

Правильные семейства функций и порождаемые ими квазигруппы

Комбинаторные и алгебраические свойства

Содержание доклада

1. Мотивация и основные определения
2. Правильные семейства функций
3. Эквивалентные определения правильности
4. Свойства правильных семейств

Содержание

- 1 Мотивация и основные определения
- 2 Правильные семейства функций
- 3 Эквивалентные определения правильности
- 4 Свойства правильных семейств

«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»; Глухов, «О применениях квазигрупп в криптографии».

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 $\mathbb{E}_k = \mathbb{Z}_k$)
F	семейство (набор) функций $F = (f_1, \dots, f_n)$, $F: Q^n \rightarrow Q^n$
f_i	i -я функция семейства F
n	размер семейства
$\text{Func}(Q)$	множество функций $f: Q \rightarrow Q$
$\text{Perm}(Q)$	множество подстановок (биекций) на Q

Еще немного об обозначениях

Примеры/определения

Как правило, НЕ мои.

Утверждения

Тоже не мои.

Леммы-теоремы-утверждения

Мои.

Квазигруппа

Квазигруппа

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:

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

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

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:

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

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

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:

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

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 изотоп:

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

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**:

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

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 таблицы⁵.
- 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.

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



⁵Denes и Keedwell, *Latin squares and their applications*.

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 таблицы⁵.
- 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.

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

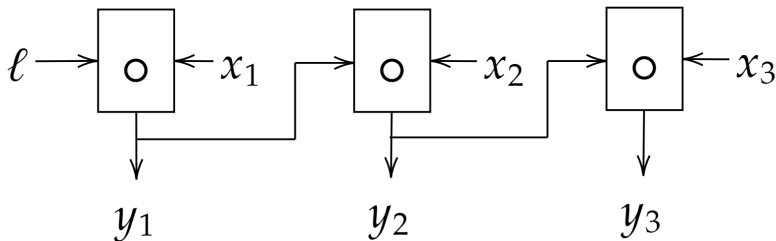

⁵Denes и Keedwell, *Latin squares and their applications*.

Пример: E -преобразование

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

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

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



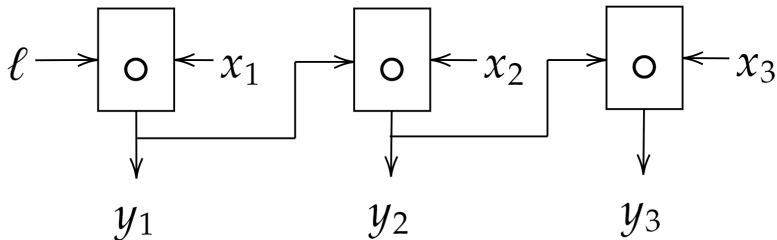
⁶Markovski и Bakeva, «Quasigroup string processing: Part 4».

Пример: 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

- Пусть на Q задано несколько структур квазигруппы: \circ_1, \dots, \circ_n .
- Можем ввести кратное E -преобразование:

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

- Каждое E_{ℓ_i} использует свою операцию \circ_i .
- Чтобы «отменить», нужно применить D , но в обратном порядке:

$$D_{\ell_1, \dots, \ell_n}(y) = D_{\ell_n}(\dots(D_{\ell_1}(y))\dots).$$

Пример: итерации E -преобразований

- Пусть на Q задано несколько структур квазигруппы: \circ_1, \dots, \circ_n .
- Можем ввести кратное E -преобразование:

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

- Каждое E_{ℓ_i} использует свою операцию \circ_i .
- Чтобы «отменить», нужно применить D , но в обратном порядке:

$$D_{\ell_1, \dots, \ell_n}(y) = D_{\ell_n}(\dots(D_{\ell_1}(y))\dots).$$

Некоторые свойства E -преобразования

Работы⁷.

- Для любых $\alpha = (a_1, \dots, a_m)$ и (c_1, \dots, c_k) уравнение $E_\alpha(x_1 \dots x_k) = c_1 \dots c_k$ имеет единственное решение (в силу обратимости E_α).
- Отображение $E_a: Q \rightarrow Q$ задает марковскую цепь: если $X_1 \dots X_n$ — случайные независимые величины, распределенные на Q , то распределение вероятностей знаков $Y_1 \dots Y_n = E_a(X_1 \dots X_n)$ задаются матрицей переходных вероятностей (распределение Y_m зависит от распределения Y_{m-1} и не зависит от Y_{m-2}, \dots, Y_1).
- Распределение Y_i сходится к равновероятному (для достаточно большого n , по свойству марковских цепей).
- Если применяем кратное E -преобразование с кратностью ℓ , то распределение подстрок длины ℓ вида $Y_i Y_{i+1} \dots Y_{i+\ell-1}$ сходится к равновероятному (для достаточно большого n).

⁷Bakeva и Dimitrova, «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis»; Markovski, Gligoroski и Bakeva, «Quasigroup String Processing: Part 1»; Markovski и Bakeva, «Quasigroup string processing: Part 4».

Некоторые свойства E -преобразования

Работы⁷.

- Для любых $\alpha = (a_1, \dots, a_m)$ и (c_1, \dots, c_k) уравнение $E_\alpha(x_1 \dots x_k) = c_1 \dots c_k$ имеет единственное решение (в силу обратимости E_α).
- Отображение $E_a: Q \rightarrow Q$ задает марковскую цепь: если $X_1 \dots X_n$ — случайные независимые величины, распределенные на Q , то распределение вероятностей знаков $Y_1 \dots Y_n = E_a(X_1 \dots X_n)$ задаются матрицей переходных вероятностей (распределение Y_m зависит от распределения Y_{m-1} и не зависит от Y_{m-2}, \dots, Y_1).
- Распределение Y_i сходится к равновероятному (для достаточно большого n , по свойству марковских цепей).
- Если применяем кратное E -преобразование с кратностью ℓ , то распределение подстрок длины ℓ вида $Y_i Y_{i+1} \dots Y_{i+\ell-1}$ сходится к равновероятному (для достаточно большого n).

⁷Bakeva и Dimitrova, «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis»; Markovski, Gligoroski и Bakeva, «Quasigroup String Processing: Part 1»; Markovski и Bakeva, «Quasigroup string processing: Part 4».

Некоторые свойства E -преобразования

Работы⁷.

