Результаты компьютерных вычислений

Вычисление функции роста группы C относительно X проведено по алгоритму из [5]. Для эффективного умножения элементов были задействованы полиномы Холла [8]. Алгоритм реализован на языке C++. В качестве инструмента распараллеливания использована библиотека OpenMP. Вычисления проводились на компьютере, имеющем 8-ядерный процессор и 64 Гб оперативной памяти под ОС Linux. Трансляция программы осуществлялась встроенным в систему компилятором gcc. Время вычисления функции роста составило примерно 36 ч.

Функция роста группы содержит в себе информацию о характеристиках соответствующего графа Кэли:

Следствие. $D_X(C) = 33$, $\overline{D}_X(C) \approx 26{,}1$.

ЛИТЕРАТУРА

1. *Кузнецов А. А., Кузнецова А. С.* Параллельный алгоритм для исследования графов Кэли групп подстановок // Вестник СибГАУ. 2014. № 1. С. 34–39.
2. *Even S. and Goldreich O.* The Minimum Length Generator Sequence is NP-Hard // J. Algorithms. 1981. No. 2. P. 311–313.
3. *Константинова Е. В.* Комбинаторные задачи на графах Кэли. Новосибирск: НГУ, 2010. 110 с.
4. *Havas G., Wall G., and Wamsley J.* The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459–470.
5. *Кузнецов А. А.* Об одном алгоритме вычисления функций роста в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2016. № 3. С. 116–125.
6. *Кузнецов А. А., Филиппов К. А.* Об одном автоморфизме порядка 2 бернсайдовой группы $B_0(2, 5)$ // Владикавказский математический журнал. 2010. № 4. С. 44–48.
7. *Шунков В. П.* О периодических группах с почти регулярной инволюцией // Алгебра и логика. 1972. № 4. С. 470–494.
8. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. № 1. С. 110–116.

УДК 519.151, 519.725, 519.165 DOI 10.17223/2226308X/10/7

ОБ ОДНОРОДНЫХ МАТРОИДАХ И БЛОК-СХЕМАХ

Н. В. Медведев, С. С. Титов

Работа посвящена вопросам, связанным с разграничением доступа посредством идеальных совершенных схем разделения секрета и матроидов. Рассматриваются однородные матроиды, т. е. такие, все циклы которых имеют одинаковую мощность, при этом, возможно, не все подмножества этой мощности являются циклами. Установлена их связь с блок-схемами, в том числе с семейством троек Штейнера, а именно доказано, что матроид, у которого когиперплоскости — тройки Штейнера, является однородным связным и разделяющим, если его мощность не меньше семи. Доказано, что блок-схема, в которой каждая пара различных элементов появляется в единственном блоке, задаёт когиперплоскости однородного связного разделяющего матроида. Выдвинуты гипотезы для дальнейшего исследования.

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

Разграничение доступа на основе схем разделения секрета (СРС) состоит в том, чтобы заранее заданные (разрешённые) коалиции участников могли однозначно вос-

становить секрет, а неразрешённые не получали никакой дополнительной (к имеющейся априорной) информации о возможном значении секрета. Такие СРС называются совершенными [1, 2]. Идеальными называются СРС, где размер доли секрета, предоставляемый каждому участнику, равен размеру самого секрета. Если разрешёнными коалициями являются любые множества из k или более элементов, то такие СРС называются пороговыми «k из N» СРС, где N — количество всех участников [1, 3, 4].

Как известно [1, 3, 5], разрешённые коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и даёт структуру доступа. Общая проблема описания матроидов, соответствующих СРС, пока не решена [1]. Актуальной задачей является описание однородных СРС [6], т. е. таких, где мощность всех разрешённых коалиций равна k, но, возможно, не все k-элементные множества входят в структуру доступа СРС. 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). Матроид называется связным, если для любых двух его элементов существует содержащий их цикл. Для исключения незаменимых участников идеальной СРС имеет смысл рассматривать только разделяющие матроиды. Матроид разделяющий тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл C, т. е. $x \notin C$, $y \in C$.

Теорема Зингера [7, 8] связывает конечные геометрии с блок-схемами. Это мотивирует к рассмотрению класса однородных матроидов, основанных на блок-схемах.

Будем понимать под блок-схемой, согласно [8], 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. При этом блок-схема с $k = 3$, $v \equiv 1, 3 \pmod 6$ и $\lambda = 1$ называется семейством троек Штейнера [8]. Заметим, что семейство троек Штейнера удовлетворяет аксиомам гиперплоскостей [9].

