О схемах разделения секрета и однородных матроидах

Н.В. Медведев
itcrypt@gmail.com

С.С. Титов
sergey.titov@usaaa.ru

Уральский государственный университет путей сообщения (Екатеринбург)

Аннотация

Работа посвящена исследованию однородных матроидов, т.е. таких, которые имеют циклы одинаковой мощности. Рассмотрены некоторые плоскости таких матроидов. Установлена их связь с блок-схемами. Дано частичное описание матроидов коранга три, а так же поставлены задачи для дальнейшего исследования.

Ключевые слова: однородные структуры доступа; схемы разделения секрета; матроиды; циклы.

1 Введение

Разграничение доступа на основе схем разделения секрета (СРС) состоит в том, чтобы заранее заданные (разрешенные) коалиции участников могли однозначно восстановить секрет, а неразрешенные – не получали никакой дополнительной информации, к имеющейся априорной, о возможном значении секрета, такие СРС называются совершенными. Идеальными называются СРС, где размер доли секрета, предоставляемый участнику, не больше размера самого секрета. Если разрешенными коалициями являются любые множества из k или более элементов, то такие СРС называются пороговыми "k из N" СРС, где N – количество всех участников [1, 2, 3].

Общая проблема описания матроидов, соответствующих СРС, пока не решена [1]. Актуальной задачей является описание однородных (*homogeneous* [4]) СРС, т.е. таких, где мощность всех разрешенных коалиций k, но, возможно, не все k-элементные множества входят в структуру доступа СРС.

Как известно [1, 5], разрешенные коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и дает структуру доступа.

2 Основные понятия и термины

Напомним [6, 7], что на множестве E определен матроид M, 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 $C \subset D$, 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. Под N будем понимать мощность матроида M, т.е. $N = |E|$. Любое максимальное независимое подмножество B, содержащееся в E, называется базой матроида M. Дополнение базы матроида будем называть кобазой $\overline{B} = E \setminus \{B\}$, и, аналогично, дополнение цикла матроида – антицикл (когиперплоскость) $\overline{C} = E \setminus C$. Из [8] известно, что аффинные и проективные пространства являются матроидами над $GF(q)$ с гиперпространствами в качестве антициклов. Рангом матроида M называется мощность любой его базы. Ранговая функция двойственного матроида M^* называется коранговой функцией (корангом) матроида M

In: G.A. Timofeeva, A.V. Martynenko (eds.): Proceedings of 3rd Russian Conference "Mathematical Modeling and Information Technologies" (MMIT 2016), Yekaterinburg, Russia, 16-Nov-2016, published at http://ceur-ws.org

[6]. 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 [6]. Под однородностью матроида понимается одинаковость мощностей его циклов n, где, возможно, не все n-элементные множества – циклы. При этом, если все его n-элементные подмножества – циклы, то такой матроид называется пороговым (равномерным). Ранее в [9] матроиды были названы почти пороговыми с близкой мощностью циклов, т.е. n или $n+1$. Матроид назовем разделяющим тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл C, т.е. $x \notin C$, $y \in C$.

3 Некоторые свойства однородных матроидов

В представленном ниже подходе к описанию однородных матроидов большую роль играют арифметические соотношения между параметрами характеризующих его объектов.

Пусть $M = (E, \mathcal{C})$ – связный разделяющий матроид на множестве E с семейством циклов $\mathcal{C}$. Пусть $N = |E| > n$, и пусть M – однородный, т.е. все его циклы C имеют мощность n:

$$C \in \mathcal{C} \Rightarrow |C| = n. \tag{1}$$

Если $a, b \in E$, $a \neq b$, то, в силу того, что M – разделяющий, существует цикл C_0 такой, что $a \in C_0$, $b \notin C_0$. В силу того, что M – связный, существуют такие два цикла C_1, C_2, что $C_1 \neq C_2$, $b \in C_1$, $b \in C_2$ и