- Для любых $\alpha = (a_1, \dots, a_m)$ и (c_1, \dots, c_k) уравнение $E_\alpha(x_1 \dots x_k) = c_1 \dots c_k$ имеет единственное решение (в силу обратимости E_α).
- Отображение $E_a: Q \rightarrow Q$ задает марковскую цепь: если $X_1 \dots X_n$ — случайные независимые величины, распределенные на Q , то распределение вероятностей знаков $Y_1 \dots Y_n = E_a(X_1 \dots X_n)$ задаются матрицей переходных вероятностей (распределение Y_m зависит от распределения Y_{m-1} и не зависит от Y_{m-2}, \dots, Y_1).
- Распределение Y_i сходится к равновероятному (для достаточно большого n , по свойству марковских цепей).
- Если применяем кратное E -преобразование с кратностью ℓ , то распределение подстрок длины ℓ вида $Y_i Y_{i+1} \dots Y_{i+\ell-1}$ сходится к равновероятному (для достаточно большого n).

⁷Bakeva и Dimitrova, «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis»; Markovski, Gligoroski и Bakeva, «Quasigroup String Processing: Part 1»; Markovski и Bakeva, «Quasigroup string processing: Part 4».

Некоторые свойства E -преобразования

Работы⁷.

- Для любых $\alpha = (a_1, \dots, a_m)$ и (c_1, \dots, c_k) уравнение $E_\alpha(x_1 \dots x_k) = c_1 \dots c_k$ имеет единственное решение (в силу обратимости E_α).
- Отображение $E_a: Q \rightarrow Q$ задает марковскую цепь: если $X_1 \dots X_n$ — случайные независимые величины, распределенные на Q , то распределение вероятностей знаков $Y_1 \dots Y_n = E_a(X_1 \dots X_n)$ задаются матрицей переходных вероятностей (распределение Y_m зависит от распределения Y_{m-1} и не зависит от Y_{m-2}, \dots, Y_1).
- Распределение Y_i сходится к равновероятному (для достаточно большого n , по свойству марковских цепей).
- Если применяем кратное E -преобразование с кратностью ℓ , то распределение подстрок длины ℓ вида $Y_i Y_{i+1} \dots Y_{i+\ell-1}$ сходится к равновероятному (для достаточно большого n).

⁷Bakeva и Dimitrova, «Some probabilistic properties of quasigroup processed strings useful for cryptanalysis»; Markovski, Gligoroski и Bakeva, «Quasigroup String Processing: Part 1»; Markovski и Bakeva, «Quasigroup string processing: Part 4».

Механизмы

- ГПСЧ на основе итерации E -преобразований⁸.
- Блочный шифр INRU⁹, E -преобразование используется в качестве нелинейного элемента.
- «Односторонняя функция»¹⁰ и основанные на ней хеш-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, Markovski и Kocarev, «Edon-R, An Infinite Family of Cryptographic Hash Functions.»; Gligoroski и др., «Cryptographic hash function Edon-R'»; 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».

Другие предложения (кратко)

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

- Низкоресурсная (легковесная/lightweight) хеш-функция GAGE и AEAD-алгоритм InGAGE (см. <http://gageingage.org/>, также¹¹).
- Поточный шифр Edon80¹².
- Хэш-функция NaSHA¹³.

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 cryptography¹⁴.
- 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 cryptography¹⁴.
- 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 cryptography¹⁴.
- 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 cryptography¹⁴.
- 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».

²⁰Shcherbacov, *Elements of Quasigroup Theory and Applications*; Артамонов, «Квазигруппы и их приложения»; Глухов, «Компания АКТИВ»
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».

²⁰Shcherbacov, *Elements of Quasigroup Theory and Applications*; Артамонов, «Квазигруппы и их приложения»; Глухов, «Компания АКТИВ»
применениях квазигрупп в криптографии».

Другие предложения (кратко)-3

- Схемы — аналоги протокола Диффи-Хеллмана выработки общего ключа¹⁷, гомоморфное шифрование¹⁸: используются ППС/ПДС- 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».

²⁰Shcherbacov, *Elements of Quasigroup Theory and Applications*; Артамонов, «Квазигруппы и их приложения»; Глухов, «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:

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

- Рассмотрим для простоты случай $Q = \{0, 1\}^n$: хотим задать структуру квазигруппы на Q с помощью семейства булевых функций.
- Какие условия надо наложить на функции f_i , чтобы операция $x \circ y$ задавала структуру квазигруппы на Q ?

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

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному²⁵:

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

- Рассмотрим для простоты случай $Q = \{0, 1\}^n$: хотим задать структуру квазигруппы на Q с помощью семейства булевых функций.
- Какие условия надо наложить на функции f_i , чтобы операция $x \circ y$ задавала структуру квазигруппы на Q ?

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

Функциональное задание квазигруппы

- Можно перейти от табличного задания операции к функциональному²⁵:

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

- Рассмотрим для простоты случай $Q = \{0, 1\}^n$: хотим задать структуру квазигруппы на Q с помощью семейства булевых функций.
- Какие условия надо наложить на функции f_i , чтобы операция $x \circ y$ задавала структуру квазигруппы на Q ?

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

Содержание

- 1 Мотивация и основные определения
- 2 Правильные семейства функций**
- 3 Эквивалентные определения правильности
- 4 Свойства правильных семейств

Правильные семейства булевых функций

Правильное семейство

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 $f_i(x) = f_i(y)$ (см.^а).

^аНосов, «Критерий регулярности булевского неавтономного автомата с разделенным входом», «Построение классов латинских квадратов в булевой базе данных».

Правильные семейства можно задавать не только над \mathbb{E}_2^n , но над логикой любой значности k ²⁶, над произвольными группами²⁷; над прямыми произведениями других квазигрупп²⁸ и даже 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

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 $f_i(x) = f_i(y)$ (см.^а).

^аНосов, «Критерий регулярности булевского неавтономного автомата с разделенным входом», «Построение классов латинских квадратов в булевой базе данных».

Правильные семейства можно задавать не только над \mathbb{E}_2^n , но над логикой любой значности k ²⁶, над произвольными группами²⁷; над прямыми произведениями других квазигрупп²⁸ и даже d -квазигрупп²⁹.

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

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

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

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

Правильные семейства и квазигруппы

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 .

Существенная (не)зависимость

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

Правильные семейства и квазигруппы

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 .

Существенная (не)зависимость

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

Константные семейства

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

Треугольные семейства

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

является правильным^a.

^aНосов и Панкратьев, «Латинские квадраты над абелевыми группами».

Константные семейства

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

Треугольные семейства

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

является правильным^a.

^aНосов и Панкратьев, «Латинские квадраты над абелевыми группами».

Ортогональные функции

Две функции $f, g: \mathbb{E}_k^n \rightarrow \mathbb{E}_k$ будем называть **ортогональными**, если для любого $x \in \mathbb{E}_k^n$ выполняется хотя бы одно из двух равенств: $f(x) = 0$ или $g(x) = 0$.

