Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/13/1

ПРЕЛОМЛЯЮЩИЕ БИЕКЦИИ В ТРОЙКАХ ШТЕЙНЕРА

М. В. Ведунова, К. Л. Геут, А. О. Игнатова, С. С. Титов

Исследованы преломляющие биекции в тройках Штейнера, применяемые при построении матроидов и схем разделения секрета. Под преломляющими понимаются отображения F квазигруппы в себя, удовлетворяющие условию $F(x * y) \neq \neq F(x) * F(y)$ при любых $x \neq y$. Предложены преломляющие биекции квазигрупп Штейнера с $N = 9, 13$ и $2^n - 1$ элементами при нечётных n, не делящихся на три, а также необходимые условия существования APN-биекций в $\mathrm{GF}(2^n)$. При помощи наборов преломляющих биекций построены матроиды, являющиеся контрпримерами к гипотезе, что каждый однородный матроид определяет некоторую блок-схему.

Ключевые слова: *преломляющие биекции, квазигруппы Штейнера, матроиды.*

Исследуются биекции квазигрупп, которые по аналогии с геометрическими преобразованиями, не переводящими никакую прямую в другую прямую, названы преломляющими. Преломляющие биекции применимы при построении APN-функций и как контрпример к гипотезе в теории схем разделения секрета: оказалось, что не каждый однородный матроид определяет некоторую блок-схему [1]. APN-биекции неоднократно изучались, в том числе вопросу существования взаимно однозначных APN-функций от чётного числа переменных посвящены работы [2, 3]. Итеративные конструкции APN-функций исследованы в [4].

Построение систем троек Штейнера S, S', S'' на множестве $G = \{1, 2, \ldots, N\}$, таких, что никакие две из них не содержат ни одной общей тройки [5], выглядит следующим образом: тройка $\{u, v, w\}$ преобразуется в тройку $\{f(u), f(v), f(w)\}$, где

1) $\{f(u), f(v), f(w)\} \in S'$;
2) $\{g(u), g(v), g(w)\} \in S''$.

Утверждение 1. Если существуют три биекции $F(x) = f(x)$, $F(x) = g(x)$ и $F(x) = fg^{-1}(x)$ квазигруппы Штейнера $(S, *)$, являющиеся преломляющими, т. е. удовлетворяющие условию $F(x * y) \neq F(x) * F(y)$ при любых $x \neq y$, то соответствующие им системы S, S', S'' не содержат ни одной общей тройки.

Системы S, S', S'' образуются в результате применения преломляющих биекций к стандартным тройкам Штейнера [5].

Рассмотрим на множестве $E = \{a, b, c\} \cup G = \{a, b, c, 1, 2, \ldots, N\}$ семейство $\mathcal{H}$ четырёхэлементных подмножеств четырёх видов:

1) $H = \{a, u, v, w\}$, где $\{u, v, w\} \in S$;
2) $H' = \{b, i, j, k\}$, где $\{i, j, k\} \in S'$;
3) $H'' = \{c, x, y, z\}$, где $\{x, y, z\} \in S''$;
4) $H''' = \{a, b, c, t\}$, где $t \in G$.

Утверждение 2. Семейство $\mathcal{H}$ удовлетворяет аксиомам гиперплоскостей матроида, оно не является семейством блоков никакой блок-схемы, причём двойственный матроид — однородный с мощностью циклов, равной $n = N - 1$.

Таким образом описывается конструкция контрпримера. На данный момент рассмотрены линейные системы с $N = 2^n - 1$, а также системы с $N = 9$ и нелинейные с $N = 13$. Оказалось, что при $N = 7$ таких S, S', S'' нет, при $N = 9$, 13 и 31 такие системы существуют, при $N = 15$ — пока неизвестно.

Системы троек Штейнера на N элементах существуют тогда и только тогда, когда $N = 1 \pmod 6$ или $N = 3 \pmod 6$ [5].

Утверждение 3. При $N = 9$ существуют системы троек Штейнера S_9, S'_9, S''_9 без общих троек.

Доказательство и построение преобразований, преломляющих прямые, производится методом решения задачи блокировки прямых [6], поскольку система троек S_9 есть семейство прямых на аффинной плоскости порядка три.

Утверждение 4. Биекции

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 13 & 1 & 2 & 4 & 8 & 12 & 11 & 10 & 7 & 6 & 9 & 5 & 3 \end{pmatrix},$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 6 & 10 & 2 & 11 & 3 & 1 & 12 & 4 & 5 & 7 & 13 & 9 \end{pmatrix},$$

$$f(g^{-1}) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 7 & 4 & 9 & 1 & 8 & 5 & 3 & 11 & 2 & 13 & 10 & 6 \end{pmatrix},$$

преобразующие стандартные тройки S_{13} первого типа [5], являются преломляющими.