$$C_0 = D_b(C_1, C_2) = (C_1 \cup C_2) \setminus J_b(C_1, C_2), \tag{2}$$

где [5]

$$J_b(C_1, C_2) = \bigcap \{C : b \in C \subset (C_1 \cup C_2)\}. \tag{3}$$

Из (2) вытекает, что

$$C_0 = (C_1 \cap C_0) \cup (C_2 \cap C_0). \tag{4}$$

Следовательно, $|C_1 \cap C_0| + |C_2 \cap C_0| \geq |C_0| = n$, и поэтому для $C_0' = C_1$ или для $C_0' = C_2$ выполняется неравенство $|C_0' \cap C_0| \geq \lceil n/2 \rceil$. Итак, доказано

Утверждение 1. В связном разделяющем однородном матроиде для любых двух различных элементов a, b и любого цикла C, содержащего a, но не содержащего b, существует цикл C', содержащий b и такой, что

$$|C \cap C'| \geq \lceil n/2 \rceil = \lfloor n + 1/2 \rfloor. \tag{5}$$

Пусть $e \in E$ – любой элемент и $C_1 \neq C_2$ – два содержащих его различных цикла. Согласно определению

$$J_e(C_1, C_2) = \bigcap \{C : e \in C \subset (C_1 \cup C_2)\}. \tag{6}$$

Поскольку

$$J_e(C_1, C_2) \subset (C_1 \cap C_2), \tag{7}$$

имеем

$$|D_e(C_1, C_2)| = |(C_1 \cup C_2) \setminus J_e(C_1, C_2)| \geq |(C_1 \cup C_2) \setminus (C_1 \cap C_2)| = |C_1 \oplus C_2|. \tag{8}$$

Следовательно, $D_e(C_1, C_2)$ может быть минимальным по включению (и, значит, циклом) только если $n = |D_e(C_1, C_2)| \geq |C_1 \oplus C_2|$.

Пусть F – максимальное по включению подмножество в E, в котором каждое n-элементное подмножество является циклом. Можно считать, что $|F| \geq n$.

Утверждение 2. Множество F является подпространством матроида M.

Доказательство. От противного, если F не замкнуто, то существует $e \in E \setminus F$, лежащий в замыкании F, т.е. существует такой цикл C_1, что $\{e\} = C_1 \setminus F$. Возьмем любой элемент $d \in F \setminus C_1$. Тогда $C_2 = \{d\} \cup (C_1 \cap F) \subset F$, и, поскольку $|C_2| = n$, то по предположению C_2 является циклом. Значит, $C_1 \oplus C_2 = \{e, d\}$, и поэтому любое n-элементное подмножество в $\{e, d\} \cup (C_1 \cap C_2)$ является циклом, т.е. любой элемент x

в $C_1 \setminus \{e\}$ можно заменить на любой элемент $d \in F \setminus C_1$, и при этом множество $\{e\} \cup (C_1 \setminus \{x\}) \cup \{d\}$ также будет циклом. Отсюда вытекает, что любое n-элементное подмножество в $\{e\} \cup F$ есть цикл, что противоречит максимальности F.

Поскольку M – не пороговый (не равномерный), то $F \neq E$. Для каждого $a \in E \setminus F$ обозначим через $k(a)$ минимальную мощность множества $C' \setminus F$ по всем таким циклам $C' \in \mathcal{C}$, что $a \in C'$. Согласно утверждению 1 имеем

$$k(a) \leq n - \lceil n/2 \rceil \tag{9}$$

Поскольку F – подпространство матроида, имеем $1 < k(a)$.