Семейство ортогональных функций

Пусть $F = (f_1, \dots, f_n)$ — семейство попарно ортогональных функций, и f_i не зависит существенно от x_i . Тогда F является правильным^a.

$$\begin{aligned} f_1 &= \bar{x}_2 x_3 \cdots x_{n-1} x_n, \\ f_2 &= \bar{x}_3 x_4 \cdots x_n x_1, \\ &\vdots \\ f_n &= \bar{x}_1 x_2 \cdots x_{n-2} x_{n-1} \end{aligned}$$

^aНосов и Панкратьев, «О функциональном задании латинских квадратов».

Ортогональные функции

Две функции $f, g: \mathbb{E}_k^n \rightarrow \mathbb{E}_k$ будем называть **ортогональными**, если для любого $x \in \mathbb{E}_k^n$ выполняется хотя бы одно из двух равенств: $f(x) = 0$ или $g(x) = 0$.

Семейство ортогональных функций

Пусть $F = (f_1, \dots, f_n)$ — семейство попарно ортогональных функций, и f_i не зависит существенно от x_i . Тогда F является правильным^a.

$$\begin{aligned} f_1 &= \bar{x}_2 x_3 \cdots x_{n-1} x_n, \\ f_2 &= \bar{x}_3 x_4 \cdots x_n x_1, \\ &\vdots \\ f_n &= \bar{x}_1 x_2 \cdots x_{n-2} x_{n-1} \end{aligned}$$

^aНосов и Панкратьев, «О функциональном задании латинских квадратов».

Класс квадратичных семейств

Семейство F вида 1 является правильным для любого $n \geq 1$:

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

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

Преобразования, сохраняющие правильность

Преобразование сдвига

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

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

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

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

^aНосов и Панкратьев, «О функциональном задании латинских квадратов».

Преобразования, сохраняющие правильность

Преобразование сдвига

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

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

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

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

^aНосов и Панкратьев, «О функциональном задании латинских квадратов».

Преобразования, сохраняющие правильность-2

Преобразование перекодировки

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 $F(x) = (f_1(x), \dots, f_n(x))$ правильное, то $\Phi(F(\Psi(x)))$ также правильное.

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

Замечание

Сдвиги являются частными случаями преобразования перекодировки.

Преобразования, сохраняющие правильность-2

Преобразование перекодировки

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 $F(x) = (f_1(x), \dots, f_n(x))$ правильное, то $\Phi(F(\Psi(x)))$ также правильное.

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

Замечание

Сдвиги являются частными случаями преобразования перекодировки.

Преобразования, сохраняющие правильность-2

Преобразование перекодировки

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 $F(x) = (f_1(x), \dots, f_n(x))$ правильное, то $\Phi(F(\Psi(x)))$ также правильное.

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

Замечание

Сдвиги являются частными случаями преобразования перекодировки.

Преобразования, сохраняющие правильность-3

Согласованная перенумерация

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

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

Если $F(x)$ — правильное, то $\sigma(F)$ также правильное^a.

^aНосов и Панкратьев, «О функциональном задании латинских квадратов».

Преобразования, сохраняющие правильность-3

Согласованная перенумерация

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

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

Если $F(x)$ — правильное, то $\sigma(F)$ также правильное^a.

^aНосов и Панкратьев, «О функциональном задании латинских квадратов».

Преобразования, сохраняющие правильность-4

Проекция

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.

Общий вид биекций, сохраняющих правильность

- Пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in Perm(Q^n)$. Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

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

- Тогда Φ и Ψ должны быть изометриями Q^n (в метрике Хэмминга).
- Изометрии \mathbb{E}_k^n , $|Q| = k$ — это перенумерации и перекодировки.
- Оба этих класса преобразований сохраняют правильность (перенумерации должны быть согласованы).

Общий вид биекций, сохраняющих правильность

- Пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in Perm(Q^n)$. Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

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

- Тогда Φ и Ψ должны быть изометриями Q^n (в метрике Хэмминга).
- Изометрии \mathbb{E}_k^n , $|Q| = k$ — это перенумерации и перекодировки.
- Оба этих класса преобразований сохраняют правильность (перенумерации должны быть согласованы).

Общий вид биекций, сохраняющих правильность

- Пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in Perm(Q^n)$. Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

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

- Тогда Φ и Ψ должны быть изометриями Q^n (в метрике Хэмминга).
- Изометрии $\mathbb{E}_k^n, |Q| = k$ — это перенумерации и перекодировки.
- Оба этих класса преобразований сохраняют правильность (перенумерации должны быть согласованы).

Общий вид биекций, сохраняющих правильность

- Пусть Φ, Ψ — биекции на Q^n : $\Phi, \Psi \in Perm(Q^n)$. Рассмотрим стабилизатор множества всех правильных семейств, заданных на Q^n :

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

- Тогда Φ и Ψ должны быть изометриями Q^n (в метрике Хэмминга).
- Изометрии \mathbb{E}_k^n , $|Q| = k$ — это перенумерации и перекодировки.
- Оба этих класса преобразований сохраняют правильность (перенумерации должны быть согласованы).

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.

Открытые вопросы-1

- Построение достаточно широких классов правильных семейств с «хорошими» свойствами, в том числе и для логик большей значности $k > 2$?
- Есть отношение эквивалентности на множестве правильных семейств, как быстро строить представителей?
- Можно ли поставить классам эквивалентности во взаимно-однозначное соответствие какие-то геометрические объекты, группы симметрий которых соответствуют согласованным перенумерациям и перекодировкам (для логик значности $k > 2$)?

Открытые вопросы-1

- Построение достаточно широких классов правильных семейств с «хорошими» свойствами, в том числе и для логик большей значности $k > 2$?
- Есть отношение эквивалентности на множестве правильных семейств, как быстро строить представителей?
- Можно ли поставить классам эквивалентности во взаимно-однозначное соответствие какие-то геометрические объекты, группы симметрий которых соответствуют согласованным перенумерациям и перекодировкам (для логик значности $k > 2$)?

Открытые вопросы-1

- Построение достаточно широких классов правильных семейств с «хорошими» свойствами, в том числе и для логик большей значности $k > 2$?
- Есть отношение эквивалентности на множестве правильных семейств, как быстро строить представителей?
- Можно ли поставить классам эквивалентности во взаимно-однозначное соответствие какие-то геометрические объекты, группы симметрий которых соответствуют согласованным перенумерациям и перекодировкам (для логик значности $k > 2$)?

Содержание

- 1 Мотивация и основные определения
- 2 Правильные семейства функций
- 3 Эквивалентные определения правильности**
- 4 Свойства правильных семейств

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).

Ориентация с единственным стоком USO

Ориентация с единственным стоком^a (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.

^aSzabó и Welzl, «Unique sink orientations of cubes».

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).

Ориентация с единственным стоком USO

Ориентация с единственным стоком^a (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.

^aSzabó и Welzl, «Unique sink orientations of cubes».

