

УДК 519.719.1

ОЦЕНКА РАНГА СЛУЧАЙНОЙ КВАДРАТИЧНОЙ ФОРМЫ НАД КОНЕЧНЫМ ПОЛЕМ

А. В. Черемушкин

ФГУП «НИИ «Квант», г. Москва, Россия

Изучаются свойства распределения ранга случайной квадратичной формы над конечным полем $\text{GF}(q)$. Отдельно рассматриваются случаи чётной и нечётной характеристик поля. Доказаны асимптотические нижние оценки значения ранга для почти всех квадратичных форм f от n переменных вида

$$\text{rank}(f) \geq n - \left\lceil \sqrt{2 \log_q n} + c \right\rceil + 1,$$

$0 < c < 1$, при $n \rightarrow \infty$.

Ключевые слова: конечное поле, симплектическая группа, квадратичная форма.

DOI 10.17223/20710410/35/3

ON THE RANK OF RANDOM QUADRATIC FORM OVER FINITE FIELD

A. V. Cheremushkin

Technology Federal State Unitary Enterprise “Research Institute Kvant”, Moscow, Russia

E-mail: avc238@mail.ru

The weights of Boolean functions of degree two are closely related to the ranks of quadratic forms. Though the weights of Reed — Muller codes are intensively researched in coding theory, the ranks of quadratic forms are not sufficiently studied. The article contains some asymptotic properties of the rank of a random quadratic form $f(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij} x_i x_j$ over finite field $\text{GF}(q)$. The cases of odd and

even characteristics are separately considered. If q is odd, then the $\text{rank}(f)$ of f is defined as the rank of the symmetric matrix (b_{ij}) with $b_{ii} = a_{ii}$, $b_{ij} = (a_{ij} + a_{ji})/2$, $j \neq i$, $1 \leq i, j \leq n$. It is proved that, for any odd q and $0 < c < 1$, the lower bound for the rank of the almost all quadratic forms f in n variables is the following: $\text{rank}(f) \geq n - \left\lceil \sqrt{2 \log_q n} + c \right\rceil + 1$ as $n \rightarrow \infty$. In the case of even q , the $\text{rank}(f)$ of f is defined as the rank of a bilinear form $f(x + y) + f(x) + f(y)$. If $q = 2^m$, $m \geq 1$, $n = 2k + \varepsilon$, $\varepsilon \in \{0, 1\}$, $0 < c < 1$, then the lower bound for the rank of the almost all quadratic forms f in n variables is the following:

$$\text{rank}(f) \geq 2k - 2 \left\lceil \sqrt{\frac{1}{2} \log_q k} + \frac{c + (-1)^\varepsilon}{4} \right\rceil + 2 \text{ as } k \rightarrow \infty. \text{ An another form of}$$

this inequality is $\text{rank}(f) > n - \left\lceil \sqrt{2 \log_q n} + c' \right\rceil + 1$, where $0 < c' < 1$. As a corollary, an asymptotic lower bound for the minimal size $\beta_0(G)$ of a vertex cover of a graph G with n vertices is obtained. The vertex cover of G is a set S of vertices in G such that every arc in G is incident to a vertex in S . Let $n = 2k + \varepsilon$, $\varepsilon = 0, 1$, $c > 0$. Then for the almost all graphs G with n vertices, the lower bound for the minimal vertex cover

$$\text{size is the following: } \beta_0(G) \geq k - \left\lceil \sqrt{\frac{1}{2} \log_2 k} + \frac{c + (-1)^\varepsilon}{4} \right\rceil + 1 \text{ as } k \rightarrow \infty.$$

Keywords: *finite field, symplectic group, quadratic form.*

1. Случай конечного поля нечётного порядка

Каждой квадратичной форме

$$f(x_1, \dots, x_n) = \sum_{1 \leq i, j \leq n} a_{ij} x_i x_j$$

над полем $\text{GF}(q)$, $q = p^m$, $p \geq 3$, от $n \geq 1$ переменных можно поставить в соответствие симметричную матрицу (b_{ij}) с элементами $b_{ii} = a_{ii}$ и $b_{ij} = (a_{ij} + a_{ji})/2$, $j \neq i$, $1 \leq i, j \leq n$. Ранг этой матрицы называется рангом квадратичной формы. Из классификации квадратичных форм [1, 2] следует, что квадратичную форму можно линейным преобразованием аргументов привести к одному из следующих вариантов:

