УДК 519.12

В.И. МАСОЛ, И.Н. КУЗНЕЦОВ

ПРИМЕНЕНИЕ УСКОРЕННОГО МОДЕЛИРОВАНИЯ К ОЦЕНКЕ КОЛИЧЕСТВА НЕКОТОРЫХ *k*-МЕРНЫХ ПОДПРОСТРАНСТВ НАД КОНЕЧНЫМ ПОЛЕМ

Ключевые слова: *векторное пространство, поле Галуа, вес пространства, метод взвешенного моделирования, несмещенная оценка, относительная среднеквадратическая погрешность.*

Рассмотрим n-мерное векторное пространство V_n над конечным полем GF(q), содержащим q элементов, где q — степень простого числа. Известно [1, с. 219], что общее число различных k-мерных подпространств $V_{k,n}$ пространства V_n равно

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

Весом вектора $v \in V_n$ называется число отличных от нуля компонент вектора v. 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 $\omega \in \{1, \ldots, n-k+1\}$, обозначим $\left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right]$. Очевидно, что

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{\omega=1}^{n-k+1} \left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right], \quad 1 \le k \le n.$$

Эффективность кодирования информации с помощью линейных (n,k)-кодов (именно так называют ещё подпространство $V_{k,n}$) принято характеризовать числом $\frac{k}{n}$ (см., например, [2, с. 12]). Повышение эффективности приводит к снижению веса ω, что не везде желательно для процесса кодирования информации, так как уменьшает его корректирующие возможности, сводя их к нулю при $\omega = 1$. Тем не менее подпространства $V_{k,n}$ небольшого веса ω, в частности $\omega = 1$, находят применение при кодировании (поскольку позволяют увеличивать эффективность) с последующей передачей высоконадежными каналами связи, о чем было сказано в [3]. В свою очередь, оценка числа подпространств $V_{k,n}$ заданного веса ω представляет интерес как для задач кодирования, так и для решения проблемы защиты информации от несанкционированного доступа.

Для вычисления $\left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right]$ при $\omega = 1$ и $\omega = 2$ в [4, 5] предложены рекуррентные формулы. В настоящей статье для оценки $\left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right]$ разработан принципиально новый подход, основанный на ускоренном моделировании малых вероятностей. В основе предлагаемого метода лежит идея И.Н. Коваленко [6–8] о разложении искомой характеристики по степеням некоторого параметра. В теории надежности такой подход многократно использовался для повышения точности вычислений. При этом неизвестная характеристика раскладывается в ряд по степеням малого параметра, причем коэффициенты этого ряда оцениваются методом Монте-Карло. Высокая эффективность вычислений достигается за счет быстрой сходимости ряда. В отличие от задач теории надежности в настоящей статье предлагается разложить $\left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right]$ по степеням большого параметра q (типичные значения $q = 2^8$, $q = 2^{16}$ или $q = 2^{32}$).

В статье предложен метод ускоренного моделирования, позволяющий 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 $\omega=3$. Доказана ограниченность относительной среднеквадратической погрешности оценок при $q\to\infty$. Высокая точность метода иллюстрируется численными примерами.

ОБЩАЯ СХЕМА УСКОРЕННОГО МОДЕЛИРОВАНИЯ

Переформулируем поставленную выше задачу эквивалентным образом. При этом ключевую роль играет алгоритм [9] построения множества базисных векторов k-мерного подпространства $V_{k,n}$ пространства V_n $(1\le k\le n)$. Этот алгоритм сводится к построению матрицы A:

$$A=\begin{array}{c}\begin{array}{ccccccccccccccc} & & & r_1 & & & & r_2 & & & & r_k & & & \\ & & & \downarrow & & & & \downarrow & & & & \downarrow & & & \end{array}\\ \begin{pmatrix} a_{11} & \dots & a_{1r_1-1} & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ a_{21} & \dots & a_{2r_1-1} & 0 & a_{2r_1+1} & \dots & a_{2r_2-1} & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{k1} & \dots & a_{kr_1-1} & 0 & a_{kr_1+1} & \dots & a_{kr_2-1} & 0 & a_{kr_2+1} & \dots & a_{kr_k-1} & 1 & 0 & \dots & 0 \end{pmatrix}\end{array}.$$

Пусть $\bar r=(r_1,\,\dots,r_k)$ — k-мерный вектор, компонентами которого являются упорядоченные натуральные числа, $U=\{\bar r\colon\ 1\le r_1<r_2<\ldots<r_k\le n\}$.

Алгоритм [9]

1. Выбираем произвольный вектор $\bar r\in U$.
2. В матрице A с k строками и n столбцами образуем единичную матрицу размерности $k\times k$, 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 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 $\bar r\in U$;

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

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

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

Учитывая, что $\left[\begin{matrix} n \\ k \end{matrix}\middle|\,\omega;\bar r\right]=0$ при $\bar r\notin\bigcup\limits_{L=(k-1)(\omega-1)}^{(k-1)(n-k)}U_\omega(L)$, имеем: для любого $\omega\in\{1,\,\dots,n-k+1\}$

$$\left[\begin{matrix} n \\ k \end{matrix}\middle|\,\omega\right]=\sum_{\bar r\in U}\left[\begin{matrix} n \\ k \end{matrix}\middle|\,\omega;\bar r\right]=\sum_{L=(k-1)(\omega-1)}^{(k-1)(n-k)}\ \sum_{\bar r\in U_\omega(L)}\left[\begin{matrix} n \\ k \end{matrix}\middle|\,\omega;\bar r\right]=$$

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

$$=Z_\omega\sum_{L=(k-1)(\omega-1)}^{(k-1)(n-k)}\frac{|U_\omega(L)|\,q^{L+\omega-1}}{Z_\omega}\ \sum_{\bar r\in U_\omega(L)}c_\omega(\bar r)\ \frac{1}{|U_\omega(L)|}=Z_\omega\ \mathbf{M}_\nu\ \mathbf{M}\{c_\omega(\bar\gamma)\,|\,\nu\},\quad(1)$$

где
$$Z_\omega = \sum_{L=(k-1)(\omega-1)}^{(k-1)(n-k)} |U_\omega(L)|\ q^{L+\omega-1},\ c_\omega(\bar r) = \frac{1}{q^{L+\omega-1}} \left[\begin{matrix} n \\ k \end{matrix} \middle| \omega; \bar r \right], \tag{2}$$

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

Для того чтобы воспользоваться соотношениями (1), (2), необходимо уметь вычислять $|U_\omega(L)|$ и $c_\omega(\bar r)$ при любых фиксированных L, $\bar r$ и ω. Основную проблему представляет вычисление $c_\omega(\bar r)$. В следующих разделах приведены явные аналитические формулы для $c_1(\bar r)$ и $c_2(\bar r)$, а также нижняя и верхняя оценки для $c_3(\bar r)$. Остановимся подробнее на нахождении $|U_\omega(L)|$.

Количество элементов во множестве $U_\omega(L)$ при фиксированных n, k и L обозначим $\alpha_\omega(n,k,L)$ ($|U_\omega(L)| = \alpha_\omega(n,k,L)$). Справедлива следующая рекуррентная формула: при $2 \le i \le k$, $i+\omega-1 \le m \le n$, $(i-1)(\omega-1) \le l \le (i-1)(m-i)$,
$$\alpha_\omega(m,i,l) = \sum_{j=i+\left]\frac{l}{i-1}\right[}^{\min\{m,\, l+i-(\omega-1)(i-2)\}} \alpha_\omega(j-1, i-1, l-(j-i)), \tag{3}$$
где $\left]\frac{l}{i-1}\right[= \min\left\{ j : j \ge \frac{l}{i-1} \right\}$. Соотношение (3) дополняется граничными условиями:

- $\alpha_\omega(m,1,0) = m-\omega+1$ для любого $m \ge \omega$;
- $\alpha_\omega(\mu, \iota, (\omega-1)(\iota-1)) = 1$ для любых $m \ge \omega+1$, $2 \le i \le m-\omega+1$.

Формула (3) вытекает из следующих соображений. Определим значения, какие может принимать r_i, если известно, что $r_1 \ge \omega$ и
$$(r_2-2)+(r_3-3)+\dots+(r_i-i) = l. \tag{4}$$
Поскольку $r_s - s \ge \omega-1$ для любого $s = 2, \dots, i-1$, то из (4) следует, что $(\omega-1)(i-2)+r_i-i \le l$, т.е. $r_i \le l+i-(\omega-1)(i-2)$. В то же время $r_i \le m$, поэтому $r_i \le \min\{m, l+i-(\omega-1)(i-2)\}$. Из (4) следует, что
$$r_i = l-(r_{i-1}+r_{i-2}+\dots+r_2)+\frac{(i-1)(i+2)}{2} \ge l-[(r_i-1)+(r_i-2)+\dots$$
$$\dots+(r_i-i+2)]+\frac{(i-1)(i+2)}{2} = l-(i-2)r_i+i(i-1),$$
поэтому $r_i \ge i+\left]\frac{l}{i-1}\right[$. Если $r_i = j$, то $\omega \le r_1 < r_2 < \dots < r_{i-1} \le j-1$; при этом значение l уменьшается на $j-i$ (именно столько позиций было расположено в i-й строчке для заполнения элементами поля — см. алгоритм).

