Секция 5

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ И ГРАФОВ

УДК 512.56, 519.7 DOI 10.17223/2226308X/14/34

БАЗИСЫ НАД ПОЛЕМ GF(2), ПОРОЖДЁННЫЕ ПРИ ПОМОЩИ ОПЕРАЦИИ ШУРА — АДАМАРА

К. Л. Геут, С. С. Титов

Рассмотрена проблема построения, описания и применения базисов векторных пространств над полем из двух элементов, порождённых при помощи операции Шура — Адамара.

Ключевые слова: *NSUCRYPTO, база матроида, базис векторного пространства, код Рида — Маллера.*

Рассматривается векторное пространство $\mathbb{F}_2^r$, состоящее из всех двоичных векторов длины r. Для любых d таких векторов можно определить их покомпонентное произведение [1]. Пустое произведение (когда в нём нет элементов) равно вектору из всех единиц.

Пусть $s, d \in \mathbb{N}$, $s \geqslant d > 1$, $r = \sum\limits_{i=0}^{d} \binom{s}{i}$, $\mathcal{B}$ — базис векторного пространства $\mathbb{F}_2^r$ и $\mathcal{F} \subseteq \mathbb{F}_2^r$ — семейство s двоичных векторов, такое, что все возможные покомпонентные произведения до d векторов из семейства $\mathcal{F}$ (включая пустое произведение) образуют базис $\mathcal{B}$ [2, 3].

Для векторов $a = (a_1, ..., a_n)$ и $b = (b_1, ..., b_n)$ из F_q^n покоординатное умножение $a * b = (a_i b_i, ..., a_n b_n)$ называется произведением Шура или произведением Адамара [4].

В задаче «Bases» [5] для данных s, d и r требуется описать все (или хотя бы некоторые) базисы $\mathcal{B}$, для которых такое семейство $\mathcal{F}$ существует, или доказать, что таких базисов нет. Предлагается дать также практическое применение таких базисов. Эту задачу естественно рассматривать на языке бинарных матроидов, элементами которых являются вектор-столбцы (или вектор-строки) некоторых матриц над полем GF(2), их циклов, подпространств, независимых множеств и, наконец, баз этих матроидов. В этой работе данная проблематика связывается с кодами Рида — Маллера порядка d, основанных на булевых функциях степени d [6, 7], поскольку покомпонентное произведение векторов можно интерпретировать как конъюнкцию значений соответствующих аргументов булевой функции в полиноме Жегалкина (алгебраической нормальной форме, ANF). В связи с этой интерпретацией становятся естественными предлагаемые применения этих базисов в теории кодирования и схемах разделения секрета.

Покомпонентные произведения определённых в условии задачи векторов должны быть, очевидно, ненулевыми и линейно независимыми, в том числе — разными, поэтому можно считать их некоторыми r вектор-строками в таблице некоторой булевой функции f, зависящей от s аргументов $t^1, \ldots, t^s$ и степени не выше d (после некоторой, может быть, перенумерации её аргументов), так что таблица истинности булевой

функции f вместе со вспомогательными столбцами (для конъюнкций аргументов по два, три и т. д.) будет выглядеть так (табл. 1):

Таблица 1

1	t^1	...	t^s	t^1t^2	...	t^1t^s	...	$t^1 \dots t^d$	...	...	f
1	...	...	...	...	...	...	...	...	...	...	...
1	x_1^1	...	x_1^s	...	...	$x_1^1x_1^s$	...	...	...	...	f_1
...	...	...	...	...	...	...	...	...	...	...	...
1	x_r^1	...	x_r^s	...	...	$x_r^1x_1^s$	...	...	...	...	f_r
...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...

Эту таблицу можно рассматривать как расширенную матрицу системы линейных уравнений над GF(2) с некоторой матрицей $\mathcal{B}$ и правым столбцом f. Следовательно, базис получается тогда и только тогда, когда существует биекция между всеми булевыми функциями f, зависящими от s аргументов $t^1, \dots, t^s$ степени не выше d, и всем списком значений $f_1, \dots, f_r$ на этих булевых векторах значений аргументов $x^1, \dots, x^s$.

