

А. В. А н а ш к и н (Москва, Лаб. ТВП). Об обратной матрице к MDS матрице специального вида.

УДК 512.643.8

DOI https://doi.org/10.52513/08698325_2022_29_1_1

Резюме: Приводится обратная матрица к MDS матрице размера 5×5 над конечным полем характеристики 2, элементы которой выбираются из множества {единичный элемент поля, некоторый элемент, не равный единичному, и его квадрат}.

Ключевые слова: MDS матрица, максимально рассеивающая матрица, циркулянтная матрица, поле Галуа $\mathbf{GF}(2^t)$.

В работе [1] изучаются квадратные MDS матрицы над конечным полем характеристики 2. Одним из основных критериев для матрицы над конечным полем быть MDS матрицей является условие, что все ее квадратные подматрицы невырождены [2].

Сформулируем основные результаты работы [1]. Поле $\mathbf{GF}(2^t)$, над которым далее рассматриваются матрицы, считаем фиксированным. Для некоторого непустого множества D — подмножества поля $\mathbf{GF}(2^t)$, через $W(m, D)$ обозначим множество всех MDS матриц размера $m \times m$, $m \in \mathbf{N}$, элементы которых принадлежат множеству D .

З а м е ч а н и е 1. Если один из элементов матрицы равен 0, то матрица не является MDS-матрицей и, значит, можем считать, что $0 \notin D$.

З а м е ч а н и е 2. Пусть матрица B принадлежит множеству $W(m, D)$. Если $c \in \mathbf{GF}(2^t)$, $c \neq 0$, то $cB \in W(m, cD)$. В частности, при исследовании множеств $W(m, D)$ при различных m и D можно ограничиться рассмотрением множеств D с условием $e \in D$, где e — единица поля $\mathbf{GF}(2^t)$. В том числе и из результатов работы [1] вытекают следующие утверждения.

Утверждение 1. Если $|D| = 1$ и $m > 2$, то $W(m, D) = \emptyset$.

Утверждение 2. Если $|D| = 2$ и $m > 4$, то $W(m, D) = \emptyset$.

Далее рассматриваем случай, когда $|D| = 3$ и $D = D(\alpha) = \{e, \alpha, \alpha^2\}$, $\alpha \in \mathbf{GF}(2^t)$, и, значит, $\alpha \neq 0$ и $\alpha \neq e$, что равносильно тому, что α не является корнем многочлена первой степени над полем $\mathbf{GF}(2)$.

Утверждение 3. Если $|D| = 3$, $D = D(\alpha) = \{e, \alpha, \alpha^2\}$, $\alpha \in \mathbf{GF}(2^t)$ и $m > 5$, то $W(m, D) = \emptyset$.

В группе $\mathbf{GL}(m, \mathbf{GF}(2^t))$ квадратных обратимых матриц размера $m \times m$ над полем $\mathbf{GF}(2^t)$ рассмотрим подгруппу $\bar{S}_m$ перестановочных матриц, $|\bar{S}_m| = m!$.

Поскольку перестановка строк и столбцов MDS матрицы не изменяет ее свойство быть MDS матрицей, рассмотрим действие группы $\bar{S}_m \times \bar{S}_m$ на непустом множестве $W(m, D)$, полагая

$$(g, h)(A) = g^{-1} \cdot A \cdot h \quad \text{для } A \in W(m, D) \text{ и } (g, h) \in \bar{S}_m \times \bar{S}_m.$$

Утверждение 4. Пусть $D = D(\alpha) = \{e, \alpha, \alpha^2\}$, $\alpha \in \mathbf{GF}(2^t)$. Множество $W(5, D)$ непусто тогда и только тогда, когда элемент α не является корнем ни одного неприводимого многочлена степени не выше 3 над полем $\mathbf{GF}(2)$. При этом

группа $\bar{S}_5 \times \bar{S}_5$ действует на множестве $W(5, D(\alpha))$ транзитивно, т. е. с точностью до перестановки строк и столбцов множество $W(5, D(\alpha))$ состоит всего из одной матрицы.

З а м е ч а н и е 3. Поскольку в кольце многочленов над полем характеристики 2 выполняются соотношения $x^5 + x^4 + e = (x^2 + x + e)(x^3 + x + e)$ и $x^5 + x + e = (x^2 + x + e)(x^3 + x^2 + e)$, упоминание многочленов $x^5 + x + e$ и $x^5 + x^4 + e$ в следствиях 6 и 7 работы [1, с. 23 и с. 27, соответственно] является излишним.

