Быстрая нумерация элементов грассманиана

Ю. С. Медведева
Институт вычислительных технологий СО РАН, Новосибирск, Россия
e-mail: mjulja@gmail.com

Грассманиан $G_q(n,k)$ — множество всех k-мерных подпространств векторного пространства F_q^n над конечным полем размера q. Задача кодирования элементов грассманиана рассматривалась во многих работах и находит применение в сетевом кодировании. В настоящей работе предлагается нумерационный метод кодирования элементов грассманиана, превосходящий по скорости методы кодирования элементов грассманиана, известные ранее.

Ключевые слова: кодирование, нумерационное кодирование, быстрое кодирование, теория информации.

Введение

Пусть F_q — конечное поле размера q. Грассманианом называется множество всех k-мерных подпространств векторного пространства F_q^n, обозначаемое $G_q(n,k)$, для любых k и n, $0 < k \leq n$. Нумерационным кодированием элементов грассманиана $G_q(n,k)$ является сопоставление каждому элементу грассманиана его номера, т. е. двоичного слова из промежутка $[0,\ldots,|G_q(n,k)|-1]$. Задача кодирования элементов грассманиана в течение последних сорока лет рассматривалась во многих работах, например в [1 – 7]. В [8] было показано, как использовать коды с исправлением ошибок на множестве $G_q(n,k)$ в случайном сетевом кодировании. Это приложение привело к появлению большого числа исследований в данной области [9 – 19]. В работе Н. Зильберштейн и Т. Эциона [20] представлен алгоритм нумерационного кодирования элементов грассманиана, сложность которого равна $O(nk(n-k)\log n \log\log n)$. В настоящей работе предлагается улучшенный алгоритм нумерационного кодирования элементов грассманиана, сложность которого $O(\log n M[n^2])$, где $M[a]$ — время умножения двух слов длины a. Таким образом при использовании алгоритма быстрого умножения Фюрера [21] сложность предлагаемого алгоритма равна $O(n^2\log^2 n 2^{O(\log^* n)})$. Улучшенный алгоритм основан на методе быстрой нумерации комбинаторных объектов [22]

1. Определения и предварительные результаты

Известно, что мощность грассманиана $G_q(n,k)$ равна $\begin{bmatrix} n \\ k \end{bmatrix}_q$ [23], где $\begin{bmatrix} n \\ k \end{bmatrix}_q$ есть q-ичный гауссов коэффициент, определяемый следующим образом:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{q-1} \frac{q^{n-i}-1}{q^{k-i}-1}.$$

Алгоритм нумерации элементов грассманиана, представленный в настоящей работе, как и описанный в [20], основан на методе Ковера [24] для нумерации элементов произвольного множества векторов длины n над конечным алфавитом $A = \{0, 1, \ldots, k-1\}$, расположенных в лексикографическом порядке.

Обозначим через $S \in A^n$ нумеруемое множество, через $n_S(x_1, x_2, \ldots, x_{j-1}, m)$ — количество векторов из S, у которых первые j координаты равны $(x_1, x_2, \ldots, x_{j-1}, m)$. Согласно методу Ковера, номер элемента множества $x \in S$, упорядоченного лексикографически, найдем по формуле

$$code(x) = \sum_{j=1}^{n} \sum_{m<x_j} n_S(x_1, x_2, \ldots, x_{j-1}, m). \tag{1}$$

Любое k-мерное подпространство $X \in G_q(n, k)$ может быть представлено в виде матрицы $k \times n$, строки которой составляют базис X. Такую матрицу $k \times n$ назовём матрицей ступенчатого вида по строкам, если соблюдены следующие условия: старший коэффициент каждой строки находится правее старшего коэффициента предыдущей строки, все старшие коэффициенты имеют значение 1, каждый старший коэффициент является единственным ненулевым элементом в своём столбце. Каждое подпространство X можно представить в виде единственной матрицы ступенчатого вида по строкам. Обозначим такую матрицу $RE(X) = (X_n, \ldots, X_2, X_1)$. Будем нумеровать её столбцы справа налево, т. е. называть X_1 первым столбцом, а X_n — последним. Например, некоторое трёхмерное подпространство $X \in G_2(8, 3)$ векторного пространства F_2^8 можно представить в виде матрицы 3×8:

$$RE(X) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

В работе [20] вводится понятие расширенного представления элементов грассманиана, которое используется и в предлагаемом алгоритме нумерации.

Каждое k-мерное подпространство $X \in G_q(n, k)$ имеет вектор идентификации $v(X)$ [25]; $v(X)$ — это вектор длины n, состоящий из нулей и единиц, имеющий вес k, позиции единиц в котором совпадают с номерами столбцов, в которых находятся старшие коэффициенты $RE(X)$. Для трёхмерного пространства $X \in G_2(8, 3)$ из рассматриваемого примера таким вектором будет вектор $v(X) = (0, 1, 0, 1, 0, 1, 0, 0)$.

Расширенное представление подпространства X, обозначаемое $EXT(X)$, является матрицей $(k+1) \times n$, верхней строкой которой является вектор идентификации $v(X) = (v(X)_n, \ldots, v(X)_1)$, а оставшейся частью — матрица ступенчатого вида по строкам, представляющая X:

$$EXT(X) = \begin{pmatrix} V(X)_n & \ldots & V(X)_2 & V(X)_1 \\ X_n & \ldots & X_2 & X_1 \end{pmatrix}.$$

Для восьмимерного пространства $X \in G_2(8, 3)$ из примера

$$EXT(X) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Такое представление избыточно, но может быть использовано для эффективного нумерационного кодирования.