Пусть k – минимальное такое число, т.е. $k = \min k(a), a \in E \setminus F$. Из предыдущего ясно, что $2 \leq k \leq n - \lceil n/2 \rceil$. Если $k(a_1) = k$, т.е. на элементе $a_1 \in E \setminus F$ этот минимум достигается, то существует такой цикл C', что $C' \setminus F = \{a_1, ..., a_k\}$, $|C' \setminus F| = k$. По утверждению 1 имеем $C' \cap F \neq \oslash$. Дополняя это множество $C' \cap F$ до подмножества $C \subset F$ мощности n, можем считать $C' = \{a_1, ..., a_k, f_1, ..., f_{n-k}\}$, $C = \{f_1, ..., f_{n-k}, ..., f_n\} \in \mathcal{C}$. Поскольку никакое подмножество в $\{a_1, ..., a_k\}$ мощности $(k-1)$ не равно $(C'' \setminus F)$ ни для какого $C'' \in \mathcal{C}$, то любое такое подмножество вместе с любым $(n-1)$-элементным подмножеством в F является независимым и, следовательно, есть база некоторого подпространства F'. Ясно, что $F \subset F'$ и $\mathrm{rank}F' = (k-1)+(n-1) = n+k-2$. Следовательно, в любом $(n-1)$-элементном подмножестве множества F существует единственное его $(n-k)$-элементное подмножество D такое, что $\{a_1, a_2, ..., a_k\} \cup D$ – цикл (достаточно для этого в базу F' включить элементы $a_2, ..., a_k$). Введем во множестве $C = \{f_1, ..., f_n\} \subset F$ следующее бинарное отношение: $u \equiv v$ тогда и только тогда, когда в $C \setminus \{u\}$ и в $C \setminus \{v\}$ такое подмножество D одно и то же. Легко проверяется рефлексивность, симметричность и транзитивность этого отношения, т.е. это – отношение эквивалентности. Соответствующее ему разбиение множества C имеет, очевидно, одинаковые мощности классов эквивалентности, а именно $n - (n-k) = k$, т.к. мощность каждого такого D равна $(n-k)$.

Следовательно, $\{a_1, ..., a_k\}$ задает разбиение любого n-элементного подмножества $C \subset F$ на k-элементные подмножества, дополнение каждого из которых до C, объединенное с $\{a_1, ..., a_k\}$, есть цикл. Отсюда вытекает

Утверждение 3. Мощность циклов n делится на k.

Теперь допустим, что $|F| \geq n+1$. Взяв $G \subset F$, $|G| = n+1$, видим, что $A \dot{\cup} B$ есть база в F', где

A – любое такое подмножество в $\{a_1, ..., a_k\}$, что $|A| = k-1$;

B – любое такое подмножество в G, что $|B| = n-1$;

$\dot{\cup}$ – обозначает объединение непересекающихся множеств.

Следовательно, для любых двух различных элементов $x, y \in G$, $x \neq y$, существует единственный цикл $C_{xy} = \{a_1, ..., a_k\} \dot{\cup} D_{xy}$, где $D_{xy} \subset G \setminus \{x, y\} = B_{xy}$, $|D_{xy}| = n-k$.

Рассмотрим случай минимального значения $k = 2$. По утверждению 3 в этом случае n четно. Здесь $|D_{xy}| = n - k = n - 2$, так что D_{xy} получается удалением из G еще одного, кроме x и y, однозначно определенного по ним элемента z:

$$D_{xy} = G \setminus \{x, y, z\}. \tag{10}$$

Значит, на G имеется семейство троек $\{x, y, z\}$, которые удовлетворяют следующим свойствам:

1. Если $x \in G$, то $|G \setminus \{x\}| = n$, и поэтому имеется разбиение $C = G \setminus \{x\}$ на двухэлементные подмножества, каждое из которых в объединении с $\{x\}$ дает такую тройку. Следовательно, каждый элемент x содержится ровно в $r = n/2$ тройках.

2. В силу единственности D_{xy} каждая пара x, y различных элементов содержится точно в одной тройке $(\lambda = 1)$.

