УДК 519.12

В. И. Масол

Некоторые применения алгоритмов построения подпространств над конечным полем

1. Пусть $GF(q)$ — конечное поле, содержащее q элементов (q — степень простого числа). Векторное пространство размерности n над полем $GF(q)$ обозначим V_n. Рассмотрим алгоритм построения множества базисных векторов k-мерного подпространства V_K в пространстве V_n, $k = \overline{1, n}$.

Алгоритм 1 (см., например, [1]). Выбираем k-подмножество $S = (a_1, a_2, \ldots, a_k)$, $a_1 < a_2 < \ldots < a_k$, множества $N = \{1, 2, \ldots, n\}$. В матрице B с k строками и n столбцами образуем единичную $k \times k$ матрицу из столбцов с номерами из S. В i-й строке матрицы B записываем нуль во все позиции $j > a_i$, $i = \overline{1, k}$. Оставшиеся места матрицы B заполняем элементами поля независимым образом.

Различные применения алгоритма 1 можно найти в [1; 2, с. 219] и в пп. 2—4.

Обозначим через $|v|$ число отличных от нуля компонент вектора $v \in V_n$. Весом подпространства $V_k, k = \overline{1,n}$, назовем число $\min\limits_{v \in V_k, v \neq 0} |v|$. Некоторые свойства веса подпространств приведены в обзоре [3]

k-Мерное подпространство, имеющее вес ω, обозначим через $V_{(k|\omega)}$, а число указанных подпространств в пространстве V_n — через $\left[\begin{array}{c|c} n & \omega \\ k & \end{array}\right]$. Ясно, что число $\begin{bmatrix} n \\ k \end{bmatrix}$ k-мерных подпространств в пространстве V_n удовлетворяет равенству

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{\omega \geqslant 1} \left[\begin{array}{c|c} n & \omega \\ k & \end{array}\right] \tag{1}$$

при $k > 0$ Примем $\begin{bmatrix} n \\ 0 \end{bmatrix} = 1$, $n \geqslant 0$. В п. 5 приведены алгоритм построения k-мерных подпространств, имеющих вес $\omega \geqslant 2$, и его обоснование.

2. Пусть $N_{k,\omega,r}$ — число подпространств $V_{(k|\omega)}$ в пространстве V_n, содержащих фиксированное r-мерное подпространство. Используя алгоритм 1, несложно убедиться в том, что справедлива следующая теорема.

Теорема 1. *Для целых* $n \geqslant k \geqslant r \geqslant 0$ $N_{k,1,r} = \left\{\begin{bmatrix} n-r \\ k-r \end{bmatrix}\right.$, *если подпространство* V_r *имеет вес* $\omega = 1$; $\left.\left[\begin{array}{c|c} n-r & 1 \\ k-r & \end{array}\right] \text{— } \textit{в противном случае}\right\}$,

$$N_{k,2,r} = \begin{cases} \begin{bmatrix} n-r \\ k-r \end{bmatrix} - \left[\begin{array}{c|c} n-r & 1 \\ k-r & \end{array}\right], & \textit{если } V_r \textit{ имеет вес } \omega = 2; \\ \left[\begin{array}{c|c} n-r & 2 \\ k-r & \end{array}\right], & \textit{если } r = 0 \text{ или } r \geqslant 1 \textit{ и } V_r \textit{ имеет вес } \omega \geqslant 3. \end{cases} \tag{2}$$

3. Пусть $m=n-k$, $m\geqslant 0$. Если $m=0$, то для $n>0$ $\left[\begin{matrix} n \\ k \end{matrix}\right] = \left[\begin{matrix} n \\ k \end{matrix}\middle| 1\right] = 1$; если $m>0$ и $k>0$, то правая часть равенства (1) содержит по крайней мере два слагаемых (в частности, при $m=1$ для $n\geqslant 2$ имеем $\left[\begin{matrix} n \\ n-1 \end{matrix}\right] = \left[\begin{matrix} n \\ n-1 \end{matrix}\middle| 1\right] + \left[\begin{matrix} n \\ n-1 \end{matrix}\middle| 2\right]$); если и только если $m\geqslant 0$ и $k=1$, то в правую часть (1) войдет максимальное число слагаемых, равное n. Указанные факты легко установить с помощью алгоритма 1. Основным результатом п. 3 является следующая теорема.

