О крестовых матрицах над полем $\mathbb{Z}_2$

А. В. Решетников* Д. Ю. Манилов†

Данная работа, выполненная нами в июне 2015 г., положила начало многолетнему исследованию, посвящённому глубокому изучению свойств крестовых матриц – то есть матриц, у которых все элементы какой-либо строки и все элементы какого-либо столбца равны 1*, а остальные элементы равны* 0*. Матрицы такого вида естественным образом возникли при решении головоломки о вскрытии кодового замка из компьютерной игры «Братья пилоты. По следам полосатого слона». В настоящей работе описываются методы решения головоломки, полученные как следствие теоремы о том, что линейное пространство матриц размера $n \times m$, где n и m – произвольные ч ё т н ы е числа, над полем $\mathbb{Z}_2$ имеет базис, состоящий из крестовых матриц.*

Несколько позже к изучению крестовых матриц присоединился и наш научный руководитель И. Б. Кожухов. Используя технику групповых колец (в частности: возможность представления матриц над полем в виде тензорного произведения групповых алгебр), проф. Кожухов нашёл базис линейной оболочки крестовых матриц в общем случае, т.е. когда числа n и m не обязательно чётные. В настоящее время (февраль 2026 г.) мы готовим к публикации совместную статью, где будут изложены некоторые из полученных нами результатов; остальные результаты также будут опубликованы в рецензируемых журналах. А данная заметка приобретает чисто историческое значение.

*__Решетников Артём Владимирович__
Московский Институт Электронной Техники
E-mail: a_reshetnikov@hush.com

†__Манилов Дмитрий Юрьевич__
Московский Институт Электронной Техники
E-mail: thdi@ro.ru

ЗАДАЧА О КРЕСТАХ, ЧЁТНЫЙ СЛУЧАЙ

Манилов Д. Ю., Решетников А. В.

Введение

Множество матриц над полем, имеющих фиксированное число строк и такое же число столбцов, обычно рассматривается как кольцо с операциями матричного сложения и умножения. В гораздо меньшей степени множество матриц с фиксированным числом строк и столбцов изучено как линейное пространство над полем.

В данной работе множество матриц A над полем $\mathbb{Z}_2$, имеющих фиксированное число строк n и фиксированное число столбцов m, рассматривается как линейное пространство. Одним из базисов данного пространства является множество матриц e^{ij}, у которых ровно один элемент отличен от 0, а именно, элемент, стоящий в i-й строке в j-м столбце. В задаче о крестах, формулировку и решение которой мы даём в данной работе, авторам пришлось иметь дело с множеством матриц f^{ij}, у которых единичными являются элементы, находящиеся в i-й строке *или* в j-м столбце, и только они. Было доказано, что матрицы f^{ij} образуют базис пространства A тогда и только тогда, когда либо оба числа n и m являются чётными, либо $n = m = 1$. Также для случая, когда n и m чётные, было получено в явном виде разложение произвольной матрицы из пространства A по матрицам f^{ij} как по базисным векторам.

Постановка задачи о крестах

Задачу о крестах можно сформулировать в следующем виде. *Дана матрица из нулей и единиц. На каждом ходу можно выбрать в данной матрице произвольную строку i и произвольный столбец j. При этом все элементы в i-й строке и все элементы в j-м столбце изменяют свои значения на противоположные: нули становятся единицами и наоборот, единицы становятся нулями; после чего можно сделать следующий ход. Требуется за какое-то число ходов получить из данной матрицы нулевую.*

Прежде всего, заметим, что данная задача не всегда имеет решение.

Пример 1. *Рассмотрим матрицу $a = (0, 1)$ из одной строки. При любом выборе столбца данная матрица на следующем ходу превращается в матрицу $b = (1, 0)$, которая, в свою очередь, на следующем ходу вновь превращается в исходную матрицу. Таким образом, применяя к матрице a разрешённые в задаче преобразования, можно получить либо саму матрицу a, либо матрицу b. Получить же из матрицы a нулевую матрицу невозможно.*

Оказывается, что в случае, когда исходная матрица содержит чётное количество строк и чётное количество столбцов, задача всегда имеет решение. Одно из возможных решений мы получим в результате доказательства данного утверждения. Прежде, чем изложить это доказательство, формализуем нашу задачу.

Зафиксируем два чётных числа n и m. Множество всех матриц над полем $\mathbb{Z}_2$ размера $n \times m$ (n – число строк, m – число столбцов) обозначим через A. Для произвольной матрицы $a \in A$ элемент, стоящий в её i-й строке в j-м столбце, будем обозначать через $a[i, j]$. Рассмотрим отображения $\varphi^{ij} : A \to A$, $1 \leq i \leq n$, $1 \leq j \leq m$, определённые следующим образом:

$$a\varphi^{ij}[x, y] = \begin{cases} \neg a[x, y], & \text{если } (x = i) \text{ или } (y = j); \\ a[x, y], & \text{если } (x \neq i) \text{ и } (y \neq j), \end{cases}$$

где символ «$\neg$» обозначает операцию

$$\neg 0 = 1, \quad \neg 1 = 0.$$

Множество всех таких отображений обозначим через Φ:

$$\Phi = \{\varphi^{ij} | 1 \leq i \leq n, 1 \leq j \leq m\}.$$

Определение 1. *Пусть $a \in A$ – произвольная матрица. Набор отображений φ_1, φ_2, ..., $\varphi_N \in \Phi$ назовём решением задачи о крестах для матрицы a, если композиция данных отображений переводит матрицу a в нулевую матрицу:*

$$a\varphi_1\varphi_2...\varphi_N = 0.$$

Тогда наша задача состоит в том, чтобы для произвольной матрицы из множества A найти решение задачи о крестах или доказать, что решения задачи о крестах для данной матрицы не существует.