3. Более того, для разных $x_1 \neq x_2$ ни один смежный класс разбиения множества $G \setminus \{x_1\}$ не совпадает ни с одним смежным классом разбиения множества $G \setminus \{x_2\}$, т.к. иначе имелись бы два цикла C_1 и C_2 с $C_1 \oplus C_2 = \{x_1, x_2\}$, откуда вытекало бы, что каждое n-элементное подмножество в $C_1 \cup C_2$ – есть цикл, в том числе циклы C' и C'' такие, что $C' \setminus F = \{a_1\}$, $C'' \setminus F = \{a_2\}$ что противоречит замкнутости F. Следовательно, число таких троек равно $\frac{n(n+1)}{3 \cdot 2}$.

Из этих свойств вытекает, что полученное семейство троек образует блок-схему [10] с параметрами:

$(n+1)$ – количество элементов;

$\frac{(n+1)n}{6}$ – количество блоков (троек);

3 – количество элементов в блоке (в тройке);

$r = \frac{n}{2}$ – количество блоков (троек), содержащий любой данный элемент;

$\lambda = 1$ – каждая пара различных элементов содержится точно в одном блоке (в тройке).

Итак, получаем блок-схему $D(n+1, \frac{(n+1)n}{6}, \frac{n}{2}, 3, 1)$ (см. раздел 15.4 в [10]), т.е. систему троек Штейнера. Такие тройки существуют, как известно, при $n \equiv 0(\mathrm{mod}\ 6)$ или $n \equiv 2(\mathrm{mod}\ 6)$. Таким образом, однородные матроиды оказываются связанными с блок-схемами.

4 Обобщение конструкции

Проведем проверку аксиом когиперплоскостей для троек Штейнера. Пусть $H_1^* = \{x, y, z\}$ и $H_2^* = \{u, v, w\}$, где $|\{x, y, z\}| = |\{u, v, w\}| = 3$, $xy = z, uv = w$. Определяем циклы $C_1 = E \setminus \{x, y, z\}$ и $C_2 = E \setminus \{u, v, w\}$ так, что $e \in C_1 \cap C_2$ и $e \in E \setminus \{x, y, z, u, v, w\}$. Следовательно, существуют d, c такие, что $C = E \setminus \{c, d, e\} \in \mathcal{C}$. Действительно, если $H_1^* \cap H_2^* = \oslash$, то $C_1 \cup C_2 \setminus \{e\} = E \setminus \{e\}$ и в качестве $H^* = E \setminus C$ подойдет любая тройка $\{c, d, e\}$, где $cd = e$. Если $H_1^* \cap H_2^* \neq \oslash$, то при $C_1 \neq C_2$ имеем в точности $|H_1^* \cap H_2^*| = 1$.

Пусть $H_1^* \cap H_2^* = \{d\}$, имеем $e \neq d$, т.к. $e \in E \setminus \{H_1^* \cup H_2^*\}$. Значит, если обозначить $c = ed$, то $|\{c, d, e\}| = 3$, можно положить $H^* = \{c, d, e\}, C = E \setminus H^*$. Итак, доказано

Утверждение 4. Семейство троек Штейнера удовлетворяет аксиомам гиперплоскостей.

Матроид, у которого когиперплоскости – тройки Штейнера, является однородным связным и разделяющим. Рассмотрим каждое из этих свойств. Очевидно, что матроид является однородным, т.к. $k = 3$ и мощности когиперплоскостей будут одинаковыми.

Докажем, что матроид является связным. При $x \neq y$, $z = xy$, т.е. $\{x, y, z\}$ – тройка Штейнера. Как известно, при $N > 3$ имеем $N \geq 7$. Если, от противного, любая тройка Штейнера пересекается с $\{x, y\}$, то в каждой такой тройке есть либо x, либо y. При $N > 3$ существует такой u, что $u \notin \{x, y, z\}$, тогда $uz = v$. Ясно, что $u \neq z$, т.к. $\{u, v, z\}$ – тройка Штейнера, $v \neq x$, иначе $u = y$, и $v \neq y$, т.к. иначе было бы $u = x$. Итак, построена тройка $\{u, v, z\}$, не содержащая ни x, ни y, что и требовалось доказать.