Предположим, что найдены явные аналитические формулы для вычисления коэффициента $c_\omega(\bar r)$ при любом ω и любых значениях параметров $L, \bar r$. Формулы (1), (2) позволяют предложить простой алгоритм построения несмещенных оценок для $\left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right]$.

1. С помощью описанного выше рекуррентного алгоритма (см. (3)) вычисляем $|U_\omega(L)| = \alpha_\omega(n,k,L)$ для всех $L = (k-1)(\omega-1), \dots, (k-1)(n-k)$.
2. Согласно (2) вычисляем Z_ω.
3. Строим реализацию случайной величины ν, которая равна $L \in \{(k-1)(\omega-1), \dots$ $\dots, (k-1)(n-k)\}$ с вероятностью $\frac{|U_\omega(L)|\, q^{L+\omega-1}}{Z_\omega}$.
4. Строим реализацию случайного вектора $\bar\gamma$, имеющего равномерное распределение на множестве $U_\omega(\nu)$ (при этом существенным образом используется соотношение (3), позволяющее рекуррентно моделировать компоненты вектора $\bar\gamma$).
5. Вычисляем $c_\omega(\bar r)$.

6. В качестве оценки для $\left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right]$, построенной в одной реализации алгоритма, выбираем $\hat{\beta}_\omega(\bar{\gamma}) = Z_\omega \; c_\omega(\bar{\gamma})$.

Замечание. При фиксированном ω вычисление Z_ω (первые два шага алгоритма) проводится всего один раз.

Теорема 1. Оценка $\hat{\beta}_\omega(\bar{\gamma})$ является несмещенной, т.е. $\mathbf{M}\hat{\beta}_\omega(\bar{\gamma}) = \left[\begin{matrix} n \\ k \end{matrix} \middle| \omega \right]$.

Утверждение теоремы следует непосредственно из соотношений (1) и (2).

В следующих двух разделах приведены формулы, позволяющие вычислять $c_\omega(\bar{r})$ в явном виде при $\omega = 1$, $\omega = 2$, а также строить верхние и нижние оценки для $c_\omega(\bar{r})$ при $\omega = 3$.

НАХОЖДЕНИЕ $c_\omega(\bar{r})$ ПРИ $\omega = 1$ И $\omega = 2$

Пусть $\bar{r} = (r_1, \ldots, r_k)$ — вектор, определяющий номера столбцов, образующих единичную матрицу в матрице A (см. алгоритм построения множества базисных векторов k-мерного подпространства $V_{k,n}$). Количество позиций в i-й строчке $(i = 1, \ldots, k)$, доступных для заполнения элементами поля, равно $r_i - i$. 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 размерности $k \times (r_k - k)$. Если $N(\bar{r})$ — общее количество вариантов размещения элементов поля, то

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

Введем некоторые обозначения, облегчающие дальнейшее изложение:

- Γ — множество элементов поля Галуа (q элементов);
- $\{\xi_j^{(i)},\ j = 1, \ldots, r_i - i,\ i = 1, \ldots, k\}$ — независимые в совокупности одинаково распределенные случайные величины, принимающие значения из Γ с одной и той же вероятностью $\frac{1}{q}$;
- $\bar{\xi}^{(i)} = (\xi_1^{(i)}, \xi_2^{(i)}, \ldots, \xi_{r_i - i}^{(i)}, \underbrace{0, \ldots, 0}_{r_k - r_i + i - k})$, $i = 1, \ldots, k$, — векторы размерности $\rho_\kappa - \kappa$;
- $\mu(\bar{x})$ — количество ненулевых компонент вектора $\bar{x}$ размерности $r_k - k$;
- $z_i = q^{r_i - i} - 1 - (r_i - i)(q - 1)$, $v_i = q^{r_i - i} - 1 - (r_i - 1)(q - 1)$, $i = 1, \ldots, k$. (6)

Воспользуемся соотношением

$$\left[\begin{matrix} n \\ k \end{matrix} \middle| \omega; \bar{r} \right] = N(\bar{r})\, \mathbf{P}\{Y_\omega(\bar{r})\}, \tag{7}$$

где $Y_\omega(\bar{r})$ — событие, состоящее в том, что строчки матрицы A с выбранными случайным образом элементами $\{a_{ij}\}$ (при фиксированном $\bar{r}$) являются базисными векторами k-мерного подпространства веса ω. Из формул (2), (5) и (7) следует, что

$$c_\omega(\bar{r}) = \frac{1}{q^{L+\omega-1}} \left[\begin{matrix} n \\ k \end{matrix} \middle| \omega; \bar{r} \right] = \frac{N(\bar{r})}{q^{L+\omega-1}}\, \mathbf{P}\{Y_\omega(\bar{r})\} = q^{r_1 - \omega}\, \mathbf{P}\{Y_\omega(\bar{r})\}. \tag{8}$$

Справедливо следующее утверждение.

Теорема 2. При $\omega = 1$ имеет место равенство

$$c_1(\bar{r}) = 1 + \sum_{i=2}^{k} \frac{1}{q^{r_i - r_1 - i + 1}} \prod_{j=1}^{i-1} \left[1 - \frac{1}{q^{r_j - j}}\right]. \tag{9}$$

Пусть $\omega = 2$. Если $r_1 = 2$, то

$$c_2(\bar{r}) = \left(1 - \frac{1}{q}\right) \prod_{i=2}^{k} \left(1 - \frac{1}{q^{r_i - i}}\right). \tag{10}$$

Пусть $r_1 \ge 3$. Если $\upsilon_m \le 0$ (см. (6)) для некоторого $m \in \{2, \dots, k\}$, то

$$c_2(\bar{r}) = q^{r_1 - 2} \prod_{i=1}^{k} \left(1 - \frac{1}{q^{r_i - i}}\right). \tag{11}$$

Если же $\upsilon_m > 0$ для всех $m \in \{2, \dots, k\}$, то

$$c_2(\bar{r}) = \frac{(r_1 - 1)(q-1)}{q} + \sum_{i=2}^{k} \left\{ \frac{1 + (r_i - 1)(q-1)}{q^{r_i - i - r_1 + 2}} \prod_{j=1}^{i-1} \left[1 - \frac{1 + (r_j - 1)(q-1)}{q^{r_j - j}} \right] - \right.$$

$$\left. - \frac{1}{q^{r_i - i - r_1 + 2}} \prod_{j=1}^{i-1} \left(1 - \frac{1}{q^{r_j - j}}\right) \right\}. \tag{12}$$

Доказательство. Для того чтобы k-мерное подпространство имело вес $\omega = 1$, необходимо и достаточно, чтобы хотя бы в одной строчке на всех допустимых позициях были расположены нули. Иначе говоря,

$$\mathbf{P}\{Y_\omega(\bar{r})\} = \mathbf{P}\left\{ \bigcup_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) = 0\} \right\} = 1 - \prod_{i=1}^{k} \left[1 - \frac{1}{q^{r_i - i}} \right] = \sum_{i=1}^{k} \frac{1}{q^{r_i - i}} \prod_{j=1}^{i-1} \left[1 - \frac{1}{q^{r_j - j}} \right].$$

В последнем равенстве использовалось соотношение

$$1 - \prod_{i=1}^{k} (1 - g_i) = \sum_{i=1}^{k} g_i \prod_{j=1}^{i-1} (1 - g_j), \tag{13}$$

где $0 \le g_i \le 1$, $1 \le i \le k$. Учитывая соотношение (8) при $\omega = 1$, получаем равенство (9).

Выведем аналогичные формулы для $c_2(\bar{r})$ при фиксированных L и $\bar{r}$. Для того чтобы k-мерное подпространство имело вес $\omega = 2$, необходимо и достаточно, чтобы произошло одно из двух несовместных событий:

- $B = \{\mu(\bar{\xi}^{(i)}) = 1$ для некоторого $i \in \{1, \dots, k\}$ и $\mu(\bar{\xi}^{(j)}) \ge 1$, $j \ne i\}$;
- $C = \{\mu(\bar{\xi}^{(i)}) \ge 2$ для всех $i \in \{1, \dots, k\}$, и существуют $j, l \in \{1, \dots, k\}$, $j < l$, такие, что $\alpha \bar{\xi}^{(j)} + \bar{\xi}^{(l)} = \bar{0}$ для некоторого $\alpha \in \Gamma, \alpha \ne 0\}$.

