УДК 519.12

И.Н. КУЗНЕЦОВ

ВЕРХНИЕ И НИЖНИЕ ОЦЕНКИ КОЛИЧЕСТВА НЕКОТОРЫХ *k*-МЕРНЫХ ПОДПРОСТРАНСТВ ЗАДАННОГО ВЕСА НАД КОНЕЧНЫМ ПОЛЕМ

Ключевые слова: *векторное пространство, поле Галуа, вес подпространства, ускоренное моделирование, многопроцессорный комплекс СКИТ-3*.

Данная статья является продолжением работы [1]. Напомним постановку задачи, некоторые определения и обозначения.

Рассматривается n-мерное векторное пространство V_n над конечным полем GF(q) (поле Галуа), содержащим q элементов, где q — степень простого числа. Известно [2, с. 219], что общее количество различных k-мерных подпространств $V_{k,n}$ пространства V_n равно

$$\begin{bmatrix} n \\ k \end{bmatrix} = \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1}, \quad 1 \le k \le n. \tag{1}$$

Весом вектора $v \in V_n$ называется число отличных от нуля компонент этого вектора. Весом k-мерного подпространства $V_{k,n}$ пространства V_n называется число, равное минимальному весу вектора $v \in V_{k,n}$, отличного от нулевого. Число k-мерных подпространств $V_{k,n}$ пространства V_n, каждое из которых имеет вес ω, обозначим $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$. Из алгоритма [3] построения множества базисных векторов k-мерного подпространства $V_{k,n}$ следует, что его вес не может превышать $n-k+1$, поэтому

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{\omega=1}^{n-k+1} \begin{bmatrix} n \\ k \end{bmatrix}_{\omega}, \quad 1 \le k \le n. \tag{2}$$

Оценки количества подпространств $V_{k,n}$ заданного веса ω представляют интерес как для задач кодирования [4, 5], так и для решения проблемы защиты информации от несанкционированного доступа.

Следует отметить полное отсутствие каких-либо результатов, позволяющих вычислять или оценивать $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$ для произвольных значений n, k и ω. Имеются лишь частные результаты. Так, в [6, 7] приведены рекуррентные формулы вычисления $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$ при $\omega = 1$ и $\omega = 2$. В [1] предложен принципиально новый подход, основанный на ускоренном моделировании малых вероятностей. В его основе лежит идея И.Н. Коваленко [8–10] о разложении искомой характеристики по степеням некоторого параметра. В теории надежности такой подход был многократно успешно использован для повышения точности вычислений. Оцениваемая характеристика раскладывалась в ряд по степеням малого параметра (аналитическая часть), а коэффициенты этого ряда оценивались методом Монте-Карло (статистическая часть). Выделение малого параметра позволяло существенно повысить точность оценок, а быстрая сходимость ряда способствовала повышению эффективности вычислений. В отличие от задач теории надежности в [1] предложено разложить $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$ по степеням большого параметра q (типичные значения $q = 2^8$, $q = 2^{16}$ и выше). Метод

ускоренного моделирования позволил строить несмещенные оценки для $\left[\begin{matrix} n \\ k \end{matrix}\middle|\, \omega \right]$ при $\omega = 1$ и $\omega = 2$, а также верхние и нижние оценки при $\omega = 3$. При этом доказана ограниченность относительной среднеквадратической погрешности оценок при $q \to \infty$.

В настоящей статье результаты работы [1] обобщаются для произвольного значения ω, а именно, при $k = 1$ и $k = 2$ для $\left[\begin{matrix} n \\ k \end{matrix}\middle|\, \omega \right]$ приведены аналитические формулы в явном виде, а для $k > 2$ сформулирован алгоритм ускоренного моделирования, позволяющий строить верхние и нижние оценки. Точность оценок исследуется на численных примерах. Использование ускоренного моделирования на многопроцессорном комплексе СКИТ-3 позволило получить оценки высокой точности для больших значений n, k и ω.

ОБЩАЯ СХЕМА УСКОРЕННОГО МОДЕЛИРОВАНИЯ

Для перечисления всех k-мерных подпространств $V_{k,n}$ векторного пространства V_n ключевую роль играет алгоритм [3] построения множества базисных векторов этого подпространства. Данный алгоритм сводится к построению матрицы A размера $k \times n$. Пусть $\bar{r} = (r_1, \ldots, r_k)$ — k-мерный вектор, компонентами которого являются упорядоченные натуральные числа, $U = \{\bar{r} : 1 \le r_1 < r_2 < \ldots < r_k \le n\}$.

1. Выбираем произвольный вектор $\bar{r} \in U$.

2. В матрице A с k строками и n столбцами образуем единичную матрицу размера $k \times k$, столбцы которой имеют номера, задаваемые вектором $\bar{r}$.

3. В i-й строке матрицы A $(1 \le i \le k)$ записываем нуль во все позиции $j > r_i$.

4. Оставшиеся места в матрице A заполняем элементами поля независимым образом.

Строки построенной матрицы A являются базисными векторами некоторого подпространства $V_{k,n} \subset V_n$. Поэтому задача нахождения количества k-мерных подпространств веса ω сводится к определению количества матриц A с базисными векторами, линейная комбинация которых дает возможность построить вектор, содержащий ровно ω ненулевых компонент, и в то же время не существует линейной комбинации базисных векторов с меньшим числом ненулевых компонент.

Обозначим:

$\left[\begin{matrix} n \\ k \end{matrix}\middle|\, \omega; \bar{r} \right]$ — количество k-мерных подпространств веса ω при фиксированном векторе $\bar{r} \in U$;

$$U_\omega(L) = \{\bar{r} \in U : r_1 \ge \omega, (r_2 - 2) + (r_3 - 3) + \ldots + (r_k - k) = L\},$$

$$(k-1)(\omega-1) \le L \le (k-1)(n-k);$$

$|U_\omega(L)|$ — число элементов во множестве $U_\omega(L)$.

В работе [1] доказано соотношение

$$\left[\begin{matrix} n \\ k \end{matrix}\middle|\, \omega \right] = Z_\omega \mathbf{M}_\nu \mathbf{M}\{c_\omega(\bar{\gamma}_\nu) | \nu\}, \tag{3}$$

где

$$Z_\omega = \sum_{L=(k-1)(\omega-1)}^{(k-1)(n-k)} |U_\omega(L)| q^{L+\omega-1}, \; c_\omega(\bar{r}) = \frac{1}{q^{L+\omega-1}} \left[\begin{matrix} n \\ k \end{matrix}\middle|\, \omega; \bar{r} \right], \tag{4}$$

математическое ожидание $\mathbf{M}_\nu$ берется по распределению случайной величины ν, принимающей значение $L \in \{(k-1)(\omega-1), \ldots, (k-1)(n-k)\}$ с вероятностью $\frac{1}{Z_\omega} |U_\omega(L)| q^{L+\omega-1}$; при фиксированном $\nu = L$ случайный вектор $\bar{\gamma}_L$ имеет равномерное распределение на множестве $U_\omega(L)$.

Формула (3) — типичный пример использования метода существенной выборки. Разложение по степеням q (см. алгоритм моделирования случайной величины ν) позволяет ранжировать слагаемые в соответствии с их «весом». При этом коэффициент $c_\omega(\bar r)$ равномерно ограничен для любых значений $\bar r$, ω и q. Рекуррентные формулы для вычисления $|U_\omega(L)|$ приведены в [1]. Проблема оценки $c_\omega(\bar r)$ для произвольных значений $n, k, \bar r$ и ω существенно более сложная. Именно этому вопросу уделяется основное внимание в данной статье.

Если предположить, что известен какой-либо способ вычисления коэффициента $c_\omega(\bar r)$ при любых значениях параметров $n, k, \bar r, \omega$ и L, то из соотношений (3), (4) следует простой алгоритм построения несмещенных оценок для $\begin{bmatrix} n \\ k \end{bmatrix}_\omega$.