Пусть x — вектор длины r над алфавитом $\{0, 1, \ldots, q-1\}$, равный $(x_1, x_2, \ldots, x_r)$. Обозначим через $\{x\}$ значение $x_1 q^{r-1} + x_2 q^{r-2} + \cdots + x_r q^0$, т. е. число, которому равен вектор x, если рассматривать его как число в q-ичной системе исчисления.

Пусть $X, Y \in G_q(n,k)$ — два k-мерных подпространства, $EXT(X)$, $EXT(Y)$ — их расширенные представления соответственно. Пусть $0 < i \leq n$ — наименьшее такое число, что столбцы $\begin{pmatrix} v(X)_i \\ X_i \end{pmatrix}$ и $\begin{pmatrix} v(Y)_i \\ Y_i \end{pmatrix}$ не совпадают. Тогда считаем, что $X < Y$, если $\left\{ \begin{pmatrix} v(X)_i \\ X_i \end{pmatrix} \right\} < \left\{ \begin{pmatrix} v(Y)_i \\ Y_i \end{pmatrix} \right\}$. Это определение задает порядок на $G_q(n,k)$.

Перейдём к описанию алгоритма нумерации, предлагаемого в [20].

Обозначим через $N \begin{pmatrix} v_j & \ldots & v_1 \\ X_j & \ldots & X_1 \end{pmatrix}$ количество элементов $G_q(n,k)$, первые j столбцов которых равны $\begin{pmatrix} v_j & \ldots & v_1 \\ X_j & \ldots & X_1 \end{pmatrix}$. Будем рассматривать множество q-ичных векторов длины $k+1$ как конечный алфавит. Тогда для кодирования и декодирования элементов грассманиана можно использовать метод Ковера. Элементы грассманиана рассматриваются как векторы длины n над данным алфавитом. При этом $N \begin{pmatrix} v_j & \ldots & v_1 \\ X_j & \ldots & X_1 \end{pmatrix}$ будет соответствовать $n_S(x_1, x_2, ...x_j)$.

Обозначим через w_j вес первых j элементов вектора $v(X)$, т. е. $w_j = \sum\limits_{l=1}^{j} v_l$.

Лемма. *Для любого j, $1 \leq j \leq n$, справедливо равенство*

$$N \begin{pmatrix} v_j & \ldots & v_1 \\ X_j & \ldots & X_1 \end{pmatrix} = \begin{bmatrix} n-j \\ k-w_j \end{bmatrix}_q.$$

Доказательство. Пусть подпространство $X \in G_q(n,k)$, первые столбцы его расширенного представления $EXT(X)$ равны $\begin{pmatrix} v_j & \ldots & v_1 \\ X_j & \ldots & X_1 \end{pmatrix}$. Среди последних $n-j$ элементов $v(X)$ будет $k-w_j$ единиц, и нижние w_j элементов последних $n-j$ столбцов $EXT(X)$ будут нулевыми. Следовательно, матрица $(n-j) \times (k+1-w_j)$, получаемая из $EXT(X)$ вычёркиванием j первых столбцов и w_j нижних строк, является расширенным представлением подпространства, принадлежащего множеству $G_q(n-j, k-w_j)$. Отсюда имеем

$$N \begin{pmatrix} v_j & \ldots & v_1 \\ X_j & \ldots & X_1 \end{pmatrix} = \begin{bmatrix} n-j \\ k-w_j \end{bmatrix}_q.$$

Лемма доказана.

Теорема 1. *Пусть $X \in G_q(n,k)$ — подпространство, для которого*

$$EXT(X) = \begin{pmatrix} v_n & \ldots & v_2 & v_1 \\ X_n & \ldots & X_2 & X_1 \end{pmatrix}.$$

Обозначим его номер среди элементов $G_q(n,k)$, расположенных в лексикографическом порядке, через $I_{EXT}(X)$. Тогда справедливо следующее равенство:

$$I_{EXT}(X) = \sum_{j=1}^{n} \left(v_j q^{k-w_{j-1}} + (1-v_j) \frac{\{X_j\}}{q^{w_{j-1}}} \right) \begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q. \qquad (2)$$

Доказательство. Из формулы (1) следует

$$I_{EXT}(X) = \sum_{j=1}^{n} \sum_{\substack{u \\ W \end{matrix}}^{\begin{matrix} v_j \\ < X_j \end{matrix}} N \begin{pmatrix} u & v_{j-1} & \dots & v_1 \\ W & X_{j-1} & \dots & X_1 \end{pmatrix}. \tag{3}$$

При вычислении j-го слагаемого в формуле (3) будем разделять два случая.

Случай 1: $v_j = 1$. Это означает, что столбец X_j состоит из $k-1$ нулей и единицы на $(k - w_{j-1})$-й позиции сверху, т. е. $\{X_j\} = q^{w_{j-1}}$. Значит, $EXT(X)$ имеет вид

$$\begin{pmatrix} v_n & \dots & v_{j+1} & 1 & v_{j-1} & \dots & v_1 \\ X_n & \dots & X_{j+1} & \{q^{w_{j-1}}\}_q & X_{j-1} & \dots & X_1 \end{pmatrix}.$$

Следовательно, подпространство $Y \in G_q(n,k)$ такое, что у $EXT(Y)$ и $EXT(X)$ совпадают первые $j-1$ столбца, лексикографически предшествует X тогда и только тогда, когда $EXT(Y)$ имеет вид

$$\begin{pmatrix} v'_n & \dots & v'_{j+1} & 0 & v_{j-1} & \dots & v_1 \\ Y_n & \dots & Y_{j+1} & Y_j & X_{j-1} & \dots & X_1 \end{pmatrix}.$$

Заметим, что нижние w_{j-1} элементов Y_j являются нулями (поскольку старшие коэффициенты последних w_{j-1} строк содержатся в $(X_{j-1} \dots X_1)$). Верхние $k - w_{j-1}$ элементы Y_j могут иметь любые значения.