Тогда $Y_\omega(\bar{r}) = B \cup C$. При этом

$$\mathbf{P}\{B\} = \mathbf{P}\left\{ \bigcup_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) = 1\} \cap \bigcap_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) \ge 1\} \right\} = \mathbf{P}\left\{ \bigcap_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) \ge 1\} \right\} -$$

$$- \mathbf{P}\left\{ \bigcap_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) \ge 2\} \right\} = \prod_{i=1}^{k} \left[1 - \frac{1}{q^{r_i - i}} \right] - \prod_{i=1}^{k} \left[1 - \frac{1 + (r_i - i)(q-1)}{q^{r_i - i}} \right]. \tag{14}$$

Обозначим:

$C^{(j,l)} = \{\alpha \bar{\xi}^{(j)} + \bar{\xi}^{(l)} = \bar{0}$ для некоторого $\alpha \in \Gamma, \alpha \ne 0\}$, $1 \le j < l \le k$;

$C_i = \bigcap\limits_{1 \le j < l \le i} \bar{C}^{(j,l)}$, $i = 2, \dots, k$, $C_k \subset C_{k-1} \subset \dots \subset C_2$, $\bar{C}_k = \bigcup\limits_{1 \le j < l \le k} C^{(j,l)}$.

Если $r_1 = 2$, то $\mathbf{P}\{C\} = 0$ и

$$c_2(\bar{r}) = \mathbf{P}\{B\} = \left(1 - \frac{1}{q}\right) \prod_{i=2}^{k} \left(1 - \frac{1}{q^{r_i - i}}\right).$$

Предположим, что $r_1 \ge 3$. Тогда

$$\mathbf{P}\{C\} = \mathbf{P}\left\{ \bigcap_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) \ge 2\} \cap \bigcup_{1 \le j < l \le k} C^{(j,l)} \right\} =$$

$$= \mathbf{P}\left\{ \bigcap_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) \ge 2\} \right\} \left[1 - \mathbf{P}\left\{ C_k \,\middle|\, \bigcap_{i=1}^{k} \{\mu(\bar{\xi}^{(i)}) \ge 2\} \right\} \right] =$$

$$=\prod_{i=1}^{k}\frac{z_i}{q^{r_i-i}}\left[1-\prod_{m=2}^{k}\mathbf{P}\left\{C_m \;\middle|\; C_{m-1}\cap\bigcap_{i=1}^{k}\{\mu(\bar{\xi}^{(i)})\geq 2\}\right\}\right], \tag{15}$$

где C_1 — достоверное событие. Поскольку $C_m = C_{m-1}\cap\bigcap_{j=1}^{m-1}\overline{C}^{(j,m)}$, $m=2,\ldots,k$, то с учетом обозначений (6) получим соотношение

$$\mathbf{P}\left\{C_m \;\middle|\; C_{m-1}\cap\bigcap_{i=1}^{k}\{\mu(\bar{\xi}^{(i)})\geq 2\}\right\}=\mathbf{P}\,\{\bigcap_{j=1}^{m-1}\overline{C}^{(j,m)}\;|C_{m-1}\cap\{\mu(\bar{\xi}^{(m)})\geq 2\}\}=$$

$$=1-\mathbf{P}\left\{\bigcup_{j=1}^{m-1}C^{(j,m)}\;\middle|\;C_{m-1}\cap\{\mu(\bar{\xi}^{(m)})\geq 2\}\right\}=1-\frac{(m-1)(q-1)}{z_m}=\frac{v_m}{z_m} \tag{16}$$

(общее число вариантов размещения элементов в m-й строчке, благоприятствующих условию $\{\mu(\bar{\xi}^{(m)})\geq 2\}$, равно $z_m = q^{r_m-m}-1-(r_m-m)(q-1)$; из них лишь $(m-1)(q-1)$ вариантов благоприятствуют событию $\bigcup_{j=1}^{m-1}C^{(j,m)}$). Поэтому из (15) и (16) следует равенство

$$\mathbf{P}\{C\}=\prod_{i=1}^{k}\frac{z_i}{q^{r_i-i}}\left[1-\prod_{m=2}^{k}\frac{v_m}{z_m}\right]. \tag{17}$$

Если $v_m = q^{r_m-m}-1-(r_m-1)(q-1)\leq 0$ для некоторого $m\in\{2,\ldots,k\}$, то $\mathbf{P}\{C\}=\prod_{i=1}^{k}\frac{z_i}{q^{r_i-i}}$. В этом случае

$$c_2(L,\bar{r})=q^{r_1-2}\,[\mathbf{P}\{B\}+\mathbf{P}\{C\}]=q^{r_1-2}\prod_{i=1}^{k}\left(1-\frac{1}{q^{r_i-i}}\right).$$

Предположим теперь, что $v_m>0$ для всех $m\in\{2,\ldots,k\}$. Тогда из (14) и (17) следует, что

$$c_2(L,\bar{r})\;=\;q^{r_1-2}\,[\mathbf{P}\{B\}+\mathbf{P}\{C\}]=q^{r_1-2}\left\{\prod_{i=1}^{k}\left[1-\frac{1}{q^{r_i-i}}\right]-\prod_{i=1}^{k}\frac{v_i}{q^{r_i-i}}\right\}$$

(при этом учитывается, что $z_1=v_1$). Обозначив $\varepsilon_i = 1-\frac{v_i}{q^{r_i-i}}$, $i=1,\ldots,k$, из (13) имеем

$$c_2(L,\bar{r})\;=q^{r_1-2}\left\{1-\sum_{i=1}^{k}\frac{1}{q^{r_i-i}}\prod_{j=1}^{i-1}\left(1-\frac{1}{q^{r_j-j}}\right)-1+\sum_{i=1}^{k}\varepsilon_i\prod_{j=1}^{i-1}(1-\varepsilon_j\;)\right\}=$$

$$=\frac{(r_1-1)(q-1)}{q}+\sum_{i=2}^{k}\left\{\frac{1+(r_i-1)(q-1)}{q^{r_i-i-r_1+2}}\prod_{j=1}^{i-1}\left[1-\frac{1+(r_j-1)(q-1)}{q^{r_j-j}}\right]-\right.$$

$$\left.-\frac{1}{q^{r_i-i-r_1+2}}\prod_{j=1}^{i-1}\left(1-\frac{1}{q^{r_j-j}}\right)\right\}.$$

Теорема 2 доказана.

ВЕРХНЯЯ И НИЖНЯЯ ОЦЕНКИ ДЛЯ $c_3(\bar{r})$

Для того чтобы k-мерное подпространство имело вес $\omega=3$, необходимо и достаточно, чтобы произошло событие

$$Y_\omega(\bar{r})=D\cap E\cap(F\cup G\cup H),$$

где:

$D=\{\mu(\bar{\xi}^{(i)})\ge 2,\ i=1,\ \dots,k\}$,
$E=\bigcap\limits_{1\le i<j\le k}E^{(i,j)},\ E^{(i,j)}=\{\alpha\,\bar{\xi}^{(i)}+\bar{\xi}^{(j)}\ne\bar{0}$ для всех $\alpha\in\Gamma,\ \alpha\ne 0\}$,
$F=\bigcup\limits_{1\le i\le k}F^{(i)},\ F^{(i)}=\{\mu(\bar{\xi}^{(i)})=2\},\ \ i=1,\ \dots,k;$
$G=\bigcup\limits_{1\le i<j\le k}G^{(i,j)},\ G^{(i,j)}=\{\alpha\,\bar{\xi}^{(i)}+\bar{\xi}^{(j)}=\bar{1}$ для некоторого $\alpha\in\Gamma,\ \alpha\ne 0\}$,
$H=\bigcup\limits_{1\le i<j<l\le k}H^{(i,j,l)}$,
$H^{(i,j,l)}=\{\alpha\,\bar{\xi}^{(i)}+\beta\,\bar{\xi}^{(j)}+\bar{\xi}^{(l)}=\bar{0}$ для некоторых $\alpha,\beta\in\Gamma,\ \alpha\ne 0,\ \beta\ne 0\}$.

Символическая запись $\alpha\,\bar{\xi}^{(i)}+\bar{\xi}^{(j)}=\bar{1}$ означает, что линейная комбинация указанных векторов равна вектору размерности r_k-k, у которого лишь одна из компонент отлична от нуля. Имеет место равенство

$$Q_\omega(\bar{r})=\mathbf{P}\{Y_\omega(\bar{r})\}=\mathbf{P}\{D\,E\,F\}+\mathbf{P}\{D\,E\,\bar{F}\,G\}+\mathbf{P}\{D\,E\,\bar{F}\,\bar{G}\,H\}. \tag{18}$$

Справедливо следующее утверждение.

Теорема 3. Если $v_m=q^{r_m-m}-1-(r_m-1)(q-1)\le 0$ для некоторого $m\in\{2,\ \dots,k\}$, то $c_3(\bar{r})=0$.