Рассмотрение булевых функций от s аргументов степени вплоть до d означает рассмотрение кода Рида — Маллера порядка d, список значений всех аргументов можно расположить в естественном порядке их двоичных представлений [2, 8].

Пусть X и Y — некоторые множества, F — некоторое подмножество множества всех функций $f : X \to Y$. Естественно назвать подмножество $Z \subseteq X$ множеством единственности класса функций F, если для любой функции $g : Z \to Y$ существует единственная функция f из класса F, такая, что её ограничение на Z совпадает с g, то есть $f_{|Z} = g$.

В нашем случае $Y = \{0, 1\}$, F — подмножество булевых функций степени d, $X = V_s$ — пространство булевых векторов длины s. Искомые базисы при этом оказываются множествами, однозначно определяющими булеву функцию степени не выше d по любым заданным на этом множестве значениям функции.

Если транспонировать табл. 1 (без столбца значений функции), то получим матрицу, которую естественно назвать матрицей Рида — Маллера порядка d. Векторный матроид вектор-столбцов этой матрицы тоже естественно назвать матроидом Рида — Маллера, циклами которого являются минимальные по включению множества линейно зависимых векторов, а базами — искомые базисы как максимальные подматрицы с ненулевым определителем. При этом верхняя строка (имеющая нулевой номер) определителя состоит из одних единиц, а строки с первой по s-ю являются вектор-строками семейства $\mathcal{F}$, определяющего базис $\mathcal{B}$, составленный из всех строк этой подматрицы. Каждый вектор-столбец матрицы Рида — Маллера удобно обозначать номером N двоичного представления набора аргументов $t^1 \dots t^s$.

Например, для $s = 3$, $d = 2$ и $r = 7$ имеем матрицу Рида — Маллера, приведённую в табл. 2.

Можно предложить конструкцию для базисов $\mathcal{B}$ с таким семейством $\mathcal{F}$ для всех s, d, $s \geqslant d > 1$, на основе кодов Рида — Маллера порядка d, которая даёт серию искомых базисов для всех параметров s, d, r.

Конструкция 1. Определим семейство $\mathcal{F}$ как множество столбцов матрицы Рида — Маллера при следующем условии: слово $x_i^1 \dots x_i^s$ значений аргументов $t^1, \dots, t^s$ имеет вес Хэмминга не больше d.

Таблица 2

N	0	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1	1
t^1	0	1	0	1	0	1	0	1
t^2	0	0	1	1	0	0	1	1
t^3	0	0	0	0	1	1	1	1
t^1t^2	0	0	0	1	0	0	0	1
t^1t^3	0	0	0	0	0	1	0	1
t^2t^3	0	0	0	0	0	0	1	1

Для примера в табл. 2 берутся все столбцы, кроме столбца 7, потому что в этой конструкции в базис входят те столбцы, у которых в строках t^1, t^2, t^3 имеется не более двух единиц.

Очевидно, что значения коэффициентов соответствующей функции f определяются рекуррентно и однозначно, как и в доказательстве теоремы об ANF [8, теоремы 2.6 и 2.10]: коэффициент перед композицией для подмножества T (мощности не больше d) в множестве $\{t^1, \ldots, t^s\}$ аргументов определяется как сумма значений f и значений коэффициентов для всех подмножеств $R \subseteq T$, так что это множество T — множество единственности [8] для семейства булевых функций степени не выше d и, следовательно, базис. Обозначим этот базис через $\mathcal{B}_0$.

Таким образом, трактовка искомого базиса как множества единственности полинома Жегалкина булевой функции степени не выше d равносильна невырожденности некоторой подматрицы в полной матрице кода Рида — Маллера порядка d (в соответствии с теоремой Кронекера — Капелли).

Конструкция 2. Поскольку полная аффинная группа является группой автоморфизмов кодов Рида — Маллера, её можно использовать для описания целого класса искомых базисов.

