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,

содержащееся в M, называется базой матроида M; дополнение цикла матроида — когиперплоскостью $\overline{C} = M \setminus C$.

Блок-схема $D(v, b, r, k, \lambda)$, согласно [6], — такое размещение v различных элементов по b блокам, что каждый блок содержит точно k различных элементов, каждый элемент появляется точно в r различных блоках и каждая пара различных элементов появляется в λ блоках. Блок-схема с $k = 3$ вполне естественно называется системой троек. При этом параметры должны удовлетворять аксиомам $3b = rv$, $2r = \lambda(v-1)$. Система троек с $\lambda = 1$ называется системой троек Штейнера. Условие $v \equiv 1, 3 \pmod 6$ необходимо и достаточно для существования штейнеровской системы троек.

Утверждение 1. Если каждый цикл однородного разделяющего связного матроида является его гиперплоскостью, то ему соответствует блок-схема.

Доказательство. Пусть $M = (E, \mathcal{C})$ — связный разделяющий однородный матроид с мощностью $n \geqslant 4$ циклов $C \in \mathcal{C}$, такой, что $n^* = |E| - |C| = |E| - n = 4$. Для каждой когиперплоскости H^*, т. е. гиперплоскости двойственного матроида $M^* = (E, \mathcal{H}^*)$, имеем $|H^*| = |E \setminus C| = 4$, $H^* \in \mathcal{H}^*$. Пусть $H_1^* \in \mathcal{H}^*$, $H_2^* \in \mathcal{H}^*$, $H_1^* \neq H_2^*$.

Предположим, что пересечение любых различных гиперплоскостей матроида M^* не более чем одноэлементно. Пусть $H_1^* \cap H_2^* = \{e\}$, $d \notin H_1^* \cup H_2^*$ (отметим, что ввиду $n \geqslant 4$, $n^* = 4$, $|E| = n + n^* \geqslant 8$ такой элемент d существует), тогда по второй аксиоме гиперплоскостей существует гиперплоскость $H^* \in \mathcal{H}^*$, такая, что $\{e, d\} \subset H^*$. По предположению $H^* \cap H_1^* = \{e\} = H^* \cap H_2^*$.

В силу разделимости матроида M каждый его элемент e принадлежит не менее чем двум когиперплоскостям. В самом деле: если $a \neq e$, то существует такой цикл C_a, что $a \in C_a$ и $e \notin C_a$, т. е. $e \in H_a^* = E \setminus C_a$; взяв $b \neq e$, $b \in H_a^*$, найдём цикл C_b, такой, что $b \in C_b$, $e \notin C_b$, т. е. $e \in H_b^* = E \setminus C_b$, причём $H_a^* \neq H_b^*$, так как $b \in H_a^*$, но $b \notin H_b^*$. Ввиду произвольности элемента d, в силу предположения получаем разбиение множества $E \setminus \{e\}$ множествами $H^* \setminus \{e\}$. Поскольку в качестве e можно взять любой элемент множества E, получаем блок-схему с параметрами $v = |E|$, $k = n^* = 4$, $\lambda = 1$, $r = \dfrac{v-1}{\lambda(k-1)} = \dfrac{v-1}{3}$, $b = \dfrac{vr}{k} = \dfrac{v(v-1)}{12}$. Итак, в этом случае получаем систему четвёрок Штейнера.

Каждая пара различных элементов в M^* независима, так как M^* простой, и поэтому существует единственная содержащая эту пару гиперплоскость H^*. Следовательно, ранг гиперплоскостей в M^* равен двум, а любое трёхэлементное множество — либо цикл, если оно входит в некоторую четвёрку, либо база, если не входит ни в какую четвёрку. Значит, ранг r^* матроида M^* равен трём.

Предположим, что пересечение любых двух различных гиперплоскостей матроида M^* не более чем двухэлементно. Пусть $H_1^* \cap H_2^* = \{e, f\}$, $e \neq f$. В силу связности матроида M для любых двух различных его элементов e и f существует содержащий их цикл C. Поскольку M — связный и разделяющий, то M^* простой; значит, $\{e, f\}$ — независимое множество в M^* и его можно дополнить до гиперплоскости $H_1^* = E \setminus C_1$, где C_1 — цикл в M.