- (а) $x_1 x_2 + x_3 x_4 + \dots + x_{2s-1} x_{2s} + x_{2s+1}^2$, $r = 2s + 1 \leq n$;
- (б) $x_1 x_2 + x_3 x_4 + \dots + x_{2s-1} x_{2s} + d x_{2s+1}^2$, $r = 2s + 1 \leq n$ и элемент $d \in \text{GF}(q)^*$ не является квадратичным вычетом;
- (с) $x_1 x_2 + x_3 x_4 + \dots + x_{2s-1} x_{2s}$, $r = 2s \leq n$;
- (д) $x_1 x_2 + x_3 x_4 + \dots + x_{2s-1}^2 - d x_{2s}^2$, $r = 2s \leq n$ и элемент $d \in \text{GF}(q)^*$ не является квадратичным вычетом.

Вероятность того, что квадратичная форма от n переменных имеет ранг r , определяется как относительная доля таких форм:

$$p_r(n) = Q_r(n)/q^{n(n+1)/2}, \quad (1)$$

где $Q_r(n)$ — число квадратичных форм от n переменных, имеющих ранг r ; $q^{n(n+1)/2}$ — число симметричных матриц над полем $\text{GF}(q)$ размера $n \times n$.

Группы инерции этих квадратичных форм имеют следующие порядки [1, 3]:
— для случаев (а) и (б)

$$2(q^{2s} - 1)q^{2s-1} \dots (q^2 - 1)q^1 = 2q^{s^2} \prod_{i=1}^s (q^{2i} - 1),$$

— для случая (с)

$$2(q^{2s-1} - q^{s-1})(q^{2s-2} - 1)q^{2s-3} \dots (q^2 - 1)q^1,$$

— для случая (д)

$$2(q^{2s-1} + q^{s-1})(q^{2s} - 2)q^{2s-3} \dots (q^2 - 1)q^1.$$

Соответственно для числа квадратичных форм возможны следующие значения:

$$\begin{aligned} Q_{2s+1}(n) &= \frac{(q^n - 1) \dots (q^n - q^{2s})}{(q^{2s} - 1)q^{2s-1} \dots (q^2 - 1)q^1} = \\ &= \frac{(q^n - 1)(q^{n-1} - 1)q^1(q^{n-2} - 1)q^2}{(q^{2s} - 1)q^{2s-1}} \cdot \frac{(q^{n-3} - 1)q^3(q^{n-4} - 1)q^4}{(q^{2s-2} - 1)q^{2s-3}} \cdot \dots \times \\ &\quad \times \frac{(q^{n-2s+1} - 1)q^{2s-1}(q^{n-2s} - 1)q^{2s}}{(q^2 - 1)q^1} = \\ &= \frac{q^{s(s+1)}(q^n - 1)(q^{n-1} - 1) \dots (q^{n-2s} - 1)}{(q^{2s} - 1)(q^{2s-2} - 1) \dots (q^2 - 1)}, \end{aligned} \quad (2)$$

$$\begin{aligned}
Q_{2s}(n) &= \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{2s-1})}{2(q^{2s-1} - q^{s-1})(q^{2s-2} - 1)q^{2s-3} \dots (q^2 - 1)q^1} + \\
&\quad + \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{2s-1})}{2(q^{2s-1} + q^{s-1})(q^{2s-2} - 1)q^{2s-3} \dots (q^2 - 1)q^1} = \\
&= \left(\frac{(q^n - 1)(q^n - q)q^{2s-1}}{(q^s - 1)(q^s + 1)q^{2s-2}} \right) \frac{(q^n - q^2)(q^n - q^3) \dots (q^n - q^{2s-1})}{(q^{2s-2} - 1)q^{2s-3} \dots (q^2 - 1)q^1} = \\
&= \frac{(q^n - 1)(q^{n-1} - 1)q^{2s+1}}{(q^{2s} - 1)q^{2s-1}} \cdot \frac{(q^{n-2} - 1)q^2(q^{n-3} - 1)q^3}{(q^{2s-2} - 1)q^{2s-3}} \cdot \dots \times \\
&\times \frac{(q^{n-2s+2} - 1)q^{2s-2}(q^{n-2s+1} - 1)q^{2s-1}}{(q^2 - 1)q^1} = \frac{(q^n - 1)(q^{n-1} - 1)q^{2s}}{(q^{2s} - 1)} \times \\
&\times \frac{(q^{n-2} - 1)q^2(q^{n-3} - 1)}{(q^{2s-2} - 1)} \cdot \dots \cdot \frac{(q^{n-2s+2} - 1)q^{2s-2}(q^{n-2s+1} - 1)}{(q^2 - 1)} = \\
&= \frac{q^{s(s+1)}(q^n - 1)(q^{n-1} - 1) \cdot \dots \cdot (q^{n-2s+1} - 1)}{(q^{2s} - 1)(q^{2s-2} - 1) \cdot \dots \cdot (q^2 - 1)}.
\end{aligned} \tag{3}$$

Приведём свойства этих чисел, необходимые в дальнейшем.