Рассмотрим полную аффинную группу, действующую на множестве вектор-столбцов $(t^1, \ldots, t^s)^{\mathrm{T}}$. Ясно, что преобразования этой группы реализуют перестановки столбцов матрицы Рида — Маллера. В силу того, что эта группа является группой автоморфизмов, она переводит множество единственности в множество единственности, то есть базис в базис. Отсюда следует

Утверждение 1. Пусть $\mathcal{B}_0$ — построенный в конструкции 1 базис. Тогда для любого аффинного преобразования векторов — значений аргументов $(t^1, \ldots, t^s)^{\mathrm{T}}$ множество преобразованных вектор-строк базиса $\mathcal{B}_0$ также образует базис.

Такие базисы можно использовать для построения кода Рида — Маллера, который определяется через порождающую матрицу, содержащую, в том числе, все возможные произведения l строк [8, 9].

Так как количество и длины этих строк определяют параметры кода, то построение базиса определённой размерности регулирует кодирующие способности кода, построенного посредством такого базиса.

Однако существуют базисы, не получающиеся из базиса $\mathcal{B}_0$ посредством аффинного преобразования, и их описание приводит к задаче аффинной классификации булевых функций, которая решена для квадратичных булевых функций, т. е. для $d = 2$ [8].

Перечисление искомых базисов может быть произведено при помощи графа баз соответствующего матроида, поскольку он оказывается связным.

Пусть M — матроид, B' и B — две его базы: $B', B \in \mathcal{B}$. Определим, что эти базы соединены ребром в графе $\Gamma(\mathcal{B})$ баз этого матроида, если $|B' \oplus B| = 2$, где $\oplus$ означает

симметрическую разность множеств:

$$B' \oplus B = (B' \setminus B) \cup (B \setminus B') = (B' \cup B) \setminus (B' \cap B).$$

Поскольку $|B \oplus B| = 0$ и $B' \oplus B = B \oplus B'$, имеем симметричное антирефлексивное бинарное отношение на множестве $\mathcal{B}$ баз матроида M, т. е. действительно получается граф с вершинами — элементами множества $\mathcal{B}$.

Каковы свойства этого графа? Ясно, что если M дискретен, т.е. в нем нет циклов, то семейство $\mathcal{B}$ баз одноэлементно и ребер нет. Если в M есть единственный цикл $C-E$ — множество всех элементов матроида M, то базами являются все подмножества в E мощности $|E|-1$, и граф представляет собой $(|E|-1)$-элементную клику. Вне этих крайних случаев имеем $|B' \oplus B| = 2m$ — чётное число, поскольку $|B'| = |B|$.

Пусть $|B' \oplus B| = 2m$, $m > 1$:

$$\underbrace{0\ldots0}_{B'}\overbrace{0\ldots0}^{B}0\ldots0$$

По аксиоме замены для каждого $b' \in B' \setminus B$ существует такой $b \in B \setminus B'$, что $B_1 = (B' \setminus \{b'\}) \cup \{b\}$ является базой. Вычисляем

$$|B_1 \oplus B| = |(B_1 \cup B) \setminus (B \cap B_1)| = |B_1 \cup B| - |B_1 \cap B| =$$
$$= (|B' \cup B| - 1) - (|B' \cap B| + 1) = (|B' \cup B| - |B' \cap B|) - 2 = 2(m-1),$$

при этом

$$|B_1 \oplus B'| = |B_1 \cup B'| - |B_1 \cap B'| = (|B'| + 1) - (|B'| - 1) = 2,$$

то есть B_1 и B' соединены ребром в графе $\Gamma(\mathcal{B})$. Отсюда индукцией по m получаем

Утверждение 2. Граф $\Gamma(\mathcal{B})$ связен.

Первоначально этот результат был получен в работе [10] для максимальных совместных подсистем линейных неравенств и применён в алгоритме выделения всех максимальных совместных подсистем несовместной системы линейных неравенств [11].