USO: один пример

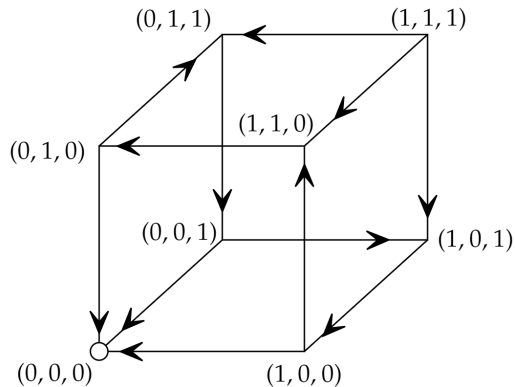
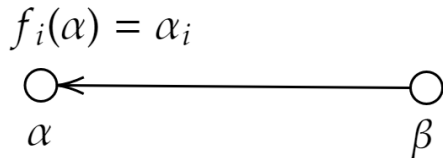


Рис. 1: Одностокковая ориентация трехмерного булева куба B_3

Пусть F — семейство булевых функций.

Граф семейства $\Gamma(F)$

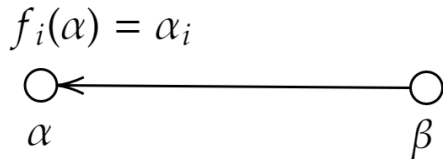
- Вершины: $V = \{\alpha \in \mathbb{E}_2^n\}$.
- Пусть $\alpha \neq \beta$, $\rho(\alpha, \beta) = 1$, $\alpha_i \neq \beta_i$, добавим ориентированное ребро $(\beta, \alpha) \in E$ тогда и только тогда, когда $f_i(\alpha) = \alpha_i$.



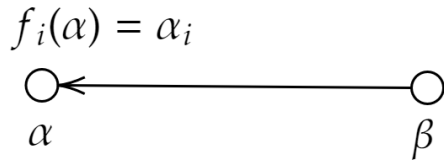
Пусть F — семейство булевых функций.

Граф семейства $\Gamma(F)$

- 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 $f_i(\alpha) = \alpha_i$.

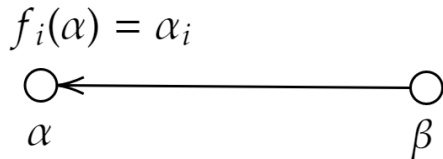


Неподвижные точки графа $\Gamma(F)$



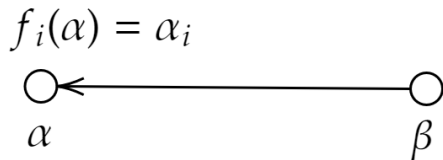
- Чему в терминах графа $\Gamma(F)$ соответствует неподвижная точка α отображения $x \rightarrow F(x)$?
- $f_i(\alpha) = \alpha_i$ для всех $1 \leq i \leq n$.
- Следовательно, α — сток в $\Gamma(F)$.
- Ориентации подкубов в $\Gamma(F)$ задаются проекциями F' семейства F .

Неподвижные точки графа $\Gamma(F)$



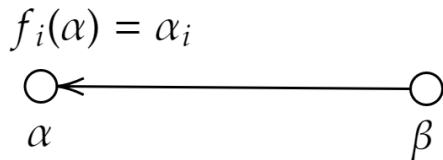
- Чему в терминах графа $\Gamma(F)$ соответствует неподвижная точка α отображения $x \rightarrow F(x)$?
- $f_i(\alpha) = \alpha_i$ для всех $1 \leq i \leq n$.
- Следовательно, α — сток в $\Gamma(F)$.
- Ориентации подкубов в $\Gamma(F)$ задаются проекциями F' семейства F .

Неподвижные точки графа $\Gamma(F)$



- Чему в терминах графа $\Gamma(F)$ соответствует неподвижная точка α отображения $x \rightarrow F(x)$?
- $f_i(\alpha) = \alpha_i$ для всех $1 \leq i \leq n$.
- Следовательно, α — сток в $\Gamma(F)$.
- Ориентации подкубов в $\Gamma(F)$ задаются проекциями F' семейства F .

Неподвижные точки графа $\Gamma(F)$



- Чему в терминах графа $\Gamma(F)$ соответствует неподвижная точка α отображения $x \rightarrow F(x)$?
- $f_i(\alpha) = \alpha_i$ для всех $1 \leq i \leq n$.
- Следовательно, α — сток в $\Gamma(F)$.
- Ориентации подкубов в $\Gamma(F)$ задаются проекциями F' семейства F .

USO и правильность: два описания одного объекта

Взаимно-однозначное соответствие

Граф $\Gamma(F)$ семейства булевых функций F является одностокковой ориентацией тогда и только тогда, когда F — правильное семейство^a.

^aЦарегородцев, «О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов»; Царегородцев, «О соответствии между правильными семействами и рёберными ориентациями булевых кубов».

- Существует взаимно-однозначное соответствие между «алгебраическим» и «геометрическим» описаниями.
- Это позволяет переводить результаты с одного «языка» на другой.
- Некоторые примеры переноса: вероятностный алгоритм порождения правильных семейств с помощью процедуры МСМС³⁰, оценка на число булевых правильных семейств³¹, новые классы правильных семейств.

³⁰Schurr, «Unique sink orientations of cubes»; Галатенко и др., «Порождение правильных семейств функций».

³¹Царегородцев, «О свойствах правильных семейств булевых функций».

USO и правильность: два описания одного объекта

Взаимно-однозначное соответствие

Граф $\Gamma(F)$ семейства булевых функций F является одностокковой ориентацией тогда и только тогда, когда F — правильное семейство^a.

^aЦарегородцев, «О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов»; Царегородцев, «О соответствии между правильными семействами и рёберными ориентациями булевых кубов».

- Существует взаимно-однозначное соответствие между «алгебраическим» и «геометрическим» описаниями.
- Это позволяет переводить результаты с одного «языка» на другой.
- Некоторые примеры переноса: вероятностный алгоритм порождения правильных семейств с помощью процедуры МСМС³⁰, оценка на число булевых правильных семейств³¹, новые классы правильных семейств.

³⁰Schurr, «Unique sink orientations of cubes»; Галатенко и др., «Порождение правильных семейств функций».

³¹Царегородцев, «О свойствах правильных семейств булевых функций».

Рекурсивная треугольность

Рекурсивная ориентация

Рекурсивно одностокковая ориентация булева n -мерного куба \mathbb{E}_n задается следующим характеристическим свойством: найдется такое направление i , вдоль которой все ребра ориентированы в одном направлении, и ориентация на каждом из подкубов $x_i = 0$ и $x_i = 1$ размерности $(n - 1)$ также является рекурсивно одностокковой (recursively combed cube orientation^a).