Теорема 2. *Условие*

$$(q^m-(q-1)\,m-1)/(q-1)<k, \tag{3}$$

где $1\leqslant k\leqslant n$, является необходимым и достаточным для того, чтобы выполнялось равенство

$$\left[\begin{matrix} n \\ k \end{matrix}\right] = \left[\begin{matrix} n \\ k \end{matrix}\middle| 1\right] + \left[\begin{matrix} n \\ k \end{matrix}\middle| 2\right]. \tag{4}$$

Лемма. *Для $m\geqslant 2$ максимальное число T строк, которые может включать в себя матрица B, построенная согласно алгоритму 1 и являющаяся базисом подпространства $V_{(T\,|\omega)}$, $\omega\geqslant 3$, удовлетворяет соотношению*

$$T\leqslant (q^m-(q-1)\,m-1)/(q-1). \tag{5}$$

Доказательство леммы. Пусть матрица B построена согласно алгоритму 1, имеет k строк и, не нарушая общности дальнейшего изложения, примем, что содержащаяся в ней единичная $k\times k$ матрица (см. алгоритм 1) занимает столбцы с номерами $m+1$, $m+2$, ..., n. Подматрицу матрицы B, включающую в себя столбцы с номерами $1, 2, \ldots, m$, обозначим B'. Очевидно, что следующие два условия являются необходимыми и достаточными для того, чтобы матрица B порождала подпространство, имеющее вес $\omega\geqslant 3$:

$У_1$. Каждая строка матрицы B' имеет вес $\omega\geqslant 2$;

$У_2$. Любые две строки матрицы B' являются линейно независимыми над полем $GF(q)$.

С помощью $У_1$ и $У_2$ несложно установить соотношение (5). Лемма доказана.

Доказательство теоремы 2. Для $m\in\{0, 1\}$ и $1\leqslant k\leqslant n$ справедливость теоремы 2 следует из фактов, приведенных в п. 3 перед ее формулировкой. Для $m\geqslant 2$ обоснование необходимости и достаточности условия (3) с учетом леммы не вызывает затруднений. Теорема 2 доказана.

4. Различные доказательства соотношения $\left[\begin{matrix} n \\ k \end{matrix}\right] = \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\right] + q^k \left[\begin{matrix} n-1 \\ k \end{matrix}\right]$ приведены в [1; 4, с. 125; 5]. В [1] последнее равенство получено с помощью алгоритма 1.

Теорема 3. *Для целых $n\geqslant k\geqslant 1$* $\left[\begin{matrix} n \\ k \end{matrix}\middle| 1\right] = \left[\begin{matrix} n-1 \\ k \end{matrix}\middle| 1\right] + \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\right] + \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 1\right](q^m-1)$, *где* $\left[\begin{matrix} d \\ p \end{matrix}\middle| 1\right] = 0$, *если либо* $p=0$, либо $p>d$.

Теорема 4. *Для целых $n\geqslant k\geqslant 1$*

$$\left[\begin{matrix} n \\ k \end{matrix}\middle| 2\right] = \left[\begin{matrix} n-1 \\ k \end{matrix}\middle| 2\right] + \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 2\right](q^m-1) + \left(\left[\begin{matrix} n-1 \\ k-1 \end{matrix}\right] - \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 1\right] - \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 2\right]\right)(n-1)(q-1), \tag{6}$$

где $\left[\begin{matrix} d \\ p \end{matrix}\middle| 2\right] = 0$, *если либо* $p=0$, *либо* $p>d$.

