22 Матрицы Belt

Задача. В алгоритме выработки имитовставки стандарта СТБ 34.101.31 (Belt) используются две матрицы над полем $\mathbb{F}_2$:

$$M_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Вместе с единичной матрицей M_0 они образуют множество S, которое обладает следующим свойством: сумма любого числа любых различных элементов S является обратимой матрицей. Найдите еще одну матрицу M_3, после добавления которой к S свойство останется справедливым.

Решение. Матрица M_1 является клеткой Фробениуса с неприводимым характеристическим многочленом $f(x) = x^4 + x + 1$. Степени M_1^i, $i = 0, 1, \ldots, 15$, вместе с нулевой матрицей образуют поле из 16 элементов. Матрица M_2 является элементом этого поля: $M_2 = M_1^{14}$.

В задаче требуется дополнить набор (M_0, M_1, M_2) до базиса поля. Дополнить можно матрицей

$$M_1^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

□

Обсуждение. Возникает вопрос: можно ли построить множество S с бóльшим числом элементов? Оказывается, что нет.

Теорема. Пусть $S = \{M_1, \ldots, M_k\}$ — множество матриц порядка n над конечным полем F. Пусть для любых $x_1, \ldots, x_k \in F$, не равных одновременно нулю, матрица

$$x_1 M_1 + \ldots + x_k M_k \qquad (\star)$$

обратима. Тогда $k \leq n$.

Следующие доказательства теоремы принадлежат соответственно Г. В. Матвееву и С. А. Мазанику.

Доказательство 1. Определитель матрицы $(\star)$ — это многочлен $f(x_1, \ldots, x_k) \in F[x_1, \ldots, x_k]$. Степень этого многочлена не превосходит n и $f(0, \ldots, 0) = 0$. Если $k > n$, то по теореме Шевалле[1] найдется ненулевой вектор $(c_1, \ldots, c_k) \in F^n$ такой, что $f(c_1, \ldots, c_k) = 0$, т. е. матрица $c_1 M_1 + \ldots + c_k M_k$ не будет обратимой. □

Доказательство 2. Пусть $m_1, \ldots, m_k$ — первые строки матриц $M_1, \ldots, M_k$. Если $k > n$, то найдется ненулевой вектор $(c_1, \ldots, c_k) \in F^n$ такой, что $c_1 m_1 + \ldots + c_k m_k = (0, \ldots, 0)$ и матрица $c_1 M_1 + \ldots + c_k M_k$ не будет обратимой. □

[1] [Лиддл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988, стр. 333].