План решения задачи о крестах

Идея решения заключается в следующем. Рассмотрим какое-нибудь взаимно однозначное линейное отображение $\lambda : A \to A$. Заметим, что $0\lambda = 0$. Действительно, пусть $a \in A$ – произвольная матрица, тогда в силу линейности отображения λ имеем

$$0\lambda = (a + a)\lambda = a\lambda + a\lambda = 0. \tag{1}$$

Обратное к λ отображение будем обозначать λ^{-1}; оно определено для всех матриц $a \in A$ ввиду взаимной однозначности отображения λ.

Далее, для каждого отображения $\varphi^{ij} \in \Phi$ определим отображение $\psi^{ij} : A \to A$:

$$a\psi^{ij} = a\lambda^{-1}\varphi^{ij}\lambda. \tag{2}$$

Множество всех таких отображений обозначим через Ψ:

$$\Psi = \{\psi^{ij} | 1 \le i \le n, 1 \le j \le m\}.$$

Заметим, что для любых отображений ψ_1, ψ_2, ..., $\psi_N \in \Psi$ выполняется следующее свойство:

$$a\psi_1\psi_2...\psi_N = a\lambda^{-1}\varphi_1...\varphi_N\lambda. \tag{3}$$

Докажем его индукцией по N. При $N = 1$ утверждение (3) прямо следует из определения (2). Предположим, что утверждение (3) уже доказано для некоторого N. Тогда для $K = N + 1$ имеем

$$a\psi_1...\psi_K = (a\lambda^{-1}\varphi_1...\varphi_N\lambda)\psi_K = (a\lambda^{-1}\varphi_1...\varphi_N\lambda)\lambda^{-1}\varphi_K\lambda = a\lambda^{-1}\varphi_1...\varphi_K\lambda.$$

Таким образом, равенство (3) имеет место для любых N.

Теперь если для какой-либо матрицы $a \in A$ удалось найти набор отображений ψ_1, ψ_2, ..., $\psi_N \in \Psi$, композиция которых переводит матрицу a в нулевую матрицу, то есть если выполняется условие

$$a\psi_1\psi_2...\psi_N = 0, \tag{4}$$

то композиция соответствующих отображений φ_1, φ_2, ..., φ_N переведёт матрицу $a\lambda^{-1}$ в нулевую матрицу:

$$\begin{array}{ccccccccc}
a & \xrightarrow{\psi_1} & a\psi_1 & \xrightarrow{\psi_2} & a\psi_1\psi_2 & \xrightarrow{\psi_3} & ... & \xrightarrow{\psi_N} & 0 \\
\uparrow{\scriptstyle\lambda} & & \uparrow{\scriptstyle\lambda} & & \uparrow{\scriptstyle\lambda} & & & & \uparrow{\scriptstyle\lambda} \\
a\lambda^{-1} & \xrightarrow{\varphi_1} & a\lambda^{-1}\varphi_1 & \xrightarrow{\varphi_2} & a\lambda^{-1}\varphi_1\varphi_2 & \xrightarrow{\varphi_3} & ... & \xrightarrow{\varphi_N} & a\lambda^{-1}\varphi_1\varphi_2...\varphi_N
\end{array}$$

При составлении данной коммутативной диаграммы мы использовали свойство (3). Из равенства (1) следует

$$a\lambda^{-1}\varphi_1\varphi_2...\varphi_N = 0, \tag{5}$$

поскольку λ взаимно однозначно.

Осталось подобрать отображение λ таким образом, чтобы для любой матрицы $a \in A$ заведомо существовал набор отображений ψ_1, ψ_2, ...,

$\psi_N \in \Psi$, обеспечивающий выполнение условия (4). Тогда произвольную матрицу $b \in A$ можно будет представить в виде $b = a\lambda^{-1}$ для некоторой матрицы $a \in A$, ввиду взаимной однозначности отображения λ. После чего с помощью (2) получим набор отображений φ_1, φ_2, ..., $\varphi_N \in \Phi$, переводящих матрицу b в нулевую матрицу.

Существование решения задачи о крестах

Все операции будем выполнять в поле $\mathbb{Z}_2$.

Прежде всего, дадим более простое определение для отображений φ^{ij}. Для этого введём матрицы $f^{ij} \in A$, $1 \le i \le n$, $1 \le j \le m$ следующим образом:

$$f^{ij}[x,y] = \begin{cases} 1, & \text{если } (x = i) \text{ или } (y = j); \\ 0, & \text{если } (x \neq i) \text{ и } (y \neq j). \end{cases} \tag{6}$$

Предложение 1. *Для любой матрицы $a \in A$ при всех $1 \le i \le n$, $1 \le j \le m$ выполняется равенство*

$$a\varphi^{ij} = a + f^{ij}.$$

Доказательство очевидно. □

Следствие. *Композиция любых отображений φ_1, φ_2, ..., $\varphi_N \in \Phi$, не зависит от того, в каком порядке применяются данные отображения.*

Пусть $a \in A$ – произвольная матрица. *Матрицей переключений* для матрицы a будем называть матрицу a^*, определённую следующим образом:

$$a^*[x,y] = \sum_{i=1}^{n} a[i,y] + \sum_{j=1}^{m} a[x,j] + a[x,y]. \tag{7}$$

Предложение 2. *Для любой матрицы $a \in A$ справедливо следующее представление матрицы переключений a^*:*

$$a^*[x,y] = \sum_{i=1}^{n}\sum_{j=1}^{m} a[i,j]f^{xy}[i,j]. \tag{8}$$

Доказательство. Рассмотрим сумму, стоящую в правой части равенства (8). Разобьём её на четыре слагаемых:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a[i,j]f^{xy}[i,j] = \sum_{i\neq x}\sum_{j\neq y} a[i,j]f^{xy}[i,j] +$$

$$+\sum_{i\neq x} a[i,y]f^{xy}[i,y] + \sum_{j\neq y} a[x,j]f^{xy}[x,j] + a[x,y]f^{xy}[x,y].$$

