативности, эксперимент $n = 3$

$a(Q)$	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

Индекс ассоциативности, эксперимент $n = 4$





Полиномиальная полнота, теория

- Пусть $\mathcal{F}\colon Q^n \to Q^n$ — правильное, $(Q, \circ)$ — квазигруппа. Введем обозначение $\sigma_{\mathcal{F}} \in Perm(Q^n)$:

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

- Для изучения полиномиальной полноты нужно, в частности, хорошо понимать свойства подстановок $\sigma_{\mathcal{F}}$.

Полиномиальная полнота, теория

- Пусть $\mathcal{F}\colon Q^n \to Q^n$ — правильное, $(Q, \circ)$ — квазигруппа. Введем обозначение $\sigma_{\mathcal{F}} \in Perm(Q^n)$:

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

- Для изучения полиномиальной полноты нужно, в частности, хорошо понимать свойства подстановок $\sigma_{\mathcal{F}}$.

Полиномиальная полнота, теория

$$\sigma_{\mathcal{F}}(x)\colon x \to x \circ \mathcal{F}(x),$$

- Если $(Q, \circ)$ — группа (т.е., операция $\circ$ ассоциативна), то множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).
- Множество «правильных подстановок» $\mathcal{S}^{\mathsf{prop}}$ **не является** подгруппой $Perm(Q^n)$.
- Замыкание $\mathcal{S}^{\mathsf{prop}}$ действует транзитивно на Q^n.
- При $Q = \mathbb{E}_2$ замыкание $\mathcal{S}^{\mathsf{prop}}$ порождает все множество подстановок $Perm(\mathbb{E}_2^n)$.
- У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.

Полиномиальная полнота, теория

$$\sigma_{\mathcal{F}}(x)\colon x \to x \circ \mathcal{F}(x),$$

- Если $(Q, \circ)$ — группа (т.е., операция $\circ$ ассоциативна), то множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).
- Множество «правильных подстановок» $\mathcal{S}^{\mathsf{prop}}$ **не является** подгруппой $Perm(Q^n)$.
- Замыкание $\mathcal{S}^{\mathsf{prop}}$ действует транзитивно на Q^n.
- При $Q = \mathbb{E}_2$ замыкание $\mathcal{S}^{\mathsf{prop}}$ порождает все множество подстановок $Perm(\mathbb{E}_2^n)$.
- У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.

Полиномиальная полнота, теория

$$\sigma_{\mathcal{F}}(x)\colon x \to x \circ \mathcal{F}(x),$$

- Если $(Q, \circ)$ — группа (т.е., операция $\circ$ ассоциативна), то множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).
- Множество «правильных подстановок» $\mathcal{S}^{\mathsf{prop}}$ **не является** подгруппой $Perm(Q^n)$.
- Замыкание $\mathcal{S}^{\mathsf{prop}}$ действует транзитивно на Q^n.
- При $Q = \mathbb{E}_2$ замыкание $\mathcal{S}^{\mathsf{prop}}$ порождает все множество подстановок $Perm(\mathbb{E}_2^n)$.
- У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.

Полиномиальная полнота, теория

$$\sigma_{\mathcal{F}}(x)\colon x \to x \circ \mathcal{F}(x),$$

- Если $(Q, \circ)$ — группа (т.е., операция $\circ$ ассоциативна), то множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).
- Множество «правильных подстановок» $\mathcal{S}^{\mathsf{prop}}$ **не является** подгруппой $Perm(Q^n)$.
- Замыкание $\mathcal{S}^{\mathsf{prop}}$ действует транзитивно на Q^n.
- При $Q = \mathbb{E}_2$ замыкание $\mathcal{S}^{\mathsf{prop}}$ порождает все множество подстановок $Perm(\mathbb{E}_2^n)$.
- У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.

Полиномиальная полнота, теория

$$\sigma_{\mathcal{F}}(x)\colon x \to x \circ \mathcal{F}(x),$$

- Если $(Q, \circ)$ — группа (т.е., операция $\circ$ ассоциативна), то множество «правильных подстановок» замкнуто относительно взятия обратного элемента (в случае, когда Q — группа).
- Множество «правильных подстановок» $\mathcal{S}^{\mathsf{prop}}$ **не является** подгруппой $Perm(Q^n)$.
- Замыкание $\mathcal{S}^{\mathsf{prop}}$ действует транзитивно на Q^n.
- При $Q = \mathbb{E}_2$ замыкание $\mathcal{S}^{\mathsf{prop}}$ порождает все множество подстановок $Perm(\mathbb{E}_2^n)$.
- У подстановки $\sigma_{\mathcal{F}}(x) = x \oplus \mathcal{F}(x)$ чётное число неподвижных точек.