Пусть $v_m>0,\ m=2,\ \dots,k$. Если $r_1=3$, то

$$c_3(\bar{r})=\left(1-\frac{1}{q}\right)^2\prod_{i=2}^{k}\left[1-\frac{1+(r_i-1)(q-1)}{q^{r_i-i}}\right]. \tag{19}$$

Если же $r_1>3$, то справедливы оценки:

$$\left(1-\frac{1}{q}\right)^2[h(\bar{r})-g(\bar{r})]=\gamma^{(\mathrm{low})}(\bar{r})\le c_3(\bar{r})\le\gamma^{(\mathrm{up})}(\bar{r})=\left(1-\frac{1}{q}\right)^2 h(\bar{r}), \tag{20}$$

где:

$$h(\bar{r})=\sum_{m=1}^{k}\frac{w_1}{w_m}C^2_{r_m-m}\prod_{j=2}^{m}\frac{w_j}{q^{r_j-j}}\prod_{j=m+1}^{k}\frac{v_j}{q^{r_j-j}}+$$
$$+\prod_{j=2}^{k}\frac{w_j}{q^{r_j-j}}\sum_{m=2}^{k}\frac{w_1}{w_m}[(r_m-m)(m-1)+C^2_{m-1}], \tag{21}$$

$$g(\bar{r})=\left[\sum_{m=2}^{k}\frac{w_1}{w_m}(m-1)(m+2)\frac{1}{q-1}+C^2_{m-1}\min\left(1,\frac{m+1}{q-1}\right)\right]+$$
$$+w_1(q-1)^2\left[\sum_{i=2}^{k}\sum_{\substack{3\le j\le k,\\ j\ne i}}\frac{r_i-i}{w_i\,w_j}(i-1)C^2_{j-1}+\sum_{2\le i<j\le k}\frac{f_{ij}(\bar{r})}{w_i\,w_j}\right], \tag{22}$$

$$w_j=q^{r_j-j}-1-(r_j-1)(q-1)-C^2_{r_j-j}(q-1)^2, \tag{23}$$

$$f_{ij}(\bar{r})=j(i-1)(r_i-i)(r_j-j)+i(i-1)(r_j-j)+(r_i-i)C^2_{i-1}+$$
$$+C^2_{i-1}C^2_{j-1}+(i-1)C^2_{i-1}+(i-1)(j-i-1). \tag{24}$$

Доказательство. Если $v_m=q^{r_m-m}-1-(r_m-1)(q-1)\le 0$ для некоторого $m\in\{2,\ \dots,k\}$, то существуют $i,j\in\{1,\ \dots,k\},\ i<j$, такие, что $\alpha\,\bar{\xi}^{(i)}+\bar{\xi}^{(j)}=\bar{0}$ для некоторого $\alpha\in\Gamma,\ \alpha\ne 0$ (см. доказательство теоремы 2), т.е. $\mathbf{P}\{E\}=0$ и $Q_\omega(\bar{r})=0$. Следовательно, $c_3(\bar{r})=0$.

Предположим, что $v_m>0,\ m=2,\ \dots,k$. Оценим в отдельности каждое из слагаемых, стоящих в правой части соотношения (18). Обозначим:

$$\psi_i(j) = \mathbf{P}\{\mu(\bar{\xi}^{(i)}) = j\} = \frac{1}{q^{r_i - i}} C_{r_i - i}^{j} (q-1)^j, \ 0 \le j \le r_i - i, \quad i = 1, \ldots, k, \tag{25}$$

$$\varphi_i(j) = \mathbf{P}\{\mu(\bar{\xi}^{(i)}) > j\} = 1 - \sum_{l=0}^{j} \psi_i(l), \ 0 \le j \le r_i - i, \quad i = 1, \ldots, k. \tag{26}$$

Вычисление вероятности $\mathbf{P}\{D\,E\,F\}$. Обозначим:

$U_m = \{\mu(\bar{\xi}^{(i)}) > 2, \ i = 1, \ldots, m-1, \ \mu(\bar{\xi}^{(m)}) = 2, \ \mu(\bar{\xi}^{(i)}) \ge 2, \ i = m+1, \ldots, k\}$, $m = 1, \ldots, k$;

$$E_l = \bigcap_{1 \le i < j \le l} E^{(i,j)}, \ l = 2, 3, \ldots, k.$$

Очевидно, что

$$E_2 \supset E_3 \supset \ldots \supset E_k = E. \tag{27}$$

Поскольку $D\,F = \bigcup_{m=1}^{k} U_m$ и $U_m \cap U_l = \varnothing$ при $m \ne l$, то

$$\mathbf{P}\{D\,E\,F\} = \sum_{m=1}^{k} \mathbf{P}\{E\,U_m\} = \sum_{m=1}^{k} \mathbf{P}\{U_m\}\,\mathbf{P}\{E \mid U_m\}, \tag{28}$$

где

$$\mathbf{P}\{U_m\} = \psi_m(2) \prod_{j=1}^{m-1} \varphi_j(2) \prod_{j=m+1}^{k} \varphi_j(1). \tag{29}$$

Учитывая (27), имеем

$$\mathbf{P}\{E \mid U_m\} = \mathbf{P}\{E_k \big| U_m\} = \prod_{j=2}^{k} \mathbf{P}\{E_j \mid E_{j-1}\,U_m\}, \tag{30}$$

где E_1 рассматриваем как достоверное событие. Событие U_m означает, что $\mu(\bar{\xi}^{(m)}) = 2$ и $\mu(\bar{\xi}^{(l)}) > 2$ при $l < m$, поэтому

$$\mathbf{P}\{E_m \mid E_{m-1}\,U_m\} = 1. \tag{31}$$

Пусть $j < m$. Тогда

$$\mathbf{P}\{E_j \mid E_{j-1}\,U_m\} = 1 - \frac{(j-1)(q-1)}{q^{r_j - j} - 1 - (r_j - j)(q-1) - C_{r_j - j}^{2}(q-1)^2} = \frac{w_j}{q^{r_j - j}\,\varphi_j(2)}, \tag{32}$$

где w_j и $\varphi_j(2)$ определяются согласно (23) и (26). Если же $j > m$, то

$$\mathbf{P}\{E_j \mid E_{j-1}\,U_m\} = 1 - \frac{(j-1)(q-1)}{q^{r_j - j} - 1 - (r_j - j)(q-1)} = \frac{\upsilon_j}{q^{r_j - j}\,\varphi_j(1)}. \tag{33}$$

Если $r_1 = 3$, то $\mathbf{P}\{U_m\} = 0$, $m = 2, \ldots, k$, а также $D\,\bar{F} = \varnothing$, поэтому

$$c_3(\bar{r}) = \mathbf{P}\{Y_\omega(\bar{r})\} = \mathbf{P}\{U_1\}\,\mathbf{P}\{E \mid U_1\}.$$

Воспользовавшись соотношениями (29), (30) и (33) при $m = 1$, получим (19).

Предположим, что $r_1 \ge 4$. Из формул (5), (28)–(33) находим вероятность

$$\mathbf{P}\{D\,E\,F\} = \sum_{m=1}^{k} \psi_m(2) \prod_{j=1}^{m-1} \varphi_j(2) \prod_{j=m+1}^{k} \varphi_j(1) \prod_{j=1}^{m-1} \frac{w_j}{q^{r_j - j}\,\varphi_j(2)} \prod_{j=m+1}^{k} \frac{\upsilon_j}{q^{r_j - j}\,\varphi_j(1)} =$$

$$= \frac{(q-1)^2}{N(\bar{r})} \sum_{m=1}^{k} C_{r_m - m}^{2} \prod_{j=1}^{m-1} w_j \prod_{j=m+1}^{k} \upsilon_j \tag{34}$$

(если $w_j < 0$ для некоторых j, то в формуле (34) их следует заменить нулями).