1. С помощью рекуррентного алгоритма [1] вычисляем $|U_\omega(L)|$ для всех $L = (k-1), (\omega-1), \dots, (k-1), (n-k)$.

2. Согласно (4) вычисляем Z_ω.

3. Строим реализацию случайной величины ν, которая равна $L \in \{(k-1)\times$ $\times(\omega-1), \dots, (k-1)(n-k)\}$ с вероятностью $\dfrac{|U_\omega(L)|\, q^{L+\omega-1}}{Z_\omega}$. Пусть $\nu = L$.

4. Строим реализацию случайного вектора $\bar\gamma_L$, имеющего равномерное распределение на множестве $U_\omega(L)$. Пусть $\bar\gamma_L = \bar r$.

5. Вычисляем $c_\omega(\bar r)$.

6. В качестве оценки для $\begin{bmatrix} n \\ k \end{bmatrix}_\omega$, построенной в одной реализации алгоритма, выбираем $\hat\beta_\omega(n,k) = Z_\omega c_\omega(\bar r)$.

Замечания. 1. При фиксированном ω вычисление Z_ω (первые два шага алгоритма) проводится один раз.

2. Несмещенность оценки $\hat\beta_\omega(n,k)$ вытекает непосредственно из формул (3), (4).

Пусть $\bar r = (r_1, \dots, r_k)$ — вектор, определяющий номера столбцов, образующих единичную матрицу в матрице A. Дальнейшие рассуждения проводятся при фиксированном $\bar r$. Количество позиций в i-й строке $(i = 1, \dots, k)$, доступных для заполнения элементами поля, равно $r_i - 1 - (i-1) = r_i - i$. Очевидно, что $r_i - i \le r_j - j$ при $i < j$. В дальнейшем исключим из рассмотрения столбцы матрицы A с номерами, задаваемыми вектором $\bar r$, а также столбцы с номерами $j > r_k$. В результате получим прямоугольную матрицу $B = (b_{ij})$ размера $k \times (r_k - k)$ такую, что $b_{ij} = 0$ при $j > r_i - i$; на всех остальных позициях (i, j) может размещаться один из q элементов поля. Если $N(\bar r)$ — общее количество вариантов размещения элементов поля в матрице B, то

$$N(\bar r) = \prod_{i=1}^{k} q^{r_i - i} = q^{\sum_{i=1}^{k}(r_i - i)}. \tag{5}$$

Обозначим $Y_\omega(\bar r)$ событие, состоящее в том, что при случайном равновероятном выборе b_{ij}, $j \le r_i - i$, соответствующие строки матрицы A образуют базис k-мерного векторного подпространства веса ω. Тогда

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\omega;\, \bar r} = N(\bar r)\mathbf{P}\{Y_\omega(\bar r)\}. \tag{6}$$

Поскольку $L = \sum_{i=2}^{k}(r_i - i)$, из формул (4)–(6) следует

$$c_\omega(\bar r) = \frac{1}{q^{L+\omega-1}} \begin{bmatrix} n \\ k \end{bmatrix}_{\omega;\, \bar r} = \frac{N(\bar r)}{q^{L+\omega-1}}\, \mathbf{P}\{Y_\omega(\bar r)\} = q^{r_1 - \omega}\, \mathbf{P}\{Y_\omega(\bar r)\}. \tag{7}$$

В дальнейшем сосредоточим внимание на оценках вероятности $\mathbf{P}\{Y_\omega(\bar r)\}$.

ВСПОМОГАТЕЛЬНЫЙ АЛГОРИТМ

В настоящем разделе изложен вспомогательный алгоритм, лежащий в основе построения верхних и нижних оценок вероятности $\mathbf{P}\{Y_\omega(\bar{r})\}$.

Рассмотрим поле Галуа с s ненулевыми элементами. Пусть $\bar{x}$ — фиксированный m-мерный вектор, компонентами которого являются ненулевые элементы этого поля. Обозначим $\varphi_m^{(1)}(\sigma,s)$ число векторов $\bar{y}$, обладающих двумя свойствами: существует элемент поля Галуа $\beta \neq 0$ такой, что вектор $\bar{x}+\beta\bar{y}$ содержит ровно σ ненулевых компонент (вес линейной комбинации $\bar{x}$ и $\bar{y}$ равен σ); для всех $\gamma \neq \beta$ вектор $\bar{x}+\gamma\bar{y}$ содержит не менее σ ненулевых компонент. Иначе говоря, минимальный вес векторов $\bar{x}+\beta\bar{y}$ равен σ. Кроме того, обозначим

$$\varphi_m^{(0)}(\sigma,s)=\varphi_m^{(1)}(\sigma,s)+\varphi_m^{(1)}(\sigma+1,s)+\ldots+\varphi_m^{(1)}(m-1,s),\ \ 0\le\sigma\le m-1. \tag{8}$$

Лемма. При $\sigma < m-1$ справедливы рекуррентные соотношения:

$$\varphi_m^{(0)}(\sigma,s)=\varphi_m^{(0)}(\sigma+1,s)+\sum_{j=1}^{\left[\frac{m}{m-\sigma}\right]}\frac{m!}{[(m-\sigma)!]^j[m-j(m-\sigma)]!}C_s^j c_j(m,\sigma,s), \tag{9}$$

$$\varphi_m^{(1)}(\sigma,s)=\sum_{j=1}^{\left[\frac{m}{m-\sigma}\right]}\frac{m!}{[(m-\sigma)!]^j[m-j(m-\sigma)]!}C_s^j c_j(m,\sigma,s), \tag{10}$$

где

$$c_j(m,\sigma,s)=\begin{cases}1, & \text{если}\quad m'(j)=0,\\ (s-j)^{m'(j)}, & \text{если}\quad 0<m'(j)<m-\sigma,\\ (s-j)^{(m-\sigma)}-(s-j), & \text{если}\quad m'(j)=m-\sigma,\\ \varphi_{m'(j)}^{(0)}(m'(j)-(m-\sigma)+1,s-j), & \text{если}\quad m'(j)>m-\sigma,\end{cases}$$

$m'(j)=m-j(m-\sigma)$.

Начальные условия: $\varphi_m^{(0)}(\sigma,s)=0$, если $\sigma\ge m$ или $s=0$; $\varphi_m^{(0)}(m-1,s)=0$, если $s<m$;

$$\varphi_m^{(0)}(m-1,s)=\varphi_m^{(1)}(m-1,s)=\prod_{j=1}^{m}(s-j+1),\ \ s\ge m. \tag{11}$$

Доказательство. Случай $\sigma=m-1$ (см. формулу (11)) является самым простым. Действительно, первая компонента вектора $\bar{y}$ может принимать любое из s значений, вторая компонента по очевидным причинам может принимать на одно значение меньше (иначе вес линейной комбинации опустится ниже, чем $m-1$). Аналогично, третья компонента может принимать на два значения меньше, и т.д.

Из (8) вытекает, что при $\sigma < m-1$

$$\varphi_m^{(0)}(\sigma,s)=\varphi_m^{(0)}(\sigma+1,s)+\varphi_m^{(1)}(\sigma,s). \tag{12}$$

Поэтому достаточно доказать равенство (10); соотношение (9) следует из (10) и (12).