Докажем, что матроид является разделяющим. Пусть $\{x, y, z\}$ – тройка Штейнера, при $N > 3$ существует такое u, что $u \notin \{x, y, z\}$, тогда $yu = v$. Если $v = x$, то $u = z$, вопреки $u \notin \{x, y, z\}$. Если же $v = z$, то $u = x$, вопреки $u \notin \{x, y, z\}$. Значит, тройка $\{u, v, u\}$ не содержит x, что и требовалось доказать.

Теперь при $k \geq 3$, $\lambda = 1$, $n = |E| - k$ рассмотрим блок-схему и проверим аксиомы гиперплоскостей для блоков.

Любая пара в единственном блоке $B = H^*$, $|B| = k$.

1) Если $H_1^* \cap H_2^* = \oslash, e \in E \setminus (H_1^* \cup H_2^*), C_1 \cup C_2 \setminus \{e\} = E \setminus \{e\}; C_i = E \setminus H_i^*$, то подойдет любая H^* такая, что $e \in H^*$.

2) Если $H_1^* \cap H_2^* \neq \oslash$, то при $|H_1^* \cap H_2^*| \geq 2$ имеем $H_1^* = H_2^*$, поэтому $0 < |H_1^* \cap H_2^*| < 2$, т.е. при $H_1^* \neq H_2^*$ имеем $|H_1^* \cap H_2^*| = 1$. Пусть $H_1^* \cap H_2^* = \{d\}$. Тогда нам надо найти H^* такую, что $\{d, e\} \subset H^*$. Из-за $\lambda = 1$ такая H^* существует и единственная. Проверка аксиом гиперплоскостей завершена. Итак, доказано

Утверждение 5. Блок-схема с $\lambda = 1$ задает когиперплоскости однородного связного разделяющего матроида.

Доказательство. Аналогично случаю при $k = 3$.

Очевидно, что для $\lambda = 2$ блок-схема не удовлетворяет аксиомам гиперплоскостей.

Это рассмотрение указывает на сложность задачачи описания однородных матроидов и позволяет поставить следующие задачи:

- описание блок-схем для однородных матроидов;
- построение СРС по однородному матроиду, построенному как блок-схема.

5 Однородные матроиды коранга три

В [11] дано описание однородных матроидов коранга три. При этом утверждение доказано в не явном предположении, что существует не более одной линии, проходящей через точку b, не лежащей на данной линии, и не пересекающейся с ней. Ниже дано уточненное изложение этого вопроса.

Определение *линии* bc: $x \in bc$ тогда и только тогда, когда во всех циклах, не содержащих ни b, ни c, нет и x.

Рассмотрим матроид, в котором любой цикл содержит элементы либо a, либо b, либо c, либо пару их, либо все три. (Значит, $\{a, b, c\}$ – кобаза). Из непороговости вытекает, что мощность m антициклов ≥ 3.

Пусть A_1, A_2 – циклы, такие, что $a \in A_1$, $a \in A_2$ ($b \notin A_i$, $c \notin A_i$), где $(i = 1, 2)$. Тогда если $A_1 \neq A_2$, то в $(A_1 \cup A_2) \setminus \{a\}$ есть цикл A, причем $a \notin A$, $b \notin A$, $c \notin A$ (противоречие с вышеописанным предположением).

Следовательно, существует единственный цикл A такой что $a \in A$, $b \notin A$, $c \notin A$. Аналогично – для элементов b, c матроида M и циклов B, C. Если a_1, a_2 таковы, что не существуют циклов, не содержащих $\{a_1, b, c\}$ или $\{a_2, b, c\}$, то A_i $(i = 1, 2)$ – единственный цикл, такой, что $a_i \in A_i$, $b \notin A_i$, $c \notin A_i$ $(i = 1, 2)$. Если $A_1 \cap A_2 \neq \oslash$, то при $A_1 \neq A_2$ эта единственность нарушается для любого $a \in A_1 \cap A_2$ по второй аксиоме циклов. Если же $A_1 \cap A_2 = \oslash$, то цикл A_1 не содержит $\{a_2, b, c\}$, и A_2 не содержит $\{a_1, b, c\}$ вопреки предположению. Итак, существует единственный цикл A, не содержащий ни b, ни c, и поэтому можно определить лишь $bc = \overline{A}$.