З а м е ч а н и е 4. Нетрудно показать, что стабилизатор любого элемента $B \in W(5, D(\alpha))$ в группе $\bar{S}_5 \times \bar{S}_5$ имеет порядок 10 (и изоморфен группе диэдра). И следовательно, количество различных элементов в множестве $W(5, D(\alpha))$ (при условии, что это множество не пусто!) равно:

$$|W(5, \alpha)| = \frac{|\bar{S}_5 \times \bar{S}_5|}{10} = 1440.$$

Поскольку ни в поле $\mathbf{GF}(4)$, ни в поле $\mathbf{GF}(8)$ нет подходящих под условие утверждения 4 элементов α , то справедливо следующее

Следствие 1. Если $t = 2$ или $t = 3$, $\alpha \in \mathbf{GF}(2')$, то $W(5, D(\alpha)) = \emptyset$.

Утверждение 5. Пусть $D = D(\alpha) = \{e, \alpha, \alpha^2\}$, $\alpha \in \mathbf{GF}(2')$. Множество $W(4, D)$ непусто тогда и только тогда, когда элемент α не является корнем ни одного неприводимого многочлена степени не выше 3 над полем $\mathbf{GF}(2)$. При этом группа $S_4 \times S_4$ при действии на множестве $W(4, D(\alpha))$ имеет три орбиты, т. е. с точностью до перестановки строк и столбцов множество $W(4, D(\alpha))$ состоит из трех матриц.

Вернемся к случаю $t = 5$ и сформулируем некоторые новые результаты. В работе [1] приведена матрица

$$B = \begin{pmatrix} \alpha & e & e & a^2 & a^2 \\ e & \alpha & \alpha^2 & e & \alpha^2 \\ e & \alpha^2 & \alpha & \alpha^2 & e \\ \alpha^2 & e & \alpha^2 & \alpha & e \\ \alpha^2 & \alpha^2 & e & e & \alpha \end{pmatrix}$$

из $W(5, D(\alpha))$.

З а м е ч а н и е 5. Перестановкой строк и столбцов матрицу B можно привести к циркулянтной матрице: $C = \text{Cir}(\alpha, e, \alpha^2, \alpha^2, e)$.

Утверждение 6. Пусть $\text{НОД}(t, 3) = 1$, тогда среди квадратных матриц размера 5×5 над полем $\mathbf{GF}(2')$ не менее $1440 \cdot (2^t - 4)$ MDS матриц, элементы каждой из которых имеют следующий вид: единичный элемент поля, некоторый элемент, не равный единичному, и его квадрат.

Действительно, совпадение множеств $\{\alpha, \alpha^2\}$ и $\{\beta, \beta^2\}$ возможно только в случае, если $\alpha = \beta$ или $(\alpha = \beta^2 \text{ и } \alpha^2 = \beta)$. Но в последнем случае получаем, что $\alpha^4 = \alpha$, что равносильно $\alpha(\alpha + e)(\alpha^2 + \alpha + e) = 0$. Таким образом, для любого элемента α из поля $\mathbf{GF}(2')$, который не является корнем неприводимого многочлена степени не выше второй над полем $\mathbf{GF}(2)$, множество $W(5, D(\alpha)) \neq \emptyset$ и, следовательно, $|W(5, D(\alpha))| = 1440$. При этом, если $\alpha, \beta \in \mathbf{GF}(2')$, $\alpha \neq \beta$, и каждый из этих элементов не является корнем неприводимого многочлена степени не выше второй над полем $\mathbf{GF}(2)$, то множества $\{\alpha, \alpha^2\}$ и $\{\beta, \beta^2\}$ не пересекаются, а значит, не пересекаются и множества $W(5, D(\alpha))$ и $W(5, D(\beta))$.

Таким образом, к важным результатам работы [1] для случая $t = 5$ следует отнести единственный вид матрицы из $W(5, D(\alpha))$, к которому перестановкой строк и столбцов приводится произвольная MDS матрица, элементы которой выбираются из множества $\{e, \alpha, \alpha^2\}$, независимость этого вида от элемента α , а также достаточно большое количество таких MDS матриц.