^aGao, Gartner и Lamperski, «A new combinatorial property of geometric unique sink orientations».

Рекурсивно треугольное семейство

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

Рекурсивная треугольность

Рекурсивная ориентация

Рекурсивно одностокковая ориентация булева n -мерного куба \mathbb{E}_n задается следующим характеристическим свойством: найдется такое направление i , вдоль которой все ребра ориентированы в одном направлении, и ориентация на каждом из подкубов $x_i = 0$ и $x_i = 1$ размерности $(n - 1)$ также является рекурсивно одностокковой (recursively combed cube orientation^a).

^aGao, Gartner и Lamperski, «A new combinatorial property of geometric unique sink orientations».

Рекурсивно треугольное семейство

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

Рекурсивная треугольность

Замечание

Рекурсивно треугольные семейства более общее понятие, чем треугольные: треугольные семейства являются такими рекурсивно треугольными, что каждая из проекций $\Pi_i^a(F)$ постоянна вдоль одного и того же направления j .

Теорема

Рекурсивно треугольные семейства являются правильными.

Рекурсивная треугольность

Замечание

Рекурсивно треугольные семейства более общее понятие, чем треугольные: треугольные семейства являются такими рекурсивно треугольными, что каждая из проекций $\Pi_i^a(F)$ постоянна вдоль одного и того же направления j .

Теорема

Рекурсивно треугольные семейства являются правильными.

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

Оценка на число булевых правильных семейств

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

где A, B — некоторые положительные константы^a.

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

Булевых треугольных семейств экспоненциально мало

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

для некоторого $D > 0$ ^a. Таким образом, почти все булевы правильные семейства не являются треугольными.

^aЦарегородцев, «О свойствах правильных семейств булевых функций».

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

Оценка на число булевых правильных семейств

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

где A, B — некоторые положительные константы^a.

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

Булевых треугольных семейств экспоненциально мало

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

для некоторого $D > 0$ ^a. Таким образом, почти все булевы правильные семейства не являются треугольными.

^aЦарегородцев, «О свойствах правильных семейств булевых функций».

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

Оценка на число булевых правильных семейств

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

где A, B — некоторые положительные константы^a.

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

Булевых треугольных семейств экспоненциально мало

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

для некоторого $D > 0$ ^a. Таким образом, почти все булевы правильные семейства не являются треугольными.

^aЦарегородцев, «О свойствах правильных семейств булевых функций».

Рекуррентное соотношение

Число рекурсивно треугольных семейств

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

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

Замечание

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

Рекуррентное соотношение

Число рекурсивно треугольных семейств

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

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

Замечание

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

Сложность распознавания правильности

- В общем случае проверка правильности является сложной задачей: если семейство задано в форме КНФ, то задача проверки правильности coNP-полна³².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости³³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма³⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma(F)$, задаваемая семейством F , является одностокковой.
- Алгоритм опирается на еще одно характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

³²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

³³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

³⁴Bosshard 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-полна³².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости³³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма³⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma(F)$, задаваемая семейством F , является одностокковой.
- Алгоритм опирается на еще одно характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

³²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

³³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

³⁴Bosshard 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-полна³².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости³³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма³⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma(F)$, задаваемая семейством F , является одностокковой.
- Алгоритм опирается на еще одно характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

³²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

³³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

³⁴Bosshard 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-полна³².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости³³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма³⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma(F)$, задаваемая семейством F , является одностокковой.
- Алгоритм опирается на еще одно характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

³²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

³³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

³⁴Bosshard 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-полна³².
- В определенных случаях задача проверки правильности может быть упрощена, в частности, за счет вида графа существенной зависимости³³.
- Алгоритм проверки правильности булева семейства требует порядка $\Theta(4^n)$ операций вычисления правильного семейства на двоичном наборе x (проверка по определению правильности).
- Предложена адаптация алгоритма³⁴ со сложностью $\Theta(3^n)$, проверяющего, что ориентация $\Gamma(F)$, задаваемая семейством F , является одностокковой.
- Алгоритм опирается на еще одно характеристическое свойство правильных семейств: булево семейство правильно тогда и только тогда, когда каждая его проекция не является самодвойственным отображением.

³²Носов, «Критерий регулярности булевского неавтономного автомата с разделенным входом».

³³Рыков, «О правильных семействах функций, используемых для задания латинских квадратов».

³⁴Bosshard и Gärtner, «Pseudo unique sink orientations».

Неподвижные точки правильного семейства

Булев случай

Булево семейство F является правильным тогда и только тогда, когда семейство F и каждая из его проекций имеет единственную неподвижную точку.

Общий случай

Семейство $F: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки F все её проекции имеют единственную неподвижную точку.

В булевом случае свойство единственности неподвижной точки дает ещё одно характеристическое свойство правильных семейств, которое изучалось в контексте математической биологии (в частности, при изучении экспрессии генов³⁵).

³⁵Richard, «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

Булев случай

Булево семейство F является правильным тогда и только тогда, когда семейство F и каждая из его проекций имеет единственную неподвижную точку.

Общий случай

Семейство $F: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки F все её проекции имеют единственную неподвижную точку.

В булевом случае свойство единственности неподвижной точки дает ещё одно характеристическое свойство правильных семейств, которое изучалось в контексте математической биологии (в частности, при изучении экспрессии генов³⁵).

³⁵Richard, «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

Булев случай

Булево семейство F является правильным тогда и только тогда, когда семейство F и каждая из его проекций имеет единственную неподвижную точку.

Общий случай

Семейство $F: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ является правильным тогда и только тогда, когда для любой перекодировки F все её проекции имеют единственную неподвижную точку.

В булевом случае свойство единственности неподвижной точки дает ещё одно характеристическое свойство правильных семейств, которое изучалось в контексте математической биологии (в частности, при изучении экспрессии генов³⁵).

³⁵Richard, «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

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

Правильные семейства \leftrightarrow HUFP-сети

Булево семейство F является правильным $\Leftrightarrow F$ 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

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

Правильные семейства \leftrightarrow HUFP-сети

Булево семейство F является правильным $\Leftrightarrow F$ 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

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

Правильные семейства \leftrightarrow HUFP-сети

Булево семейство F является правильным $\Leftrightarrow F$ 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 F — семейство размера n .

Глобальный граф взаимодействий $G(F)$

- Вершины: $V = \{1, \dots, n\}$.
- Ребра: $i \rightarrow j$ тогда и только тогда, когда f_j существенно зависит от x_i .
- Эквивалентно: «дискретная» частная производная f_j по x_i не равна тождественно нулю.

Ациклические глобальные графы

Если $G(F)$ — ациклический, то F — HUPF-сеть^a.

^aRobert, «Iterations sur des ensembles finis et automates cellulaires contractants».