Поэтому $bc = \overline{A}$, т.е. для каждой линии (вне которой есть хотя бы одна точка) существует единственный цикл, дополнением которой он является.

Утверждение 6. Вне каждой линии есть точка.

Доказательство: В противном случае не существовали бы три точки a, b, c.

Предположим, как было указано выше, что для любой точкивне любой данной линии, существует не более одной линии, содержащей эту точку и не пересекающейся с данной линией.

Следствие 1. $N = |M| = n + |bc|$ для любых точек $b \neq c$ и определяемой ими линии bc.

Следствие 2. Если $w \in uv$, $u \neq v \neq w \neq u$, то $u \in vw$, $v \in uw$, как дополнение единственного цикла.

Итак, циклов (и антициклов) всего

$$\frac{C_N^2}{C_{N-n}^2} = \frac{N(N-1)}{(N-n)(N-n-1)}.$$

Пусть $m = N - n$ есть мощность антициклов, т.е. количество точек на каждой линии. Тогда пары точек $u \neq v$ и $a \neq b$ определяет одну и ту же линию, когда они обе ей принадлежат, и таких пар на линии всего C_m^2. А всего пар различных элементов матроида – C_N^2. Поэтому количество всех линий как антициклов равно

$$\frac{C_N^2}{C_m^2} = \frac{N(N-1)}{m(m-1)} = \frac{N(N-1)}{(N-n)(N-n-1)}.$$

Зафиксируем точку b и линию ac, $b \notin ac$. Тогда, поскольку для каждой точки x на линии ac получаем $(m-1)$ точку на линии bx (кроме b), итого получаем (поскольку все эти линии разные для разных x, т.к. иначе было бы $b \in ac = x_1x_2$) всего $m(m-1)+1$ точек. Если этими точками исчерпываются все элементы матроида, то $N = m^2 - m + 1$, и линий всего

$$\frac{(m^2 - m + 1)(m^2 - m)}{m(m-1)} = m^2 - m + 1$$

("проективный случай" проективная плоскость порядка $(m-1)$).

Итого получаем $N = [m(m-1)+1] + (m-1) = (m+1)(m-1) + 1 = (m^2-1) + 1 = m^2$ ("аффинный случай" – аффинная плоскость порядка m), а линий всего

$$\frac{N(N-1)}{m(m-1)} = \frac{m^2(m^2-1)}{m(m-1)} = m(m+1).$$

Случай 1.

Далее произведем проверку аксиом проективной плоскости, взяв линии в качестве прямых.

Аксиома 1. Две различные точки определяют единственную прямую.

Доказательство следует из разделимости матроида.

Аксиома 2. Две прямые пересекаются в единственной точке.

Пусть однородный матроид M мощности $|M| = N = m^2 - m + 1$, где m – мощность линий (антициклов), и a, b, c – его элементы, не содержащиеся в одном антицикле. По описанному выше построению все точки (элементы матроида) исчерпываются точками линий, соединяющих точку b с точками ac.

Пусть $L_1 = \overline{C_1}$, $L_2 = \overline{C_2}$ – две разные линии, дополнения циклов C_1 и C_2, $C_1 \neq C_2$. Ясно, что если линии пересекутся в двух или более точках, то они совпадут (см. первую аксиому плоскости). Если же они не пересекутся, $L_1 \cap L_2 = \oslash$, то $C_1 \cup C_2 = M$.

Пусть $w \in M$ – любой элемент, C – цикл, содержащий w. Тогда линия $L = \overline{C}$ не проходит через w и содержит m точек. Линии, проходящие через w и через различные точки линии L, различны, и их всего m штук. Точек на всех этих линиях, как было вычислено выше, всего $N = m^2 - m + 1$. Следовательно, этими точками исчерпываются все элементы матроида, и других линий, проходящих через w, больше нет.