Первое слагаемое обращается в 0, так как по определению матрицы f^{xy} если $i \neq x$ и $j \neq y$, то $f^{xy}[i,j] = 0$. Во всех остальных случаях $f^{xy}[i,j] = 1$, и мы имеем не что иное, как матрицу переключений a^*:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a[i,j]f^{xy}[i,j] = \sum_{i\neq x} a[i,y] + \sum_{j\neq y} a[x,j] + a[x,y] =$$

$$= \left(\sum_{i\neq x} a[i,y] + a[x,y])\right) + \left(\sum_{j\neq y} a[x,j] + a[x,y])\right) + a[x,y] =$$

$$= \sum_{i=1}^{n} a[i,y] + \sum_{j=1}^{m} a[x,j] + a[x,y] = a^*[x,y].$$

□

Рассмотрим следующее отображение $\lambda : A \to A$:

$$a\lambda = a^*. \tag{9}$$

Докажем, что оно является линейным и взаимно однозначным. Прежде всего докажем линейность данного отображения.

Предложение 3. *Для произвольных матриц $a, b \in A$ и произвольного числа $k \in \mathbb{Z}_2$ матрицы переключений a^* и b^* удовлетворяют свойствам*

$$(a+b)^* = a^* + b^*; \tag{10}$$

$$(ka)^* = ka^*. \tag{11}$$

Доказательство. Чтобы доказать свойство (10), возьмём две произвольные матрицы $a, b \in A$ и найдём матрицу переключений для их суммы. Будем использовать представление (8):

$$(a+b)^*[x,y] = \sum_{i=1}^{n}\sum_{j=1}^{m}(a+b)[i,j]f^{xy}[i,j] =$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{m} a[i,j]f^{xy}[i,j] + \sum_{i=1}^{n}\sum_{j=1}^{m} b[i,j]f^{xy}[i,j] = a^*[x,y] + b^*[x,y].$$

Свойство (10) доказано, свойство (11) очевидно. □

Замечание. *Для доказательства свойства (11) можно было воспользоваться формулой (1): так как при выводе данной формулы мы не пользовались взаимной однозначностью отображения λ, то она верна для всех отображений $\lambda : A \to A$, удовлетворяющих условию $(a+b)\lambda = a\lambda + b\lambda$ при всех $a, b \in A$. Таким образом, для всех таких отображений выполняется свойство $(ka)\lambda = k(a\lambda)$ при любых $a \in A$, $k \in \mathbb{Z}_2$.*

Чтобы доказать взаимную однозначность отображения λ, достаточно показать[1], что $\lambda^{-1} = \lambda$:

Предложение 4. *Для любой матрицы $a \in A$ выполняется следующее условие:*

$$(a^*)^* = a. \tag{12}$$

Доказательство. Пусть $a \in A$ – произвольная матрица. Воспользуемся определением матрицы переключений (7):

$$\begin{aligned}
(a^*)^*[x,y] &= \sum_{i=1}^{n} a^*[i,y] + \sum_{j=1}^{m} a^*[x,j] + a^*[x,y] = \\
&= \sum_{i=1}^{n} \left(\sum_{k=1}^{n} a[k,y] + \sum_{l=1}^{m} a[i,l] + a[i,y] \right) + \\
&+ \sum_{j=1}^{m} \left(\sum_{k=1}^{n} a[k,j] + \sum_{l=1}^{m} a[x,l] + a[x,j] \right) + \\
&+ \sum_{i=1}^{n} a[i,y] + \sum_{j=1}^{m} a[x,j] + a[x,y] = \\
&= n \cdot \sum_{k=1}^{n} a[k,y] + \sum_{i=1}^{n} \sum_{l=1}^{m} a[i,l] + \sum_{i=1}^{n} a[i,y] + \\
&+ \sum_{j=1}^{m} \sum_{k=1}^{n} a[k,j] + m \cdot \sum_{l=1}^{m} a[x,l] + \sum_{j=1}^{m} a[x,j] + \\
&+ \sum_{i=1}^{n} a[i,y] + \sum_{j=1}^{m} a[x,j] + a[x,y].
\end{aligned}$$

[1]Поскольку λ – *линейное* отображение, то из предложения 4 действительно следует существование отображения λ^{-1} и выполнение равенства $\lambda^{-1} = \lambda$. В самом деле, пусть $a^* = b^*$. Тогда $a^* - b^* = 0$; следовательно, $(a-b)^* = 0$. Отсюда $(a-b)^{**} = (a-b)^*\lambda = 0\lambda = 0$, согласно (1). Но $(a-b)^{**} = a - b$ ввиду предложения 4; поэтому $a - b = 0$. То есть $a = b$, так что λ – вложение $A \to A$. Очевидно, что λ сюръективно.

Так как числа n и m являются чётными, то первое и пятое слагаемые обращаются в 0:

$$n \cdot \sum_{k=1}^{n} a[k, y] = m \cdot \sum_{l=1}^{m} a[x, l] = 0.$$

Второе слагаемое есть сумма s всех элементов матрицы a, поэтому оно совпадает с четвёртым слагаемым, которое также представляет из себя сумму всех элементов матрицы a. В сумме они дают 0:

$$\sum_{i=1}^{n} \sum_{l=1}^{m} a[i, l] + \sum_{j=1}^{m} \sum_{k=1}^{n} a[k, j] = s + s = 0.$$

Третье слагаемое совпадает с седьмым, шестое – с восьмым. Таким образом, из девяти слагаемых отличным от 0 может быть лишь девятое слагаемое. Окончательно получаем:

$$(a^*)^*[x, y] = a[x, y].$$

□

Предложения 3 и 4 доказывают, что отображение λ, определённое по формуле (9), является линейным и взаимно однозначным, поэтому к нему применимы все рассуждения из предыдущего раздела. Если для каждой матрицы $a \in A$ удастся подобрать набор отображений ψ_1, ψ_2, ..., $\psi_N \in \Psi$, которые переводят матрицу a в нулевую матрицу, то доказательство существования решения будет завершено полностью. Чтобы убедиться, что такой набор отображений действительно существует, выясним, что представляет из себя произвольное отображение $\psi^{ij} \in \Psi$.