Пусть $b \notin H_1^*$, тогда $\{e, f, b\}$ — независимое множество в M^* и его можно дополнить до гиперплоскости $H_2^* \neq H_1^*$, только если ранг гиперплоскостей равен трём. Следовательно, ранг M^* равен четырём. Допустим, что $\{a, b, c\}$ — трёхэлементный цикл. Тогда он лежит в плоскости ранга два (так как M^* простой), которая должна быть пересечением гиперплоскостей, что противоречит предположению. Значит, все трёхэлементные подмножества независимы и каждое из них является базой единственной

(в силу предположения) гиперплоскости в M^*, которая сама поэтому представляет собой цикл. Отсюда каждое четырёхэлементное подмножество — либо цикл в M^*, если оно является четвёркой (т. е. гиперплоскостью в M^*), либо база в M^*, если не является. Поэтому каждое пятиэлементное подмножество зависимо (и само является циклом, если не содержит четвёрку).

Предположим, что имеется пересечение двух гиперплоскостей матроида M^* по трёхэлементному множеству, $|H_1^* \cap H_2^*| = 3$. Тогда для $C_i = E \setminus H_i^*$ $(i = 1, 2)$ имеем $|C_1 \oplus C_2| = 2$ и поэтому каждое n-элементное подмножество $(n+1)$-элементного множества $F = (C_1 \cup C_2)$ является циклом. Если F не замкнуто (т. е. не является плоскостью матроида M), то существует $a \in E \setminus F$ и цикл $C \in \mathcal{C}$, такой, что $C \setminus F = \{a\}$, но тогда, очевидно, и в множестве $\{a\} \cup F$ каждое n-элементное подмножество является циклом. Обозначим $\{a, b, c\} = E \setminus F$; в силу разделимости матроида M существует цикл, содержащий b, но не содержащий c, однако тогда и в множестве $\{a, b\} \cup F$ каждое n-элементное подмножество — цикл.

В силу связности матроида M найдётся цикл, соединяющий оставшийся элемент c с множеством $\{a, b\} \cup F$, откуда замыкание множества F совпадает с носителем E матроида M, причём каждое n-элементное его подмножество есть цикл, а это означает равномерность матроида M.

Для того чтобы матроид M не был равномерным, необходимо, чтобы F было его плоскостью. Однако в силу разделимости матроида M существует цикл C_a, такой, что $a \in C_a$, $b \notin C_a$. Ввиду замкнутости F необходимо $c \in C_a$; аналогично — найдётся цикл C'_a, такой, что $a \in C'_a$, $c \notin C'_a$, но $b \in C'_a$. Это означает, что F — гиперплоскость матроида M, и поэтому $E \setminus F$ есть цикл двойственного матроида M^*. Значит, цикл $\{a, b, c\}$ есть плоскость (как пересечение гиперплоскостей) в M^* ранга два (так как M^* простой) и поэтому гиперплоскости матроида M^* имеют ранг равный трём.

Пусть $\{b_1, b_2, b_3\}$ — база произвольной гиперплоскости H^*, не являющейся циклом матроида M. Поскольку $|H^*| = 4$, имеется единственный цикл, скажем, $\{b_1, b_2, h\}$, при $H^* = \{b_1, b_2, b_3, h\}$. Однако тогда для любого элемента $x \in E$, $x \notin H^*$ имеем: множества $\{b_1, b_2, x\}$, $\{b_1, b_3, x\}$, $\{b_2, b_3, x\}$ независимы, так как множество $\{b_1, b_2, b_3, x\}$ независимо и поэтому является базой матроида M^*. Зафиксируем $x = b_0$. Тогда для любого $y \notin \{b_0, b_1, b_2, b_3\} = B^*$ найдётся единственный цикл C^*, такой, что $C^* \setminus B^* = \{y\}$, и при $y \neq h$ необходимо $b_0 \in C^*$. Поскольку мощность гиперплоскости матроида M не может быть меньше n, если он не равномерный, то мощность её дополнения не может быть больше четырёх. Отсюда $|C^*| \leqslant 4$, в случае равенства C^* — гиперплоскость матроида M^* и поэтому его дополнение — цикл матроида M, являющийся также и его гиперплоскостью. ■

Утверждение 2. Если матроид связный и разделяющий, то двойственный ему матроид простой.