Это означает, что в данном случае j-е слагаемое в формуле (3) равно

$$\sum_{s=0}^{q^{k-w_{j-1}-1}} N \begin{pmatrix} 0 & v_{j-1} & \dots & v_1 \\ \{s \cdot q^{w_{j-1}}\}_q & X_{j-1} & \dots & X_1 \end{pmatrix}.$$

При этом по лемме

$$\sum_{s=0}^{q^{k-w_{j-1}-1}} N \begin{pmatrix} 0 & v_{j-1} & \dots & v_1 \\ \{s \cdot q^{w_{j-1}}\}_q & X_{j-1} & \dots & X_1 \end{pmatrix} = q^{k-w_{j-1}} \begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q. \tag{4}$$

Случай 2: $v_j = 0$. Поскольку $w_{j-1} = \sum\limits_{l-1}^{j-1} v_l$, то отсюда следует, что последние w_{j-1} элемента столбца X_j являются нулями, т. е. $\{X_j\}$ делится на $q^{w_{j-1}}$. Значит, $EXT(X)$ имеет вид

$$\begin{pmatrix} v_n & \dots & v_{j+1} & 0 & v_{j-1} & \dots & v_1 \\ X_n & \dots & X_{j+1} & X_j & X_{j-1} & \dots & X_1 \end{pmatrix}.$$

Следовательно, подпространство $Y \in G_q(n,k)$ такое, что первые $j-1$ столбцов $EXT(Y)$ и $EXT(X)$ совпадают, лексикографически предшествует X тогда и только тогда, когда $EXT(Y)$ имеет вид

$$\begin{pmatrix} v'_n & \dots & v'_{j+1}0 & v_{j-1} & \dots & v_1 & \\ Y_n & \dots & Y_{j+1} & \{s \cdot q^{w_{j-1}}\}_q & X_{j-1} & \dots & X_1 \end{pmatrix},$$

где $0 \le s \le \dfrac{\{X_j\}}{q^{w_j-1}} - 1$. Это означает, что в данном случае j-е слагаемое формулы (3) равно

$$\sum_{s=0}^{\frac{\{X_j\}}{q^{w_j-1}}} N \begin{pmatrix} 0 & v_{j-1} & \dots & v_1 \\ \{s \cdot q^{w_{j-1}}\}_q & X_{j-1} & \dots & X_1 \end{pmatrix}.$$

При этом по лемме

$$\sum_{s=0}^{\frac{\{X_j\}}{q^{w_j-1}}} N \begin{pmatrix} 0 & v_{j-1} & \dots & v_1 \\ \{s \cdot q^{w_{j-1}}\}_q & X_{j-1} & \dots & X_1 \end{pmatrix} = \frac{\{X_j\}}{q^{w_j-1}} \begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q. \tag{5}$$

Из формул (4) и (5) в случаях 1 и 2 получаем уравнение (2).

Теорема 1 доказана.

Алгоритм нумерации элементов грассманиана, предлагаемый в [20], представляет собой вычисление номера элемента грассманиана по формуле (2). При этом гауссовы коэффициенты $\begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q$, $1 \le j \le n$, предлагается вычислять начиная с $j = n$ по формулам

$$\begin{bmatrix} 0 \\ k-w_{n-1} \end{bmatrix}_q = 1,$$

$$\begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q = \begin{cases} \begin{bmatrix} n-(j+1) \\ k-w_j \end{bmatrix}_q \cdot \dfrac{q^{n-j}-1}{q^{n-k-j+w_j}-1}, & \text{если } w_j = w_{j-1}, \\ \begin{bmatrix} n-(j+1) \\ k-w_j \end{bmatrix}_q \cdot \dfrac{q^{n-j}-1}{q^{k-w_j+1}-1}, & \text{если } w_j = w_{j-1}+1. \end{cases} \tag{6}$$

Рассмотрим пример вычисления номера элемента грассманиана по данному алгоритму. Пусть $X \in G_2(8,3)$ — подпространство, имеющее представление

$$EXT(X) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Найдем по формулам (1) значения $\begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q$ при $j = n, \dots, 1$:

$$\begin{bmatrix} 8-8 \\ 3-3 \end{bmatrix}_2 = 1,$$
$$\begin{bmatrix} 8-7 \\ 3-2 \end{bmatrix}_2 = 1 \cdot \frac{2^1-1}{2^{3-3+1}-1} = 1,$$
$$\begin{bmatrix} 8-6 \\ 3-2 \end{bmatrix}_2 = 1 \cdot \frac{2^2-1}{2^{8-3-6+2}-1} = 3,$$
$$\begin{bmatrix} 8-5 \\ 3-1 \end{bmatrix}_2 = 3 \cdot \frac{2^3-1}{2^{3-2+1}-1} = 7,$$

$$\begin{bmatrix} 8-4 \\ 3-1 \end{bmatrix}_2 = 7 \cdot \frac{2^4-1}{2^{8-3-4+1}-1} = 35,$$
$$\begin{bmatrix} 8-3 \\ 3-0 \end{bmatrix}_2 = 35 \cdot \frac{2^5-1}{2^{3-1+1}-1} = 155,$$
$$\begin{bmatrix} 8-2 \\ 3-0 \end{bmatrix}_2 = 155 \cdot \frac{2^6-1}{2^{8-3-2+0}-1} = 1395,$$
$$\begin{bmatrix} 8-1 \\ 3-0 \end{bmatrix}_2 = 1395 \cdot \frac{2^7-1}{2^{8-3-1+0}-1} = 11811.$$