Рассмотрим матрицы $e^{ij} \in A$, $1 \leq i \leq n$, $1 \leq j \leq m$, у каждой из которых ровно один элемент $[i, j]$ отличен от 0:

$$e^{ij}[x, y] = \begin{cases} 1, & \text{если } (x = i) \text{ и } (y = j); \\ 0, & \text{если } (x \neq i) \text{ или } (y \neq j). \end{cases} \tag{13}$$

Они образуют базис в линейном пространстве A, и произвольная матрица $a \in A$ может быть разложена по e^{ij} как по базисным векторам следующим образом:

$$a = \sum_{i=1}^{n} \sum_{j=1}^{m} e^{ij} a[i, j]. \tag{14}$$

Кроме того, матрицы e^{ij} обладают важным для нас свойством:

Предложение 5. *Для любой матрицы* e^{ij}, $1 \leq i \leq n$, $1 \leq j \leq m$, *её матрица переключений имеет вид:*

$$(e^{ij})^* = f^{ij}.$$

Доказательство данного утверждения прямо следует из формулы (8) и определения матрицы e^{ij}. $\square$

Следствие. *Для любой матрицы* f^{ij}, $1 \leq i \leq n$, $1 \leq j \leq m$, *её матрица переключений имеет вид:*

$$(f^{ij})^* = e^{ij}.$$

Теперь мы можем в явном виде указать, как преобразуется произвольная матрица $a \in A$ под действием какого-либо отображения $\psi^{ij} \in \Psi$:

Предложение 6. *Для любой матрицы* $a \in A$ *при всех* $1 \leq i \leq n$, $1 \leq j \leq m$ *выполняется равенство*

$$a\psi^{ij} = a + e^{ij}.$$

Доказательство. Из формул (2), (9) и предложения 1 следует, что

$$a\psi^{ij} = (a^*\varphi^{ij})^* = (a^* + f^{ij})^*.$$

По свойствам (10) и (12) получаем

$$(a^* + f^{ij})^* = (a^*)^* + (f^{ij})^* = a + (f^{ij})^*.$$

Окончательно, по следствию из предложения 5 получаем

$$a + (f^{ij})^* = a + e^{ij}.$$

$\square$

Из только что доказанного предложения 6 следует, что все отображения $\psi^{ij} \in \Psi$, определяемые формулой (2), имеют вид:

$$a\psi^{ij}[x, y] = \begin{cases} \neg a[x, y], & \text{если } (x = i) \text{ и } (y = j); \\ a[x, y], & \text{если } (x \neq i) \text{ или } (y \neq j). \end{cases}$$

Ясно теперь, что какой бы ни была матрица $a \in A$, если в набор ψ_1, ψ_2, ..., $\psi_N \in \Psi$ включить такие и только такие преобразования ψ^{ij}, что для индексов i, j выполняется условие $a[i, j] = 1$, то под действием всех этих преобразований матрица a перейдёт в нулевую матрицу вне зависимости от того, в каком порядке к матрице применить данные преобразования. Это означает, что будет выполнено условие (4). Но мы показали, что из него следует условие (5), а для любой матрицы $b \in A$ можно указать такую матрицу $a \in A$, что будет выполнено равенство $b = a\lambda^{-1}$, а именно, можно положить $a = b^*$. Следовательно:

Предложение 7. *Для любой матрицы $a \in A$ существует решение задачи о крестах в смысле определения 1.*

Методы решения задачи о крестах

В данном разделе считаем, что n и m – произвольные натуральные числа (не обязательно чётные, как это было в предыдущих разделах).

В случае $n = m = 1$ решение задачи о крестах тривиально. Для случая, когда оба числа n и m являются чётными, мы собираемся получить решение задачи о крестах в явном виде. В остальных случаях мы покажем, что задача о крестах не обязательно имеет решение. Нам понадобится лемма и теорема.

Пусть a – произвольная матрица над полем $\mathbb{Z}_2$, состоящая из n строк и m столбцов. Составим для неё следующие суммы:

$$s_{i,\bullet} = \sum_{j=1}^{m} a[i,j], \quad 1 \le i \le n;$$

$$s_{\bullet,j} = \sum_{i=1}^{n} a[i,j], \quad 1 \le j \le m.$$

Для матриц f^{ij} сохраним определение через формулу (6).

Лемма 8. *Пусть для матрицы a существует разложение по матрицам f^{ij}. Тогда справедливы слудеющие утверждения:*

(i) если число строк в матрице a нечётно, то все её суммы $s_{\bullet,j}$ равны одному и тому же числу;

(ii) если число столбцов в матрице a нечётно, то все её суммы $s_{i,\bullet}$ равны одному и тому же числу.