Утверждение 1. Матроид, у которого когиперплоскости — тройки Штейнера, является однородным связным и разделяющим, если его мощность не меньше семи.

Утверждение 2. Нетривиальная блок-схема с $\lambda = 1$ задает когиперплоскости однородного связного разделяющего матроида.

Семейства циклов и когиперплоскостей построенного таким образом однородного матроида оказываются дополнительными блок-схемами [8].

Утверждение 3. Блок-схема с $\lambda = 2$ не удовлетворяет аксиомам гиперплоскостей.

Приведённые утверждения позволяют выдвинуть следующие гипотезы.

Гипотеза 1. Однородный матроид определяется некоторой блок-схемой.

Гипотеза 2. Каждому однородному матроиду, основанному на блок-схеме, соответствует идеальная схема разделения секрета.

Таким образом, однородные матроиды оказываются связанными с блок-схемами и идеальными схемами разделения секрета.

ЛИТЕРАТУРА

1. Введение в криптографию / под общ. ред. В. В. Ященко. СПб.: Питер, 2001.

2. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2(2). С. 50–57.
3. *Блейкли Г. Р., Кабатянский Г. А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. 1997. Т. 33. № 3. С. 102–110.
4. *Болотова Е. А., Коновалова С. С., Титов С. С.* Свойства решеток разграничения доступа, совершенные шифры и схемы разделения секрета // Проблемы безопасности и противод. терроризму: материалы IV Междунар. науч. конф. М.: МЦНМО, 2009. Т. 2. С. 71–86.
5. *Welsh D. J. A.* Matroid Theory. Academic Press, 1976.
6. *Marti-Farre J. and Padro C.* Secret sharing schemes on sparse homogeneous access structures with rank three // Electronic J. Combinatorics. 2004. No. 1(1). Research Paper 72. 16 p.
7. *Singer J.* A theorem in finite projective geometry and some applications to number theory // Trans. Amer. Math. 1938. No. 17. P. 356–372.
8. *Холл М.* Комбинаторика. М.: Мир, 1970.
9. Theory of Matroids. Encyclopedia of Mathematics and its Applications / ed. N. White. Cambrige University Press, 1986. V. 26.

УДК 519.7 DOI 10.17223/2226308X/10/8

О МАКСИМАЛЬНЫХ МЕТРИЧЕСКИ РЕГУЛЯРНЫХ МНОЖЕСТВАХ[1]

А. К. Облаухов

Исследуются метрически регулярные подмножества булева куба. Доказано, что максимальные по мощности метрически регулярные множества имеют максимальное расстояние, равное единице, и являются дополнениями минимальных покрывающих кодов радиуса 1. Получена нижняя оценка суммы мощностей пары метрически регулярных множеств, являющихся метрическими дополнениями друг друга.

Ключевые слова: *метрически регулярное множество, метрическое дополнение, минимальный покрывающий код.*

Рассмотрим $\mathbb{F}_2^n$ — пространство двоичных векторов длины n. *Расстояние Хэмминга* $\mathrm{d}(x, y)$ между двумя векторами $x, y \in \mathbb{F}_2^n$ равно количеству координат, в которых эти векторы различаются.

Пусть $X \subseteq \mathbb{F}_2^n$ — произвольное множество, $y \in \mathbb{F}_2^n$ — произвольный вектор. Расстояние от y до X определяется как $\mathrm{d}(y, X) = \min\limits_{x \in X} \mathrm{d}(y, x)$. *Максимальным расстоянием* от множества X называется $\mathrm{d}(X) = \max\limits_{z \in \mathbb{F}_2^n} \mathrm{d}(z, X)$. Этот параметр множества также известен в теории кодирования как *радиус покрытия*. Множество X называется *покрывающим кодом* радиуса d, если $\mathrm{d}(X) = d$.

Рассмотрим множество $Y = \{y \in \mathbb{F}_2^n : \mathrm{d}(y, X) = \mathrm{d}(X)\}$ векторов, находящихся на максимальном расстоянии от X. Это множество называется *метрическим дополнением* [1] множества X и обозначается $\widehat{X}$. Если $\widehat{\widehat{X}} = X$, то множество X называется *метрически регулярным*.

Задача исследования максимальных и минимальных (по мощности) метрически регулярных множеств возникает на пути изучения *бент-функций*, множество которых является метрически регулярным [2]. Бент-функции часто используются в криптографии из-за высокой нелинейности, обеспечивающей повышенную устойчивость шифров

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.