Вычислим по теореме 1 значение I_{EXT}:

$$I_{EXT} = \frac{1}{2^0} \cdot 11811 + \frac{7}{2^0} \cdot 1395 + 2^{3-0} \cdot 155 + \frac{0}{2^1} \cdot 35 + 2^{3-1} \cdot 7 + \frac{4}{2^2} \cdot 3 + 2^{3-2} \cdot 1 + \frac{0}{2^3} \cdot 1 = 22849.$$

Определим сложность вычисления номера $I_{EXT}(\cdot)$ в (2). Обратим внимание на то, что все целые числа, используемые в вычислениях, заданы в q-ичной системе исчисления. Пусть $M[a,b]$ означает количество операций, требуемое для умножения двух q-ичных чисел длин a и b. Известно [26], что для $a > b$ $M[a,b] = a \log b \log\log b$. Пусть $M[a]$ означает количество операций, требуемое для умножения двух q-ичных чисел длины a.

Посчитаем длину q-ичной целого, которое представляет наибольший гауссов коэффициент в (2). Этот гауссов коэффициент равен

$$\begin{bmatrix} n-1 \\ k \end{bmatrix}_q = \frac{(q^{n-1}-1)\dots(q^{n-k}-1)}{(q^k-1)\dots(q-1)},$$

его длина меньше $k(n-k)$.

Если $w_j = w_{j-1}$, то

$$\begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q = \begin{bmatrix} n-(j+1) \\ k-w_j \end{bmatrix}_q \frac{q^{n-j}-1}{q^{n-k-j+w_j}-1}. \tag{7}$$

Если $w_j = w_{j-1}+1$, то

$$\begin{bmatrix} n-j \\ k-w_{j-1} \end{bmatrix}_q = \begin{bmatrix} n-(j+1) \\ k-w_j \end{bmatrix}_q \frac{q^{n-j}-1}{q^{k-w_j+1}-1}. \tag{8}$$

Гауссовы коэффициенты в (2) могут быть выведены из вектора идентификации. Они вычисляются по формулам (7) и (8). Сложность вычисления всех гауссовых коэффициентов при выполнении алгоритма равна $O(nM[k(n-k),n])$.

Умножение или деление на q^i осуществляется сдвигом на i знаков, для $n-k$ значений j $v_j = 0$, длина $\{X_j\}$ равна k, следовательно, сложность этих операций равна $O((n-k)M[k(n-k),k])$. При вычислениях по формуле (2) производится максимум n операций сложения целых чисел, чья длина составляет максимум $k(n-k+1)$ знаков, следовательно, сложность этих операций может быть опущена.

Складывая сложности всех операций, получаем, что сложность вычисления $I_{EXT}(\cdot)$ номера X по формуле (2) равна $O(nM[k(n-k),n])$, т. е. $O(nk(n-k)\log n \log\log n)$ операций.

2. Быстрый алгоритм нумерации элементов грассманиана

Перейдем к описанию представленного в настоящей работе алгоритма нумерации элементов грассманиана, основанного на расширенном представлении этих элементов, сложность которого меньше сложности алгоритма, рассмотренного в [20].

Предлагаемый алгоритм основан на методе быстрой нумерации комбинаторных объектов [22].

В [20] было приведено доказательство того, что

$$I_{EXT}(X) = \sum_{j=1}^{n} \left(v_j q^{k-w_{j-1}} + (1-v_j)\frac{\{X_j\}}{q^{w_{j-1}}} \right) \begin{bmatrix} n-j \\ k-w_j \end{bmatrix}_q .$$

Введём при $j = 2, 3, ..., n$ величины

$$P\binom{v_1}{X_1} = N\binom{v_1}{X_1} \Big/ \begin{bmatrix} n \\ k \end{bmatrix}_q ,$$

$$P\left(\begin{matrix} v_j \\ X_j \end{matrix}\middle|\begin{matrix} v_{j-1} & \dots & v_2 & v_1 \\ X_{j-1} & \dots & X_2 & X_1 \end{matrix}\right) = N\begin{pmatrix} v_j & \dots & v_2 & v_1 \\ X_j & \dots & X_2 & X_1 \end{pmatrix} \Big/ N\begin{pmatrix} v_{j-1} & \dots & v_2 & v_1 \\ X_{j-1} & \dots & X_2 & X_1 \end{pmatrix},$$

$$q\binom{v_1}{X_1} = \sum_{\substack{u \\ W < X_1^{v_1}}} P\binom{u}{W},$$

$$q\left(\begin{matrix} v_j \\ X_j \end{matrix}\middle|\begin{matrix} v_{j-1} & \dots & v_2 & v_1 \\ X_{j-1} & \dots & X_2 & X_1 \end{matrix}\right) = \sum_{\substack{u \\ W < X_j^{v_j}}} P\left(\begin{matrix} u \\ W \end{matrix}\middle|\begin{matrix} v_{j-1} & \dots & v_2 & v_1 \\ X_{j-1} & \dots & X_2 & X_1 \end{matrix}\right).$$

Из этих определений и формулы (1) следует, что

$$I_{EXT}(X) = \begin{bmatrix} n \\ k \end{bmatrix}_q \left(q\binom{v_1}{X_1} + q\left(\begin{matrix} v_2 \\ X_2 \end{matrix}\middle|\begin{matrix} v_1 \\ X_1 \end{matrix}\right) P\binom{v_1}{X_1} + q\left(\begin{matrix} v_3 \\ X_3 \end{matrix}\middle|\begin{matrix} v_2 & v_1 \\ X_2 & X_1 \end{matrix}\right) P\left(\begin{matrix} v_2 \\ X_2 \end{matrix}\middle|\begin{matrix} v_1 \\ X_1 \end{matrix}\right) P\binom{v_1}{X_1} + \dots \right).$$