Равенство (10) вытекает из следующих соображений. Вектор $\bar{x}+\beta\bar{y}$ содержит ровно σ ненулевых компонент лишь в случае, когда для некоторого $\beta\neq 0$ существует группа из $m-\sigma$ компонент вектора $\bar{y}$, удовлетворяющих соотношениям $x_{i_l}+\beta y_{i_l}=0$, $l=1,\ldots,m-\sigma$. Таких групп может быть не более чем $\left[\frac{m}{m-\sigma}\right]$. Рассмотрим случай, когда вектор $\bar{y}$ содержит ровно j групп компонент, удовлетворяющих указанному свойству. Из правил комбинаторики следует, что число способов, которыми вектор из m элементов можно разбить на j групп из $m-\sigma$ элементов и

одну группу из $m' = m - j(m-\sigma)$ элементов, равно

$$C_m(m-\sigma,\dots,m-\sigma,m') = \frac{m!}{[(m-\sigma)!]^j\, m'!}.$$

При этом j группам в качестве соответствующих коэффициентов $\{\beta_j\}$ должны быть выделены j попарно различных элементов поля Галуа (что можно сделать C_s^j способами). Коэффициент $c_j(m,\sigma,s)$ определяет число m'-мерных векторов $\overline{y'}$ таких, что для любого ненулевого элемента β поля Галуа, принимающего $s-j$ значений, вес линейной комбинации $\overline{x'} + \beta\overline{y'}$ будет больше, чем $m'-(m-\sigma)$. Здесь $\overline{x'}$ — m'-мерный вектор, получаемый из $\bar{x}$ исключением компонент из j указанных групп. Если $m' = 0$, то $c_j(m,\sigma,s) = 1$. Если $0 < m' < m-\sigma$, то компоненты вектора $\overline{y'}$ могут принимать любые значения, за исключением j фиксированных значений, т.е. $c_j(m,\sigma,s) = (s-j)^{m'}$. Если $m' = m-\sigma$, то из всех возможных комбинаций надо исключить те случаи, когда все компоненты вектора $\overline{y'}$ отличаются от соответствующих компонент вектора $\overline{x'}$ на один и тот же множитель ($s-j$ возможных значений). Поэтому $c_j(m,\sigma,s) = (s-j)^{m'} - (s-j)$. Пусть $m' > m-\sigma$. В этом случае задача сводится к определению количества векторов $\overline{y'}$ таких, что вес любой линейной комбинации $\overline{x'} + \beta\overline{y'}$ будет не меньше, чем $\sigma' = m' - (m-\sigma) + 1$. Поэтому $c_j(m,\sigma,s) = \varphi_{m'}^{(0)}(\sigma', s')$, где $s' = s-j$. Просуммировав по всем возможным значениям j (соответствующие множества векторов $\bar{y}$ не пересекаются), получим формулу (10). Лемма доказана.

НАХОЖДЕНИЕ $\begin{bmatrix} n \\ k \end{bmatrix}_\omega$ ПРИ $k = 1, 2$

Для простейших случаев $k = 1$ и $k = 2$ значение $\begin{bmatrix} n \\ k \end{bmatrix}_\omega$ может быть найдено в явном виде.

Теорема 1. Справедливы следующие равенства:

$$\begin{bmatrix} n \\ 1 \end{bmatrix}_\omega = (q-1)^{\omega-1} \sum_{r=\omega}^{n} C_{r-1}^{\omega-1}, \tag{13}$$

$$\begin{bmatrix} n \\ 2 \end{bmatrix}_\omega = \sum_{r_1=\omega}^{n-1} \sum_{r_2=r_1+1}^{n} \left\{ \sum_{l=\omega-1}^{r_1-1} C_{r_1-1}^{l} (q-1)^l \sum_{(s_1,s_2)\in S(l)} C_l^{s_1} C_{r_2-2-l}^{s_2} (q-1)^{s_2} \psi(l,s_1,s_2) + \right.$$

$$\left. + \sum_{l=\omega}^{r_1-1} C_{r_1-1}^{l} (q-1)^l \sum_{(s_1,s_2)\in U(l)} C_l^{s_1} C_{r_2-2-l}^{s_2} (q-1)^{s_2} \pi(l,s_1,s_2) \right\}. \tag{14}$$

Здесь

$$S(\omega-1) = \{(s_1,s_2): 0 \le s_1 \le \omega-1,\ 0 \le s_2 \le r_2 - \omega - 1,\ s_1 + s_2 \ge \omega - 1\}, \tag{15}$$

$$S(l) = \{(s_1,s_2):\ s_1 + s_2 = \omega - 1,\ 0 \le s_2 \le \min\{\omega-1, r_2-2-l\}\},\ l = \omega,\dots,r_1-1, \tag{16}$$

$$U(l) = \{(s_1,s_2):\ s_1 + s_2 \ge \omega,\ 0 \le s_1 \le l,\ 0 \le s_2 \le r_2 - 2 - l\},\ l = \omega,\dots,r_1-1, \tag{17}$$

$$\psi(l,s_1,s_2) = \sum_{\sigma=s_1-s_2-l+\omega-2}^{s_1-1} \varphi_{s_1}^{(1)}(\sigma, q-1),\ \text{если}\ s_1 - s_2 - l + \omega - 2 > 0, \tag{18}$$

$$\psi(l, s_1, s_2) = (q-1)^{s_1}, \text{ если } s_1 - s_2 - l + \omega - 2 \le 0, \tag{19}$$

$$\pi(l, s_1, s_2) = \varphi^{(1)}_{s_1}(s_1 - s_2 - l + \omega - 2,\ q-1), \text{ если } 0 \le s_1 - s_2 - l + \omega - 2 < s_1, \tag{20}$$

$$\pi(l, s_1, s_2) = 0 \text{ в противном случае,} \tag{21}$$

$\{\varphi^{(1)}_{s_1}(\sigma, q-1)\}$ определяются согласно рекуррентным формулам (9)–(11).

Доказательство. Пусть $k = 1$. Событие $Y_\omega(\bar{r})$ наступает тогда и только тогда, когда единственная строка матрицы B содержит ровно $\omega - 1$ ненулевых элементов. Поэтому

$$\mathbf{P}\{Y_\omega(\bar{r})\} = C^{\omega-1}_{r_1-1}\left(\frac{q-1}{q}\right)^{\omega-1}\left(\frac{1}{q}\right)^{r_1-\omega}. \tag{22}$$

Воспользовавшись соотношениями (5), (6) и (22), получим формулу (13):

$$\begin{bmatrix} n \\ 1 \end{bmatrix}\omega = \sum_{r_1=\omega}^{n} \begin{bmatrix} n \\ 1 \end{bmatrix}\omega;\ r_1 = (q-1)^{\omega-1} \sum_{r_1=\omega}^{n} C^{\omega-1}_{r-1}.$$

Случай $k = 2$ существенно более сложен. Имеет место

$$\begin{bmatrix} n \\ 2 \end{bmatrix}\omega = \sum_{r_1=\omega}^{n-1} \sum_{r_2=r_1+1}^{n} \begin{bmatrix} n \\ 2 \end{bmatrix}\omega;\ r_1,\ r_2 \Bigg]. \tag{23}$$

Вычислим вероятность события $Y_\omega(\bar{r})$, а далее воспользуемся формулами (5) и (6). Введем события:

• Z_1 = {первая строка матрицы B содержит $\omega - 1$ ненулевых элементов, вторая — не менее $\omega - 1$ ненулевых элементов; любая линейная комбинация первых двух строк матрицы B имеет по крайней мере $\omega - 2$ ненулевых элементов};

• Z_2 = {первая строка матрицы B содержит более $\omega - 1$ ненулевых элементов, вторая — $\omega - 1$ ненулевых элементов; любая линейная комбинация первых двух строк матрицы B имеет по крайней мере $\omega - 2$ ненулевых элементов};

• $Z_{1,2}$ = {первые две строки матрицы B содержат более $\omega - 1$ ненулевых элементов; существует линейная комбинация первых двух строк этой матрицы, содержащая $\omega - 2$ ненулевых элементов, а любые другие линейные комбинации содержат не менее $\omega - 2$ ненулевых элементов}.