Верхние и нижние оценки вероятности $\mathbf{P}\{D\,E\,\overline{F}\,G\}$. Очевидно, что

$$\sum_{1\le i<j\le k}\mathbf{P}\{D\,E\,\overline{F}\,G^{(i,j)}\}-\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2\le k,\\ j_1<j_2}}\mathbf{P}\{D\,E\,\overline{F}\,G^{(i_1,j_1)}\,G^{(i_2,j_2)}\}-$$

$$-\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2\le k,\\ j_1=j_2,\ i_1<i_2}}\mathbf{P}\{D\,E\,\overline{F}\,G^{(i_1,j_1)}\,G^{(i_2,j_2)}\}\le\mathbf{P}\{D\,E\,\overline{F}\,G\}\le\sum_{1\le i<j\le k}\mathbf{P}\{D\,E\,\overline{F}\,G^{(i,j)}\}. \qquad (35)$$

Построим верхние и нижние оценки для $\mathbf{P}\{D\,E\,\overline{F}\,G^{(i,j)}\}$. Обозначим $S_m=\{\mu(\overline{\xi}^{(l)})\ge 3,\ l=1,\ \ldots,m\},\ m=1,\ \ldots,k$. Поскольку $D\,\overline{F}=S_k$, то

$$\mathbf{P}\{D\,E\,\overline{F}\,G^{(i,j)}\}=\mathbf{P}\{E\,S_k\,G^{(i,j)}\}=\mathbf{P}\{S_1\}\prod_{m=2}^{j-1}\mathbf{P}\{E_m\,S_m\mid E_{m-1}\,S_{m-1}\}\times$$

$$\times\,\mathbf{P}\{E_j\,S_j\,G^{(i,j)}\mid E_{j-1}\,S_{j-1}\}\prod_{m=j+1}^{k}\mathbf{P}\{E_m\,S_m\mid E_{m-1}\,S_{m-1}\,G^{(i,j)}\}. \qquad (36)$$

Очевидно, что

$$\mathbf{P}\{E_m\,S_m\mid E_{m-1}\,S_{m-1}\}=\mathbf{P}\{\mu(\overline{\xi}^{(m)})\ge 3\}-\mathbf{P}\left\{\bigcup_{i=1}^{m-1}\overline{E}^{(i,j)}\,\middle|\,E_{m-1}\,S_{m-1}\right\}=$$

$$=\varphi_m(2)-\frac{(m-1)(q-1)}{q^{r_m-m}}=\frac{w_m}{q^{r_m-m}},\ m=1,\ \ldots,j-1 \qquad (37)$$

(как и ранее, w_m заменяем нулем, если $w_m<0$). Аналогично

$$\mathbf{P}\{E_m\,S_m\mid E_{m-1}\,S_{m-1}\,G^{(i,j)}\}=\frac{w_m}{q^{r_m-m}},\ m=j+1,\ \ldots,k. \qquad (38)$$

Рассмотрим подробнее вероятность $\mathbf{P}\{E_j\,S_j\,G^{(i,j)}\mid E_{j-1}\,S_{j-1}\}$. Имеем

$$\mathbf{P}\{E_j\,S_j\,G^{(i,j)}\mid E_{j-1}\,S_{j-1}\}=$$

$$=\mathbf{P}\{S_j\,G^{(i,j)}\mid E_{j-1}\,S_{j-1}\}-\mathbf{P}\{\overline{E}_j\,S_j\,G^{(i,j)}\mid E_{j-1}\,S_{j-1}\}. \qquad (39)$$

Предположим, что символы $\overline{\xi}^{(i)}=(\xi_1^{(i)},\ \ldots,\xi_{r_i-i}^{(i)},0,\ \ldots,0)$ i-й строчки фиксированы. Подсчитаем количество вариантов расположения символов в j-й строчке, благоприятствующих событию $\{\mu(\overline{\xi}^{(j)})\ge 3\}\cap G^{(i,j)}$. Возможны три случая.

Случай 1. $\mu(\overline{\xi}^{(j)})=\mu(\overline{\xi}^{(i)})=s\ge 3$. Число комбинаций, благоприятствующих событию $G^{(i,j)}$, равно $s(q-1)(q-2)$. Действительно, в j-й строчке ненулевые символы можно размещать лишь на тех же позициях, что и в i-й строчке. Выберем одну из этих позиций (s способов). Тогда $\overline{\xi}^{(i)}=\overline{a}^{(i)}+\overline{b}^{(i)}$, где вектор $\overline{a}^{(i)}$ получается из $\overline{\xi}^{(i)}$ обнулением всех позиций, за исключением выделенной; аналогично $\overline{b}^{(i)}$ получается из $\overline{\xi}^{(i)}$ обнулением лишь выделенной позиции. Событие $G^{(i,j)}$ произойдет тогда и только тогда, когда вектор $\overline{\xi}^{(j)}$ имеет вид $\overline{\xi}^{(j)}=\alpha\,\overline{a}^{(i)}+\beta\,\overline{b}^{(i)}$, $\alpha,\beta\in\Gamma,\alpha\ne\beta,\alpha\ne 0,\beta\ne 0$ ($(q-1)(q-2)$ комбинаций).

Случай 2. $\mu(\overline{\xi}^{(j)})-1=\mu(\overline{\xi}^{(i)})=s\ge 3$. Рассуждения, аналогичные приведенным выше, позволяют сделать вывод, что число комбинаций, благоприятствующих событию $G^{(i,j)}$, равно $(r_j-j-s)(q-1)^2$.

Случай 3. $\mu(\overline{\xi}^{(j)})+1=\mu(\overline{\xi}^{(i)})=s\ge 4$. Число соответствующих комбинаций равно $s(q-1)$. Заметим, что данный случай возникает лишь при $s\ge 4$.

Таким образом, общее число комбинаций не превосходит $(r_j-j)(q-1)^2$. Следовательно,

$$\mathbf{P}\{S_j\,G^{(i,j)}\mid E_{j-1}\,S_{j-1}\}\le\frac{(r_j-j)(q-1)^2}{q^{r_j-j}}. \qquad (40)$$

Если же отбросить комбинации, соответствующие случаю 3 при $s=3$, то получим оценку снизу

$$\mathbf{P}\{S_j\, G^{(i,j)}\ \ |E_{j-1}\, S_{j-1}\} \ge \frac{(r_j - j)(q-1)^2 - 3(q-1)}{q^{r_j - j}}. \qquad (41)$$

В то же время

$$\mathbf{P}\{\overline{E}_j\, S_j\ \ G^{(i,j)}\ |E_{j-1}\ S_{j-1}\} \le \sum_{l=1}^{j-1} \mathbf{P}\{\overline{E}^{(l,j)}\ |E_{j-1}\ S_{j-1}\} = \frac{(j-1)(q-1)}{q^{r_j - j}}. \qquad (42)$$

Объединяя формулы (36)–(42), получаем оценку

$$\frac{(q-1)^2}{N(\bar r)} \prod_{m=1}^{k} w_m\ \frac{1}{w_j}\left(r_j - j - \frac{j+2}{q-1}\right) \le \mathbf{P}\{D\,E\,\overline{F}\ G^{(i,j)}\} \le \frac{(q-1)^2}{N(\bar r)} \prod_{m=1}^{k} w_m\ \frac{r_j - j}{w_j}. \qquad (43)$$

Просуммировав по i и j $(1 \le i < j \le k)$, будем иметь

$$\frac{(q-1)^2}{N(\bar r)} \prod_{m=1}^{k} w_m\ \sum_{j=2}^{k} \frac{j-1}{w_j}\left(r_j - j - \frac{j+2}{q-1}\right) \le \sum_{1\le i<j\le k} \mathbf{P}\{D\,E\,\overline{F}\ G^{(i,j)}\} \le$$

$$\le \frac{(q-1)^2}{N(\bar r)} \prod_{m=1}^{k} w_m\ \sum_{j=2}^{k} \frac{j-1}{w_j}(r_j - j). \qquad (44)$$

Для подсчета числа комбинаций, благоприятствующих событиям $G^{(i_1,j_1)}$ и $G^{(i_2,j_2)}$, воспользуемся описанным выше подходом. В результате получим верхние оценки:

$$\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2\le k,\\ j_1<j_2}} \mathbf{P}\{D\,E\,\overline{F}\ G^{(i_1,j_1)}\ G^{(i_2,j_2)}\} \le \sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2\le k,\\ j_1<j_2}} (q-1)^4\ \frac{r_{j_1} - j_1}{w_{j_1}}\ \frac{r_{j_2} - j_2}{w_{j_2}} \prod_{m=1}^{k} \frac{w_m}{q^{r_m - m}} =$$

$$= \frac{(q-1)^4}{N(\bar r)} \prod_{m=1}^{k} w_m \sum_{2\le i<j\le k} (i-1)(j-1)\frac{r_i - i}{w_i}\ \frac{r_j - j}{w_j}; \qquad (45)$$

$$\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2\le k,\\ j_1=j_2,\ i_1<i_2}} \mathbf{P}\{D\,E\,\overline{F}\ G^{(i_1,j_1)}\ G^{(i_2,j_2)}\} \le \sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2\le k,\\ j_1=j_2,\ i_1<i_2}} (q-1)^4\ \frac{r_{i_2} - i_2}{w_{i_2}}\ \frac{r_{j_2} - j_2}{w_{j_2}} \prod_{m=1}^{k} \frac{w_m}{q^{r_m - m}} =$$

$$= \frac{(q-1)^4}{N(\bar r)} \prod_{m=1}^{k} w_m \sum_{2\le i<j\le k} (i-1)\frac{r_i - i}{w_i}\ \frac{r_j - j}{w_j}. \qquad (46)$$

