ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 25 МАТЕМАТИКИ Выпуск 3
2018

А. В. Анашкин (Москва, лаб. ТВП). **Еще один способ построения максимально рассеивающих матриц.**

В работе [1] вводится определение максимально рассеивающих матриц. Показывается, что подобное свойство матриц является следствием свойства «быть MDS отображением» [2] для произвольного отображения. Отмечается, что множество максимально рассеивающих матриц включает в себя множество матриц, которые получаются из MDS-матриц над большим полем [3], но, вообще говоря, не совпадает с последним (см. пример в конце работы [4]).

Критерий для матрицы быть MDS-матрицей: любая ее квадратная подматрица невырождена (теорема 8, стр. 312 [3]). Критерий для отображения $F : A^{n_1} \to A^{n_2}$, где A — конечное множество, $n_1, n_2 \in \mathbb{N}$, быть MDS: любая «редукция», или «усечение», (определение см. [2]) отображения F до преобразования множества A^s, $1 \leqslant s \leqslant \min(n_1, n_2)$, приводит к биективному отображению.

Отметим, что в [2] не приводится отдельного частного критерия для случая, когда множество A — это векторное пространство, а отображение F является линейным. Подобный критерий легко формулируется и приведен, в частности, в работе [1]. Для описания заявленного в названии способа построения максимально рассеивающих матриц напомним необходимые определения и утверждения.

Под весом вектора $a \in GF(q^k)^m$, $a = (a_1, \ldots, a_m)$, понимаем величину $w(a) = |\{i | a_i \neq 0,\ 1 \leqslant i \leqslant m\}|$.

Характеристикой рассеивания (в зарубежных работах — branch number) матрицы B размера $m \times m$ над полем $GF(q^k)$ называют величину $\beta(B) = \min_{a \neq 0}(w(a) + w(aB))$. Нетрудно видеть, что для любой такой матрицы B справедливо:

$$\beta(B) = \min_{a \neq 0}(w(a) + w(aB)) \leqslant \min_{a \neq 0, w(a)=1}(w(a) + w(aB)) \leqslant 1 + m.$$

Матрицу B размера $m \times m$ над полем $GF(q^k)$, для которой выполняется условие $\beta(B) = m + 1$, называют MDS-матрицей.

Пусть $n = km$. Рассмотрим множество векторов длины n и множество матриц размера $n \times n$ над полем $GF(q)$. Для вектора $a \in GF(q)^n$ с заданным и зафиксированным разбиением на подвекторы: $a = (a_1, a_2, \ldots, a_k, a_{k+1}, \ldots, a_n) = (a^{(1)}, \ldots, a^{(m)})$, $a^{(j)} = (a_{k(j-1)+1}, a_{k(j-1)+2}, \ldots, a_{k(j-1)+k-1}, a_{kj})$, $a^{(j)} \in GF(q)^k$, $1 \leqslant j \leqslant m$, его обобщенным весом, согласованным с заданным разбиением, называют величину $W(a) = |\{j | a^{(j)} \neq 0,\ 1 \leqslant j \leqslant m\}|$. Характеристикой рассеивания, согласованной с заданным разбиением векторов, матрицы B размера $n \times n$ над полем $GF(q)$ называют величину: $\beta(B) = \min_{a \neq 0}(W(a) + W(aB))$.

Как и ранее для любой матрицы B размера $n \times n$ над полем $GF(q)$ справедливо неравенство $\beta(B) \leqslant m + 1$. Матрицу B, для которой выполняется равенство $\beta(B) = m + 1$, назовем матрицей с максимальной характеристикой рассеивания или просто максимально рассеивающей матрицей.

Отметим еще раз, что для конкретной матрицы как значение ее характеристики рассеивания β, так и свойство матрицы «быть максимально рассеивающей», зависит

от разбиения вектора на подвекторы. Само же разбиение возникает из естественных приложений, см., например, [6].

При заданном q максимально рассеивающие матрицы существуют не при всех значениях n и m. Например, для всех обратимых матриц при $q = 2$, $n = 2$ и $m = 2$ значение β равно 2, а для необратимых может быть и 1.

Термин «матрица с максимальным коэффициентом рассеивания» предложен Ф. М. Малышевым для обозначения матриц, на которых достигается максимум β (коэффициент рассеивания) на множестве всех (вообще говоря, обратимых) квадратных матриц заданного размера (величина n) и с заданным разбиением на подвекторы (величина m). При таком определении матрицы с «максимальным коэффициентом рассеивания» существуют всегда, но не при всех возможных значениях тройки (q, n, m) указанный максимум достигает значения $m + 1$.

Для матрицы B размера $n \times n$ над полем $GF(q)$ для произвольного числа s, $1 \leqslant s \leqslant m$, и двух наборов чисел $1 \leqslant i_1 < i_2 < \cdots < i_s \leqslant m$ и $1 \leqslant j_1 < j_2 < \cdots < j_s \leqslant m$ определим ее подматрицу $B(s; i_1, \ldots, i_s, j_1, \ldots, j_s)$ размера $k \cdot s \times k \cdot s$, стоящую на пересечении строк с номерами $i_1(k-1)+1, i_1(k-1)+2, \ldots, i_1k, i_2(k-1)+1, i_2(k-1)+2, \ldots, i_sk$ и столбцов с номерами $j_1(k-1)+1, j_1(k-1)+2, \ldots, j_1k, j_2(k-1)+1, j_2(k-1)+2, \ldots, j_sk$.