Доказательство. Пусть матрицу a удалось представить в виде суммы некоторых матриц $f_1, ..., f_N$, каждая из которых является матрицей вида f^{ij} при некоторых значениях i, j:

$$a = f_1 + ... + f_N.$$

Реккуррентным образом введём следующие обозначения:

$$a_0 = 0; \quad a_{k+1} = a_k + f_k.$$

Индукцией по k докажем, что каждая из матриц a_k удовлетворяет условиям (i) и (ii). Для матрицы a_0 это очевидно, предположим, что это

также доказано для некоторой матрицы a_k. Если число строк нечётно, то в матрице f_k сумма всех элементов любого столбца равна 1:

$$\sum_{i=1}^{n} f_k[i,j] = 1.$$

По предположению индукции, для любых j_1, j_2 суммы всех элементов в j_1-ом и j_2-ом столбцах совпадают:

$$\sum_{i=1}^{n} a_k[i,j_1] = \sum_{i=1}^{n} a_k[i,j_2].$$

Следовательно,

$$\sum_{i=1}^{n} f_{k+1}[i,j_1] = \sum_{i=1}^{n}(f_k[i,j_1] + a_k[i,j_1]) = 1 + \sum_{i=1}^{n}(a_k[i,j_1]) =$$

$$= 1 + \sum_{i=1}^{n}(a_k[i,j_2]) = \sum_{i=1}^{n}(f_k[i,j_2] + a_k[i,j_2]) = \sum_{i=1}^{n} f_{k+1}[i,j_2].$$

То есть, в матрице a_{k+1} сумма всех элементов любого столбца равна одному и тому же числу, не зависящему от номера столбца. Тогда матрица a удовлетворяет условию (i).

Аналогично доказывается, что если число строк нечётно, то матрица a удовлетворяет условию (ii). □

Теорема 9. *Пусть n и m – произвольные натуральные числа, M – множество матриц над полем $\mathbb{Z}_2$, состоящих из n строк и m столбцов. Множество матриц f^{ij}, определяемых по формуле (6), является базисом линейного пространства M тогда и только тогда, когда оба числа n и m являются чётными (за исключением вырожденного случая $n = m = 1$, тогда $\{f^{11}\}$ – базис в M), при этом произвольная матрица $a \in M$ раскладывается по матрицам f^{ij} следующим образом:*

$$a = \sum_{i=1}^{n}\sum_{j=1}^{m} f^{ij} a^*[i,j], \tag{15}$$

где матрица a^* определяется формулой (7). Разложение матрицы a^* по матрицам f^{ij} имеет вид:

$$a^* = \sum_{i=1}^{n}\sum_{j=1}^{m} f^{ij} a[i,j]. \tag{16}$$

Доказательство. Случай $n = m = 1$ является тривиальным, поэтому считаем, что $n \geq 2$ или $m \geq 2$.

Для начала рассмотрим случай, когда какое-то из чисел n и m является нечётным. Предположим, что для матрицы e^{11}, определяемой по формуле (13), существуют такие отображения φ_1, ..., $\varphi_N \in \Phi$, что их композиция превращает матрицу e^{11} в нулевую матрицу:

$$e^{11}\varphi_1, ..., \varphi_n = 0.$$

По предложению 1 данное равенство эквивалентно

$$e^{11} + f_1 + ... + f_N = 0,$$

где каждая из матриц f_1, ..., f_N имеет вид f^{ij} для некоторых значений i, j. Но тогда для матрицы e^{11} получаем разложение по матрицам f^{ij}:

$$e^{11} = f_1 + ... + f_N,$$

что невозможно по лемме 8.

Перейдём к случаю, когда оба числа n и m являются чётными. Возьмём произвольную матрицу $a \in M$ и запишем для её матрицы переключений разложение по матрицам e^{ij}:

$$a^* = \sum_{i=1}^{n} \sum_{j=1}^{m} e^{ij} \cdot a^*[i, j].$$

Воспользуемся свойством 3:

$$(a^*)^* = \sum_{i=1}^{n} \sum_{j=1}^{m} (e^{ij})^* \cdot a^*[i, j].$$

Здесь мы учли, что множитель $a^*[i, j]$ является числом из поля $\mathbb{Z}_2$. К левой части равенства применяем свойство 4, к правой – предложение 5. Получаем формулу (15). Формула (16) доказывается аналогично. □

Только что доказанная теорема 9 даёт один из методов решения задачи о крестах для случая, когда матрица a имеет как чётное число строк, так и чётное число столбцов. А именно, вычисляем матрицу a^* по формуле (7) (она быстрее, чем формулы (8) и (16)); в качестве преобразований φ^{ij} выбираем все те, для которых $a^*[i, j] = 1$. Тогда из формулы (15) следует, что сумма соответствующих матриц f^{ij} совпадёт с исходной матрицей a, таким образом композиция данных преобразований превратит матрицу a в нулевую матрицу.

Данный алгоритм требует $O(n \cdot m \cdot \max\{n, m\})$ операций для вычисления матрицы переключений и имеет следующие преимущества: во-первых, последовательность преобразований, которая приводит исходную матрицу к нулевой матрице, вычисляется без выполнения самих преобразований; во-вторых, из всех возможных последовательностей преобразований, которые приводят исходную матрицу к нулевой матрице, алгоритм выдаёт последовательность минимальной длины (это следует из того, что матрицы f^{ij} образуют базис).

Если вернуться к первоначальной формулировке задачи, когда к исходной матрице разрешается применять преобразования до того, как получена окончательная последовательность преобразований, то можно предложить другой алгоритм, требующий всего лишь $O(n \cdot m)$ вычислений. Сначала применяем к исходной матрице a все те преобразования φ^{ij}, для которых $a[i, j] = 1$. Согласно формуле (16), данная последовательность преобразований приведёт матрицу a к матрице $a + a^*$. Действительно, если обозначить эти преобразования через φ_1, φ_2, ..., φ_N, а соответствующие им крестовые матрицы – через f_1, f_2, ..., f_N, то

$$a\varphi_1\varphi_2...\varphi_N = a + f_1 + ... + f_N = a + \sum_{i=1}^{n}\sum_{j=1}^{m} f^{ij}a[i, j] = a + a^*.$$

Далее применяем к получившейся матрице все те преобразования φ^{ij}, для которых $(a + a^*)[i, j] = 1$. Получим нулевую матрицу:

$$(a + a^*) + \sum_{i=1}^{n}\sum_{j=1}^{m} f^{ij} \cdot (a + a^*)[i, j] =$$

$$(a + a^*) + \sum_{i=1}^{n}\sum_{j=1}^{m} f^{ij}a[i, j] + \sum_{i=1}^{n}\sum_{j=1}^{m} f^{ij}a^*[i, j] =$$

$$(a + a^*) + (a^* + a^{**}) = (a + a^*) + (a^* + a) = 0.$$

Преимуществом данного алгоритма является высокая скорость его работы. Недостатком алгоритма является то, что последовательность производимых им переключений является не самой короткой.