Эквивалентно: если F — булево треугольное семейство, то F правильно.

Пусть F — семейство размера n .

Глобальный граф взаимодействий $G(F)$

- Вершины: $V = \{1, \dots, n\}$.
- Ребра: $i \rightarrow j$ тогда и только тогда, когда f_j существенно зависит от x_i .
- Эквивалентно: «дискретная» частная производная f_j по x_i не равна тождественно нулю.

Ациклические глобальные графы

Если $G(F)$ — ациклический, то F — HUPF-сеть^a.

^aRobert, «Iterations sur des ensembles finis et automates cellulaires contractants».

Эквивалентно: если F — булево треугольное семейство, то F правильно.

Пусть F — семейство размера n .

Глобальный граф взаимодействий $G(F)$

- Вершины: $V = \{1, \dots, n\}$.
- Ребра: $i \rightarrow j$ тогда и только тогда, когда f_j существенно зависит от x_i .
- Эквивалентно: «дискретная» частная производная f_j по x_i не равна тождественно нулю.

Ациклические глобальные графы

Если $G(F)$ — ациклический, то F — HUPF-сеть^a.

^aRobert, «Iterations sur des ensembles finis et automates cellulaires contractants».

Эквивалентно: если F — булево треугольное семейство, то F правильно.

Пусть F — семейство размера n .

Локальный граф взаимодействий $G(F, \alpha)$

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

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

Пусть F — семейство размера n .

Локальный граф взаимодействий $G(F, \alpha)$

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

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

Локальный граф взаимодействий-2

Локально треугольные семейства

$F: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ локально треугольно, если $G(F, \alpha)$ ацикличен 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

Локально треугольные семейства являются правильными (в логиках любой значности).

Теорема

Всякое рекурсивно треугольное семейство является локально треугольным.

Локальный граф взаимодействий-2

Локально треугольные семейства

$F: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ локально треугольно, если $G(F, \alpha)$ ацикличен 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

Локально треугольные семейства являются правильными (в логиках любой значности).

Теорема

Всякое рекурсивно треугольное семейство является локально треугольным.

Локальный граф взаимодействий-2

Локально треугольные семейства

$F: \mathbb{E}_k^n \rightarrow \mathbb{E}_k^n$ локально треугольно, если $G(F, \alpha)$ 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

Локально треугольные семейства являются правильными (в логиках любой значности).

Теорема

Всякое рекурсивно треугольное семейство является локально треугольным.

Локальный граф взаимодействий-3

Пусть F — семейство размера n .

Теорема

Если для любого t , $1 \leq t \leq n$ существует не более $2^t - 1$ наборов α , таких что $G(F, \alpha)$ имеет цикл длины не более чем t , то F является HUPF-сетью.

- Непонятно, является ли это условие критерием.
- Интуитивная интерпретация / «перевод» на язык правильных семейств общего вида пока что отсутствуют.

Локальный граф взаимодействий-3

Пусть F — семейство размера n .

Теорема

Если для любого t , $1 \leq t \leq n$ существует не более $2^t - 1$ наборов α , таких что $G(F, \alpha)$ имеет цикл длины не более чем t , то F является HUPF-сетью.

- Непонятно, является ли это условие критерием.
- Интуитивная интерпретация / «перевод» на язык правильных семейств общего вида пока что отсутствуют.

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-ориентаций³⁶, 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 гиперкубами³⁷.

Соответствие между семействами и кликами

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 .

³⁶Borzechowski, Doolittle и Weber, «A Universal Construction for Unique Sink Orientations».

³⁷Mathew, Östergård и Popa, «Enumerating cube tilings»; Sikirić, Itoh и Poyarkov, «Cube packings, second moment and holes».

Ещё одна альтернативная характеристика

Существует ещё несколько альтернативных характеристик правильных семейств.

- (Не)ортогональность аффинных пространств, построенных по правильным семействам.

Открытые вопросы-2

- Больше эквивалентных определений правильных семейств для логик значности $k > 2$.
- В чем «глубинная» причина того, что некоторые эквивалентности «работают» только в случае $k = 2$ и «ломаются» при переходе к $k > 2$?
- Дальнейший перенос и обобщение результатов, полученных в рамках исследований HUFР-сетей и одностокowych ориентаций.

Открытые вопросы-2

- Больше эквивалентных определений правильных семейств для логик значности $k > 2$.
- В чем «глубинная» причина того, что некоторые эквивалентности «работают» только в случае $k = 2$ и «ломаются» при переходе к $k > 2$?
- Дальнейший перенос и обобщение результатов, полученных в рамках исследований HUFР-сетей и одностокowych ориентаций.

Открытые вопросы-2

- Больше эквивалентных определений правильных семейств для логик значности $k > 2$.
- В чем «глубинная» причина того, что некоторые эквивалентности «работают» только в случае $k = 2$ и «ломаются» при переходе к $k > 2$?
- Дальнейший перенос и обобщение результатов, полученных в рамках исследований HUFР-сетей и одностокowych ориентаций.

Содержание

- 1 Мотивация и основные определения
- 2 Правильные семейства функций
- 3 Эквивалентные определения правильности
- 4 Свойства правильных семейств**

Мощность образа правильного семейства

Пусть $F = (f_1, \dots, f_n)$ — 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.
- Оказывается, что количество порождаемых квазигрупп одним правильным семейством F зависит от мощности образа этого семейства³⁸.

Связь мощности образа и количества порождаемых квазигрупп

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

³⁸Галатенко и др., «О порождении n -квазигрупп с помощью правильных семейств функций».

Мощность образа правильного семейства

Пусть $F = (f_1, \dots, f_n)$ — 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.
- Оказывается, что количество порождаемых квазигрупп одним правильным семейством F зависит от мощности образа этого семейства³⁸.

Связь мощности образа и количества порождаемых квазигрупп

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

³⁸Галатенко и др., «О порождении n -квазигрупп с помощью правильных семейств функций».

Мощность образа правильного семейства

Пусть $F = (f_1, \dots, f_n)$ — 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.
- Оказывается, что количество порождаемых квазигрупп одним правильным семейством F зависит от мощности образа этого семейства³⁸.

Связь мощности образа и количества порождаемых квазигрупп

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

³⁸Галатенко и др., «О порождении n -квазигрупп с помощью правильных семейств функций».

Мощность образа правильного семейства

Пусть $F = (f_1, \dots, f_n)$ — 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.
- Оказывается, что количество порождаемых квазигрупп одним правильным семейством F зависит от мощности образа этого семейства³⁸.

Связь мощности образа и количества порождаемых квазигрупп

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

³⁸Галатенко и др., «О порождении n -квазигрупп с помощью правильных семейств функций».