Доказательство. Пусть матроид $M = (E, \mathcal{C})$ связный, $|E| \geqslant 2$; тогда двойственный матроид $M^* = (E, \mathcal{H}^*)$ не имеет одноэлементных циклов. Действительно: если $\{e\}$ — цикл в M^* (т. е. коцикл в M), то $H = E \setminus \{e\} \neq \varnothing$ — гиперплоскость в M. Однако для любого $h \in H$ существует, ввиду связности, цикл C, содержащий и e, и h. При этом $|C| > 1$, $|C \setminus H| = |\{e\}| = 1$, откуда e принадлежит гиперплоскости H — противоречие.

Пусть матроид M разделяющий, $|E| \geqslant 3$. Тогда M^* не имеет двухэлементных циклов. Действительно: если $\{e, f\}$ — двухэлементный цикл в M^*, то $H = E \setminus \{e, f\} \neq \varnothing$ — гиперплоскость в M. В силу того, что M разделяющий, существует цикл, содержа-

щий e, но не содержащий f, и существует цикл, содержащий f, но не содержащий e. Эти циклы не могут быть одноэлементными, т. е. $\{e\}$ и $\{f\}$, по первой аксиоме циклов. Следовательно, существует цикл C, такой, что $|C| > 1$ и, без ограничения общности, $e \in C$, $f \notin C$. Но тогда $|C \setminus H| = |\{e\}| = 1$, откуда e принадлежит гиперплоскости H — противоречие. ■

Таким образом, вариантом однородного неравномерного матроида, которому не соответствует блок-схема, может быть только реализация случая с возможностью пересечения его когиперплоскостей по трёхэлементному множеству.

Утверждение 3. Однородный связный разделяющий матроид с мощностью циклов $n = 5$ является равномерным.

Доказательство. Пусть $M = (E, \mathcal{C})$; при $|E| = 5$ матроид не разделяющий, а при $|E| = 6$ он, очевидно, равномерный, так как тогда любые два различных цикла пересекаются по четырёхэлементному множеству и поэтому любое пятиэлементное подмножество их объединения, равного E, является циклом. Аналогично при $|E| = 7$: если $E = \{a, b\} \cup C$, где C — цикл, не содержащий ни a, ни b, то в силу разделимости существует цикл C_1, содержащий a, но не содержащий b, и тогда $|C_1 \cap C| = 4$, откуда во множестве $\{a\} \cup C$ каждое пятиэлементное подмножество есть цикл. В силу связности существующий цикл, содержащий $\{a, b\}$, пересекается с любым циклом, содержащим b, но не содержащим a, по четырёхэлементному множеству, откуда вытекает равномерность матроида M. Эти же рассуждения применимы при $|E| = 8$.

Пусть теперь $|E| \geqslant 9$, $e \in E$ — произвольный элемент матроида, $D \in \mathcal{C}$ — произвольный его цикл, не содержащий e. Тогда в силу связности этот цикл может быть представлен в виде $D = (C_1 \cup C_2) \setminus J_e(C_1, C_2)$, где C_1, C_2 — циклы, содержащие e, $J_e(C_1, C_2) = \bigcap\{C : e \in C \subset (C_1 \cup C_2)\}$.

Допустим, существует такой цикл D, что нет циклов, содержащих e и не пересекающихся с D по четырёхэлементному множеству. Отсюда $|C_1 \cap C_2| < 4$, и из $|D| = |C_1| = |C_2| = n = 5$ вытекает, что $|C_1 \cap C_2| > |J_e(C_1, C_2)| \geqslant 2$. Поэтому $|C_1 \cap C_2| = 3$, $|J_e(C_1, C_2)| = 2$.

Пусть $J_e(C_1, C_2) = \{e, f\}$, $C_1 \cap C_2 = \{e, f, g\}$. Тогда $D = (C_1 \oplus C_2) \cup \{g\}$ и существует такой цикл $C \subset (C_1 \cup C_2)$, что $\{e, f\} \subset C$, $g \notin C$. Отсюда следует, что $|(C_1 \oplus C_2) \cap C| = 3$. Однако тогда либо $|C_1 \cap C| = 4$, либо $|C_2 \cap C| = 4$.

Пусть, без ограничения общности, $|C_1 \cap C| = 4$. Тогда в шестиэлементном множестве $(C_1 \cup C)$ каждое пятиэлементное множество есть цикл, в том числе $C' = (D \cap (C_1 \cup \cup C)) \cup \{e\}$. Однако ясно, что $|C' \cap D| = 4$ вопреки предположению о D и e. Итак, от противного утверждение доказано. ■

Представленный подход может быть применён к решению более сложных задач обобщения связи блок-схем и однородных матроидов.