Итак, **доказано**:

Утверждение 7. Через любую точку w проходят ровно m линий.

Всего пар различных линий

$$C_N^2 = \frac{N(N-1)}{2} = \frac{(m^2-m+1)(m^2-m)}{2} = \frac{(m^2-m+1)m(m-1)}{2}.$$

Следовательно, количество пар различных линий, проходящих через любую данную точку, равно $C_m^2 = \frac{m(m-1)}{2}$. Умножая это количество на мощность матроида, получаем количество всех пар линий, имеющих непустое пересечение, и поскольку это число совпадает с количеством всех вообще пар линий, делаем вывод, что непересекающихся линий нет. Итак, доказано:

Утверждение 8. В "проективном случае" каждая пара различных линий пересекается в единственной точке.

Аксиома 3. Существуют четыре точки, никакие три из которых не лежат на одной линии.

Итак, пусть $m \geq 3$, точки a, b, c не лежат на одной линии (антицикле). Возьмем, поскольку $m \geq 3$, третью точку x на линии ac отличную от a и c. Соединим ее линией с b, и опять-таки пользуясь тем, что $m \geq 3$, третью точку d на линии bx, отличную от b и x. Из аксиомы 1 следует, что $d \notin ac$, $d \notin ab$, $d \notin bc$. По построению $a \notin bc$, $b \notin ac$, $c \notin ab$. Так, что $a \notin dc$, $a \notin db$, $b \notin dc$, $c \notin ad$, $b \notin ad$, $c \notin bd$, действительно, никакие три не лежат на одной линии. Итак, в самом деле в "проективном случае" получаем конечную проективную плоскость.

Случай 2.

Далее рассмотрим проверку аксиом аффинной плоскости.

Аксиома 1 совпадает с проективным случаем.

Аксиома 2. Через любую точку вне данной линии проходит единственная линия, не пересекающая данную (по [12]).

Пусть однородный матроид (в "аффинном случае") мощности $|M| = N = m^2$, где m – мощность антициклов, и a, b, c – его элементы, не содержащиеся в одном антицикле (как в вышеописанном построении). Все точки матроида исчерпываются точками линий, соединяющими точку b с точками ac и точками единственной линии, проходящей через b и не пересекающейся с ac. Таким образом, через точку b проходит всего $(m+1)$ линий. Ясно, что через любую точку w проходит не более $(m+1)$ линий, содержащих как раз $(m-1)(m+1)+1 = (m^2-1)+1 = m^2 = N$ точек. А так как через w и любую точку, отличную от w, можно провести единственную прямую, то, следовательно, через каждую точку проходят ровно $m+1$ линий, и так можно получить все точки матроида. Поэтому среди этих $(m+1)$ линий есть в точности одна, не пересекающая данную линию, в которой всего m точек.

Аксиома 3. Совпадает с проективным случаем.

По нашему предположению, этих линий не более одной.

Итак, доказано

Утверждение 9. Однородный связный разделяющий матроид коранга три, в котором для любой точки вне данного антицикла существует не более одного антицикла не пересекающегося с данным, является либо аффинной плоскостью порядка m, либо проективной плоскостью порядка $(m-1)$ с прямыми линиями в качестве антициклов.

6 Заключение

Итак, в работе показана связь однородных матроидов с блок-схемами, а именно с семейством троек Штейнера. Доказано, что блок-схема с параметром $\lambda = 1$ задает когиперплоскости однородного связного разделяющего матроида. Представлено частичное описание однородных матроидов коранга три. Сформулированы задачи для дальнейшего исследования однородных матроидов.

Список литературы

[1] *Vvedenie v kriptografiju* [Introduction to cryptography]. Pod obshh. red. V. V. Yashchenko. SPb, Piter, 2001. (in Russian) = *Введение в криптографию*. Под общ. ред. В. В. Ященко. СПб, Питер, 2001.