Данные события несовместны, поэтому

$$\mathbf{P}\{Y_\omega(\bar{r})\} = \mathbf{P}\{Z_1\} + \mathbf{P}\{Z_2\} + \mathbf{P}\{Z_{1,2}\}. \tag{24}$$

Вероятность события Z_1 вычисляется следующим образом. Среди $r_1 - 1$ позиций первой строки выбираем $\omega - 1$ позиций, на которых расположены ненулевые элементы (вероятность чего равна $C^{\omega-1}_{r_1-1}\left(\frac{q-1}{q}\right)^{\omega-1}\left(\frac{1}{q}\right)^{r_1-\omega}$). Множество этих позиций обозначим E. Рассмотрим расположение символов во второй строке. Введем событие $H(s_1, s_2)$ = {во второй строке на позициях из множества E расположено s_1 ненулевых символов, а на остальных доступных для заполнения позициях расположено s_2 ненулевых символов}. Очевидно, что $(s_1, s_2) \in S(\omega - 1)$ (см. (15)). Вероятность данного события равна

$$p(l, s_1, s_2) = C^{s_1}_{l}\left(\frac{q-1}{q}\right)^{s_1}\left(\frac{1}{q}\right)^{l-s_1} C^{s_2}_{r_2-2-l}\left(\frac{q-1}{q}\right)^{s_2}\left(\frac{1}{q}\right)^{r_2-2-l-s_2} \tag{25}$$

при $l = \omega - 1$. В силу расположения нулевых и ненулевых символов в каждой из

строк линейная комбинация этих строк содержит не менее $(\omega-1-s_1)+s_2$ ненулевых символов. Если $s_2 \ge s_1-1$, то третье условие события Z_1 выполнено. В этом случае положим $\theta(\omega-1,s_1,s_2)=1$. Если $s_2 < s_1-1$, то, воспользовавшись леммой предыдущего раздела, для вероятности выполнения третьего условия события Z_1 получим равенство

$$\theta(\omega-1,s_1,s_2)=\frac{\psi(\omega-1,s_1,s_2)}{(q-1)^{s_1}},$$

где $\psi(\omega-1,s_1,s_2)$ вычисляется согласно формулам (18), (19). Окончательно имеем

$$\mathbf{P}\{Z_1\}=C_{r_1-1}^{\omega-1}\left(\frac{q-1}{q}\right)^{\omega-1}\left(\frac{1}{q}\right)^{r_1-\omega}\sum_{(s_1,s_2)\in S(\omega-1)}p(\omega-1,s_1,s_2)\,\theta(\omega-1,s_1,s_2). \qquad (26)$$

Аналогичными рассуждениями получаем формулы для вероятностей событий Z_2 и $Z_{1,2}$:

$$\mathbf{P}\{Z_2\}=\sum_{l=\omega}^{r_1-1}C_{r_1-1}^{l}\left(\frac{q-1}{q}\right)^{l}\left(\frac{1}{q}\right)^{r_1-1-l}\sum_{(s_1,s_2)\in S(l)}p(l,s_1,s_2)\frac{\psi(l,s_1,s_2)}{(q-1)^{s_1}}, \qquad (27)$$

$$\mathbf{P}\{Z_{1,2}\}=\sum_{l=\omega}^{r_1-1}C_{r_1-1}^{l}\left(\frac{q-1}{q}\right)^{l}\left(\frac{1}{q}\right)^{r_1-1-l}\sum_{(s_1,s_2)\in U(l)}p(l,s_1,s_2)\frac{\pi(l,s_1,s_2)}{(q-1)^{s_1}}, \qquad (28)$$

где $S(l)$, $U(l)$, $\{\psi(l,s_1,s_2)\}$ и $\{\pi(l,s_1,s_2)\}$ вычисляются согласно формулам (16)–(21). Объединяя (5), (6), (23)–(28), получаем формулу (14).

Теорема доказана.

ВЕРХНИЕ И НИЖНИЕ ОЦЕНКИ ВЕРОЯТНОСТИ $\mathbf{P}\{Y_\omega(\bar r)\}$

Пусть, как и ранее, вектор $\bar r$ фиксирован (он генерируется с помощью описанного выше алгоритма построения несмещенных оценок для $\begin{bmatrix} n \\ k \end{bmatrix}_\omega$). Предположим, что в каждой доступной для заполнения позиции матрицы $B=(b_{ij})$ с вероятностью $1/q$ может быть расположен один из элементов поля Галуа. Событие $Y_\omega(\bar r)=$ {строки матрицы A являются базисом k-мерного векторного подпространства веса ω} наступит тогда и только тогда, когда произойдет одно из k несовместных событий $D_\omega^{(i)}(\bar r)$, $i=1,\dots,k$. Выполнение события $D_\omega^{(i)}(\bar r)$ обусловлено тремя условиями:

а) первые $i-1$ строки матрицы A — базис $(i-1)$-мерного векторного пространства веса не менее $\omega+1$;

б) i-я строка матрицы A содержит ровно ω ненулевых элементов либо для некоторых $m\in\{1,\dots,i-1\}$, $1\le j_1<j_2<\dots<j_m\le i-1$ существует линейная комбинация i-й строки со строками $j_1,\dots,j_m$, в которой будет ω ненулевых элементов; в то же время не существует линейных комбинаций i-й строки с предыдущими, определяющих вектор с меньшим числом ненулевых элементов;

в) для всех $j=i+1,\dots,k$ первые j строк матрицы A — базис j-мерного векторного пространства веса ω.

Очевидно, что

$$\mathbf{P}\{Y_\omega(\bar r)\}=\sum_{i=1}^{k}\mathbf{P}\{D_\omega^{(i)}(\bar r)\}. \qquad (29)$$

Вычислить точное значение вероятности события $D_\omega^{(i)}(\bar r)$ не представляется возможным. Как будет видно из дальнейшего, это связано с проблемой нахождения вероятности наступления одного из s зависимых событий. Ничего более эффективного, чем формула включений–исключений, до сих пор не найдено. Если s — число со многими

нулями, то задача нахождения вероятностей всех попарных пересечений указанных событий становится нереальной. Поэтому в качестве верхней оценки используем сумму вероятностей соответствующих событий; нижняя оценка тривиальна.

Общая схема предлагаемого подхода состоит в следующем. Обозначим:

$$\nu_{jl} = \begin{cases} 0, \text{ если в } l\text{-й позиции } j\text{-й строки матрицы } B \\ \quad \text{расположен нулевой элемент,} \\ 1 \quad \text{в противном случае,} \end{cases}$$

$$l = 1,\dots,r_k - k,\ \ j = 1,\dots,k,\ \ \bar{\nu} = (\nu_{jl});$$

$$p_j(l;\bar{r}) = C^l_{r_j-j}\left(1-\frac{1}{q}\right)^l\left(\frac{1}{q}\right)^{r_j-j-l} = C^l_{r_j-j}\,\frac{(q-1)^l}{q^{r_j-j}},\ j = 1,\dots,k,\ l = 0,\dots,r_j - j, \quad (30)$$

— вероятность того, что j-я строка матрицы B содержит l ненулевых элементов (соответствующая строка матрицы A содержит $l+1$ ненулевых элементов). Выполнение условий а) – в) означает, что каждая из строк $1,\dots,i-1$ матрицы A содержит не менее $\omega+1$ ненулевых элементов, а строки $i,\dots,k$ — не менее ω ненулевых элементов. Поэтому

$$\mathbf{P}\{D^{(i)}_\omega(\bar{r})\} = \prod_{j=1}^{i-1}\sum_{l=\omega}^{r_j-j} p_j(l;\bar{r}) \prod_{j=i+1}^{k}\sum_{l=\omega-1}^{r_j-j} p_j(l;\bar{r}) \sum_{s=\omega-1}^{r_i-i} p_i(s;\bar{r})\mathbf{M}_{\bar{\nu}(s)}\mathbf{P}\{D^{(i)}_\omega(\bar{r})\,|\,\bar{\nu}(s)\}, \quad (31)$$

где соответствующие математические ожидания берутся по значениям случайных векторов $\bar{\nu}(s) = \{\nu_{jl}(s)\}$. Каждая из компонент $\nu_{jl}(s)$, $l = 1,\dots,r_j - j$, принимает значение 0 с вероятностью $\frac{1}{q}$ и 1 — с вероятностью $\frac{q-1}{q}$ при условии, что $\nu_{j1}(s)+\dots+\nu_{jr_j-j}(s) \ge \omega$, $j = 1,\dots,i-1$, $\nu_{i1}(s)+\dots+\nu_{ir_i-i}(s) = s$, $\nu_{j1}(s)+\dots$ $\dots+\nu_{jr_j-j}(s) \ge \omega-1$, $j = i+1,\dots,k$.