Лемма 1. При нечётном $q \geq 3$ и $0 \leq 2s \leq n - 2$ справедливы следующие соотношения:

$$\frac{Q_{2s+1}(n)}{Q_{2s+3}(n)} = \frac{1}{(q^{n-2s-1} - 1)(q^{n-2s-2} - 1)} \left(1 - \frac{1}{q^{2s+2}} \right); \tag{4}$$

$$\frac{Q_{2s}(n)}{Q_{2s+2}(n)} = \frac{1}{(q^{n-2s} - 1)(q^{n-2s-1} - 1)} \left(1 - \frac{1}{q^{2s+2}} \right); \tag{5}$$

$$\frac{Q_{2s}(n)}{Q_{2s+1}(n)} = \frac{1}{q^{n-2s} - 1}; \tag{6}$$

$$\frac{Q_{2s+1}(n)}{Q_{2s+2}(n)} = \frac{1}{(q^{n-2s-1} - 1)} \left(1 - \frac{1}{q^{2s+2}} \right). \tag{7}$$

Поэтому числа $Q_s(n)$, $1 \leq s \leq n$, образуют монотонно возрастающие последовательности.

Доказательство. Из формул (2) и (3) вытекают соотношения

$$\begin{aligned}
\frac{Q_{2s+3}(n)}{Q_{2s+1}(n)} &= \frac{(q^{n-2s-1} - 1)(q^{n-2s-2} - 1)q^{2s+2}}{(q^{2s+2} - 1)}, \\
\frac{Q_{2s+2}(n)}{Q_{2s}(n)} &= \frac{(q^{n-2s} - 1)(q^{n-2s-1} - 1)q^{2s+2}}{(q^{2s+2} - 1)}, \\
\frac{Q_{2s+1}(n)}{Q_{2s}(n)} &= q^{n-2s} - 1, \\
\frac{Q_{2s+2}(n)}{Q_{2s+1}(n)} &= \frac{(q^{n-2s-1} - 1)q^{2s+2}}{(q^{2s+2} - 1)}.
\end{aligned}$$

Лемма доказана. ■

Лемма 2. При нечётном $q \geq 3$ для числа квадратичных форм с максимальным значением ранга справедливы следующие формулы:

$$Q_{2k}(2k) = q^{k(2k+1)} \left(1 - \frac{1}{q^{n-1}}\right) \left(1 - \frac{1}{q^{n-3}}\right) \dots \left(1 - \frac{1}{q}\right),$$

$$Q_{2k+1}(2k+1) = q^{k(2k+1)} \left(1 - \frac{1}{q^n}\right) \left(1 - \frac{1}{q^{n-2}}\right) \dots \left(1 - \frac{1}{q}\right).$$

Доказательство. При $n = 2k$ имеем

$$\begin{aligned} Q_{2k}(2k) &= \frac{q^{k(k+1)}(q^n - 1)(q^{n-1} - 1) \dots (q^{n-2k+1} - 1)}{(q^{2k} - 1)(q^{2k-2} - 1) \dots (q^2 - 1)} = \\ &= q^{k(k+1)}(q^{n-1} - 1)(q^{n-3} - 1) \dots (q^1 - 1) = \\ &= q^{k(2k+1)} \left(1 - \frac{1}{q^{n-1}}\right) \left(1 - \frac{1}{q^{n-3}}\right) \dots \left(1 - \frac{1}{q}\right). \end{aligned}$$

Аналогично при $n = 2k + 1$ имеем

$$\begin{aligned} Q_{2k+1}(2k+1) &= \frac{q^{k(k+1)}(q^n - 1)(q^{n-1} - 1) \dots (q^{n-2k} - 1)}{(q^{2k} - 1)(q^{2k-2} - 1) \dots (q^2 - 1)} = \\ &= q^{k(k+1)}(q^n - 1)(q^{n-2} - 1) \dots (q^1 - 1) = \\ &= q^{k(2k+1)} \left(1 - \frac{1}{q^n}\right) \left(1 - \frac{1}{q^{n-2}}\right) \dots \left(1 - \frac{1}{q}\right). \end{aligned}$$