Д о к а з а т е л ь с т в о т е о р е м ы 4. Из алгоритма 1 следует, что матрица B, являющаяся базисной для подпространства $V_{(k|2)}$ в пространстве V_n, может быть одного и только одного из следующих трех видов:

а) n-й столбец матрица B — нулевой, а остальные $(n-1)$-мерные строки служат базисом k-мерного подпространства $V_{(k|2)}$ в пространстве V_{n-1};

б) k-я строка матрицы B содержит по крайней мере два отличных от нуля элемента поля, причем один из них равен единице и расположен на n-й позиции, а остальные строки служат базисом $(k-1)$-мерного подпространства $V_{(k-1|2)}$ в пространстве V_{n-1};

в) на позиции (k, n) в матрице B находится единица поля, остальные позиции k-й строки заполнены либо одним ненулевым элементом поля, либо конфигурацией элементов, отличных от нуля поля, совпадающей (с точностью до множителя из $GF(q)$) с конфигурацией одной из строк матрицы, остающейся после удаления из B единичной $k \times k$-матрицы, а элементы вне k-й строки и n-го столбца образуют базисную матрицу $(k-1)$-мерного подпространства, имеющего вес $\omega \geqslant 3$, в пространстве V_{n-1}.

Число подпространств, удовлетворяющих условию а), равно $\left[\begin{matrix} n-1 \\ k \end{matrix}\middle| 2\right]$, условию б) — $\left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 2\right](q^m-1)$, условию в) — $\left(\left[\begin{matrix} n-1 \\ k-1 \end{matrix}\right] - \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 1\right] - \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 2\right]\right)(n-k)(q-1)$, если вес k-й строки матрицы B равен 2; $\left(\left[\begin{matrix} n-1 \\ k-1 \end{matrix}\right] - \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 1\right] - \left[\begin{matrix} n-1 \\ k-1 \end{matrix}\middle| 2\right]\right)(k-1)(q-1)$, если вес k-й строки матрицы B больше или равен 3. Суммируя числа, найденные выше, получаем (6).

Теорема 3 доказывается аналогично теореме 4.

5. Пусть $m \geqslant 1$ и $k \geqslant 1$. Рассмотрим алгоритм построения множества базисных векторов k-мерного подпространства $V_{(K|\omega)} \subset V_n$, $\omega \geqslant 2$.

А л г о р и т м 2. Выбираем k-подмножество $S = (a_1, a_2, \ldots, a_k)$, $2 \leqslant a_1 < a_2 < \ldots < a_k$ и k-подмножество $(t_1, t_2, \ldots, t_k)$ из множества N так, чтобы $t_i \in N \setminus \{S \cup (a_i+1, a_i+2, \ldots, n)\}$, $i = \overline{1, k}$. В матрице B с k строками и n столбцами образуем единичную $k \times k$-матрицу из столбцов с номерами из S. В i-й строке матрицы B записываем нуль во все позиции с номерами $j > t_i$, $j \neq a_i$; ненулевым элементом заполняем позицию t_i; на местах с номерами $\mu < t_i$, $\mu \notin S$, помещаем элементы поля независимым образом, $i = \overline{1, k}$.

Очевидно, что каждое заполнение матрицы B согласно алгоритму 2 приводит к базису некоторого k-мерного подпространства, имеющего вес $\omega \geqslant 2$, пространства V_n. Методом полной математической индукции по параметру $k \geqslant 1$ несложно обосновать следующий результат.

Т е о р е м а 5. *Каждому k-мерному подпространству $V_{(k|\omega)}$, имеющему вес $\omega \geqslant 2$, $V_{(k|\omega)} \subset V_n$, соответствует одна и только одна базисная матрица, построенная согласно алгоритму* 2.

З а м е ч а н и е. С помощью алгоритма 2 можно установить соотношения (2) и (6).

1. *Calabi E., Wilf H. S.* On the sequential and random selection of subspaces over a finite field // J. Combin. Theory A.— 1977.— 22, N 1.— P. 107—109.
2. *Эндрюс Г.* Теория разбиений.— М. : Наука, 1982.— 256 с.
3. *Гоппа В. Д.* Коды и информация // Успехи мат. наук.— 1984.— 39, № 1.— С. 77—120.
4. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики.— М. : Наука, 1982.— 384 с.
5. *Goldman J. R., Rota G.-C.* On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions // Studie in Appl. Math.— 1970.— 49, N 3.— P. 239—258.

Киев. ун-т

Получено 27.01.88