Верхние и нижние оценки вероятности $\mathbf{P}\{D\,E\,\overline{F}\,\overline{G}\,H\}$. Очевидно, что

$$\mathbf{P}\{D\,E\,\overline{F}\,\overline{G}\ H\} \le \sum_{1\le i<j<l\le k} \mathbf{P}\{D\,E\,\overline{F}\ H^{(i,j,l)}\}, \qquad (47)$$

$$\mathbf{P}\{D\,E\,\overline{F}\,\overline{G}\ H\} = \mathbf{P}\{D\,E\,\overline{F}\ H\} - \mathbf{P}\{D\,E\,\overline{F}\ G\,H\} \ge \sum_{1\le i<j<l\le k} \mathbf{P}\{D\,E\,\overline{F}\ H^{(i,j,l)}\} -$$

$$- \sum_{\substack{1\le i_1<j_1<l_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ l_1<l_2}} \mathbf{P}\{D\,E\,\overline{F}\ H^{(i_1,j_1,l_1)}\ H^{(i_2,j_2,l_2)}\} - \sum_{\substack{1\le i_1<j_1<l_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ l_1=l_2,\ j_1<j_2}} \mathbf{P}\{D\,E\,\overline{F}\ H^{(i_1,j_1,l_1)}\ H^{(i_2,j_2,l_2)}\} -$$

$$- \sum_{\substack{1\le i_1<j_1<l_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ l_1=l_2,\ j_1=j_2,\ i_1<i_2,}} \mathbf{P}\{DE\overline{F}\ H^{(i_1,j_1,l_1)}\ H^{(i_2,j_2,l_2)}\} - \sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k}} \mathbf{P}\{DE\overline{F}\ G^{(i_1,j_1)}\ H^{(i_2,j_2,l_2)}\}. \qquad (48)$$

Рассмотрим вероятность $\mathbf{P}\{D\,E\,\overline{F}\ H^{(i,j,l)}\}$. Используя введенные выше обозначения, имеем

$$\mathbf{P}\{D\,E\,\bar{F}\,H^{(i,j,l)}\}=\mathbf{P}\{E\,S_k\,H^{(i,j,l)}\}=\mathbf{P}\{S_1\}\prod_{m=2}^{l-1}\mathbf{P}\{E_m\,S_m\,|\,E_{m-1}\,S_{m-1}\}\times$$

$$\times\mathbf{P}\{E_l\,S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}\prod_{m=l+1}^{k}\mathbf{P}\{E_m\,S_m\,|\,E_{m-1}\,S_{m-1}\,H^{(i,j,l)}\}. \quad (49)$$

Как и ранее, вероятности $\mathbf{P}\{E_m S_m\,|\,E_{m-1}\,S_{m-1}\}$, $m<l$, и $\mathbf{P}\{E_m S_m\,|\,E_{m-1}S_{m-1}H^{(i,j,l)}\}$, $m>l$, вычисляются согласно (37) и (38) (с заменой $G^{(i,j)}$ на $H^{(i,j,l)}$). В то же время вероятность $\mathbf{P}\{E_l\,S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}$ удовлетворяет соотношению

$$\mathbf{P}\{E_l\,S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}=\mathbf{P}\{S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}-$$

$$-\mathbf{P}\{\bar{E}_l\,S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}. \quad (50)$$

При фиксированных $\bar{\xi}^{(i)}$ и $\bar{\xi}^{(j)}$ событие $H^{(i,j,l)}$ будет выполнено тогда и только тогда, когда $\bar{\xi}^{(l)}=\alpha\,\bar{\xi}^{(i)}+\beta\,\bar{\xi}^{(j)}$ для некоторых $\alpha,\beta\in\Gamma$, $\alpha\neq 0,\beta\neq 0$. Число таких вариантов равно $(q-1)^2$. Учитывая, что при этом вовсе необязательно произойдет событие $\{\mu(\bar{\xi}^{(l)})\geq 3\}$, получим оценку сверху

$$\mathbf{P}\{S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}\leq\frac{(q-1)^2}{q^{r_l-l}}. \quad (51)$$

В то же время число вариантов, когда может оказаться, что $\mu(\bar{\xi}^{(l)})\leq 2$, не превосходит $2\,(q-1)$ (коэффициент β однозначно выбирается по α, $\bar{\xi}^{(i)}$ и $\bar{\xi}^{(j)}$; исключение составляет случай $\mu(\bar{\xi}^{(i)})=3$ и $\mu(\bar{\xi}^{(j)})=3$, когда β может принимать два значения). Поэтому имеем оценку снизу

$$\mathbf{P}\{S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}\geq\frac{(q-1)^2-2\,(q-1)}{q^{r_l-l}}. \quad (52)$$

Далее имеем очевидную оценку

$$\mathbf{P}\{\bar{E}_l\,S_l\,H^{(i,j,l)}\,|\,E_{l-1}\,S_{l-1}\}\leq\sum_{m=1}^{l-1}\mathbf{P}\{\bar{E}^{(m,l)}\,|\,E_{l-1}\,S_{l-1}\}=\frac{(l-1)\,(q-1)}{q^{r_l-l}}. \quad (53)$$

Из формул (37), (38) и (49)–(53) окончательно получаем оценку

$$\frac{(q-1)^2}{w_l}\max\left\{0,1-\frac{l+1}{q-1}\right\}\prod_{m=1}^{k}\frac{w_m}{q^{r_m-m}}\leq\mathbf{P}\{D\,E\,\bar{F}\,H^{(i,j,l)}\}\leq\frac{(q-1)^2}{w_l}\prod_{m=1}^{k}\frac{w_m}{q^{r_m-m}}.$$

Просуммировав по i, j и l $(1\leq i<j<l\leq k)$, имеем

$$\frac{(q-1)^2}{N(\bar{r})}\prod_{m=1}^{k}w_m\sum_{l=3}^{k}\frac{C_{l-1}^2}{w_l}\max\left\{0,1-\frac{l+1}{q-1}\right\}\leq\sum_{1\leq i<j<l\leq k}\mathbf{P}\{D\,E\,\bar{F}\,H^{(i,j,l)}\}\leq$$

$$\leq\frac{(q-1)^2}{N(\bar{r})}\prod_{m=1}^{k}w_m\sum_{l=3}^{k}\frac{C_{l-1}^2}{w_l}. \quad (54)$$

Используя описанный выше подход и соотношение (51), получаем оценки:

$$\sum_{\substack{1\leq i_1<j_1<l_1\leq k,\\ 1\leq i_2<j_2<l_2\leq k,\\ l_1<l_2}}\mathbf{P}\{D\,E\,\bar{F}\,H^{(i_1,j_1,l_1)}\,H^{(i_2,j_2,l_2)}\}\leq\frac{(q-1)^4}{N(\bar{r})}\prod_{m=1}^{k}w_m\sum_{\substack{1\leq i_1<j_1<l_1\leq k,\\ 1\leq i_2<j_2<l_2\leq k,\\ l_1<l_2}}\frac{1}{w_{l_1}\,w_{l_2}}=$$

$$=\frac{(q-1)^4}{N(\bar{r})}\prod_{m=1}^{k}w_m\sum_{3\leq i<j\leq k}C_{i-1}^2\,C_{j-1}^2\,\frac{1}{w_i\,w_j}; \quad (55)$$

$$\sum_{\substack{1\le i_1<j_1<l_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ l_1=l_2,\ j_1<j_2}} \mathbf{P}\{D\,E\,\overline{F}\,H^{(i_1,j_1,l_1)}\,H^{(i_2,j_2,l_2)}\}\le \frac{(q-1)^4}{N(\bar r)}\prod_{m=1}^{k} w_m \sum_{\substack{1\le i_1<j_1<l_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ l_1=l_2,\ j_1<j_2}} \frac{1}{w_{j_2}\,w_{l_1}}=$$

$$=\frac{(q-1)^4}{N(\bar r)}\prod_{m=1}^{k} w_m \sum_{3\le i<j\le k}(i-1)\,C_{i-1}^{2}\,\frac{1}{w_i\,w_j}\ ; \qquad (56)$$

$$\sum_{\substack{1\le i_1<j_1<l_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ l_1=l_2,\ j_1=j_2,\ i_1<i_2}} \mathbf{P}\{D\,E\,\overline{F}\,H^{(i_1,j_1,l_1)}\,H^{(i_2,j_2,l_2)}\}\le \frac{(q-1)^4}{N(\bar r)}\prod_{m=1}^{k} w_m \sum_{\substack{1\le i_1<j_1<l_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ l_1=l_2,\ j_1=j_2,\ i_1<i_2}} \frac{1}{w_{i_2}\,w_{l_1}}=$$

$$=\frac{(q-1)^4}{N(\bar r)}\prod_{m=1}^{k} w_m \sum_{2\le i<j\le k}(i-1)\,(j-i-1)\,\frac{1}{w_i\,w_j}\,. \qquad (57)$$