Лемма доказана. ■

Лемма 3. При нечётном $q \geq 3$ для вероятности максимального значения ранга справедливы следующие формулы:

$$p_{2k}(2k) = \left(1 - \frac{1}{q^{2k-1}}\right) \left(1 - \frac{1}{q^{2k-3}}\right) \dots \left(1 - \frac{1}{q}\right),$$

$$p_{2k+1}(2k+1) = \left(1 - \frac{1}{q^{2k+1}}\right) \left(1 - \frac{1}{q^{2k-1}}\right) \dots \left(1 - \frac{1}{q}\right).$$

В частности, $p_{2k+1}(2k+1) = \left(1 - \frac{1}{q^{2k+1}}\right) p_{2k}(2k)$ при $k \geq 2$.

Доказательство непосредственно следует из формулы (1) и леммы 2.

Лемма 4. При нечётном $q \geq 3$, $n \geq 2$ и $1 \leq i \leq n$ справедлива оценка

$$\frac{Q_{n-i}(n)}{Q_n(n)} < \frac{1}{(q^i - 1)(q^{i-1} - 1) \dots (q^2 - 1)(q^1 - 1)}.$$

Доказательство. Из равенств (4)–(7) леммы 1 следует, что при $n = 2k$ и $1 \leq i \leq k$ выполнены равенства

$$\begin{aligned} \frac{Q_{2k-2i}(2k)}{Q_{2k}(2k)} &< \frac{1}{(q^{2i} - 1)(q^{2i-1} - 1) \dots (q^2 - 1)(q^1 - 1)}, \\ \frac{Q_{2k-2i-1}(2k)}{Q_{2k}(2k)} &< \frac{1}{(q^{2i+1} - 1)(q^{2i} - 1) \dots (q^2 - 1)(q^1 - 1)}. \end{aligned}$$

Таким образом, при всех $1 \leq i \leq 2k$ справедлива оценка

$$\frac{Q_{2k-i}(2k)}{Q_{2k}(2k)} < \frac{1}{(q^i - 1)(q^{i-1} - 1) \cdot \dots \cdot (q^2 - 1)(q^1 - 1)}.$$

При нечётном $n = 2k + 1$ и $1 \leq i \leq k$ аналогично получаем

$$\begin{aligned} \frac{Q_{2k-2i+1}(2k+1)}{Q_{2k+1}(2k+1)} &< \frac{1}{(q^{2i} - 1)(q^{2i-1} - 1) \cdot \dots \cdot (q^2 - 1)(q^1 - 1)}, \\ \frac{Q_{2k-2i}(2k+1)}{Q_{2k+1}(2k+1)} &< \frac{1}{(q^{2i+1} - 1)(q^{2i} - 1) \cdot \dots \cdot (q^2 - 1)(q^1 - 1)}. \end{aligned}$$

Таким образом, при всех $1 \leq i \leq 2k + 1$ справедлива оценка

$$\frac{Q_{2k+1-i}(2k+1)}{Q_{2k+1}(2k+1)} < \frac{1}{(q^i - 1)(q^{i-1} - 1) \cdot \dots \cdot (q^2 - 1)(q^1 - 1)}.$$

Лемма доказана. ■

Теорема 1. Пусть q нечётно и $0 < c < 1$. При $n \rightarrow \infty$ для ранга почти всех квадратичных форм f от n переменных при $n \rightarrow \infty$ справедлива оценка

$$\text{rank}(f) \geq n - \left\lceil \sqrt{2 \log_q n + c} \right\rceil + 1.$$

Доказательство. Оценим долю квадратичных форм от n переменных ранга, не превышающего $n - i$:

$$\sum_{j=0}^{n-i} Q_j(n) q^{-n(n+1)/2} < \sum_{j=0}^{n-i} \frac{Q_j(n)}{Q_n(n)} < n \frac{Q_{n-i}(n)}{Q_n(n)} < \frac{n}{(q^1 - 1)(q^2 - 1) \cdot \dots \cdot (q^{i-1} - 1)(q^i - 1)}$$