Ограниченность мощности образа

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

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

Мощность образа квадратичного семейства

Семейство

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

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

$$\begin{bmatrix} f_1(x_1, \dots, x_n) \\ f_2(x_1, \dots, x_n) \\ \vdots \\ f_n(x_1, \dots, x_n) \end{bmatrix} = \begin{bmatrix} \overline{x}_2 \cdot x_3 \\ \overline{x}_3 \cdot x_4 \\ \vdots \\ \overline{x}_1 \cdot x_2 \end{bmatrix}. \quad (3)$$

Правильность семейства

Семейство (3) является правильным.

Мощность образа семейства

Мощность образа семейства (3) равна Lucas_n (n -е число Люка):

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

$$\begin{bmatrix} f_1(x_1, \dots, x_n) \\ f_2(x_1, \dots, x_n) \\ \vdots \\ f_n(x_1, \dots, x_n) \end{bmatrix} = \begin{bmatrix} \overline{x}_2 \cdot x_3 \\ \overline{x}_3 \cdot x_4 \\ \vdots \\ \overline{x}_1 \cdot x_2 \end{bmatrix}. \quad (3)$$

Правильность семейства

Семейство (3) является правильным.

Мощность образа семейства

Мощность образа семейства (3) равна Lucas_n (n -е число Люка):

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

$$\begin{bmatrix} f_1(x_1, \dots, x_n) \\ f_2(x_1, \dots, x_n) \\ \vdots \\ f_n(x_1, \dots, x_n) \end{bmatrix} = \begin{bmatrix} \bar{x}_2 \cdot x_3 \\ \bar{x}_3 \cdot x_4 \\ \vdots \\ \bar{x}_1 \cdot x_2 \end{bmatrix}. \quad (3)$$

Правильность семейства

Семейство (3) является правильным.

Мощность образа семейства

Мощность образа семейства (3) равна Lucas_n (n -е число Люка):

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

Подстановки, порождаемые правильными семействами

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

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

является подстановкой: $\sigma_F \in Perm(Q^n)$.

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

Обратимость «правильных подстановок»

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

$$G(x) = (-x) + \sigma_F^{-1}(x)$$

также является правильным.

Т.е., если F — правильное, то существует правильное семейство G со свойством

$$\sigma_F^{-1}(x) = \sigma_G(x).$$

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

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

Обратимость «правильных подстановок»

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

$$G(x) = (-x) + \sigma_F^{-1}(x)$$

также является правильным.

Т.е., если F — правильное, то существует правильное семейство G со свойством

$$\sigma_F^{-1}(x) = \sigma_G(x).$$

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

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

Обратимость «правильных подстановок»

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

$$G(x) = (-x) + \sigma_F^{-1}(x)$$

также является правильным.

Т.е., если F — правильное, то существует правильное семейство G со свойством

$$\sigma_F^{-1}(x) = \sigma_G(x).$$

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

О подстановках, порождаемых правильными семействами-2

Незамкнутость относительно композиций

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

Транзитивность действия

Замыкание S^{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

В случае $Q = \mathbb{E}_2$ известно^a, что замыкание σ_F порождает все множество подстановок $Perm(\mathbb{E}_2^n)$.

^aSchurr, «Unique sink orientations of cubes».

О подстановках, порождаемых правильными семействами-2

Незамкнутость относительно композиций

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

Транзитивность действия

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

В случае $Q = \mathbb{E}_2$ известно^a, что замыкание σ_F порождает все множество подстановок $\text{Perm}(\mathbb{E}_2^n)$.

^aSchurr, «Unique sink orientations of cubes».

О подстановках, порождаемых правильными семействами-2

Незамкнутость относительно композиций

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

Транзитивность действия

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

В случае $Q = \mathbb{E}_2$ известно^a, что замыкание σ_F порождает все множество подстановок $\text{Perm}(\mathbb{E}_2^n)$.

^aSchurr, «Unique sink orientations of cubes».

О подстановках, порождаемых правильными семействами-3

Пусть F — правильное семейство булевых функций.

Четность числа элементов в прообразе

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

Количество неподвижных точек σ_F

У подстановки $\sigma_F(x) = x \oplus F(x)$ чётное число неподвижных точек.

О подстановках, порождаемых правильными семействами-3

Пусть F — правильное семейство булевых функций.

Четность числа элементов в прообразе

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

Количество неподвижных точек σ_F

У подстановки $\sigma_F(x) = x \oplus F(x)$ чётное число неподвижных точек.

Об индексах ассоциативности

Ассоциативные тройки

Тройка (a, b, c) элементов квазигруппы Q называется ассоциативной, если

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

Число таких троек называется индексом ассоциативности квазигруппы Q .

- С точки зрения некоторых криптосистем желательно, чтобы таких троек было как можно меньше.
- Имеется множество результатов, в которых оценивается минимальное число таких троек в квазигруппах порядка k .
- Имеются результаты о том, сколько в среднем таких троек в квазигруппе, где усреднение берется по всем изотопам.

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

Открытые вопросы-3

- Пока что очень мало понятно про то, каковы алгебраические свойства квазигрупп, порождаемых правильными семействами (в частности, каковы свойства подстановок σ_F).
- Хотелось бы, чтобы по виду правильного семейства можно было определять алгебраические свойства квазигруппы: наличие/отсутствие подквазигрупп, полиномиальная полнота, индекс ассоциативности и т.д...
- Пока что очень мало понятно про подстановки, порождаемые правильными семействами, в случае логики $k > 2$.

Открытые вопросы-3

- Пока что очень мало понятно про то, каковы алгебраические свойства квазигрупп, порождаемых правильными семействами (в частности, каковы свойства подстановок σ_F).
- Хотелось бы, чтобы по виду правильного семейства можно было определять алгебраические свойства квазигруппы: наличие/отсутствие подквазигрупп, полиномиальная полнота, индекс ассоциативности и т.д...
- Пока что очень мало понятно про подстановки, порождаемые правильными семействами, в случае логики $k > 2$.

Открытые вопросы-3

- Пока что очень мало понятно про то, каковы алгебраические свойства квазигрупп, порождаемых правильными семействами (в частности, каковы свойства подстановок σ_F).
- Хотелось бы, чтобы по виду правильного семейства можно было определять алгебраические свойства квазигруппы: наличие/отсутствие подквазигрупп, полиномиальная полнота, индекс ассоциативности и т.д...
- Пока что очень мало понятно про подстановки, порождаемые правильными семействами, в случае логики $k > 2$.