Идея метода заключается в расстановке скобок в данном выражении таким образом, что при вычислении номера большинство операций производится над короткими числами. Такой расстановкой скобок будет следующая:

$$\begin{aligned} I_{EXT}(X) = \begin{bmatrix} n \\ k \end{bmatrix}_q \Bigg(\Bigg(q\binom{v_1}{X_1} + q\left(\begin{matrix} v_2 \\ X_2 \end{matrix}\middle|\begin{matrix} v_1 \\ X_1 \end{matrix}\right) P\binom{v_1}{X_1} \Bigg) + \Bigg(\Bigg(q\left(\begin{matrix} v_3 \\ X_3 \end{matrix}\middle|\begin{matrix} v_2 & v_1 \\ X_2 & X_1 \end{matrix}\right) + \\ + q\left(\begin{matrix} v_4 \\ X_4 \end{matrix}\middle|\begin{matrix} v_3 & \dots & v_1 \\ X_3 & \dots & X_1 \end{matrix}\right) P\left(\begin{matrix} v_3 \\ X_3 \end{matrix}\middle|\begin{matrix} v_2 & v_1 \\ X_2 & X_1 \end{matrix}\right) \Bigg) P\left(\begin{matrix} v_2 \\ X_2 \end{matrix}\middle|\begin{matrix} v_1 \\ X_1 \end{matrix}\right) P\binom{v_1}{X_1} \Bigg) + \dots \end{aligned} \tag{9}$$

Положим

$$\begin{aligned} &\rho_1^0 = P\binom{v_1}{X_1}, \lambda_1^0 = q\binom{v_1}{X_1}, \quad \rho_j^0 = P\left(\begin{matrix} v_j \\ X_j \end{matrix}\middle|\begin{matrix} v_{j-1} & \dots & v_2 & v_1 \\ X_{j-1} & \dots & X_2 & X_1 \end{matrix}\right), \\ &\lambda_j^0 = q\left(\begin{matrix} v_j \\ X_j \end{matrix}\middle|\begin{matrix} v_{j-1} & \dots & v_2 & v_1 \\ X_{j-1} & \dots & X_2 & X_1 \end{matrix}\right), \quad j = 2, \dots, n, \quad \rho_j^s = \rho_{2j-1}^{s-1}\rho_{2j}^{s-1}, \\ &\lambda_j^s = \lambda_{2j-1}^{s-1} + \rho_{2j-1}^{s-1}\lambda_{2j}^{s-1}, \quad s = 1, \dots, \log n, \quad j = 1, \dots, n/2^s. \end{aligned} \tag{10}$$

Тогда

$$\lambda_1^{\log n} = \left(\left(q\binom{v_1}{X_1}+q\binom{v_2}{X_2}\middle|\binom{v_1}{X_1}P\binom{v_1}{X_1}\right)+\left(\left(q\binom{v_3}{X_3}\middle|\binom{v_2\ v_1}{X_2\ X_1}+\right.\right.$$
$$\left.\left.+q\binom{v_4}{X_4}\middle|\binom{v_3\ \dots\ v_1}{X_3\ \dots\ X_1}P\binom{v_3}{X_3}\middle|\binom{v_2\ v_1}{X_2\ X_1}\right)P\binom{v_2}{X_2}\middle|\binom{v_1}{X_1}P\binom{v_1}{X_1}\right)+\dots \tag{11}$$

Отсюда и формулы (9) имеем

$$I_{EXT}(X) = \lambda_1^{\log n}|G(n,k)| = \lambda_1^{\nu}\begin{bmatrix} n \\ k \end{bmatrix}_q. \tag{12}$$

По определениям ρ_j^0, $P\binom{v_j}{X_j}\middle|\binom{v_{j-1}\ \dots\ v_2\ v_1}{X_{j-1}\ \dots\ X_2\ X_1}$ и лемме

$$\rho_j^0 = P\binom{v_j}{X_j}\middle|\binom{v_{j-1}\ \dots\ v_2\ v_1}{X_{j-1}\ \dots\ X_2\ X_1} = N\binom{v_j\ \dots\ v_2\ v_1}{X_j\ \dots\ X_2\ X_1}\Big/N\binom{v_{j-1}\ \dots\ v_2\ v_1}{X_{j-1}\ \dots\ X_2\ X_1} =$$
$$= \begin{bmatrix} n-j \\ k-w_j \end{bmatrix}_q \Big/ \begin{bmatrix} n-j+1 \\ k-w_{j-1} \end{bmatrix}_q = \begin{cases} \dfrac{q^{n-j-k+w_j+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 0, \\ \dfrac{q^{k-w_j+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 1. \end{cases} \tag{13}$$