ЛИТЕРАТУРА

1. *Деундяк В. М., Косолапов Ю. В.* О некоторых свойствах произведения Шура — Адамара для линейных кодов и их приложениях // Прикладная дискретная математика. 2020. № 50. С. 72–86.
2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. *Чижов И. В.* Обобщённые автоморфизмы кода Рида — Маллера и криптосистема Мак-Элиса — Сидельникова // Прикладная дискретная математика. Приложение. 2009. № 1. С. 36–37.
4. *Деундяк В. М., Косолапов Ю. В.* О некоторых свойствах произведения Шура — Адамара для линейных кодов и их приложениях // Прикладная дискретная математика. 2020. № 50. С. 72–86.
5. International Olympiad in Cryptography NSUCRYPTO. `https://nsucrypto.nsu.ru` (дата обращения 30.10.2020).
6. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. С. 3–20.

7. *Ведунова М. В., Геут К. Л., Игнатова А. О.* Преломляющие биекции в тройках Штейнера // Прикладная дискретная математика. Приложение. 2020. № 13. С. 6–8.
8. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
9. *Высоцкая В. В.* Квадрат кода Рида — Маллера и классы эквивалентности секретных ключей криптосистемы Мак-Элиса — Сидельникова // Прикладная дискретная математика. Приложение. 2017. № 10. С. 66–68.
10. *Гайнанов Д. Н., Новокшенов Л. И., Тягунов Л. И.* О графах, порождаемых несовместными системами линейных неравенств // Матем. заметки. 1983. № 33:2. С. 146–150.
11. *Мазуров В. Д., Хачай М. Ю.* Бустинг и полиномиальная аппроксимируемость задачи о минимальном аффинном разделяющем комитете // Тр. ИММ УрО РАН. 2013. Т. 19. № 2. С. 231–236.

УДК 621.391.7 DOI 10.17223/2226308X/14/35

О РАЗЛОЖИМОСТИ ПРОИЗВЕДЕНИЯ ШУРА — АДАМАРА СУММЫ ТЕНЗОРНЫХ ПРОИЗВЕДЕНИЙ КОДОВ РИДА — МАЛЛЕРА

Ю. В. Косолапов, Е. А. Лелюк

В рамках оценки стойкости кодовых криптосистем типа Мак-Элиса рассматривается задача исследования разложимости квадрата кода K, являющегося суммой специального вида двух тензорных произведений кодов Рида — Маллера. В ряде случаев удалось найти условия на параметры кодов-множителей, при которых квадрат кода K раскладывается в прямую сумму кодов Рида — Маллера; найдены также условия, при которых такое разложение невозможно.

Ключевые слова: *криптосистема типа Мак-Элиса, сумма тензорных произведений, произведение Шура — Адамара, разложимость.*

Кодовые криптосистемы типа Мак-Элиса рассматриваются в качестве альтернативы современным асимметричным криптосистемам, так как при выборе подходящего кода являются стойкими к атакам с помощью компьютера на основе квантовой модели вычисления [1]. Оригинальная система Мак-Элиса на кодах Гоппы в настоящее время считается стойкой, но высокая стойкость достигается за счёт ключа большого размера [2]. С целью уменьшения размера ключа предложены криптосистемы типа Мак-Элиса на других кодах. Но для некоторых широко известных кодов, таких, как обобщённые коды Рида — Соломона, двоичные коды Рида — Маллера, системы типа Мак-Элиса оказываются нестойкими и для компьютеров на основе классической модели Тьюринга [3 – 5]. Для усиления стойкости криптосистем в [6] предлагается использовать тензорное произведение кодов Рида — Маллера. В [7] исследуется класс кодов, обобщающий конструкцию тензорного произведения. Коды из этого класса представляют собой сумму нескольких тензорных произведений специального вида. Эти коды эффективно декодируются, поэтому на их основе можно построить криптосистему типа Мак-Элиса. Но для применения криптосистемы необходимо проанализировать её стойкость. При анализе стойкости кодовых криптосистем к атакам на ключ часто исследуются свойства произведения Шура — Адамара кодов, которые лежат в основе этих криптосистем [8].

В настоящей работе ставится задача исследования разложимости квадрата суммы специального вида двух тензорных произведений кодов Рида — Маллера.