Полиномиальная полнота, эксперимент $n = 2$

$$\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n \quad \mathbf{x} \circ \mathbf{y} = \mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \oplus \mathbf{y} \oplus \mathcal{G}(\mathbf{y}).$$

Свойства	Афинная	Неаффинная
Не простая	112	0
Простая	32	**0**

Полиномиальная полнота, эксперимент $n = 3$

$$\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n \quad \mathbf{x} \circ \mathbf{y} = \mathbf{x} \oplus \mathcal{F}(\mathbf{x}) \oplus \mathbf{y} \oplus \mathcal{G}(\mathbf{y}).$$

Свойства	Афинная	Неаффинная
Не простая	30784	231936
Простая	9216	**281600**

Содержание

Преобразование сдвига

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

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

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

Обобщение результата[25] для абелевых групп.

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

Преобразование перекодировки

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

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

Пусть $\Phi \in Func(Q)^n$, $\Psi \in Perm(Q)^n$. 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 $\Phi, \Psi \in Perm(Q)^n$, то подобные преобразования будем называть преобразованиями перекодировки.

Сдвиги являются частными случаями преобразования перекодировки.

Преобразование перекодировки

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

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

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

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

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

Сдвиги являются частными случаями преобразования перекодировки.

Преобразование перекодировки

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

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

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

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

Если $\Phi, \Psi \in Perm(Q)^n$, то подобные преобразования будем называть преобразованиями перекодировки.
Сдвиги являются частными случаями преобразования перекодировки.

Согласованная перенумерация

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

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

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

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

Проекция

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

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

Полученное семейство является правильным.

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

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:

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

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:

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

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:

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

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:

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

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:

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

Описать структуру этого множества.

Общий вид биекций, сохраняющих правильность

Стабилизатор правильных семейств

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.

Неподвижные точки правильного семейства

Неподвижные точки

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

Это свойство задает соответствие между правильными булевыми семействами и двумя другими объектами: USO-ориентациями булевых кубов (используются в задачах оптимизации[26]) и HUFP-сетями (используются в задачах математической биологии[27]).

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

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

Неподвижные точки правильного семейства

Неподвижные точки

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

Это свойство задает соответствие между правильными булевыми семействами и двумя другими объектами: USO-ориентациями булевых кубов (используются в задачах оптимизации[26]) и HUFP-сетями (используются в задачах математической биологии[27]).

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

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

Неподвижные точки правильного семейства

- Полученные соответствия позволяют перевести (с обобщением) часть результатов, полученных в контексте оптимизации или мат. биологии на язык правильных семейств: например, вероятностный алгоритм порождения правильных семейств с помощью процедуры MCMC[28], оценка на число булевых правильных семейств[29], новые классы правильных семейств.
- В общем случае более общий критерий: семейство $\mathcal{F}\colon \mathbb{E}_k^n \to \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки $\mathcal{F}$ все её проекции имеют единственную неподвижную точку[30].

[28] Галатенко и др., «Порождение правильных семейств функций».

[29] Царегородцев, «О свойствах правильных семейств булевых функций».

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

Неподвижные точки правильного семейства

- Полученные соответствия позволяют перевести (с обобщением) часть результатов, полученных в контексте оптимизации или мат. биологии на язык правильных семейств: например, вероятностный алгоритм порождения правильных семейств с помощью процедуры MCMC[28], оценка на число булевых правильных семейств[29], новые классы правильных семейств.
- В общем случае более общий критерий: семейство $\mathcal{F}\colon \mathbb{E}_k^n \to \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки $\mathcal{F}$ все её проекции имеют единственную неподвижную точку[30].

[28] Галатенко и др., «Порождение правильных семейств функций».

[29] Царегородцев, «О свойствах правильных семейств булевых функций».

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

Характеризация через несамодвойственные проекции

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

О несамодвойственности проекций

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

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

не является самодвойственным булевым отображением.

Этот результат позволяет снизить сложность проверки правильности с $\Theta(4^n)$ операций вычисления семейства в точке до $\Theta(3^n)$ операций.

Характеризация через несамодвойственные проекции

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

О несамодвойственности проекций

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

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

не является самодвойственным булевым отображением.