По определениям λ_j^0, $q\binom{v_j}{X_j}\middle|\binom{v_{j-1}\ \dots\ v_2\ v_1}{X_{j-1}\ \dots\ X_2\ X_1}$ и лемме

$$\lambda_j^0 = q\binom{v_j}{X_j}\middle|\binom{v_{j-1}\ \dots\ v_2\ v_1}{X_{j-1}\ \dots\ X_2\ X_1} = \sum_{\substack{u \\ W < X_j^{v_j}}} P\binom{u}{W}\middle|\binom{v_{j-1}\ \dots\ v_2\ v_1}{X_{j-1}\ \dots\ X_2\ X_1} =$$
$$= \sum_{\substack{u \\ W < X_j^{v_j}}} N\begin{pmatrix} u & v_{j-1} & \dots & v_1 \\ W & X_{j-1} & \dots & X_1 \end{pmatrix}\Big/N\binom{v_{j-1}\ \dots\ v_2\ v_1}{X_{j-1}\ \dots\ X_2\ X_1} =$$
$$= \begin{cases} q^{k-w_{j-1}} \cdot \dfrac{q^{n-j-k+w_{j-1}+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 1, \\ \dfrac{\{X_j\}}{q^{w_{j-1}}} \cdot \dfrac{q^{n-j-k+w_{j-1}+1}-1}{q^{n-j+1}-1}, & \text{если } v_j = 0. \end{cases} \tag{14}$$

Перейдём к вычислениям, которые будут служить иллюстрацией алгоритма. Определим номер подпространства $X \in G_2(8,3)$, имеющего расширенное представление

$$EXT(X) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

По формулам (13) и (2) вычислим значения ρ_j^0, λ_j^0, $j = 1, \dots, 8$:

$$\rho_1^0 = \frac{2^5-1}{2^8-1} = \frac{31}{255}, \quad \rho_2^0 = \frac{2^4-1}{2^7-1} = \frac{15}{127},$$

$$\rho_3^0 = \frac{2^3-1}{2^6-1} = \frac{1}{9}, \quad \rho_4^0 = \frac{2^3-1}{2^5-1} = \frac{7}{31},$$
$$\rho_5^0 = \frac{2^2-1}{2^4-1} = \frac{1}{5}, \quad \rho_6^0 = \frac{2^2-1}{2^3-1} = \frac{3}{7},$$
$$\rho_7^0 = \frac{2^1-1}{2^2-1} = \frac{1}{3}, \quad \rho_8^0 = \frac{2^1-1}{2^1-1} = 1,$$
$$\lambda_1^0 = 1 \cdot \frac{2^5-1}{2^8-1} = \frac{31}{255}, \quad \lambda_2^0 = 7 \cdot \frac{2^4-1}{2^7-1} = \frac{105}{127},$$
$$\lambda_3^0 = 2^3 \cdot \frac{2^3-1}{2^6-1} = \frac{8}{9}, \quad q\lambda_4^0 = 0 \cdot \frac{2^3-1}{2^5-1} = 0,$$
$$\lambda_5^0 = 2^2 \cdot \frac{2^2-1}{2^4-1} = \frac{4}{5}, \quad \lambda_6^0 = 1 \cdot \frac{2^2-1}{2^3-1} = \frac{3}{7},$$
$$\lambda_7^0 = 2^1 \cdot \frac{2^1-1}{2^2-1} = \frac{2}{3}, \quad \lambda_8^0 = 0 \cdot \frac{2^1-1}{2^1-1} = 0.$$

Далее по (2) получим

$$\rho_1^1 = \frac{31}{2159}, \quad \rho_2^1 = \frac{7}{279}, \quad \rho_3^1 = \frac{3}{35}, \quad \rho_4^1 = \frac{1}{3},$$
$$\lambda_1^1 = \frac{7192}{32385}, \quad \lambda_2^1 = \frac{8}{9}, \quad \lambda_3^1 = \frac{31}{35}, \quad \lambda_4^1 = \frac{2}{3},$$
$$\rho_1^2 = \frac{7}{19431}, \quad \rho_2^2 = \frac{1}{35}, \quad \lambda_1^2 = \frac{22816}{97155}, \quad \lambda_2^2 = \frac{33}{35}, \quad \rho_1^3 = \frac{1}{97155}, \quad \lambda_1^3 = \frac{22849}{97155}.$$

По (12) имеем

$$I_{EXT}(X) = \lambda_1^3 \cdot \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{22849}{97155} \cdot \begin{bmatrix} 8 \\ 3 \end{bmatrix}_2 = 22849.$$

3. Сложность алгоритма

Теорема 2. *Объём памяти, требуемый для вычисления номера элемента грассманиана $X \in G_q(n,k)$, равен $O(n^2)$. Сложность вычисления номера элемента грассманиана $X \in G_q(n,k)$ равна $O(\log nM[n^2])$ операций, где $M[n^2]$ — время умножения двух слов длины n^2.*

Следствие 1. *При использовании алгоритма быстрого умножения Шёнхаге — Штрассена, для которого $M[n] = n \log n \log\log n$, сложность вычисления номера равна $O(n^2 \log^2 n \log\log n)$.*

Следствие 2. *При использовании алгоритма быстрого умножения Фюрера, для которого $M[n] = n \log n 2^{O(\log^* n)}$, сложность вычисления номера равна $O(n^2 \log^2 n 2^{O(\log^* n)})$.*

Доказательство. Найдём время вычисления $I_{EXT}(X)$. Оно состоит из времени вычисления ρ_j^i и λ_j^i, $i = 0, ..., \log n$, $j = 1, 2, ..., n/(2^i)$, и времени вычисления произведения $\lambda^{\log n} |G_q(n,k)|$.

Для вычисления ρ_j^0 и λ_j^0, $j = 1, 2, ..., n$, требуется вычислить n значений $P\left(\begin{matrix} v_j \\ X_j \end{matrix} \middle| \begin{matrix} v_{j-1} & \dots & v_1 \\ X_{j-1} & \dots & X_1 \end{matrix}\right)$ и n значений $q\left(\begin{matrix} v_j \\ X_j \end{matrix} \middle| \begin{matrix} v_{j-1} & \dots & v_1 \\ X_{j-1} & \dots & X_1 \end{matrix}\right)$.