ЛИТЕРАТУРА

1. *Асанов М. О., Баранский В. А., Расин В. В.* Дискретная математика: графы, матроиды, алгоритмы. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 288 с.
2. *Welsh D. J. A.* Matroid Theory. London: Academic Press, 1976.
3. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
4. *Beimel A. and Livne N.* On matroids and non-ideal secret sharing // TCC 2006. LNCS. 2006. V. 3876. P. 482–501.

5. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 11(1). Research Paper 72. 16 p.
6. *Холл М.* Комбинаторика. М.: Мир, 1970.

УДК 511.48 DOI 10.17223/2226308X/13/3

АЛГОРИТМ ВЫЧИСЛЕНИЯ ЭЛЕМЕНТА ШТИКЕЛЬБЕРГЕРА ДЛЯ МНИМЫХ МУЛЬТИКВАДРАТИЧНЫХ ПОЛЕЙ

Д. О. Олефиренко, Е. А. Киршанова, Е. С. Малыгина, С. А. Новоселов

Представлен алгоритм вычисления идеала Штикельбергера для мультиквадратичного поля $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, где $d_i \equiv 1 \pmod 4$, $i = 1, \ldots, n$, и d_i попарно взаимно просты. Мы алгоритмизируем идеи, описанные в работе Р. Кучеры 1996 г., доказываем корректность полученных алгоритмов и анализируем их сложность. Для $2^n = [K : \mathbb{Q}]$ алгоритм работает за время $\widetilde{\mathcal{O}}(2^n)$. Полученный результат полезен для решения криптоаналитических задач поиска короткого вектора в идеалах мультиквадратичных полей.

Ключевые слова: *мультиквадратичные поля, идеал Штикельбергера, элемент Штикельбергера, задача поиска короткого вектора.*

Введение

Получение идеала Штикельбергера в явном виде является важной алгоритмической задачей в вычислительной теории чисел, в теории групп классов и, с недавних пор, в криптоанализе. Для числового поля K идеал Штикельбергера I — идеал групповой алгебры $\mathbb{Z}[G_K]$, где $G_K = \mathrm{Gal}(K/\mathbb{Q})$ — группа Галуа поля K. Полезное свойство I заключается в том, что под действием элементов I на Cl_K — группу классов идеалов K — любой класс становится тривиальным (иначе говоря, J^σ — главный идеал для любого $\sigma \in I$ и любого идеала J кольца целых $\mathcal{O}_K$ числового поля K).

Для кругового поля $K = \mathbb{Q}(\zeta_n)$ идеал Штикельбергера, рассматриваемый как решётка в $\mathbb{Z}^n$ с помощью вложения $\mathbb{Z}[G_K] \hookrightarrow \mathbb{Z}^n$, обладает «хорошим» базисом. Явный вид этого базиса описан, например, в [1]. Это свойство идеала Штикельбергера в сочетании с 1) «обнуляющим» действием элементов идеала на целые идеалы $\mathbb{Z}[\zeta_n]$ и 2) существованием (относительно) быстрого алгоритма нахождения короткого вектора в *главных* идеалах $\mathbb{Z}[\zeta_n]$ позволило получить алгоритм нахождения короткого вектора в идеалах кольца целых круговых полей [1]. В современном криптоанализе нахождение короткого вектора в решётках является основополагающей задачей.

Именно приложение идеала Штикельбергера в криптоанализе является нашей главной мотивацией для его изучения. Ввиду большой группы Галуа интересными полями являются мультиквадратичные. Недавние работы по эффективному вычислению короткого вектора в мультиквадратичных полях [2] и по вычислению группы классов [3] подводят к вопросу нахождения коротких векторов в *произвольных* идеалах. Следуя примеру круговых полей, логично обратить внимание на структуру идеала Штикельбергера для мультиквадратичных расширений.

В работе предлагается алгоритм вычисления идеала Штикельбергера для мультиквадратичного поля $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, где $d_1 \equiv d_2 \equiv \ldots \equiv d_n \equiv 1 \pmod 4$ и d_i попарно взаимно просты. Алгоритм имеет сложность $\widetilde{\mathcal{O}}(2^n)$, а так как $[K : \mathbb{Q}] = 2^n$, то даже для криптографически значимых степеней он эффективен. В основе алгорит-