Этот результат позволяет снизить сложность проверки правильности с $\Theta(4^n)$ операций вычисления семейства в точке до $\Theta(3^n)$ операций.

Кликовое представление правильных семейств

- Правильные семейства находятся во взаимно-однозначном соответствии с кликами некоторым образом построенного графа («обобщенный граф Келлера»).
- Для $k = 2$ перенос из теории USO-ориентаций[31], для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n)$: $V = \mathbb{E}_{k^2}^n$,

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

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами[32].

Кликовое представление правильных семейств

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 $\mathbb{E}_k^n$.

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

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

Кликовое представление правильных семейств

- Правильные семейства находятся во взаимно-однозначном соответствии с кликами некоторым образом построенного графа («обобщенный граф Келлера»).
- Для $k = 2$ перенос из теории USO-ориентаций[31], для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n)$: $V = \mathbb{E}_{k^2}^n$,

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

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами[32].

Кликовое представление правильных семейств

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 $\mathbb{E}_k^n$.

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

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

Кликовое представление правильных семейств

- Правильные семейства находятся во взаимно-однозначном соответствии с кликами некоторым образом построенного графа («обобщенный граф Келлера»).
- Для $k = 2$ перенос из теории USO-ориентаций[31], для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n)$: $V = \mathbb{E}^n_{k^2}$,

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

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами[32].

Кликовое представление правильных семейств

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 $\mathbb{E}^n_k$.

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

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

Кликовое представление правильных семейств

- Правильные семейства находятся во взаимно-однозначном соответствии с кликами некоторым образом построенного графа («обобщенный граф Келлера»).
- Для $k = 2$ перенос из теории USO-ориентаций[31], для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n)$: $V = \mathbb{E}^n_{k^2}$,

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

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами[32].

Кликовое представление правильных семейств

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 $\mathbb{E}^n_k$.

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

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

Кликовое представление правильных семейств

- Правильные семейства находятся во взаимно-однозначном соответствии с кликами некоторым образом построенного графа («обобщенный граф Келлера»).
- Для $k = 2$ перенос из теории USO-ориентаций[31], для $k > 2$ — авторское обобщение.
- Обобщенный граф Келлера $G(k, n)$: $V = \mathbb{E}^n_{k^2}$,

$$\{v, w\} \in E \leftrightarrow \exists i,\, 1 \le i \le n \colon v_i \equiv w_i \mod k,\ v_i \ne w_i.$$

- Графы примечательны тем, что в случае $k = 2$ некоторым образом кодируют неэквивалентные замощения пространства гиперкубами[32].

Кликовое представление правильных семейств

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 $\mathbb{E}^n_k$.

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

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

Список литературы I

- Borzechowski, M., J Doolittle и S. Weber. «A Universal Construction for Unique Sink Orientations». Англ. В: *arXiv preprint arXiv:2211.06072* (2022).
- 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.
- 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.

Список литературы II

- 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.
- — .«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.

Список литературы III

- 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.
- 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., 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.

Список литературы IV

- 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.
- Myasnikov, Alexei, Vladimir Shpilrain и Alexander Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*. American Mathematical Soc., 2011.
- 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.

Список литературы V

- 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.
- Sikirić, M. 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.
- 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).
- Артамонов, В. А. «Квазигруппы и их приложения». В: *Чебышевский сборник* 19.2 (66) (2018), с. 111—122.

Список литературы VI

- 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.
- 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.
- Глухов, М. М. «О применениях квазигрупп в криптографии». В: *Прикладная дискретная математика* 2 (2) (2008), с. 28—32.

Список литературы VII

- 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.
- 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.

Список литературы VIII

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

Список литературы IX

- Носов, В. А. «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.
- — .«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 X

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), с. 91—102.
EDN: JTVVAY; журнал индексируется в RSCI. Импакт-фактор: 0.385 (РИНЦ); общий объем 0.75 п. л..
Перевод:
Tsaregorodtsev K.D. Properties of proper families of Boolean functions // Discrete Mathematics and Applications. — 2022. — Vol. 32, No. 5. — PP. 369–378.
EDN: INXYMW; журнал индексируется в WOS, Scopus. Импакт-фактор: 0.3 (JIF); общий объем 0.75 п. л.

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 (HUFP-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 одностоковыми ориентациями графов булевых кубов (USO-ориентации), а также между булевыми правильными семействами и булевыми сетями с наследственно единственной неподвижной точкой (HUFP-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.