Приложение

ЗАДАЧА О КРЕСТАХ, ОБЩИЙ СЛУЧАЙ

В данном разделе мы приводим решение задачи о крестах в общем случае[2]. Натуральные числа n и m полагаем фиксированными; множество всех матриц размера $n \times m$ над полем $\mathbb{Z}_2$ обозначаем через $M_{n\times m}$.

Сначала мы рассмотрим задачу о крестах для нечётных значений n и m, а потом разберём случай, когда ровно одно из чисел n, m является нечётным. Случай, когда оба числа n и m чётные, был разобран подробно в основной части работы, и здесь мы не будем к нему возвращаться.

Используем матрицы e^{ij}, $f^{ij} \in M_{n\times m}$, определённые формулами (13) и (6). Эти формулы можно записать по-другому следующим образом[3]:

$$e^{ij}[x,y] \,=\, \delta_{ix}\delta_{jy}; \quad f^{ij}[x,y] \,=\, \delta_{ix} + \delta_{jy} + \delta_{ix}\delta_{jy}, \tag{17}$$

где $\delta_{uv} = 1$ при $u = v$ и $\delta_{uv} = 0$ при $u \neq v$ для любых индексов u, v. Матрицы e^{ij} принято называть *матричными единицами*, а f^{ij} мы будем далее называть *крестовыми матрицами*. δ_{uv} – это *символ Кронекера*.

Для всякой матрицы $a \in M_{n\times m}$ определим её *матрицу переключений* $a^* \in M_{n\times m}$ по формуле (7). Заметим, что соотношение (8) тоже верно, какими бы ни были значения n, m (это видно из доказательства предложения 2). Следовательно, мы можем *по определению* полагать, что

$$a^* = \sum_{i=1}^{n}\sum_{j=1}^{m} f^{ij}a[i,j]. \tag{18}$$

Теорема 10. *Пусть оба числа n и m являются нечётными. Какой бы ни была матрица $a \in M_{n\times m}$, следующие условия для неё равносильны:*

(j) матрица a представима в виде суммы крестовых матриц над полем $\mathbb{Z}_2$ (т.е. является линейной комбинацией матриц $f^{ij} \in M_{n\times m}$);

(jj) $s_{i,\bullet} = s_{\bullet,j}$ для всех i, j (величины, определённые в лемме 8);

(jjj) справедливо равенство $a^* = a$.

(Манилов Д. Ю.)

[2]Изложенные здесь результаты были получены в разные годы уже после того, как заметка «Задача о крестах, чётный случай» была окончена авторами. Никакие из теорем 10 – 13 пока ещё не публиковались в каких-либо рецензируемых журналах.

[3]Все операции, производимые над элементами матриц, выполняем в поле $\mathbb{Z}_2$.

Доказательство. Утверждение $(jjj) \Rightarrow (j)$ очевидно из (18). Импликацию $(j) \Rightarrow (jj)$ легко проверить методом математической индукции: для этого достаточно почти дословно повторить рассуждения из доказательства леммы 8. Покажем, что $(jj) \Rightarrow (jjj)$. Из (17) и (18) следует, что

$$a^*[x,y] \;=\; \sum_{i=1}^{n}\sum_{j=1}^{m}(\delta_{ix}+\delta_{jy}+\delta_{ix}\delta_{jy})\cdot a[i,j] \;=$$

$$=\; \sum_{j=1}^{m} a[x,j] \;+\; \sum_{i=1}^{n} a[i,y] \;+\; a[x,y] \;=\; s_{x,\bullet} + s_{\bullet,y} + a[x,y].$$

Но если $s_{x,\bullet} = s_{\bullet,y}$, то $s_{x,\bullet} + s_{\bullet,y} = 0$ в поле $\mathbb{Z}_2$. Поэтому $(jj) \Rightarrow (jjj)$. $\square$

Следствие. *Пусть n и m нечётны. Задача о крестах для матрицы $a \in M_{n\times m}$ имеет решение (в смысле определения 1) в том и только случае, когда сумма всех элементов этой матрицы, расположенных в любой её строке, совпадает с суммой всех элементов той же матрицы, расположенных в каком угодно её столбце. Если решение существует, то оно не обязательно единственное. В качестве преобразований φ_1, ..., φ_N (в том случае, когда хотя бы одно решение задачи о крестах для заданной матрицы a существует) можно выбирать все те преобразования φ^{ij}, для которых $a[i,j] = 1$.*

Итак, следствие из теоремы 10 описывает решение задачи о крестах в том случае, когда оба числа n и m нечётные. Более сложным является случай, когда чётности чисел n и m различаются. Без доказательства приведём утверждение, которое следует из результатов работы [1]:

Предложение 11. *Пусть $H_{n\times m}$ – линейная оболочка множества всех крестовых матриц пространства $M_{n\times m}$:*

$$H_{n\times m} \;=\; \left\{ \sum_{i=1}^{n}\sum_{j=1}^{m} k_{ij} f^{ij} \;\middle|\; k_{ij} \in \mathbb{Z}_2 \right\} \;\subseteq\; M_{n\times m}.$$

Тогда размерность линейного пространства $H_{n\times m}$ равна

$$\dim H_{n\times m} \;=\; \alpha + (n-\beta)(m-\gamma),$$

где введены следующие обозначения[4]*:*

$$\alpha \;=\; \beta+\gamma-\beta\gamma; \quad \beta \;=\; n \bmod 2; \quad \gamma \;=\; m \bmod 2.$$

[4]Через $x \bmod y$ мы обозначаем остаток от деления числа x на число y. Например, если $n = 2$ и $m = 3$, то $\dim H_{n\times m} = 5$; а если $n = 3$ и $m = 3$, то тоже $\dim H_{n\times m} = 5$.