Построим вначале верхнюю оценку для вероятности $\mathbf{P}\{D^{(i)}_\omega(\bar{r})\,|\,\bar{\nu}(s)\}$, считая компоненты вектора $\bar{\nu}(s)$ известными. Отбросив условия а) и в), получим оценки

$$\mathbf{P}\{D^{(i)}_\omega(\bar{r})|\bar{\nu}(s)\} \le 1 \text{ при } s = \omega-1, \quad (32)$$

$$\mathbf{P}\{D^{(i)}_\omega(\bar{r})|\bar{\nu}(s)\} \le \sum_{m=1}^{i-1}\sum_{1\le j_1<j_2<\dots<j_m\le i-1} \mathbf{P}\{E^{(i)}_{\omega,s,m}(\bar{r},\bar{j})|\bar{\nu}(s)\} \text{ при } s = \omega,\dots,r_i - i, \quad (33)$$

где $E^{(i)}_{\omega,s,m}(\bar{r},\bar{j}) =$ {существует линейная комбинация i-й строки матрицы A, содержащей s ненулевых элементов, и строк, определяемых вектором $\bar{j} = (j_1,\dots,j_m)$, в которой ω ненулевых элементов; в то же время не существует указанных линейных комбинаций, определяющих вектор с меньшим числом ненулевых элементов}.

Построим верхнюю оценку вероятности $\mathbf{P}\{E^{(i)}_{\omega,s,m}(\bar{r},\bar{j})|\bar{\nu}(s)\}$. Для каждого $l = 1,\dots,r_i - i$ вычислим

$$\mu_l(s) = \begin{cases} 0, \text{ если } \nu_{j_z l}(s) = 0 \text{ для всех } z = 1,\dots,m, \\ 1 \quad \text{в противном случае.} \end{cases}$$

Обозначим w число индексов l таких, что $\mu_l(s) = 1$ и $\nu_{il}(s) = 1$, а δ — число индексов l таких, что $\mu_l(s)+\nu_{il}(s) = 1$. Очевидно, что любая линейная комбинация i-й строки со строками, задаваемыми вектором $\bar{j}$, содержит по крайней мере $m+1+\delta$ ненулевых элементов. Если $m+1+\delta > \omega$, то $\mathbf{P}\{E^{(i)}_{\omega,s,m}(\bar{r},\bar{j})|\bar{\nu}(s)\} = 0$. Пусть $\sigma = \omega-(m+1+\delta) \ge 0$. В этом случае

$$\mathbf{P}\{E^{(i)}_{\omega,s,m}(\bar r,\bar j)\,|\,\bar\nu(s)\}\le(q-1)^{m-1}\,\frac{\varphi^{(1)}_w(\sigma,q-1)}{(q-1)^w}=(q-1)^{m-w-1}\varphi^{(1)}_w(\sigma,q-1)\,. \quad (34)$$

Действительно, $(q-1)^{m-1}$ — число способов, какими можно построить различные (с точностью до множителя) линейные комбинации строк, определяемых вектором $\bar j$. Пусть $\bar\mu$ — фиксированная линейная комбинация m строк. Тогда $(q-1)^w$ — число всех возможных способов заполнения ненулевыми символами w позиций в i-й строке, $\varphi^{(1)}_w(\sigma,q-1)$ — число способов заполнения ненулевыми символами w позиций в i-й строке, при которых существует линейная комбинация i-й строки и вектора $\bar\mu$, в которой ровно σ ненулевых элементов, и не существует линейных комбинаций i-й строки и вектора $\bar\mu$, определяющих вектор с меньшим числом ненулевых элементов.

Соотношения (29)–(34) позволяют сформулировать алгоритм построения верхних оценок вероятности $\mathbf{P}\{Y_\omega(\bar r)\}$.

Теорема 2. Имеет место соотношение

$$\mathbf{P}\{Y_\omega(\bar r)\}\le\mathbf{M}\alpha^{(\mathrm{up})}_\omega(\bar r)\,.$$

Алгоритм построения реализаций случайной величины $\alpha^{(\mathrm{up})}_\omega(\bar r)$ формулируется следующим образом.

1. По формуле (30) вычисляем вероятности $\{p_j(l;\bar r)\}$.

2. Для каждого $i=1,\dots,k$ осуществляем следующие шаги:

• вычисляем (см. (31) и (32))

$$d^{(i)}_\omega(\bar r)=p_i(\omega-1;\bar r)\prod_{j=1}^{i-1}\sum_{l=\omega}^{r_j-j}p_j(l;\bar r)\prod_{j=i+1}^{k}\sum_{l=\omega-1}^{r_j-j}p_j(l;\bar r)\,; \quad (35)$$

• определяем моделированием, какие из компонент вектора $\bar\nu=\{\nu_{jl}\}$ нулевые, какие нет, а именно, компонента ν_{jl} принимает значение 0 с вероятностью $\dfrac{1}{q}$ и 1 — с вероятностью $\dfrac{q-1}{q}$ при условии, что $\nu_{j1}+\dots+\nu_{jr_j-j}\ge\omega,\ j=1,\dots,i,$ $\nu_{j1}+\dots\ +\nu_{jr_j-j}\ge\omega-1,\ j=i+1,\dots,k$.

3. Вычисляем оценку (см. (31), (33) и (34))

$$\alpha^{(\mathrm{up})}_\omega(\bar r)=\sum_{i=1}^{k}\left[d^{(i)}_\omega(\bar r)+h^{(i)}_\omega(\bar r)\sum_{m=1}^{i-1}\sum_{1\le j_1<j_2<\dots<j_m\le i-1}(q-1)^{m-w(\bar j)-1}\varphi^{(1)}_w(\sigma(\bar j),q-1)\right], \quad (36)$$

где

$$h^{(i)}_\omega(\bar r)=\prod_{j=1}^{i}\sum_{l=\omega}^{r_j-j}p_j(l;\bar r)\prod_{j=i+1}^{k}\sum_{l=\omega-1}^{r_j-j}p_j(l;\bar r)\,, \quad (37)$$

а значения $w(\bar j),\sigma(\bar j)$ вычисляются по тем же правилам, что и w,σ в формуле (34); здесь, как и ранее, $\bar j=(j_1,\dots,j_m)$.

Построим нижнюю оценку для вероятности $\mathbf{P}\{D^{(i)}_\omega(\bar r)\}$. Из формулы (31) следует оценка

$$\mathbf{P}\{D^{(i)}_\omega(\bar r)\}\ge p_i(\omega-1;\bar r)\prod_{j=1}^{i-1}\sum_{l=\omega}^{r_j-j}p_j(l;\bar r)\prod_{j=i+1}^{k}\sum_{l=\omega-1}^{r_j-j}p_j(l;\bar r)\,\mathbf{M}_{\bar\nu^{(i)}}\,\mathbf{P}\{D^{(i)}_\omega(\bar r)\,|\,\bar\nu^{(i)}\}\,, \quad (38)$$

где соответствующие математические ожидания берутся по значениям случайных векторов $\bar\nu^{(i)}=\{\nu^{(i)}_{jl}\}$. Каждая из компонент $\nu^{(i)}_{jl}$, $l=1,\dots,r_j-j$, принимает

значение 0 с вероятностью $\frac{1}{q}$ и 1 — с вероятностью $\frac{q-1}{q}$ при условии, что $\nu_{j1}^{(i)}+\ldots+\nu_{jr_j-j}^{(i)}\ge\omega,\ j=1,\ldots,i-1,\ \nu_{i1}^{(i)}+\ldots+\nu_{ir_i-i}^{(i)}=\omega-1,\ \nu_{j1}^{(i)}+\ldots+\nu_{jr_j-j}^{(i)}\ge\omega-1,$ $j=i+1,\ldots,k.$