(здесь использована оценка из леммы 4). В результате имеем

$$\begin{aligned} \log_q \left(\sum_{j=0}^{n-i} \frac{Q_j(n)}{Q_n(n)} \right) &< \log_q n - \sum_{m=1}^i \log_q (q^m - 1) = \log_q n - \sum_{m=1}^i \left(m - \log_q \left(1 - \frac{1}{q^m} \right) \right) = \\ &= \log_q n - \frac{i(i+1)}{2} + \sum_{m=1}^i \log_q \left(1 - \frac{1}{q^m} \right) < \log_q n - \frac{i(i+1)}{2}. \end{aligned}$$

При $i = \left\lceil \sqrt{2 \log_q n + c} \right\rceil$, $c > 0$, выражение

$$\log_q n - \frac{i(i+1)}{2} < \log_q n - \frac{i^2}{2} \leq \log_q n - \frac{(\sqrt{2 \log_q n} + c)^2}{2} = -c \sqrt{2 \log_q n} + \frac{c^2}{2}$$

стремится к $-\infty$ при $n \rightarrow \infty$. Поэтому при $n \rightarrow \infty$ доля квадратичных форм ранга, меньшего чем $n - \left\lceil \sqrt{2 \log_q n + c} \right\rceil$, стремится к нулю. ■

2. Случай конечного поля чётного порядка

Каждая квадратичная форма f над полем $\text{GF}(q)$, $q = 2^m$, $m \geq 1$, характеристики два от n переменных может иметь только чётный ранг, причем форму ранга $2r$, $1 \leq r \leq \lfloor n/2 \rfloor$, можно линейным преобразованием аргументов привести к виду

- а) $x_1 x_2 + x_3 x_4 + \dots + x_{2r-1} x_{2r} + x_{2r+1}^2$ ($2r + 1 \leq n$),
- б) $x_1 x_2 + x_3 x_4 + \dots + x_{2r-1} x_{2r} + \alpha x_{2r-1}^2 + \alpha x_{2r}^2$ ($2r \leq n$),

где $\alpha = 0$ либо α является корнем неприводимого над $\text{GF}(q)$ многочлена $\alpha x^2 + x + \alpha$ [1]. Так как ранг определяется по билинейной знакопеременной форме

$$f(x + y) + f(x) + f(y),$$

$x, y \in \text{GF}(q)^n$, которая однозначно строится по квадратичной части многочлена, содержащей смешанные произведения без квадратов, то вероятность того, что квадратичная форма от n переменных имеет ранг $2r$, можно записать в виде

$$p_{2r}(n) = Q_{2r}(n)/q^{n(n-1)/2},$$

где, как и выше, $Q_{2r}(n)$ — число квадратичных форм от n переменных, имеющих ранг $2r$, а $n(n-1)/2$ — число попарных произведений переменных. Учитывая, что группа инерции билинейной формы от $2r$ переменных ранга $2r$ совпадает с симплектической группой $\mathbf{Sp}(2r, q)$ (см., например, [1, 3, 4]), получаем

$$Q_{2r}(n) = \frac{(q^n - 1) \dots (q^n - q^{2r-1})}{|\mathbf{Sp}(2r, q)|}.$$

Так как [5, с. 414] $|\mathbf{Sp}(2r, q)| = q^{r^2} \prod_{i=1}^r (q^{2i} - 1) = (q^{2r} - 1)q^{2r-1} \dots (q^2 - 1)q^1$, то

$$\begin{aligned} Q_{2r}(n) &= \frac{(q^n - 1)(q^n - q^1)}{(q^{2r} - 1)q^{2r-1}} \dots \frac{(q^n - q^{2r-2})(q^n - q^{2r-1})}{(q^2 - 1)q^1} = \\ &= \frac{(q^n - 1)(q^{n-1} - 1)q^0}{(q^{2r} - 1)} \dots \frac{(q^{n-2r+2} - 1)(q^{n-2r+1} - 1)q^{2r-2}}{(q^2 - 1)}. \end{aligned} \quad (8)$$

Лемма 5. При $q = 2^m$, $m \geq 1$, $1 \leq r \leq n/2 - 1$ справедливо соотношение

$$\frac{Q_{2r}(n)}{Q_{2r+2}(n)} = \frac{q^2}{(q^{n-2r} - 1)(q^{n-2r-1} - 1)} \left(1 - \frac{1}{q^{2r+2}}\right). \quad (9)$$

Числа $Q_{2r}(n)$, $1 \leq r \leq n/2 - 1$, образуют монотонно возрастающую последовательность.