В работе [1], тем не менее, не приводится вид матрицы обратной, к матрице B , которая, согласно [3], также является MDS матрицей. Непосредственными вычислениями получаем:

$$B^{-1} = \alpha^{-1} f(\alpha)^{-1} \begin{pmatrix} f(\alpha) & g(\alpha) & g(\alpha) & h(\alpha) & h(\alpha) \\ g(\alpha) & f(\alpha) & h(\alpha) & g(\alpha) & h(\alpha) \\ g(\alpha) & h(\alpha) & f(\alpha) & h(\alpha) & g(\alpha) \\ h(\alpha) & g(\alpha) & h(\alpha) & f(\alpha) & g(\alpha) \\ h(\alpha) & h(\alpha) & g(\alpha) & g(\alpha) & f(\alpha) \end{pmatrix},$$

где $f(x), h(x), g(x) \in \mathbf{GF}(2)[x]$ — многочлены степени 3:

$$\begin{aligned} f(x) &= x^3 + e = (x^2 + x + e)(x + e), \\ h(x) &= x^3 + x + e, \\ g(x) &= x^3 + x^2 + e. \end{aligned}$$

Тот факт, что матрица B^{-1} состоит всего из трех различных элементов, также следует из результатов работ [1, 4]. Действительно, любая квадратная подматрица MDS матрицы также является MDS матрицей [4, пункт 1 следствия из утверждения 1], а подматрицы размера 4×4 матрицы B с точностью до перестановок строк и столбцов могут быть только трех «видов» [1]. Фактически

$$\frac{f(\alpha)}{\alpha f(\alpha)}, \quad \frac{h(\alpha)}{\alpha f(\alpha)} \quad \text{и} \quad \frac{g(\alpha)}{\alpha f(\alpha)}$$

— это значения определителей этих трех матриц.

Задавая поле $\mathbf{GF}(2^t)$, $t \geq 4$, как фактор-кольцо кольца многочленов $\mathbf{GF}(2)[x]$, по идеалу, порожденному некоторым неприводимым многочленом $g(x) \in \mathbf{GF}(2)[x]$ степени t , и выбирая в качестве элемента α корень многочлена $q(x)$, можно «вычислять» значения

$$\alpha^{-1}, \quad \frac{h(\alpha)}{\alpha f(\alpha)} \quad \text{и} \quad \frac{g(\alpha)}{\alpha f(\alpha)},$$

представляя их значениями многочленов степеней меньших, чем t , в точке α .

СПИСОК ЛИТЕРАТУРЫ

1. Анашкин А. В. Полное описание одного класса MDS-матриц над конечным полем характеристики 2. — Математические вопросы криптографии, 2017, т. 8, в. 4, с. 5–28. // *Anashkin A. V. The complete classification of a set of MDS matrices over finite field of characteristic 2. — Mathematical Aspects of Cryptography, 2017, v. 8, is. 4, p. 5–28. (In Russian.)*
2. Мак-Вильямс Н. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — Связь. М, 1979. // *MacWilliams F. J., Sloane N. J. A. The theory of error correcting codes. North-Holland Publishing Company. Amsterdam. New York. Oxford, 1977.*
3. Анашкин А. В. Об одном свойстве матриц. — Обозрение прикл. и промышл. матем., 2015, т. 22, в. 5, с. 559–561. // *Anashkin A. V. On a characteristic of matrices. — OPM Sur. Appl. Industr. Math., 2015, v. 22, is. 5, p. 559–561. (In Russian.)*
4. Анашкин А. В. Канонический вид матриц из одного класса. — Обозрение прикл. и промышл. матем., 2016, т. 23, в. 5, с. 457–459. // *Anashkin A. V. A canonical form of some matrices. — OPM Sur. Appl. Industr. Math., 2016, v. 23, is. 5, p. 457–459. (In Russian.)*

UDC 512.643.8

DOI https://doi.org/10.52513/08698325_2022_29_1_1

Anashkin A. V. (Moscow, TVP Laboratories). **On inverse of some MDS matrix.**

Abstract: We calculate the inverse matrix to the square 5×5 MDS matrix over finite field F_{2^t} whose entries are from the set: $\{1, \alpha, \alpha^2\}$.

Keywords: MDS matrix, circulant matrix, finite field F_{2^t} .