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.

к криптографическим атакам, однако многие связанные с ними задачи остаются открытыми. Например, неизвестно точное количество бент-функций в общем случае, а существующие верхняя и нижняя оценки значительно разнятся по порядку.

В работе задача поиска максимального метрически регулярного множества сведена к задаче поиска минимального покрывающего кода радиуса 1, а также получены нижние оценки мощности метрически регулярных множеств с фиксированным расстоянием.

Теорема 1. Пусть A, B — пара метрически регулярных множеств, являющихся метрическими дополнениями друг друга. Тогда существует пара метрически регулярных множеств A_1, B_1, таких, что A содержится в A_1, B содержится в B_1, а A_1 и B_1 являются метрическими дополнениями друг друга и расстояние между ними равно единице.

Следствие 1. Максимальное по мощности нетривиальное метрически регулярное множество удалено от своего метрического дополнения на расстояние 1 и совпадает с дополнением минимального по мощности покрывающего кода радиуса 1.

Таким образом, задача поиска максимального по мощности метрически регулярного множества эквивалентна задаче поиска наименьшего покрывающего кода радиуса 1. В общем случае это открытая проблема теории кодирования [3]. Однако большинство представляющих интерес для исследования множеств имеет максимальное расстояние, большее единицы, поэтому для последующих результатов зафиксируем расстояние между множествами.

Утверждение 1. Пусть A, B — пара метрически регулярных множеств в булевом кубе, являющихся метрическими дополнениями друг друга и отстоящих друг от друга на расстояние d; M, N — мощности этих множеств соответственно. Тогда

$$M + N \geqslant \frac{2^{n+1}(n-2)}{n(n-1)^{d-1} + n - 4},$$

где n — размерность булева куба.

Выдвинута гипотеза о том, что всякий минимальный по мощности покрывающий код радиуса d является метрически регулярным множеством. При помощи компьютерных вычислений гипотеза проверена для минимальных покрывающих кодов с параметрами $d = 2$, $n \leqslant 8$ и $d = 3$, $n \leqslant 10$, конструкции которых можно найти в [4, 5].

ЛИТЕРАТУРА

1. *Облаухов А. К.* О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. 2016. Т. 23. № 3. С. 93–106.
2. *Tokareva N.* Duality between bent functions and affine functions // Discr. Math. 2012. V. 312. No. 3. P. 666–670.
3. *Cohen G. et al.* Covering Codes. Elsevier, 1997. V. 54.
4. *Graham R. L. and Sloane N.* On the covering radius of codes // IEEE Trans. Inform. Theory. 1985. V. 31. No. 3. P. 385–401.
5. *Cohen G., Lobstein A., and Sloane N.* Further results on the covering radius of codes // IEEE Trans. Inform. Theory. 1986. V. 32. No. 5. P. 680–694.