Хлоп! Ооо...

Предложение 12. *Пусть одно из чисел n или m является нечётным, а другое число – чётное. Если для матрицы $a \in M_{n\times m}$ выполнены оба условия (i) и (ii) леммы 8, то существует представление матрицы a в виде суммы крестовых матриц линейного пространства $M_{n\times m}$.*

(Кожухов И. Б.)

Доказательство. Без ограничения общности считаем, что n (количество строк!) нечётно, а число m чётно. Тогда из предложения 11 следует:

$$\dim H_{n\times m} = 1 + (n-1)m.$$

Отсюда находим[5] мощность множества $H_{n\times m}$:

$$|H_{n\times m}| \,=\, 2^{1+(n-1)m} \,=\, 2\cdot 2^{(n-1)m}.$$

Пусть теперь H' – это множество всех таких матриц из пространства $M_{n\times m}$, у каждой из которых значение её величины $s_{\bullet,j}$ не зависит от j:

$$H' \,=\, \left\{ a \in M_{n\times m} \;\middle|\; \sum_{i=1}^{n} a[i,j_1] = \sum_{i=1}^{n} a[i,j_2] \text{ для всех } j_1, j_2 \right\}.$$

Покажем, прежде всего, что $|H'| = |H_{n\times m}|$.

Действительно, всего существует 2^n упорядоченных наборов, составленных из n элементов множества $\mathbb{Z}_2$:

$$\operatorname{Card}\left\{(x_1, x_2, ..., x_n) \,|\, x_1, x_2, ..., x_n \in \mathbb{Z}_2\right\} \,=\, 2^n.$$

Ровно половина из этих наборов (т.е. 2^{n-1} штук) содержит чётное число единичных элементов, остальные 2^{n-1} упорядоченных наборов содержат нечётное число единиц. Следовательно, всего существует $2^{(n-1)m}$ матриц над полем $\mathbb{Z}_2$, у которых сумма элементов любого столбца равна 0; столько же существует матриц над $\mathbb{Z}_2$, у которых сумма элементов в каждом столбце равна 1. Таким образом, $|H'| = 2\cdot 2^{(n-1)m} = |H_{n\times m}|$.

А теперь, поскольку $H' \subseteq H_{n\times m}$ ввиду леммы 8, то $H' = H_{n\times m}$. $\square$

В задаче о крестах случай, когда ровно одно из чисел n или m нечётно, долгое время оставался проработанным лишь на уровне леммы 8 и предложения 12. Сформулируем же, наконец, теорему, которая даёт в рассматриваемом случае решение задачи о крестах в явном виде:

[5]Пусть L – произвольное линейное пространство, построенное над полем F. Понятно, что множество L содержит в точности k^h элементов, где $k = |F|$ и $h = \dim L$.

Теорема 13. *Пусть n – нечётное число, а число m чётное. Следующие условия равносильны для любой $n \times m$-матрицы a над полем $\mathbb{Z}_2$:*

(j) матрица a представима в виде линейной комбинации крестовых матриц $f^{ij} \in M_{n\times m}$;

(jj) сумма элементов любого столбца матрицы a совпадает с суммой элементов любого другого её столбца (иначе говоря, для матрицы a значение её величины $s_{\bullet,j}$ из леммы 8 не зависит от индекса j);

(jjj) для любого j имеет место следующее равенство:

$$a + a^* \;=\; \sum_{i=1}^{n} (f^{ij} + g^{ij}) \cdot (a + a^*)[i, j], \tag{19}$$

где $g^{ij} = (f^{ij})^*$.

(Решетников А. В.)

Перед тем, как приступить к доказательству теоремы, найдём компоненты матрицы $f^{ij} + g^{ij}$. Для этого воспользуемся линейностью отображения $a \mapsto a^*$ и заметим, что

$$f^{ij} + g^{ij} \;=\; (e^{ij})^* + (f^{ij})^* \;=\; (e^{ij} + f^{ij})^*.$$

Таким образом, сумма $f^{ij} + g^{ij}$ является матрицей переключений:

$$f^{ij} + g^{ij} \;=\; \sum_{u=1}^{n} \sum_{v=1}^{m} f^{uv} \cdot (e^{ij} + f^{ij})[u, v],$$

согласно определению (18). Так как вычисления мы проводим в поле $\mathbb{Z}_2$, то $(e^{ij} + f^{ij})[u, v] = \delta_{iu} + \delta_{jv}$. Отсюда получаем следующие соотношения:

$$f^{ij} + g^{ij} \;=\; \sum_{u=1}^{n} \sum_{v=1}^{m} (\delta_{iu} + \delta_{jv}) f^{uv} \;=\; \sum_{v=1}^{m} f^{iv} \;+\; \sum_{u=1}^{n} f^{uj};$$

$$\sum_{v=1}^{m} f^{iv}[x, y] \;=\; \sum_{v=1}^{m} (\delta_{ix} + \delta_{vy} + \delta_{ix}\delta_{vy}) \;=\; m \cdot \delta_{ix} + 1 + \delta_{ix};$$

$$\text{аналогично } \sum_{u=1}^{n} f^{uj}[x, y] \;=\; n \cdot \delta_{jy} + 1 + \delta_{jy};$$

окончательно:

$$(f^{ij} + g^{ij})[x, y] \;=\; (m + 1)\delta_{ix} + (n + 1)\delta_{jy}. \tag{20}$$

Доказательство теоремы 13. Из равенства (18) ясно, что $(jjj) \Rightarrow (j)$. Из леммы 8 напрямую следует, что $(j) \Rightarrow (jj)$. Предложение 12 влечёт за собой $(jj) \Rightarrow (j)$, и остаётся доказать лишь импликацию $(j) \Rightarrow (jjj)$.