Построим нижнюю оценку для вероятности $\mathbf{P}\{D_\omega^{(i)}(\bar r)\,|\,\bar\nu^{(i)}\}$, считая компоненты вектора $\bar\nu^{(i)}$ известными. Введем события: $V_\omega^{(i)}(\bar r,\gamma)=\{$первые γ строк матрицы A — базис γ-мерного векторного пространства веса не менее $\omega+1\ \}$, $\gamma=1,\ldots,k.$ Очевидно, что $V_\omega^{(i)}(\bar r,\gamma+1)\subset V_\omega^{(i)}(\bar r,\gamma),\ \gamma=1,\ldots,k-1,$ причем событие $V_\omega^{(i)}(\bar r,1)$ достоверно. Тогда

$$D_\omega^{(i)}(\bar r)=\bigcap_{\gamma=2}^{i-1}V_\omega^{(i)}(\bar r,\gamma)\cap\bigcap_{\gamma=i+1}^{k}V_{\omega-1}^{(i)}(\bar r,\gamma).$$

Поэтому

$$\mathbf{P}\{D_\omega^{(i)}(\bar r)\,|\,\bar\nu^{(i)}\}=\prod_{\gamma=2}^{i-1}\mathbf{P}\{V_\omega^{(i)}(\bar r,\gamma)\,|\,\bar\nu^{(i)};\,V_\omega^{(i)}(\bar r,\gamma-1)\}\times$$

$$\times\prod_{\gamma=i+1}^{k}\mathbf{P}\{V_{\omega-1}^{(i)}(\bar r,\gamma)\,|\,\bar\nu^{(i)};\,V_{\omega-1}^{(i)}(\bar r,\gamma-1)\}\qquad(39)$$

(в силу определения вектора $\bar\nu^{(i)}$ вес γ-мерного векторного пространства при $\gamma\ge i+1$ не может быть больше ω). В то же время

$$\mathbf{P}\{V_\omega^{(i)}(\bar r,\gamma)\,|\,\bar\nu^{(i)};\,V_\omega^{(i)}(\bar r,\gamma-1)\}=1-\mathbf{P}\{\overline{V}_\omega^{(i)}(\bar r,\gamma)\,|\,\bar\nu^{(i)};\,V_\omega^{(i)}(\bar r,\gamma-1)\},\qquad(40)$$

где $\overline{V}_\omega^{(i)}(\bar r,\gamma)$ обозначает событие, дополнительное к $V_\omega^{(i)}(\bar r,\gamma)$. Наступление события $\overline{V}_\omega^{(i)}(\bar r,\gamma)$ при условии, что произошло событие $V_\omega^{(i)}(\bar r,\gamma-1)$, означает, что элементы в строке γ расположены таким образом, что линейная комбинация этой строки с предыдущими позволит получить вектор с числом ненулевых компонент, меньшим, чем $\omega+1$. Для построения верхней оценки вероятности события $\overline{V}_\omega^{(i)}(\bar r,\gamma)$ воспользуемся тем же приемом, что и ранее. Действительно, при $\gamma\ge2$

$$\mathbf{P}\{\overline{V}_\omega^{(i)}(\bar r,\gamma)\,|\,\bar\nu^{(i)};\,V_\omega^{(i)}(\bar r,\gamma-1)\}\le$$

$$\le\sum_{m=1}^{\gamma-1}\sum_{1\le j_1<j_2<\ldots<j_m\le\gamma-1}\mathbf{P}\{W_{\omega,m}^{(i)}(\bar r,\bar j,\gamma)\,|\,\bar\nu^{(i)};\,V_\omega^{(i)}(\bar r,\gamma-1)\},\qquad(41)$$

где $W_{\omega,m}^{(i)}(\bar r,\bar j,\gamma)=\{$существует линейная комбинация строки γ матрицы A и строк, определяемых вектором $\bar j=(j_1,\ldots,j_m)$, в которой не более ω ненулевых элементов$\}$. Далее для каждого $l=1,\ldots,r_\gamma-\gamma$ вычисляем

$$\mu_l=\begin{cases}0,\ \text{если}\ \nu_{j_zl}^{(i)}=0\ \text{для всех}\ z=1,\ldots,m,\\ 1\ \text{в противном случае.}\end{cases}$$

Обозначим w число индексов l таких, что $\mu_l=1$ и $\nu_{\gamma l}^{(i)}=1$, а δ — число индексов l таких, что $\mu_l+\nu_{\gamma l}^{(i)}=1$. Очевидно, что любая линейная комбинация строки γ со строками, задаваемыми вектором $\bar j$, содержит по крайней мере $m+1+\delta$ ненулевых элементов. Если $m+1+\delta>\omega$, то $\mathbf{P}\{W_{\omega,m}^{(i)}(\bar r,\bar j,\gamma)\,|\,\bar\nu^{(i)};\,V_\omega^{(i)}(\bar r,\gamma-1)\}=0$. Пусть $\sigma=\omega-(m+1+\delta)\ge0$. В этом случае

$$\mathbf{P}\{W_{\omega,m}^{(i)}(\bar{r},\bar{j},\gamma)\,|\,\bar{\nu}^{(i)};\,V_{\omega}^{(i)}(\bar{r},\gamma-1)\}\le(q-1)^{m-1}\,\frac{\sum\limits_{\tau=0}^{\sigma}\varphi_w^{(1)}(\tau,q-1)}{(q-1)^w}=$$

$$=(q-1)^{m-w-1}\sum_{\tau=0}^{\sigma}\varphi_w^{(1)}(\tau,q-1)\,. \qquad (42)$$

Действительно, $(q-1)^{m-1}$ — число способов, какими можно построить различные (с точностью до множителя) линейные комбинации строк, определяемых вектором $\bar{j}$. Пусть $\bar{\mu}$ — фиксированная линейная комбинация m строк. Тогда $(q-1)^w$ — число всех возможных способов заполнения ненулевыми символами w позиций в строке γ, а $\sum\limits_{\tau=0}^{\sigma}\varphi_w^{(1)}(\tau,q-1)$ — число способов заполнения ненулевыми символами w позиций в строке γ, при которых существует линейная комбинация строки γ и вектора $\bar{\mu}$, в которой не более σ ненулевых элементов.

Аналогично оцениваются и вероятности $\mathbf{P}\{V_{\omega-1}^{(i)}(\bar{r},\gamma)\,|\,\bar{\nu}^{(i)};\,V_{\omega-1}^{(i)}(\bar{r},\gamma-1)\}$ при $\gamma=i+1,\dots,k$.

Соотношения (29), (30), (38)–(42) позволяют сформулировать алгоритм построения нижних оценок вероятности $\mathbf{P}\{Y_\omega(\bar{r})\}$.

Теорема 3. Имеет место соотношение

$$\mathbf{P}\{Y_\omega(\bar{r})\}\ge\mathbf{M}\alpha_\omega^{(\mathrm{low})}(\bar{r})\,.$$

Алгоритм построения реализаций случайной величины $\alpha_\omega^{(\mathrm{low})}(\bar{r})$ формулируется следующим образом.

1. По формуле (30) вычисляем вероятности $\{p_j(l;\bar{r})\}$.