Для вычисления n числителей дробей $P\binom{v_j}{X_j}\Big|\binom{v_{j-1}\ \dots\ v_1}{X_{j-1}\ \dots\ X_1}$ в q-ичной системе исчислений необходимо найти n значений $n-j-k+w_j+1$ или $k-w_j+1$. Для вычисления их знаменателей требуется найти n значений $n-j+1$. Таким образом, всего нужно совершить $O(n)$ сложений (и вычитаний) чисел длины $\log n$, что имеет сложность $O(n\log n)$.

Для вычисления n дробей $q\binom{v_j}{X_j}\Big|\binom{v_{j-1}\ \dots\ v_1}{X_{j-1}\ \dots\ X_1}$ требуется найти n значений $n-j-k+w_{j-1}+1$, n значений $n-j+1$, т. е. совершить $O(n)$ сложений (и вычитаний) чисел длины $\log n$, что имеет сложность $O(n\log n)$. Умножение на $q^{k-w_{j-1}}$ в случае $v_j=1$ и на $q^{w_{j-1}}$ в случае $v_j=0$ получается сдвигом на нужное количество разрядов. Для получения числителей в случае $v_j=0$ требуется совершить $n-k$ умножений чисел $\{X_j\}$ длины k и $q^{n-j-k+w_{j-1}+1}-1$ чисел длины n, что имеет сложность $(n-k)M[n,k]$.

Таким образом, сложность вычисления всех ρ_j^0 и λ_j^0, $j=1,2,...,\ n/2$, равна $O(n\log n)+(n-k)M[n,k]$.

По формулам (13), (14) видим, что числители, как и знаменатели, дробей $P\binom{v_j}{X_j}\Big|\binom{v_{j-1}\ \dots\ v_1}{X_{j-1}\ \dots\ X_1}$ и $q\binom{v_j}{X_j}\Big|\binom{v_{j-1}\ \dots\ v_1}{X_{j-1}\ \dots\ X_1}$ не превышают q^n. Для записи числителя, как и для записи знаменателя, этих дробей в q-ичной записи требуется n знаков.

Вычисление величин ρ_j^1 или λ_j^1 в соответствии с (10) при $j=1,2,\dots,n$ требует соответственно две или три операции умножения чисел, длина которых не превышает n знаков, а общее число операций умножения для вычисления всех λ_j^1, ρ_j^1, $j=1,\ 2,\ ...,\ n/2$, равно $5n/2$. При вычислении λ_j^1 используется обычное равенство $a/b+c/d=(ad+bc)/(bd)$, требующее три умножения. В результате будут получены дроби, у которых требуется не более $2n$ знаков для записи числителя и столько же знаков для записи знаменателя. Аналогично, для вычисления ρ_j^2 и λ_j^2, $j=1,\ 2,\ \dots,n/4$, необходимо $5n/4$ операций умножения над числами длины $4n$ знаков и т. д., для вычисления ρ_j^i и λ_j^i, $j=1,\ 2,\ ...,\ n/2^i$, требуется $5n/2^i$ операций умножения над числами длины 2^in знаков.

Общее время вычислений λ_j^i и ρ_j^i, $i=1,\dots,\log n$, $j=1,\ \dots,\ n/2^i$ составит

$$\frac{5}{2}nM[n]+\frac{5n}{4}M[2n]+\dots+\frac{5n}{2^i}M[2^in]+\dots+\frac{5}{2}M[n\cdot n].$$

Обозначим через $M^*[a]$ время умножения двух чисел длины a, делённое на длину этих чисел:

$$M^*[a]=\frac{M[a]}{a}.$$

Тогда общее время вычислений λ_j^i и ρ_j^i будет

$$\frac{5n}{2}nM^*[n]+\frac{5n2n}{4}M^*[2n]+\dots+\frac{5n2^in}{2^i}M^*[2^in]+\dots+\frac{5}{2}\,n^2M^*[n^2].$$

В этой сумме $\log n$ слагаемых, каждое из которых не превышает $\dfrac{5}{2}n^2M^*[n^2]$.

Следовательно, время вычисления дробей λ_j^i и ρ_j^i равно

$$O\left(\frac{5}{2}\,n^2\log nM^*[n^2]\right)=O(\log nM[n^2]).$$

Время вычисления произведения $\lambda^{\log n}|G_(n,k)|$ состоит из времени вычисления произведения числителя $\lambda^{\log n}$ и $|G_(n,k)|$ и времени вычисления частного полученного числа и знаменателя $\lambda^{\log n}$. Количество знаков, необходимых для записи числителя $\lambda^{\log n}$, не превышает n^2. Количество знаков, нужных для записи $|G_(n,k)|$, равно $n(n-k)$. Значит время умножения числителя $\lambda^{\log n}$ и $|G_(n,k)|$ составит $M[n^2, n(n-k)]$. Длина полученного числа не превышает $2n^2$. Длина знаменателя $\lambda^{\log n}$ не превышает n^2. Так как время деления двух чисел длины a равно времени умножения двух чисел длины a [27], время деления полученного числа и знаменателя $\lambda^{\log n}$ равно $M[2n^2]$.

Таким образом, время вычисления $I_{EXT}(X)$ равно сумме времени вычисления ρ_j^0 и λ_j^0, $j = 1, 2, \ldots, n$, т. е. $O(n\log n) + (n-k)M[n,k]$, времени вычисления λ_k^i и ρ_j^i, $i = 1, \ldots, \log n$, $j = 1, \ldots, n/2^i$, т. е. $O(\log nM[n^2])$, и времени вычисления $\lambda^{\log n}|G(n,k)|$, т. е. $M[n^2, n(n-k)] + M[2n^2]$:

$$O(n\log n) + (n-k)M[n,k] + O(\log nM[n^2]) + M[n^2, n(n-k)] + M[2n^2] = O(\log nM[n^2]).$$

Оценим необходимый для осуществления нумерации объём памяти.