Аналогично, используя соотношения (40) и (51), получаем оценку

$$\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k}} \mathbf{P}\{DE\overline{F}\,G^{(i_1,j_1)}\,H^{(i_2,j_2,l_2)}\}\le \sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ j_1\ne l_2}} \mathbf{P}\{S_k\,G^{(i_1,j_1)}\,H^{(i_2,j_2,l_2)}\}+$$

$$+\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ j_1=l_2,\ i_1\le j_2}} \mathbf{P}\{S_k\,G^{(i_1,j_1)}\,H^{(i_2,j_2,l_2)}\}+\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ j_1=l_2,\ i_1>j_2}} \mathbf{P}\{S_k\,G^{(i_1,j_1)}\,H^{(i_2,j_2,l_2)}\}\le$$

$$\le\frac{(q-1)^4}{N(\bar r)}\prod_{m=1}^{k} w_m\left[\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ j_1\ne l_2}}\frac{r_{j_1}-j_1}{w_{j_1}\,w_{l_2}}+\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ j_1=l_2,\ i_1\le j_2}}\frac{r_{j_1}-j_1}{w_{j_1}\,w_{j_2}}+\sum_{\substack{1\le i_1<j_1\le k,\\ 1\le i_2<j_2<l_2\le k,\\ j_1=l_2,\ i_1>j_2}}\frac{r_{i_1}-i_1}{w_{i_1}\,w_{l_2}}\right]=$$

$$=\frac{(q-1)^4}{N(\bar r)}\prod_{m=1}^{k} w_m\left[\sum_{i=2}^{k}\sum_{\substack{j=3,\\ j\ne i}}^{k}\frac{r_i-i}{w_i\,w_j}\,(i-1)\,C_{j-1}^{2}+\right.$$

$$\left.+\sum_{2\le i<j\le k}\frac{r_j-j}{w_i\,w_j}\,i\,(i-1)+\sum_{3\le i<j\le k}\frac{r_i-i}{w_i\,w_j}\,C_{i-1}^{2}\right]. \qquad (58)$$

Объединяя оценки (34), (44)–(46) и (54)–(58), получаем результирующую оценку (20).

Теорема доказана.

ОГРАНИЧЕННОСТЬ ОТНОСИТЕЛЬНОЙ СРЕДНЕКВАДРАТИЧЕСКОЙ ПОГРЕШНОСТИ ОЦЕНОК

Одним из важнейших свойств, определяющих высокую точность (устойчивость) метода Монте-Карло, принято считать ограниченность относительной среднеквадратической погрешности (ОСКП) оценок при изменении тех или иных параметров системы. ОСКП определяется как отношение корня от дисперсии оценки к ее математическому ожиданию. Количество реализаций, требуемых для достижения заданных относительной погрешности и достоверности оценки, пропорционально квадрату ОСКП. Следующая теорема устанавливает ограниченность ОСКП оценок $\hat\beta_{\omega}(\bar\gamma)$, $\omega=1,2$, $\hat\beta_3^{(\mathrm{low})}(\bar\gamma)=Z_3\,\gamma^{(\mathrm{low})}(\bar\gamma)$ и $\hat\beta_3^{(\mathrm{up})}(\bar\gamma)=Z_3\,\gamma^{(\mathrm{up})}(\bar\gamma)$ при $q\to\infty$, т.е. с ростом числа элементов поля Галуа.

Теорема 4. ОСКП $K_{\omega}=\dfrac{\sqrt{D\,\hat{\beta}_{\omega}(\bar{\gamma})}}{M\,\hat{\beta}_{\omega}(\bar{\gamma})}$, $\omega=1,2$, $K_{3}^{(\mathrm{low})}=\dfrac{\sqrt{D\,\hat{\beta}_{3}^{(\mathrm{low})}(\bar{\gamma})}}{M\,\hat{\beta}_{3}^{(\mathrm{low})}(\bar{\gamma})}$, $K_{3}^{(\mathrm{up})}=\dfrac{\sqrt{D\,\hat{\beta}_{3}^{(\mathrm{up})}(\bar{\gamma})}}{M\,\hat{\beta}_{3}^{(\mathrm{up})}(\bar{\gamma})}$ равномерно ограничены по q.

Доказательство. Поскольку $r_i-i\geq r_1-1$ для любого i, то из соотношения (9) следует, что $1\leq c_1(\bar{r})\leq k$ равномерно по L и $\bar{r}$. Следовательно, $\mathbf{M}\,c_1(\bar{\gamma})\geq 1$ и $\mathbf{M}[c_1(\bar{\gamma})]^2\leq k\,\mathbf{M}\,c_1(\bar{\gamma})$, т.е. $K_1\leq\sqrt{k-1}$ (при этом учитывается, что Z_1 является константой).

Рассмотрим случай $\omega=2$. Для доказательства равномерной ограниченности ОСКП по q достаточно доказать ограниченность ОСКП при $q\to\infty$. Построим верхние и нижние оценки для коэффициента $c_2(\bar{r})$. Если $r_1=2$, то из (10) следует, что

$$\left(\frac{q-1}{q}\right)^k\leq c_2(\bar{r})\leq 1. \tag{59}$$

Пусть теперь $r_1\geq 3$. Это означает, что $r_m\geq m+2$ для любого $m\in\{2,\,\ldots,k\}$. Поэтому при больших значениях q случай $v_m\leq 0$ исключается (формула (11) для $c_2(\bar{r})$). Воспользовавшись тем, что $r_i-i\geq r_1-1$, из формулы (12) имеем оценки

$$c_2(\bar{r})\leq\sum_{i=1}^{k}(r_i-1)\leq k\,n. \tag{60}$$

В то же время

$$c_2(\bar{r})\underset{q\to\infty}{\sim} r_1-1+\sum_{i=2}^{k}\frac{r_i-1}{q^{r_i-i-r_1+1}}\geq r_1-1\geq 2. \tag{61}$$

Из (59)–(61) следует, что K_2 асимптотически при $q\to\infty$ не превосходит $\sqrt{k\,n-1}$, что свидетельствует о равномерной ограниченности K_2.

Рассмотрим случай $\omega=3$. Если $r_1=3$, то из (19) следует, что

$$c_3(\bar{r})=\gamma^{(\mathrm{low})}(\bar{r})=\gamma^{(\mathrm{up})}(\bar{r})\underset{q\to\infty}{\sim}1 \tag{62}$$

равномерно по $\{r_i,\ i\geq 2\}$. Предположим, что $r_1\geq 4$. Из формулы (21) с учетом (23) и (24) имеем

$$h(\bar{r})\underset{q\to\infty}{\sim}C_{r_1-1}^2+\sum_{m=2}^{k}\frac{1}{q^{r_m-m-r_1+1}}[C_{r_m-m}^2+(r_m-m)(m-1)+C_{m-1}^2]. \tag{63}$$

В то же время из (22) следует, что

$$g(\bar{r})\underset{q\to\infty}{\sim}\frac{1}{q}\sum_{m=2}^{k}\frac{1}{q^{r_m-m-r_1+1}}[(m-1)(m+2)+C_{m-1}^2\,(m+1)]+$$

$$+\sum_{i=2}^{k}\frac{(r_i-i)(i-1)}{q^{r_i-i-r_1+1}}\sum_{\substack{3\leq j\leq k,\\ j\neq i}}\frac{C_{j-1}^2}{q^{r_j-j-2}}+\sum_{i=2}^{k-1}\frac{1}{q^{r_i-i-r_1+1}}\sum_{j=i+1}^{k}\frac{f_{ij}(\bar{r})}{q^{r_j-j-2}}. \tag{64}$$

Поскольку $r_1\geq 4$, то $r_j\geq j+3$. Из сравнения формул (63) и (64) следует, что

$$\frac{g(\bar{r})}{h(\bar{r})}\underset{q\to\infty}{\to}0 \tag{65}$$

равномерно относительно $\bar{r}$. Формулы (62)–(65) позволяют сделать вывод о равномерной ограниченности ОСКП $K_3^{(\mathrm{low})}$ и $K_3^{(\mathrm{up})}$.

Теорема доказана.

ЧИСЛЕННЫЕ РЕЗУЛЬТАТЫ

На численных примерах проиллюстрируем высокую точность оценок, получаемых предложенным методом. Все приведенные ниже оценки построены с относительной погрешностью 1% и достоверностью 0,99. Введем следующие обозначения:

- $\hat{\theta}_\omega(n,k)$, $\omega = 1, 2$, — несмещенная оценка для $\left[\begin{matrix} n \\ k \end{matrix}\middle|\,\omega\right]$, построенная с указанными выше относительной погрешностью и достоверностью;
- $\hat{\theta}_3^{(\mathrm{low})}(n,k)$ и $\hat{\theta}_3^{(\mathrm{low})}(n,k)$ — верхние и нижние оценки для $\left[\begin{matrix} n \\ k \end{matrix}\middle|\,3\right]$;
- $\hat{N}_\omega(n,k)$ — количество реализаций, использованных для построения соответствующих оценок.