2. Для каждого $i=1,\dots,k$ осуществляем следующие шаги:

- по формуле (35) вычисляем $d_\omega^{(i)}(\bar{r})$;
- определяем моделированием, какие из компонент вектора $\bar{\nu}^{(i)}=\{\nu_{jl}^{(i)}\}$ нулевые, какие нет, а именно, компонента $\nu_{jl}^{(i)}$ принимает значение 0 с вероятностью $\frac{1}{q}$ и 1 — с вероятностью $\frac{q-1}{q}$ при условии, что $\nu_{j1}^{(i)}+\dots+\nu_{jr_j-j}^{(i)}\ge\omega$, $j=1,\dots,i-1$, $\nu_{i1}^{(i)}+\dots+\nu_{ir_i-i}^{(i)}=\omega-1$, $\nu_{j1}^{(i)}+\dots+\nu_{jr_j-j}^{(i)}\ge\omega-1$, $j=i+1,\dots,k$;
- по формулам (38)–(40) строим нижние оценки $\{g_\omega^{(i)}(\bar{r},\gamma)\}$ для вероятностей $\mathbf{P}\{V_\omega^{(i)}(\bar{r},\gamma)\,|\,\bar{\nu}^{(i)};\,V_\omega^{(i)}(\bar{r},\gamma-1)\}$, $\gamma=2,\dots,i-1$, и нижние оценки $\{g_{\omega-1}^{(i)}(\bar{r},\gamma)\}$ для вероятностей $\mathbf{P}\{V_{\omega-1}^{(i)}(\bar{r},\gamma)\,|\,\bar{\nu}^{(i)};\,V_{\omega-1}^{(i)}(\bar{r},\gamma-1)\}$, $\gamma=i+1,\dots,k$.

3. Вычисляем оценку (см. (29), (36) и (37))

$$\alpha_\omega^{(\mathrm{low})}(\bar{r})=\sum_{i=1}^{k}\left[d_\omega^{(i)}(\bar{r})\prod_{\gamma=2}^{i-1}g_\omega^{(i)}(\bar{r},\gamma)\prod_{\gamma=i+1}^{k}g_{\omega-1}^{(i)}(\bar{r},\gamma)\right]. \qquad (43)$$

Сформулированные алгоритмы (теоремы 2 и 3) в сочетании с формулами (3), (4) и (7) позволяют строить верхние и нижние оценки для $\left[\begin{matrix}n\\k\end{matrix}\middle|\,\omega\right]$. В то же время, как показывают многочисленные примеры, наиболее точной является аппроксимация, основанная на комбинации верхних и нижних оценок (см. (37) и (45)), а именно

$$\alpha_{\omega}^{(\mathrm{appr})}(\bar{r}) = \sum_{i=1}^{k} \left[d_{\omega}^{(i)}(\bar{r}) \prod_{\gamma=2}^{i-1} g_{\omega}^{(i)}(\bar{r},\gamma) \prod_{\gamma=i+1}^{k} g_{\omega-1}^{(i)}(\bar{r},\gamma) + \right.$$

$$\left. + h_{\omega}^{(i)}(\bar{r}) \sum_{m=1}^{i-1} \sum_{1 \le j_1 < j_2 < \ldots < j_m \le i-1} (q-1)^{m-w(\bar{j})-1} \varphi_{w}^{(1)}(\sigma(\bar{j}), q-1) \right], \qquad (44)$$

где $\{d_{\omega}^{(i)}(\bar{r})\}$ и $\{h_{\omega}^{(i)}(\bar{r})\}$ вычисляются согласно (35) и (37); остальные обозначения — см. формулировки алгоритмов построения верхних и нижних оценок (теоремы 2 и 3).

ЧИСЛЕННЫЕ РЕЗУЛЬТАТЫ

Проиллюстрируем точность оценок на численных примерах. В первом примере приведен случай, когда известно точное значение $\left[\begin{matrix} n \\ k \end{matrix} \middle| \, \omega \right]$, во втором рассмотрены те значения k и ω, для которых отсутствуют какие-либо оценки. Все приведенные ниже оценки построены с относительной погрешностью $\varepsilon = 1\%$ и достоверностью 0,99. Использование ускоренного моделирования на многопроцессорном комплексе СКИТ-3 позволило получить оценки высокой точности для достаточно больших значений n, k и ω. Выбор числа задействованных процессоров проводился исходя из условия, чтобы время вычислений для каждого варианта не превышало 30 минут. Положим $n = 50$, $q = 2^5 = 32$. Введем следующие обозначения:

$\hat{\theta}_{\omega}^{(\mathrm{low})}(n,k)$ и $\hat{\theta}_{\omega}^{(\mathrm{up})}(n,k)$ — верхние и нижние оценки для $\left[\begin{matrix} n \\ k \end{matrix} \middle| \, \omega \right]$, построенные с указанными выше достоверностью и относительной погрешностью;

$\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$ — аппроксимация для $\left[\begin{matrix} n \\ k \end{matrix} \middle| \, \omega \right]$, основанная на оценках вида (44).

Пример 1. Рассматриваются два случая, когда удается найти точное значение $\left[\begin{matrix} n \\ k \end{matrix} \middle| \, \omega \right]$: $k = 2$, ω — произвольное (см. (14)); $\omega = 2$, k — произвольное (рекуррентные формулы см. [6]). Соответствующие оценки представлены в табл. 1 ($n = 50$, $k = 2$, $q = 2^5$, $\varepsilon = 1{,}0\%$) и табл. 2 ($n = 50$, $\omega = 2$, $q = 2^5$, $\varepsilon = 1{,}0\%$).

Таблица 1

ω	$\left[\begin{matrix} n \\ k \end{matrix} \middle| \, \omega \right]$	$\hat{\theta}_{\omega}^{(\mathrm{low})}(n,k)$	$\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$	$\hat{\theta}_{\omega}^{(\mathrm{up})}(n,k)$
6	$8{,}30 \cdot 10^{86}$	$8{,}24 \cdot 10^{86}$	$8{,}32 \cdot 10^{86}$	$8{,}32 \cdot 10^{86}$
12	$5{,}63 \cdot 10^{99}$	$5{,}33 \cdot 10^{99}$	$5{,}61 \cdot 10^{99}$	$5{,}61 \cdot 10^{99}$
18	$7{,}42 \cdot 10^{110}$	$6{,}48 \cdot 10^{110}$	$7{,}33 \cdot 10^{110}$	$7{,}33 \cdot 10^{110}$
24	$4{,}44 \cdot 10^{120}$	$3{,}41 \cdot 10^{120}$	$4{,}41 \cdot 10^{120}$	$4{,}41 \cdot 10^{120}$
30	$1{,}53 \cdot 10^{129}$	$0{,}97 \cdot 10^{129}$	$1{,}52 \cdot 10^{129}$	$1{,}52 \cdot 10^{129}$
36	$2{,}70 \cdot 10^{136}$	$1{,}31 \cdot 10^{136}$	$2{,}70 \cdot 10^{136}$	$2{,}70 \cdot 10^{136}$
42	$1{,}37 \cdot 10^{142}$	$0{,}40 \cdot 10^{142}$	$1{,}36 \cdot 10^{142}$	$1{,}36 \cdot 10^{142}$
45	$1{,}14 \cdot 10^{144}$	$0{,}26 \cdot 10^{144}$	$1{,}14 \cdot 10^{144}$	$1{,}17 \cdot 10^{144}$
48	$5{,}26 \cdot 10^{138}$	$5{,}00 \cdot 10^{138}$	$5{,}26 \cdot 10^{138}$	$8{,}27 \cdot 10^{143}$
49	0	0	0	$1{,}48 \cdot 10^{143}$

В обоих случаях высокую точность демонстрирует аппроксимация $\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$ при самых разных значениях ω ($k = 2$) и k ($\omega = 2$). В широком диапазоне изменения k и ω высокой точностью обладают также их верхняя и нижняя оценки

$\hat{\theta}_{\omega}^{(\mathrm{up})}(n,k)$ и $\hat{\theta}_{\omega}^{(\mathrm{low})}(n,k)$. Только при $\omega=48$, $\omega=49$ (табл. 1) и $k=47$, $k=48$ (табл. 2) оценка $\hat{\theta}_{\omega}^{(\mathrm{up})}(n,k)$ дает несколько завышенные значения. С возрастанием ω (табл. 1) точность оценки $\hat{\theta}_{\omega}^{(\mathrm{low})}(n,k)$ вначале падает, а затем незначительно возрастает. Аналогично изменяется оценка $\hat{\theta}_{\omega}^{(\mathrm{low})}(n,k)$ и с возрастанием k (табл. 2).