Заключение

- Правильные семейства функций могут быть описаны несколькими эквивалентными способами.
- Различные способы описания дают возможность переноса результатов из смежных областей на «язык» правильных семейств; некоторые результаты допускают обобщения на правильные семейства над логиками произвольной значности.
- Правильные семейства могут задавать структуру квазигруппы; квазигруппы, в свою очередь, могут использоваться для построения различных криптографических примитивов.
- Многие важные с точки зрения криптографии свойства получаемых примитивов зависят от используемой квазигруппы; в этом контексте полезно изучать свойства квазигрупп, порождаемых правильными семействами.

Заключение

- Правильные семейства функций могут быть описаны несколькими эквивалентными способами.
- Различные способы описания дают возможность переноса результатов из смежных областей на «язык» правильных семейств; некоторые результаты допускают обобщения на правильные семейства над логиками произвольной значности.
- Правильные семейства могут задавать структуру квазигруппы; квазигруппы, в свою очередь, могут использоваться для построения различных криптографических примитивов.
- Многие важные с точки зрения криптографии свойства получаемых примитивов зависят от используемой квазигруппы; в этом контексте полезно изучать свойства квазигрупп, порождаемых правильными семействами.

Заключение

- Правильные семейства функций могут быть описаны несколькими эквивалентными способами.
- Различные способы описания дают возможность переноса результатов из смежных областей на «язык» правильных семейств; некоторые результаты допускают обобщения на правильные семейства над логиками произвольной значности.
- Правильные семейства могут задавать структуру квазигруппы; квазигруппы, в свою очередь, могут использоваться для построения различных криптографических примитивов.
- Многие важные с точки зрения криптографии свойства получаемых примитивов зависят от используемой квазигруппы; в этом контексте полезно изучать свойства квазигрупп, порождаемых правильными семействами.

Заключение

- Правильные семейства функций могут быть описаны несколькими эквивалентными способами.
- Различные способы описания дают возможность переноса результатов из смежных областей на «язык» правильных семейств; некоторые результаты допускают обобщения на правильные семейства над логиками произвольной значности.
- Правильные семейства могут задавать структуру квазигруппы; квазигруппы, в свою очередь, могут использоваться для построения различных криптографических примитивов.
- Многие важные с точки зрения криптографии свойства получаемых примитивов зависят от используемой квазигруппы; в этом контексте полезно изучать свойства квазигрупп, порождаемых правильными семействами.

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, Verica и Vesna 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.
-  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, M., J. Doolittle и S. Weber. «A Universal Construction for Unique Sink Orientations». АНГЛ. В: *arXiv preprint arXiv:2211.06072* (2022).
-  Bosshard, Vitor и Bernd Gärtner. «Pseudo unique sink orientations». В: *arXiv preprint arXiv:1704.08481* (2017).
-  Chen, Yanling, Svein Johan Knapskog и Danilo Gligoroski. «Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity». В: *Submitted to ISIT 2010* (2010), с. 14.






Список литературы II

-  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*. АНГЛ. Под ред. Elsevier Science. 2nd edition. Burlington, 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, Jean-Charles и др. «A polynomial-time key-recovery attack on MQQ cryptosystems». В: *IACR International Workshop on Public Key Cryptography*. Springer. 2015, с. 150—174.
-  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.
-  Gao, Y., B. Gartner и J. Lamperski. «A new combinatorial property of geometric unique sink orientations». АНГЛ. В: *arXiv preprint arXiv:2008.08992* (2020).

Список литературы III

-  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, Danilo. «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.
-  Gligoroski, Danilo. *On the S-box in GAGE and InGAGE*. Англ. <http://gageingage.org/upload/LWC2019NISTWorkshop.pdf>. 2019.

Список литературы IV

-  Gligoroski, Danilo и Svein Johan 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, Danilo, Smile Markovski и Svein Johan Knapskog. «A public key block cipher based on multivariate quadratic quasigroups». В: *arXiv preprint arXiv:0808.0247* (2008).
-  — . «Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups». В: *Proceedings of the American Conference on Applied Mathematics*. 2008, с. 44—49.
-  Gligoroski, Danilo и др. «GAGE and InGAGE». Англ. В: *A Submission to the NIST Lightweight Cryptography Standardization Process* (2019).
-  Gligoroski, Danilo и др. «MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme». В: *International Conference on Trusted Systems*. Springer. 2011, с. 184—203.

Список литературы V



Gribov, Aleksei Viktorovich, Pavel Andreevich Zolotych 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 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.










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







Список литературы VI

-  Markovski, Smile, Danilo Gligoroski и Ljupco Kocarev. «Unbiased random sequences from quasigroup string transformations». *Англ. В: International workshop on fast software encryption*. Springer. 2005, с. 163—180.
-  Mathew, K Ashik, Patric RJ Östergård и Alexandru Popa. «Enumerating cube tilings». 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, Aleksandra и Smile Markovski. «Quasigroup String Transformations and Hash Function Design: A Case Study: The NaSHA Hash Function». В: *International Conference on ICT Innovations*. Springer. 2009, с. 367—376.
-  Mohamed, Mohamed Saied Emam и др. «Algebraic attack on the MQQ public key cryptosystem». 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.
-  Richard, A. «Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks». Англ. В: *Theoretical Computer Science* 583 (2015), с. 1—26.
-  Robert, François. «Iterations sur des ensembles finis et automates cellulaires contractants». Фр. В: *Linear Algebra and its applications* 29 (1980), с. 393—412.
-  Ruet, P. «Asynchronous Boolean networks and hereditarily bijective maps». Англ. В: *Natural Computing* 14 (2015), с. 545—553.
-  Ruet, P. «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, Václav 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, Т. 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, Sharwan 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.
-  Галатенко, А.В. и др. «О порождении n -квазигрупп с помощью правильных семейств функций». В: *Дискретная математика* 35.1 (2023), с. 35—53.





Список литературы X

-  Галатенко, Алексей Владимирович и др. «Порождение правильных семейств функций». В: *Интеллектуальные системы. Теория и приложения* 25.4 (2021), с. 100—103.
-  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.






Список литературы XI

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






Список литературы XII

-  Марков, Виктор, Александр Васильевич Михалёв и Евгений Сергеевич Кислицын. «Неассоциативные структуры в гомоморфной криптографии». В: *Фундаментальная и прикладная математика* 23.2 (2020), с. 209—215.
-  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.

Список литературы XIII

-  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.

Список литературы XIV

-  Романьков, Виталий Анатольевич. *Алгебраическая криптология: монография*. ОмГУ им. Ф. М. Достоевского, 2020.
-  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 взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов». В: *Прикладная дискретная математика* 48 (2020), с. 16—21. (Scopus, WoS).
-  Царегородцев, К.Д. «О свойствах правильных семейств булевых функций». В: *Дискретная математика* 33.1 (2021), с. 91—102.
-  — . «О соответствии между правильными семействами и реберными ориентациями булевых кубов». В: *Интеллектуальные системы. Теория и приложения* 24.1 (2020), с. 97—100.