Утверждение1. *Пусть $n = km$, и задано и зафиксировано разбиение вектора длины n на m подвекторов длины k каждый. Матрица B размера $n \times n$ над полем $GF(q)$ является максимально рассеивающей тогда и только тогда, когда для любого числа s, $1 \leqslant s \leqslant m$, и любых двух наборов чисел $1 \leqslant i_1 < i_2 < \cdots < i_s \leqslant m$ и $1 \leqslant j_1 < j_2 < \cdots < j_s \leqslant m$ матрица $B(s; i_1, \ldots, i_s, j_1, \ldots, j_s)$ является обратимой.*

Данное утверждение позволяет предложить три очевидных способа построения максимально рассеивающих матриц при наличии уже имеющейся максимально рассеивающей матрицы B над полем $GF(q)$ со значением параметров $n = n^*$ (размер матрицы) и $m = m^*$ (подвекторов в разбиении).

1) («ассоциированные» матрицы) Каждая из трех матриц — обратная, транспонированная и обратная к транспонированной к матрице B являются максимально рассеивающими со значением параметров $n = n^*$ и $m = m^*$.

2) («вырезание» подматриц) Для любого числа s, $1 \leqslant s \leqslant m^*$, и любых двух наборов чисел $1 \leqslant i_1 < i_2 < \cdots < i_s \leqslant m^*$ и $1 \leqslant j_1 < j_2 < \cdots < j_s \leqslant m^*$ матрица $B(s; i_1, \ldots, i_s, j_1, \ldots, j_s)$ является максимально рассеивающей со значением параметров $n = s \cdot k$ и $m = s$.

3) («укрупнение клеток» матрицы) Если $m^* = m' \cdot r$, то матрица B является максимально рассеивающей со значением параметров $n = n^*$ и $m = m'$.

Максимально рассеивающие матрицы (как и MDS-матрицы) тем труднее строить, чем больше отношение $d = \frac{\text{размер матрицы}}{\text{длина подвектора}}$. В этом смысле приведенные способы построения таких матриц едва ли можно назвать конструктивными: первый — это использование естественного «производного» свойства максимально рассеивающей матрицы, а второй и третий приводят к уменьшению указанного отношения.

Дополнительно обращает на себя внимание то обстоятельство, что в первом и втором случае, и в меньшей степени в третьем, мы не уходим от исходной «структуры» матрицы B : если максимально рассеивающая матрица B получена из MDS-матрицы над большим полем (как это делается, описано в [4]), то такими же будут и построенные из нее матрицы. В частности, полученные матрицы могут «наследовать» алгебраические свойства большего поля, что потенциально может привести к возникновению «простых» алгебраических соотношений в схемах, в которых матрицы будут использованы.

На еще один способ построения максимально рассеивающих матриц указывает приведенный в [4] пример. При данном способе мы также уменьшаем d, но можем «уйти» от алгебраической структуры поля $GF(q^{\frac{n}{m}})$.

Утверждение 2. *Пусть* $s \in \mathbb{N}$ $B_{ij}^{(t)} \in GF(q)_{k(t),k(t)}$, $i,j = \overline{1,m}$, $t = \overline{1,s}$, *и* $B^{(t)} = \begin{pmatrix} B_{11}^{(t)} & B_{12}^{(t)} & \dots & B_{1m}^{(t)} \\ B_{21}^{(t)} & B_{22}^{(t)} & \dots & B_{2m}^{(t)} \\ \dots & \dots & \dots & \dots \\ B_{m1}^{(t)} & B_{m2}^{(t)} & \dots & B_{mm}^{(t)} \end{pmatrix} \in GF(q)_{k(t)m,k(t)m}$ — *максимально рассеивающая матрица при* $k(t) = k_t$, $k_t \in \mathbb{N}$, $t = \overline{1,s}$. *Тогда матрица*

$$B = \begin{pmatrix} B_{11} & B_{12} & \dots & B_{1m} \\ B_{21} & B_{22} & \dots & B_{2m} \\ \dots & \dots & \dots & \dots \\ B_{m1} & B_{m2} & \dots & B_{mm} \end{pmatrix} \in GF(q)_{n,n},$$

где $B_{ij} = \begin{pmatrix} B_{ij} & 0 & \dots & 0 \\ 0 & B_{ij}^{(2)} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & B_{ij}^{(t)} \end{pmatrix} \in GF(q)_{k,k}$, $i,j = \overline{1,m}$, *является максимально рассеивающей матрицей при* $k = \sum_{t=1}^{s} k_t$, $n = k \cdot m$.

СПИСОК ЛИТЕРАТУРЫ

1. *Анашкин А. В.* Об одном свойстве матриц. — Обозрение прикл. и промышл. матем., 2015, т. 22, в. 5, с. 559–561.
2. *Dehnavi S. M.*, *Mahmoodi Rishakani A.*, *Mirzaee Shamsabad M.R.* Characterization of MDS mappings. eprint.iacr.org, 2015/002.
3. *Мак-Вильямс Н.Дж.*, *Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: «Связь», 1979.
4. *Анашкин А. В.* Канонический вид матриц из одного класса. — Обозрение прикл. и промышл. матем., 2016, т. 23, в. 5, с. 457–459.
5. *Анашкин А. В.* Полное описание одного класса MDS-матриц над конечным полем характеристики 2. — Матем. вопросы криптографии, 2017, т. 8, в. 4, с. 5–28.
6. *Малышев Ф. М.* Двойственность разностного и линейного методов в криптографии. Матем. вопросы криптографии, 2014, т. 5, в. 3, с. 35–48.