Пусть $f(u \oplus v) \neq f(u) \oplus f(v)$ для любых различных ненулевых u и v из F_2^n, при этом в линейных системах троек Штейнера $F(0) = 0$. Это равносильно тому, что f преобразует любое двумерное подпространство пространства F_2^n в четырёхэлементное подмножество, содержащее нуль, но не являющееся двумерным подпространством, и является необходимым условием для APN-биекции f, сохраняющей нуль.

Если A и B — линейные невырожденные преобразования пространства F_2^n, то для суперпозиции биекций AfB имеем $A(f(B(u \oplus v))) = A(f(Bu \oplus Bv)) \neq A(f(Bu) \oplus \oplus f(Bv)) = Af(Bu) \oplus Af(Bv)$, $A(f(B(0))) = 0$, то есть AfB тоже обладает этим свойством.

Нетрудно проверить, что в $\mathrm{GF}(2^n)$ при $n = 3$ (т. е. $N = 7$) суперпозиция любых двух преломляющих биекций не является преломляющей. Поэтому представляет интерес случай $n > 3$.

Утверждение 5. Функция $F(u) = u^{-3}$ не сохраняет двумерные линейные подпространства в $\mathrm{GF}(2^n)$ при нечётном n, т. е. является преломляющей, тогда и только тогда, когда $\mathrm{GF}(2^n)$ не содержит $\mathrm{GF}(2^3)$, то есть n не делится на 3.

Утверждение 6. При нечётном n, где n не делится на 3, функции $f(u) = u^3$ и $F(u) = u^{-3}$ являются преломляющими вместе с функцией $g(u) = u^{-1}$.

Это утверждение вместе с утверждениями 1 и 2 позволяет строить однородные матроиды мощности $2^n + 2$, удобные для использования в схемах разделения секрета, не сводящиеся к блок-схемам, для нечётных $n \geqslant 5$ при помощи систем линейных троек Штейнера с квазигрупповой операцией $\oplus$.

Однако поскольку APN-биекции, сохраняющие нуль, являются преломляющими, стоит отметить отрицательный результат.

Утверждение 7. Биекция $F(u) = u^{-3}$ не является APN-функцией.

ЛИТЕРАТУРА

1. *Медведев Н. В., Титов С. С.* Об однородных матроидах и блок-схемах // Прикладная дискретная математика. Приложение. 2017. № 10. С. 21–23.
2. *Идрисова В. А.* Векторные 2-в-1 функции как подфункции взаимно однозначных APN-функций // Прикладная дискретная математика. Приложение. 2018. № 11. С. 39–41.
3. *Виткуп В. А.* О специальном подклассе векторных булевых функций и проблеме существования APN-перестановок // Прикладная дискретная математика. Приложение. 2016. № 9. С. 19–21.
4. *Фролова А. А.* Итеративная конструкция APN-функций // Прикладная дискретная математика. Приложение. 2013. № 6. С. 24–25.
5. *Холл М.* Комбинаторика: пер. с англ. М.: Мир, 1970. 424 с.
6. *Ведунова М. В., Игнатова А. О., Геут К. Л.* Блокировка линейных многообразий и тройки Штейнера // Прикладная дискретная математика. Приложение. 2019. № 12. С. 93–95.

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/13/2

ОБ ОДНОРОДНЫХ МАТРОИДАХ, СООТВЕТСТВУЮЩИХ БЛОК-СХЕМАМ

Н. В. Медведев, С. С. Титов

Исследуются взаимосвязи однородных матроидов и блок-схем. Эта задача связана с изучением структур доступа идеальных совершенных схем разделения секрета. Под однородностью матроида понимается одинаковая мощность его циклов, при этом, возможно, не все подмножества этой мощности являются циклами. Для мощности циклов пять доказано, что однородный связный разделяющий матроид является равномерным. При этом если матроид связный и разделяющий, то двойственный ему матроид будет простым. Доказано, что если каждый цикл однородного разделяющего связного матроида является его гиперплоскостью, то ему соответствует блок-схема.

Ключевые слова: *однородные матроиды, схемы разделения секрета, блок-схемы, циклы.*

На множестве M определён матроид, если некоторые его подмножества названы независимыми (остальные — зависимыми), причём удовлетворяются аксиомы матроида; так, в терминах циклов — минимальных (по включению) зависимых подмножеств из M — аксиом всего две: 1) нет цикла в цикле, т. е. если C, D — циклы и $C \subseteq D$, то $C = D$; 2) если $C_1 \neq C_2$ — циклы и $x \in C_1 \cap C_2$, то $C_1 \cup C_2 \setminus \{x\}$ содержит цикл [1–4]. Матроид называется связным, если для любых двух его элементов существует содержащий их цикл. Простым (или комбинаторной геометрией) называется матроид, в котором нет одноэлементных и двухэлементных циклов. Под однородностью матроида понимается одинаковость мощностей его циклов, равная n, где, возможно, не все n-элементные множества — циклы. При этом если все n-элементные подмножества — циклы, то такой матроид называется пороговым (равномерным) [5]. Матроид является разделяющим тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл C, т. е. $x \notin C$, $y \in C$. Любое максимальное независимое подмножество B,