Воспользуемся методом математической индукции. Предположим, что матрица a представима в виде суммы матриц f_1, f_2, ..., $f_N \in M_{n\times m}$, *каждая из которых является крестовой матрицей*:

$$a \;=\; f_1 + ... + f_N.$$

То есть, выполнено условие (j). Введём рекуррентные обозначения:

$$a_0 = 0; \quad a_{k+1} = a_k + f_{k+1}.$$

Тогда $a = a_N$. Проверим выполнение следующего равенства:

$$(a_k + a_k^*)[x,y] \;=\; \sum_{i=1}^{n} \delta_{ix} \cdot (a_k + a_k^*)[i,j], \quad \text{где } 0 \le k \le N. \tag{21}$$

Если $k = 0$ (базис индукции), то $a_k = a_k^* = 0$, и соотношение (21) действительно имеет место. Теперь в рамках индуктивного перехода *предположим, что* (21) *уже доказано для некоторого значения* k. Так как f_{k+1} – крестовая матрица, то $f_{k+1} = f^{uv}$ для каких-то u, v. В таком случае:

$$\begin{aligned} a_{k+1} \;&=\; a_k + f_{k+1} \;\equiv\; a_k + f^{uv}; \\ a_{k+1} + a_{k+1}^* \;&=\; (a_k + f_{k+1}) \;+\; (a_k + f_{k+1})^*; \\ (a_{k+1} + a_{k+1}^*)[x,y] \;&=\; (a_k + a_k^*)[x,y] + (f^{uv} + g^{uv})[x,y]. \end{aligned} \tag{22}$$

(Мы помним, что отображения $a_k \mapsto a_k^*$ и $f^{uv} \mapsto g^{uv}$ линейны.) По условию теоремы число n нечётно, а m – чётно. Следовательно:

$$(f^{uv} + g^{uv})[x,y] \;=\; \delta_{ux} \tag{23}$$

ввиду соотношения (20). С другой стороны:

$$\sum_{i=1}^{n} \delta_{ix} \cdot (f^{uv} + g^{uv})[i,j] \;=\; \sum_{i=1}^{n} \delta_{ix}\delta_{ui} \;\equiv\; \delta_{ux}. \tag{24}$$

Подставляя (21), (23) и (24) в (22), получаем соотношение

$$(a_{k+1} + a_{k+1}^*)[x,y] \;=\; \sum_{i=1}^{n} \delta_{ix} \cdot (a_k + a_k^*)[i,j] \;+\; \sum_{i=1}^{n} \delta_{ix} \cdot (f^{uv} + g^{uv})[i,j].$$

Но это завершает индуктивный переход и доказывает, что равенство (21) верно для любых значений $k \le N$. А отсюда сразу же следует (19), поскольку $a = a_N$ и в условиях теоремы $\delta_{ix} = (f^{ij} + g^{ij})[x,y]$. $\square$

Подводя итог, сформулируем основные следствия из теорем 9, 10 и 13:

Следствие 1. *Какой бы ни была матрица $a \in M_{n\times m}$, если для неё выполнены оба условия (i) и (ii) леммы 8, то матрица a представима в виде линейной комбинации крестовых матриц $f^{ij} \in M_{n\times m}$. В зависимости от количества строк и столбцов, разложение матрицы a по крестовым матрицам даётся одной из формул (15), $a = a^*$, либо (19).*

Следствие 2. *Пусть для матрицы $a \in M_{n\times m}$ выполнены оба условия (i) и (ii) леммы 8. Тогда для неё существует решение задачи о крестах в смысле определения 1. Для нахождения конкретного решения φ_1, φ_2, ..., φ_N достаточно представить матрицу a в виде линейной комбинации крестовых матриц f_1, f_2, ..., f_N и воспользоваться предложением 1.*

В заключение отметим, что термин «матрица переключений» в настоящее время является устаревшим. Самую суть теории крестовых матриц можно выразить простой формулой, верной над любым полем F, и даже над любым кольцом R с единицей, не обязательно ассоциативным:

$$\begin{pmatrix} (e^{ij})^* \\ (e^{\bullet j})^* \\ (e^{i\bullet})^* \\ (e^{\bullet\bullet})^* \end{pmatrix} = \begin{pmatrix} -1 & 1 & 1 & 0 \\ 0 & n-1 & 0 & 1 \\ 0 & 0 & m-1 & 1 \\ 0 & 0 & 0 & n+m-1 \end{pmatrix} \begin{pmatrix} e^{ij} \\ e^{\bullet j} \\ e^{i\bullet} \\ e^{\bullet\bullet} \end{pmatrix}$$

Обозначения приняты следующие:

$$e^{\bullet j} = \sum_{i=1}^{n} e^{ij}; \quad e^{i\bullet} = \sum_{j=1}^{m} e^{ij}; \quad e^{\bullet\bullet} = \sum_{i=1}^{n}\sum_{j=1}^{m} e^{ij}.$$

Через e^{ij} по-прежнему обозначена $n \times m$-матрица, определённая формулой (13); но её компоненты теперь выбираются из поля F или, соответственно, из кольца R. Крестовые матрицы f^{ij} определены формулой (6); понятно, что соотношения (17) для них требуют внесения исправлений. А линейное преобразование $a \mapsto a^*$ всё так же выполняется по формуле (18). Матрицу a^* предлагается называть *тенью* матрицы a.

Список литературы

[1] *Кожухов И. Б., Манилов Д. Ю., Решетников А. В.* О крестовых матрицах. // в печати (по состоянию на 15-ое февраля 2026 г.)