В табл. 1 при $q = 2^8$ и $n = 2k$ проведено сравнение оценок $\hat{\theta}_\omega(n,k)$, $\omega = 1, 2$, с соответствующими точными значениями $\left[\begin{matrix} n \\ k \end{matrix}\middle|\,\omega\right]$, $\omega = 1, 2$, а также указаны верхние и нижние оценки $\hat{\theta}_3^{(\mathrm{low})}(n,k)$, $\hat{\theta}_3^{(\mathrm{up})}(n,k)$ для числа $\left[\begin{matrix} n \\ k \end{matrix}\middle|\,3\right]$ подпространств веса $\omega = 3$, точное значение которого неизвестно. Кроме того, исследуется изменение количества затраченных реализаций при увеличении k.

Таблица 1

k	ω	$\left[\begin{matrix} n \\ k \end{matrix}\middle|\,\omega\right]$	$\hat{\theta}_\omega(n,k)$	$\hat{\theta}_3^{(\mathrm{low})}(n,k)$	$\hat{\theta}_3^{(\mathrm{up})}(n,k)$	$\hat{N}_\omega(n,k)$
5	1	$1{,}467 \cdot 10^{49}$	$1{,}468 \cdot 10^{49}$	—	—	52 763
	2	$1{,}684 \cdot 10^{52}$	$1{,}693 \cdot 10^{52}$	—	—	137 580
	3	—	—	$1{,}140 \cdot 10^{55}$	$1{,}144 \cdot 10^{55}$	156 635
10	1	$1{,}107 \cdot 10^{218}$	$1{,}113 \cdot 10^{218}$	—	—	133 640
	2	$2{,}683 \cdot 10^{221}$	$2{,}685 \cdot 10^{221}$	—	—	323 360
	3	—	—	$4{,}088 \cdot 10^{224}$	$4{,}110 \cdot 10^{224}$	410 320
20	1	$5{,}432 \cdot 10^{916}$	$5{,}450 \cdot 10^{916}$	—	—	297 924
	2	$2{,}701 \cdot 10^{920}$	$2{,}695 \cdot 10^{920}$	—	—	695 847
	3	—	—	$8{,}649 \cdot 10^{923}$	$8{,}725 \cdot 10^{923}$	916 882
30	1	$8{,}884 \cdot 10^{2096}$	$8{,}915 \cdot 10^{2096}$	—	—	462 765
	2	$6{,}683 \cdot 10^{2100}$	$6{,}681 \cdot 10^{2100}$	—	—	1 066 495
	3	—	—	$3{,}257 \cdot 10^{2104}$	$3{,}298 \cdot 10^{2104}$	1 421 617
40	1	$5{,}743 \cdot 10^{3758}$	$5{,}735 \cdot 10^{3758}$	—	—	627 701
	2	$5{,}785 \cdot 10^{3762}$	$5{,}792 \cdot 10^{3762}$	—	—	1 436 501
	3	—	—	$3{,}776 \cdot 10^{3766}$	$3{,}837 \cdot 10^{3766}$	1 927 766
50	1	$1{,}547 \cdot 10^{5902}$	$1{,}539 \cdot 10^{5902}$	—	—	792 678
	2	$1{,}953 \cdot 10^{5906}$	$1{,}964 \cdot 10^{5906}$	—	—	1 802 621
	3	—	—	$1{,}596 \cdot 10^{5910}$	$1{,}628 \cdot 10^{5910}$	2 433 320

Сравнение точных значений с оценками, полученными моделированием ($\omega = 1, 2$), свидетельствует о высокой точности предложенного метода. В частности, легко убедиться, что во всех рассмотренных случаях точные значения попадают в соответствующие однопроцентные доверительные интервалы. Следует также отметить, что в широком диапазоне изменения n достигается весьма высокая точность нижних и верхних оценок $\hat{\theta}_3^{(\mathrm{low})}(n,k)$ и $\hat{\theta}_3^{(\mathrm{up})}(n,k)$. В качестве доверительного интервала для $\left[\begin{matrix} n \\ k \end{matrix}\middle|\,3\right]$ можно выбрать $(0{,}99\,\hat{\theta}_3^{(\mathrm{low})}(n,k),\ 1{,}01\,\hat{\theta}_3^{(\mathrm{up})}(n,k))$. С увеличением k наблюдается рост числа $\hat{N}_\omega(n,k)$ требуемых реализаций, который близок к линейному.

В табл. 2 исследуется точность оценок с ростом $q = 2^{2m}$, $m = 1, 2, \ldots$. Рассматривается случай $n = 60$, $k = 30$.

Таблица 2

q	ω	$\left[{n \atop k} \middle| \omega \right]$	$\hat{\theta}_\omega(n,k)$	$\hat{\theta}_3^{(\mathrm{low})}(n,k)$	$\hat{\theta}_3^{(\mathrm{up})}(n,k)$	$\hat{N}_\omega(n,k)$
4	1	$5{,}400 \cdot 10^{525}$	$5{,}412 \cdot 10^{525}$	—	—	342 401
	2	$4{,}779 \cdot 10^{527}$	$4{,}782 \cdot 10^{527}$	—	—	789 777
	3	—	—	$2{,}181 \cdot 10^{529}$	$2{,}777 \cdot 10^{529}$	1 049 452
16	1	$2{,}468 \cdot 10^{1049}$	$2{,}465 \cdot 10^{1049}$	—	—	433 549
	2	$1{,}092 \cdot 10^{1052}$	$1{,}091 \cdot 10^{1052}$	—	—	1 001 480
	3	—	—	$2{,}736 \cdot 10^{1054}$	$3{,}166 \cdot 10^{1054}$	1 335 009
64	1	$1{,}451 \cdot 10^{1573}$	$1{,}442 \cdot 10^{1573}$	—	—	456 816
	2	$2{,}697 \cdot 10^{1576}$	$2{,}689 \cdot 10^{1576}$	—	—	1 055 104
	3	—	—	$3{,}103 \cdot 10^{1579}$	$3{,}267 \cdot 10^{1579}$	1 411 798
256	1	$8{,}884 \cdot 10^{2096}$	$8{,}915 \cdot 10^{2096}$	—	—	462 765
	2	$6{,}683 \cdot 10^{2100}$	$6{,}681 \cdot 10^{2100}$	—	—	1 066 495
	3	—	—	$3{,}257 \cdot 10^{2104}$	$3{,}298 \cdot 10^{2104}$	1 421 617
1 024	1	$5{,}490 \cdot 10^{2620}$	$5{,}477 \cdot 10^{2620}$	—	—	464 212
	2	$1{,}657 \cdot 10^{2625}$	$1{,}662 \cdot 10^{2625}$	—	—	1 067 278
	3	—	—	$3{,}272 \cdot 10^{2629}$	$3{,}283 \cdot 10^{2629}$	1 425 224
4 096	1	$3{,}399 \cdot 10^{3144}$	$3{,}392 \cdot 10^{3144}$	—	—	464 576
	2	$4{,}107 \cdot 10^{3149}$	$4{,}120 \cdot 10^{3149}$	—	—	1 067 970
	3	—	—	$3{,}255 \cdot 10^{3154}$	$3{,}258 \cdot 10^{3154}$	1 426 069

Приведенные в табл. 2 данные не только подтверждают высокую точность несмещенных оценок ($\omega = 1, 2$), построенных при различных значениях q, но и наглядно демонстрируют возрастание точности нижних и верхних оценок для $\left[{n \atop k} \middle| 3 \right]$ с ростом q.

Так, если при $q = 4$ у оценок $\hat{\theta}_3^{(\mathrm{low})}(n,k)$ и $\hat{\theta}_3^{(\mathrm{up})}(n,k)$ совпадает первая значащая цифра (что уже является высокой точностью расчета), то при $q = 4\ 096$ совпадают три значащие цифры. Заметим, что при каждом ω с ростом q количество реализаций остается примерно одним и тем же, что вполне согласуется с утверждением теоремы 4 об ограниченности ОСКП с ростом q.

СПИСОК ЛИТЕРАТУРЫ

1. Эндрюс Г. Теория разбиений. — М.: Наука, 1982. — 256 с.
2. Мак-Вальрас Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
3. Masol V.V. Investigation of linear codes possessing some extra properties // Cryptography and Coding. — 2001. — P. 301–306.
4. Масол В.И. Некоторые применения алгоритмов построения подпространств над конечным полем // Укр. мат. журн. — 1989. — **41**, № 8. — С. 1146–1148.
5. Масол В.И. Асимптотика числа некоторых k-мерных подпространств над конечным полем // Матем. заметки. — 1996. — **59**, вып. 5. — С. 729–736.
6. Коваленко И.Н. Исследования по анализу надежности сложных систем. — Киев: Наук. думка, 1975. — 210 с.
7. Коваленко И.Н. Анализ редких событий при оценке эффективности и надежности систем. — М.: Сов. радио, 1980. — 209 с.
8. 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.
9. 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.

Поступила 01.02.2010