[2] G. R. Blackley, G. A. Kabatiansky. Generalized ideal secret sharing schemes and matroids. *Problemy peredachi informacii*, 33(3):102–110, 1997. (in Russian) = Г. Р. Блейкли, Г. А. Кабатянский. Обоб-

щенные идеальные схемы, разделяющие секрет, и матроиды. *Проблемы передачи информации*, 33(3):102–110, 1997.

[3] E. A. Bolotova, S. S. Konovalova, S. S. Titov. Properties of access control lattices, perfect ciphers and secret sharing schemes. *Problemy bezopasnosti i protivod. terrorizmu: materialy IV mezhdunar. nauch. konf.*, 2:71–86, 2009. (in Russian) = Е. А. Болотова, С. С. Коновалова, С. С. Титов. Свойства решеток разграничения доступа, совершенные шифры и схемы разделения секрета. *Проблемы безопасности и противод. терроризму: материалы IV междунар. науч. конф.*, 2:71–86, 2009.

[4] J. Marti-Farre, C. Padro. Secret sharing schemes on sparse homogeneous access structures with rank three. *Electronic Journal of Combinatorics*, 11(1), Research Paper 72, 2004.

[5] D. J. A. Welsh *Matroid Theory.* London, Academic press, 1976.

[6] M. O. Asanov, V. A. Baransky, V. V. Rasin. *Diskretnaja matematika: grafy, matroidy, algoritmy* [Discrete mathematics: graphs, matroids, algorithms]. Izhevsk: NIC Reguljarnaja i haoticheskaja dinamika, 2001. (in Russian) = М. О. Асанов, В. А. Баранский, В. В. Расин. *Дискретная математика: графы, матроиды, алгоритмы.* Ижевск: НИЦ Регулярная и хаотическая динамика, 2001.

[7] N. White. *Theory of Matroids.* Cambridge University Press, 1986.

[8] N. V. Medvedev, S. S. Titov. Problems of almost threshold secret sharing schemes. *Applied Discrete Mathematics*, 5:53–54, 2012. (in Russian) = Н. В. Медведев, С. С. Титов. Проблемы почти пороговых схем разделения секрета. *Прикладная дискретная математика*, 5:53–54, 2012.

[9] N. V. Medvedev, S. S. Titov. On almost threshold matroids and secret sharing schemes. *Vestnik UrFO. Bezopasnost v informacionnoj sfere*, 1(3):31–36, 2012. (in Russian) = Н. В. Медведев, С. С. Титов. О почти пороговых матроидах и схемах разделения секрета. *Вестник УрФО. Безопасность в информационной сфере*, 1(3):31–36, 2012.

[10] M. Hall. *Combinatorial Theory.* Blaisdell, Waltham, 1967. = М. Холл. *Комбинаторика.* Москва, Мир, 1970.

[11] N. V. Medvedev, S. S. Titov. On homogeneous ideal secret sharing schemes and matroids of corank three. *Vestnik UrFO. Bezopasnost v informacionnoj sfere*, 4(18):21–26, 2015. (in Russian) = Н. В. Медведев, С. С. Титов. Об однородных идеальных схемах разделения секрета и матроидах коранга три. *Вестник УрФО. Безопасность в информационной сфере*, 4(18):21–26, 2015.

[12] E. Artin. *Geometric algebra.* Bull. Amer. Math. Soc. 64, 1958. = Э. Артин. *Геометрическая алгебра.* Москва, Наука, 1969.

About secret sharing schemes and homogeneous matroids

Nikita V. Medvedev
Ural State University of Railway Transport (Yekaterinburg, Russia)

Sergei S. Titov
Ural State University of Railway Transport (Yekaterinburg, Russia)

Abstract. This research is devoted to homogeneous matroids, which have equal power of circuits. Some flats of such matroids are considered, as well as their connection with block-schemes. A partial description of homogeneous matroids of corank three is given. The authors set tasks for further research.

Keywords: homogeneous access structure, secret sharing schemes, matroids, circuits.