Таблица 2

k	$\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$	$\hat{\theta}_{\omega}^{(\mathrm{low})}(n,k)$	$\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$	$\hat{\theta}_{\omega}^{(\mathrm{up})}(n,k)$
2	$6{,}93\cdot10^{76}$	$6{,}86\cdot10^{76}$	$6{,}96\cdot10^{76}$	$6{,}96\cdot10^{76}$
8	$1{,}28\cdot10^{447}$	$1{,}25\cdot10^{447}$	$1{,}28\cdot10^{447}$	$1{,}28\cdot10^{447}$
14	$1{,}01\cdot10^{709}$	$0{,}94\cdot10^{709}$	$1{,}01\cdot10^{709}$	$1{,}01\cdot10^{709}$
20	$3{,}38\cdot10^{862}$	$2{,}86\cdot10^{862}$	$3{,}37\cdot10^{862}$	$3{,}36\cdot10^{862}$
26	$4{,}83\cdot10^{907}$	$3{,}53\cdot10^{907}$	$4{,}82\cdot10^{907}$	$4{,}81\cdot10^{907}$
32	$2{,}93\cdot10^{844}$	$1{,}74\cdot10^{844}$	$2{,}93\cdot10^{844}$	$2{,}92\cdot10^{844}$
38	$7{,}59\cdot10^{672}$	$3{,}23\cdot10^{672}$	$7{,}60\cdot10^{672}$	$7{,}61\cdot10^{672}$
44	$8{,}36\cdot10^{392}$	$1{,}90\cdot10^{392}$	$8{,}36\cdot10^{392}$	$8{,}33\cdot10^{392}$
46	$3{,}26\cdot10^{275}$	$0{,}50\cdot10^{275}$	$3{,}25\cdot10^{275}$	$3{,}28\cdot10^{275}$
47	$1{,}20\cdot10^{212}$	$0{,}17\cdot10^{212}$	$1{,}20\cdot10^{212}$	$1{,}84\cdot10^{212}$
48	$3{,}07\cdot10^{144}$	$1{,}18\cdot10^{144}$	$3{,}04\cdot10^{144}$	$20{,}35\cdot10^{144}$
49	$1{,}19\cdot10^{73}$	$1{,}19\cdot10^{73}$	$1{,}19\cdot10^{73}$	$1{,}19\cdot10^{73}$

Пример 2. Рассмотрим случай $k=10$. Если $\omega>2$, то не существует каких-либо аналитических или приближенных формул для вычисления $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$. О точности оценок можно судить только по косвенным данным. Так, согласно формуле (2) сумма по ω значений $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$ равняется $\begin{bmatrix} n \\ k \end{bmatrix}$, которое вычисляется в явном виде по формуле (1). Проверим, так ли это для рассматриваемых n и k. Действительно, $\begin{bmatrix} 50 \\ 10 \end{bmatrix} = 1{,}19\cdot10^{602}$. Результаты вычислений при различных ω представлены в табл. 3 ($n=50$, $k=10$, $q=2^5$, $\varepsilon=1{,}0\%$). Согласно этим данным $\sum_{\omega=1}^{41}\hat{\theta}_{\omega}^{(\mathrm{appr})}(50{,}10)\approx$ $\approx 1{,}22\cdot10^{602}$, т.е. результаты достаточно близки. Расчет для многочисленных значений наборов n, k и q в широком диапазоне их изменения ($5\le n\le100$, $3\le k\le n$, $2\le q\le2^{10}$) показал, что во всех ситуациях $\sum_{\omega=1}^{41}\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$ является верхней оценкой для $\begin{bmatrix} n \\ k \end{bmatrix}$, причем превышение составляет не более 15%. Проанализируем данные, представленные в табл. 3. Как и в табл. 1, при большинстве значений ω оценки $\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$ и $\hat{\theta}_{\omega}^{(\mathrm{up})}(n,k)$ практически идентичны; только при ω, близким к максимально допустимым, верхние оценки начинают резко терять точность. К сожалению, точность нижних оценок падает как с возрастанием ω, так и с возрастанием k. Тем не менее верхние и нижние оценки позволяют устанавливать диапазон изменения $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$ при $\omega>3$ и $k>2$, чего ранее не удавалось достичь. При этом есть основания полагать, что оценка $\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$ является достаточно точной аппроксимацией для $\begin{bmatrix} n \\ k \end{bmatrix}_{\omega}$.

Таблица 3

ω	$\hat{\theta}_{\omega}^{(\mathrm{low})}(n,k)$	$\hat{\theta}_{\omega}^{(\mathrm{appr})}(n,k)$	$\hat{\theta}_{\omega}^{(\mathrm{up})}(n,k)$
5	$1{,}07\cdot 10^{554}$	$1{,}46\cdot 10^{554}$	$1{,}46\cdot 10^{554}$
10	$7{,}02\cdot 10^{564}$	$2{,}02\cdot 10^{565}$	$2{,}02\cdot 10^{565}$
15	$1{,}53\cdot 10^{574}$	$1{,}29\cdot 10^{575}$	$1{,}29\cdot 10^{575}$
20	$2{,}32\cdot 10^{582}$	$7{,}52\cdot 10^{583}$	$7{,}56\cdot 10^{583}$
25	$3{,}07\cdot 10^{589}$	$5{,}79\cdot 10^{591}$	$5{,}78\cdot 10^{591}$
30	$3{,}14\cdot 10^{595}$	$6{,}19\cdot 10^{598}$	$6{,}16\cdot 10^{598}$
31	$3{,}55\cdot 10^{596}$	$1{,}23\cdot 10^{600}$	$1{,}24\cdot 10^{600}$
32	$3{,}45\cdot 10^{597}$	$2{,}14\cdot 10^{601}$	$2{,}27\cdot 10^{601}$
33	$2{,}19\cdot 10^{598}$	$9{,}92\cdot 10^{601}$	$2{,}45\cdot 10^{602}$
34	$3{,}79\cdot 10^{596}$	$3{,}11\cdot 10^{599}$	$5{,}07\cdot 10^{602}$
35	0	0	$7{,}02\cdot 10^{602}$

Автор благодарен доктору физ.-мат. наук, профессору В.И. Масолу за постановку задачи, а также О.А. Король за помощь при реализации алгоритмов на многопроцессорном комплексе СКИТ-3.

СПИСОК ЛИТЕРАТУРЫ

1. Масол В.И., Кузнецов И.Н. Применение ускоренного моделирования к оценке количества некоторых k-мерных подпространств над конечным полем // Кибернетика и системный анализ. — 2010. — № 3. — С. 69–83.
2. Эндрюс Г. Теория разбиений. — М.: Наука, 1982. — 256 с.
3. Calabi E., Wilf H. On the sequential and random selection of subspaces over a finite field // J. Combin. Theory. Ser. A. — 1977. — **22**, N 1. — P. 107–109.
4. Мак-Вальрас Ф. Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
5. Masol V.V. Investigation of linear codes possessing some extra properties // Cryptography and Coding. — 2001. — P. 301–306.
6. Масол В.И. Некоторые применения алгоритмов построения подпространств над конечным полем // Укр. мат. журн. — 1989. — **41**, № 8. — С. 1146–1148.
7. Масол В.И. Асимптотика числа некоторых k-мерных подпространств над конечным полем // Мат. заметки. — 1996. — **59**, вып. 5. — С. 729–736.
8. Коваленко И.Н. Исследования по анализу надежности сложных систем. — Киев: Наук. думка, 1975. — 210 с.
9. Коваленко И.Н. Анализ редких событий при оценке эффективности и надежности систем. — М.: Сов. радио, 1980. — 209 с.
10. Kovalenko I.N., Kuznetsov N.Yu., Pegg Ph. A. Mathematical theory of reliability of time dependent systems with practical applications. — Chichester: Wiley, 1997. — 303 p.

Поступила 16.03.2010