Доказательство вытекает из равенства (8) и соотношения

$$Q_{2r+2}(n)/Q_{2r}(n) = \frac{(q^{n-2r} - 1)(q^{n-2r-1} - 1)q^{2r}}{(q^{2r+2} - 1)}.$$

Лемма 6. При $q = 2^m$, $m \geq 1$, для числа квадратичных форм с максимальным значением ранга справедливы следующие формулы:

$$\begin{aligned} Q_{2k}(2k) &= q^{k(2k-1)} \left(1 - \frac{1}{q^{n-1}}\right) \left(1 - \frac{1}{q^{n-3}}\right) \dots \left(1 - \frac{1}{q}\right), \\ Q_{2k}(2k+1) &= q^{k(2k+1)} \left(1 - \frac{1}{q^n}\right) \left(1 - \frac{1}{q^{n-2}}\right) \dots \left(1 - \frac{1}{q^3}\right). \end{aligned}$$

Доказательство. При $n = 2k$ имеем

$$\begin{aligned} Q_{2k}(2k) &= \frac{(q^n - 1)(q^{n-1} - 1)q^0}{(q^{2k} - 1)} \dots \frac{(q^2 - 1)(q^1 - 1)q^{2k-2}}{(q^2 - 1)} = \\ &= q^{k(k-1)}(q^{n-1} - 1)(q^{n-3} - 1) \dots (q^1 - 1) = q^{k(2k-1)} \left(1 - \frac{1}{q^{n-1}}\right) \left(1 - \frac{1}{q^{n-3}}\right) \dots \left(1 - \frac{1}{q}\right). \end{aligned}$$

Аналогично при $n = 2k + 1$ имеем

$$Q_{2k}(2k + 1) = q^{k(2k+1)} \left(1 - \frac{1}{q^n}\right) \left(1 - \frac{1}{q^{n-2}}\right) \dots \left(1 - \frac{1}{q^3}\right).$$

Лемма доказана. ■

Лемма 7. При $q = 2^m$, $m \geq 1$, для вероятности максимального значения ранга справедливы следующие формулы:

$$\begin{aligned} p_{2k}(2k) &= \left(1 - \frac{1}{q^{2k-1}}\right) \left(1 - \frac{1}{q^{2k-3}}\right) \dots \left(1 - \frac{1}{q}\right), \\ p_{2k}(2k + 1) &= \left(1 - \frac{1}{q^{2k+1}}\right) \left(1 - \frac{1}{q^{2k-1}}\right) \dots \left(1 - \frac{1}{q^3}\right). \end{aligned}$$

В частности, $p_{2k}(2k) = \left(1 - \frac{1}{q}\right) p_{2k-2}(2k-1)$ при $k \geq 1$.

Доказательство непосредственно следует из леммы 6.

Теорема 2. Пусть $q = 2^m$, $m \geq 1$, $n = 2k + \varepsilon$, $\varepsilon \in \{0, 1\}$ и $0 < c < 1$ — произвольная константа. При $n \rightarrow \infty$ для ранга почти всех квадратичных форм f от n переменных при $n \rightarrow \infty$ справедлива оценка

$$2k \geq \text{rank}(f) \geq 2k - 2 \left\lceil \sqrt{\frac{1}{2} \log_q k} + \frac{c + (-1)^\varepsilon}{4} \right\rceil + 2.$$

Доказательство. В силу равенства (9) имеем

$$Q_{2r}(n) < \frac{q^2}{(q^{n-2r-1} - 1)(q^{n-2r} - 1)} Q_{2r+1}(n), \quad (10)$$

поэтому при $n = 2k$ и $1 \leq i \leq k$ справедлива оценка

$$\begin{aligned} \frac{Q_{2(k-i)}(2k)}{Q_{2k}(2k)} &< \frac{q^{2i}}{(q^2 - 1)(q^3 - 1)(q^4 - 1) \dots (q^{n-2(k-i)-1} - 1)(q^{n-2(k-i)} - 1)} = \\ &= \frac{q^{2i}}{(q^2 - 1)(q^3 - 1)(q^4 - 1) \dots (q^{2i-1} - 1)(q^{2i} - 1)}. \end{aligned}$$

