А. Е. Т р и ш и н, **А. А. Ф р о л о в** (Москва, ТВП). **Способ построения (v,k)-матриц при помощи функции след.**

Положим $K = \mathrm{GF}(2)$, $F = \mathrm{GF}(2^n)$; $\mathrm{tr} = Tr_{F/K}$ есть функция след из поля F в поле K; δ_{ij} — символ Кронекера; $R\sum$ — знак суммирования в поле вещественных чисел; $\overline{L}$ — прямое алгебраическое дополнение над K подпространства L до пространства F; I — единичная матрица; O — нулевая матрица; J — матрица, состоящая из одних единиц.

Понятие (v,k)-матрицы определяется в работе [1]. Это квадратная матрица порядка v над полем K с k единицами в каждой строке и в каждом столбце, для которой существует обратная матрица, обладающая тем же свойством. Такие матрицы представляют интерес для современной теории кодирования.

В данном сообщении поле F будет рассматриваться как векторное пространство размерности n над полем K. Пусть $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ есть некоторый базис поля F, $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_n)$ есть базис F, являющийся дуальным для базиса $\boldsymbol{\alpha}$. Свойство дуальности означает (см. [2]), что любой элемент $x \in F$ представляется в виде $x = \sum_{i=1}^{n} \mathrm{tr}\,(\beta_i x)\alpha_i$.

Рассмотрим подпространство L_0 пространства F, состоящее из всех элементов F, на которых функция след принимает значение 0, $L_0 = \{x \in F \mid \mathrm{tr}\,(x) = 0\}$. Предположим, что базис $\boldsymbol{\alpha}$ содержит k векторов, принадлежащих L_0, $k > 2$. Будем считать, что этими векторами являются $\alpha_1, \ldots, \alpha_k$. Элементы $\alpha_1, \ldots, \alpha_k$ порождают подпространство L_α пространства L_0 размерности k. Пусть $\overline{L}_\alpha$ — прямое алгебраическое дополнение над K подпространства L_α до пространства F, порождаемое векторами $\alpha_{k+1}, \ldots, \alpha_n$. Для произвольного вектора $\gamma \in \overline{L}_\alpha$ рассмотрим аффинное подпространство $M = L_\alpha + \gamma$. Его элементы m_i занумеруем каким-либо образом числами из интервала $i, \ldots, 2^k$. Определим квадратную $(0,1)$-матрицу $\mathbf{T} = (t_{ij})_{2^k \times 2^k}$ равенством $t_{ij} = \mathrm{tr}\,(m_i m_j)$, $i, j = 1, \ldots, 2^k$. Обозначим через L_β подпространство пространства F, порождаемое векторами $\beta_1, \ldots, \beta_k$ дуального базиса, $\overline{L}_\beta$ — подпространство, порождаемое векторами $\beta_{k+1}, \ldots, \beta_n$.

Утверждение 1. 1) *Матрица* $\mathbf{T}$ *симметрична.*

2) *На главной диагонали матрицы* $\mathbf{T}$ *стоят элементы, равные* $\mathrm{tr}\,(\gamma)$.

3)

$$R\sum_{i=1}^{2^k} t_{ij} = \begin{cases} 2^{k-1}, & \text{если } m_j \notin \overline{L}_\beta, \\ 0, & \text{если } m_j \in \overline{L}_\beta,\ \mathrm{tr}\,(\gamma) = 0, \\ 2^k, & \text{если } m_j \in \overline{L}_\beta,\ \mathrm{tr}\,(\gamma) = 1. \end{cases}$$

4) $\mathbf{T}^2 = \mathbf{O}$.

Утверждение 1 позволяет предложить следующий способ построения инволютивных (v,k)-матриц. Рассмотрим три случая.