Для определения $I_{EXT}(X)$ при вычислении λ_j^i и ρ_j^i, $i = 1, \ldots, \log n$, $j = 1, \ldots, n/2^i$, используются только величины λ_j^{i-1} и ρ_j^{i-1}, $j = 1, \ldots, n/2^{i-1}$. Поэтому для нумерации достаточно иметь память для хранения двух наборов λ_j^i, ρ_j^i, $j = 1, \ldots, n/2^i$, и λ_j^{i+1}, ρ_j^{i+1}, $j = 1, \ldots, n/2^{i+1}$, $i = 1, \ldots, \log n$. Длина числителя и знаменателя каждой дроби λ_j^i и ρ_j^i не превышает $2^i n$. Отсюда требуемый объём памяти для определения номера $X \in G(n,k)$ не превышает $2^i n \cdot n/2^i + 2^{i+1} n \cdot n/2^{i+1} = O(n^2)$.

Теорема 2 доказана.

Список литературы

[1] Knuth D.E. Subspaces, subsets and partitions // J. of Combinat. Theory. 1971. Vol. 10. P. 178–189.

[2] Thomas S. Designs over finite fields // Geometriae Dedicata. 1987. Vol. 21. P. 237–242.

[3] Martin W.J, Zhu X.J. Anticodes for the Grassman and biliniar forms graphs // Designs, Codes and Crypt. 1995. Vol. 6. P. 72–79.

[4] Tomas S. Designs and partial geometries over finite fields// Geometriae Dedicata. 1996. Vol. 63. P. 247–253.

[5] Ahlswede R., Aydinian H.K, Khachatrian L.H. On perfect codes and related concepts // Designs, Codes and Crypt. 2001. Vol. 22. P. 221–237.

[6] Schwartz M., Etzion T. Codes and anticodes in the Grassman graph // J. of Combinat. Theory. Ser. A. 2002. Vol. 97. P. 27–42.

[7] Braun M., Kerber A, Laue R. Systematic construction of q-analogs of $t-(\nu,k,\lambda)$-designs // Designs, Codes and Crypt. 2005. Vol. 34. P. 55–70.

[8] Koetter R, Kshcischang F.R. Coding for errors and erasures in random network coding // IEEE Trans. Inform. Theory. 2008. Vol. 54, No. 8. P. 3579–3591.

[9] Xia S.T, Fu F.W. Johnson type bounds on constant dimension codes // Designs, Codes and Crypt. 2009. Vol. 50. P. 163–172.

[10] Etzion T, Vardy A. Error-correcting codes in projective space // Proc. Intern. Symp. on Inform. Theory. Toronto, 2008. P. 871–875.

[11] Manganiello F., Gorla E, Rosenthal J. Spread codes and spread decoding in network coding // Proc. Intern. Symp. on Inform. Theory. Toronto, 2008. P. 881–885.

[12] Silva D., Kschischang F.R, Koetter R. A rank-metric approach to error control in random network coding // IEEE Trans. on Inform. Theory. 2008. Vol. IT-54. P. 3951–3967.

[13] Silva D., Kschischang F.R. On metric for error correction in network coding // Ibid. 2009. Vol. IT-54. P. 5479–5490.

[14] Gadouleau M. and Yan Z. Constant-rank codes and their connection to constant-dimension codes // Ibid. 2010. Vol. IT-56. P. 3207–3216.

[15] Gadouleau M., Yan Z. On the decoder error probability of bounded rank distance decoders for maximum rank distance codes // Ibid. 2008. Vol. IT-54. P. 3202–3206.

[16] Gadouleau M. and Yan Z. Construction and Covering Properties of Constant-Dimension Codes. http://arxiv.org/abs/0903.2675

[17] Etzion T, Silberstein N. Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams // IEEE Trans. Inform. Theory. 2009. Vol. IT-55. P. 2909–2919.

[18] Kohnert A. and Kurz S. Construction of large constant dimension codes with a prescribed minimum distance // Lecture Notes Comput. Sci. 2008. Vol. 5393. P. 31–42.

[19] Skachek V. Recursive code construction for random networks // IEEE Trans. Inform. Theory. 2010. Vol. IT-56. P. 1378–1382.

[20] Silberstein N, Etzion T. Enumerative Coding for Grassmannian Space. http://arxiv.org/abs/0911.3256

[21] Fuerer M. Faster integer multiplication // Proc. of the Thirty-Ninth Annual ACM Symp. on Theory of Comput. San Diego, California, USA. 2007.

[22] Ryabko B.Ya. The fast enumeration of combinatorial objects // Discrete Math. and Appl. 1998. Vol. 10, No. 2.

[23] Van Lint J.H, Wilson R.M. A Course in Combinatorics. Cambridge Univ. Press, 2001.

[24] Cover T.M. Enumerative source encoding // IEEE Trans. Inform. Theory. 1973. Vol. IT-19, No. 1. P. 73–77.

[25] Etzion T, Silberstein N. Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams // Ibid. 2009. Vol. IT-55. P. 2909–2919.

[26] Knuth D.E. The Art of Computer Programming. Seminumerical Algorithms. Third Ed. Addison-Wesley, 1997. Vol. 2.

[27] Ахо А.В., Лам М.С., Сети Р., Ульман Дж.Д. Компиляторы. Принципы, технологии и инструментарий. М.: Вильямс, 2008.

Поступила в редакцию 14 июля 2012 г.