Оценим долю квадратичных форм от n переменных ранга, не превышающего $2k - 2i$:

$$\begin{aligned} \sum_{j=0}^{k-i} Q_{2j}(2k) q^{-\frac{n(n-1)}{2}} &< \sum_{j=0}^{k-i} \frac{Q_{2j}(2k)}{Q_{2k}(2k)} < k \frac{Q_{2(k-i)}(2k)}{Q_{2k}(2k)} < \\ &< \frac{kq^{2i}}{(q^2 - 1)(q^3 - 1)(q^4 - 1) \dots (q^{2i-1} - 1)(q^{2i} - 1)}. \end{aligned}$$

Оценим логарифм этого выражения:

$$\begin{aligned} \log_q \left(\sum_{j=0}^{k-i} \frac{Q_{2j}(2k)}{Q_{2k}(2k)} \right) &< \log_q k + 2i - \sum_{m=2}^{2i} \log_q (q^m - 1) = \\ &= \log_q k + 2i - \sum_{m=2}^{2i} \left(m - \log_q \left(1 - \frac{1}{q^m} \right) \right) = \\ &= \log_q k + 2i - \frac{(2i+2)(2i-1)}{2} + \sum_{m=2}^{2i} \log_q \left(1 - \frac{1}{q^m} \right) < \end{aligned}$$

$$< \log_q k - 2i^2 + i + 1. \quad (11)$$

Положим $i = \left\lceil \sqrt{\frac{1}{2} \log_q k + \frac{c+1}{4}} \right\rceil$, где $c > 0$. При таком выборе при $k \rightarrow \infty$ выражение (11) стремится к $-\infty$:

$$\begin{aligned} \log_q k - 2i^2 + i + 1 &\leq \log_q k - 2 \left(\sqrt{\frac{1}{2} \log_q k + \frac{c+1}{4}} \right)^2 + \left\lceil \sqrt{\frac{1}{2} \log_q k + \frac{c+1}{4}} \right\rceil + 1 < \\ &< \log_q k - 2 \left(\frac{1}{2} \log_q k + 2 \sqrt{\frac{1}{2} \log_q k} \frac{c+1}{4} + \left(\frac{c+1}{4} \right)^2 \right) + \sqrt{\frac{1}{2} \log_q k} + \frac{c+1}{4} + 2 = \\ &= -c \sqrt{\frac{1}{2} \log_q k} + \frac{2c^2 + c + 1}{4} + 2. \end{aligned}$$

Поэтому для $n = 2k$ при $k \rightarrow \infty$ доля квадратичных форм ранга, меньшего чем $2k - \left\lceil \sqrt{\frac{1}{2} \log_q k + \frac{c+1}{4}} \right\rceil$, стремится к нулю.

При $n = 2k + 1$ и $1 \leq i \leq k$ рассуждаем аналогично. В силу неравенства (10) справедлива оценка

$$\begin{aligned} \frac{Q_{2(k-i)}(2k+1)}{Q_{2k}(2k+1)} &< \frac{q^{2i}}{(q^2-1)(q^3-1) \cdot \dots \cdot (q^{n-2(k-i)-1}-1)(q^{n-2(k-i)}-1)} = \\ &= \frac{q^{2i}}{(q^2-1)(q^3-1) \cdot \dots \cdot (q^{2i}-1)(q^{2i+1}-1)}. \end{aligned}$$

Аналогично получаем

$$\begin{aligned} \sum_{j=0}^{k-i} Q_{2j}(2k+1) q^{-\frac{n(n-1)}{2}} &< \sum_{j=0}^{k-i} \frac{Q_{2j}(2k+1)}{Q_{2k}(2k+1)} < k \frac{Q_{2(k-i)}(2k+1)}{Q_{2k}(2k+1)} < \\ &< \frac{k q^{2i}}{(q^2-1)(q^3-1) \cdot \dots \cdot (q^{2i}-1)(q^{2i+1}-1)}. \end{aligned}$$

Оценим логарифм этого выражения:

$$\begin{aligned} \log_q \left(\sum_{j=0}^{k-i} \frac{Q_{2j}(2k+1)}{Q_{2k}(2k+1)} \right) &< \log_q k - \sum_{m=2}^{2i+1} \log_q (q^m - 1) = \\ &= \log_q k + 2i - \sum_{m=2}^{2i+1} \left(i - \log_q \left(1 - \frac{1}{q^i} \right) \right) < \log_q k + 2i - \frac{(2i+3)2i}{2} = \log_q k - 2i^2 - i. \end{aligned}$$

Полагая $i = \left\lceil \sqrt{\frac{1}{2} \log_q k + \frac{c-1}{4}} \right\rceil$, получаем, что при $k \rightarrow \infty$ последнее выражение стремится к $-\infty$. Поэтому для $n = 2k + 1$ при $k \rightarrow \infty$ доля квадратичных форм ранга, меньшего чем $2k - 2 \left\lceil \sqrt{\frac{1}{2} \log_q k + \frac{c-1}{4}} \right\rceil$, стремится к нулю. ■

Можно изменить вид нижней оценки из теоремы 2, приблизив его к виду оценки из теоремы 1.