I случай. Матрица $\mathbf{T}$ не содержит строк, состоящих только из нулей или только из единиц. Определим матрицу $\mathbf{A} = \mathbf{T} + \mathbf{I}$. Так как $\mathbf{T}^2 = \mathbf{O}$, то $\mathbf{A}^2 = \mathbf{I}$. Если $\mathrm{tr}\,(\gamma) = 0$, то на главной диагонали матрицы $\mathbf{A}$ стоят одни единицы и $\mathbf{A}$ является $(2^k, 2^{k-1} + 1)$-матрицей. Если же $\mathrm{tr}\,(\gamma) = 1$, то $\mathbf{A}$ имеет нулевую главную диагональ и является примером $(2^k, 2^{k-1} - 1)$-матрицы.

II случай. Матрица $\mathbf{T}$ имеет ровно s нулевых строк. В этом случае $\mathrm{tr}\,(\gamma) = 0$. Пусть матрица $\mathbf{T}'$ получается из матрицы $\mathbf{T}$ вычеркиванием всех нулевых строк и нулевых столбцов. Определим матрицу $\mathbf{A} = \mathbf{T}' + \mathbf{I}$, она будет $(2^k - s, 2^{k-1} + 1)$-матрицей.

III случай. Матрица $\mathbf{T}$ имеет ровно s строк, состоящих из одних единиц, $s \geqslant 1$. Тогда $\mathrm{tr}\,(\gamma) = 1$. Пусть матрица $\mathbf{T}'$ получается из матрицы $\mathbf{T}$ вычеркиванием всех единичных строк и единичных столбцов.

Если $s = 1$, то $(\mathbf{T}')^2 = J$. Следовательно, $(\mathbf{T}' + \mathbf{J})^2 = \mathbf{O}$. Определим матрицу $\mathbf{A} = \mathbf{T}' + \mathbf{J} + \mathbf{I}$, она является $(2^{k-1}, 2^{k-1} + 1)$ -матрицей.

Если $s \neq 1$, то, как следует из приведенного ниже утверждения 2, число s четно. Значит, в этом случае $(\mathbf{T}')^2 = \mathbf{O}$. Тогда $\mathbf{A} = \mathbf{T}' + \mathbf{I}$ является $(2^k - s, 2^{k-1} - s - 1)$-матрицей.

Особенностью изложенного способа является возможность построения (v, k)-матриц различных порядков. Как следует из приведенного ниже утверждения 2, построенная этим способом матрица имеет порядок, равный 2^k, либо одному из чисел $2^k \pm 2^r$ при некотором неотрицательном целом числе r.

Утверждение 2. 1) *Матрица* $\mathbf{T}$ *не содержит одновременно нулевые и единичные строки.*

2) *Строка матрицы* $\mathbf{T}$ *с номером* i *состоит из одних нулей либо из одних единиц тогда и только тогда, когда* $m_i \in \overline{L}_\beta$.

3) *Произвольный вектор* $\mathbf{m} = \mathbf{y} + \boldsymbol{\gamma}$, $\boldsymbol{\gamma} \in L_\alpha$, *аффинного подпространства* M *содержится в подпространстве* $\overline{L}_\beta$ *тогда и только тогда, когда первые* k *координат* $a_1(\mathbf{y}), \ldots, a_k(\mathbf{y})$ *вектора* $\mathbf{y}$ *в базисе* $\boldsymbol{\alpha}$ *удовлетворяют условию* $\mathbf{C}\,(a_1(\mathbf{y}), \ldots, a_k(\mathbf{y}))' = (b_1, \ldots, b_k)'$, *где* $\mathbf{C} = (c_{ij})_{k\times k}$ *есть* $(0,1)$*-матрица с элементами* $c_{ij} = \operatorname{tr}(\alpha_i\alpha_j)$, $b_i = \operatorname{tr}(\gamma\alpha_i)$, $i, j = 1, \ldots, k$, *символ* $'$ *означает транспонирование.*

СПИСОК ЛИТЕРАТУРЫ

1. *Малышев Ф. М.*, *Тараканов В.Е.* О (v, k)-конфигурациях. — Математический сборник, 2001, т. 192, № 9, с. 85–108.
2. *Лидл Р.*, *Нидеррайтер Г.* Конечные поля. М: Мир, 1988.