Следствие 1. Пусть $q = 2^m$, $m \geq 1$, $k = \lfloor n/2 \rfloor$ и $0 < c' < 1$ — произвольная константа. При $n \rightarrow \infty$ для ранга почти всех квадратичных форм f от n переменных при $n \rightarrow \infty$ справедлива оценка $\text{rank}(f) > n - \lceil \sqrt{2 \log_q n} + c' \rceil + 1$.

Действительно,

$$\begin{aligned} 2k - 2 \left\lceil \sqrt{\frac{1}{2} \log_q k} + \frac{c + (-1)^\varepsilon}{4} \right\rceil + 2 &\geq n - \left\lceil \sqrt{2 \log_q k} + \frac{c+1}{2} \right\rceil + 1 = \\ &= n - \left\lceil \sqrt{2 \log_q n - 2 \log_q \frac{n}{k}} + \frac{c+1}{2} \right\rceil + 1 > n - \left\lceil \sqrt{2 \log_q n} + \frac{c+1}{2} \right\rceil + 1. \end{aligned}$$

Приведём еще одно следствие из теоремы 2, содержащее нетривиальную асимптотическую нижнюю оценку наименьшего вершинного покрытия случайного простого, т.е. неориентированного без петель, графа. Хотя оценка представляется достаточно грубой, тем не менее автору не известно более точных результатов.

Следствие 2. Пусть $n = 2k + \varepsilon$, $\varepsilon \in \{0, 1\}$, и $c > 0$. Для почти всех простых графов с n вершинами величина наименьшего вершинного покрытия при $n \rightarrow \infty$ оценивается снизу величиной $\beta_0(G) \geq k - \left\lceil \sqrt{\frac{1}{2} \log_2 k} + \frac{c+(-1)^\varepsilon}{4} \right\rceil + 1$.

Доказательство. Каждому простому графу с n вершинами взаимно однозначно соответствует квадратичная форма от n переменных над полем из двух элементов, где каждому ребру (i, j) в графе соответствует одночлен $x_i x_j$, $1 \leq i < j \leq n$. При этом наименьшему вершинному покрытию графа соответствует такой набор переменных, фиксация которого произвольными значениями превращает квадратичную форму в функцию меньшей степени нелинейности. Так как наименьшее число одночленов второй степени у квадратичной формы ранга $r = 2s$ будет в её каноническом представлении (a)–(d), то число таких фиксаций ограничено снизу значением s , т.е. $\beta_0(G) \geq s$. Остаётся воспользоваться оценкой из теоремы 2. ■

ЛИТЕРАТУРА

1. Dixon L. E. Linear Groups with an Expositions to the Galois Field Theory. Leipzig: Publ. by B. G. Teubner, 1901.
2. Mullen G. L. and Panario D. Handbook of Finite Fields. CRC Press, A Chapman & Hall Book, 2013.
3. Дьедонне Ж. Геометрия классических групп. М.: Мир, 1974.
4. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. Бурбаки Н. Алгебра: модули, кольца, формы. М.: Наука, 1960.

REFERENCES

1. Dixon L. E. Linear Groups with an Expositions to the Galois Field Theory. Leipzig, Publ. by B. G. Teubner, 1901.
2. Mullen G. L. and Panario D. Handbook of Finite Fields. CRC Press, A Chapman & Hall Book, 2013.
3. D'edonne Zh. Geometriya klassicheskikh grupp [Geometry of Classical Groups]. Moscow, Mir Publ., 1974. (in Russian)
4. MacWilliams F. J. and Sloane N. J. A. The Theory of Error-Correcting Codes. North Holland, 1977.
5. Burbaki N. Algebra: moduli, kol'tsa, formy [Algebra: Modules, Rings Forms]. Moscow, Nauka Publ., 1960. (in Russian)