УДК 519.719.325 DOI 10.17223/2226308X/9/15

О РАСПРЕДЕЛЕНИИ РАНГА И ОЦЕНКЕ УРОВНЯ АФФИННОСТИ КВАДРАТИЧНЫХ ФОРМ

А. В. Черемушкин

Уровень аффинности двоичной функции определяется как минимальное число переменных, произвольная фиксация значений которых делает функцию аффинной. Обобщённый уровень аффинности определяется как минимальное число фиксаций линейных комбинаций переменных, некоторая фиксация значений которых делает функцию аффинной. Для квадратичной формы ранга $2r$ обобщённый уровень аффинности совпадает с r. Приводятся свойства распределения ранга случайной квадратичной формы и, как следствие, получается асимптотическая оценка обобщённого уровня аффинности квадратичных форм.

Ключевые слова: *двоичные функции, квадратичные формы, уровень аффинности.*

1. Распределение ранга квадратичных форм

Под квадратичной формой здесь понимается двоичная функция, степень нелинейности которой не превосходит двух. Каждую квадратичную форму от n переменных ранга $2r$, $1 \leqslant r \leqslant \lfloor n/2 \rfloor$, можно линейным преобразованием аргументов привести к виду

$$x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2r-1}x_{2r} \oplus l(x_1, \ldots, x_n),$$

где l — некоторая аффинная функция. Так как вид линейной функции l не влияет на значение ранга, то вероятность того, что квадратичная форма от n переменных имеет ранг $2r$, определяемую как относительную долю таких форм, можно записать в виде $p_{2r}(n) = Q_r(n)/2^{n(n-1)/2}$, где $Q_r(n)$ — число квадратичных форм от n переменных ранга $2r$. Из описания групп автоморфизмов квадратичных форм [1–3] следует, что

$$Q_r(n) = \frac{(2^n - 1)\ldots(2^n - 2^{2r-1})}{|\mathbf{Sp}(2r, 2)|},$$

где $\mathbf{Sp}(2r, 2)$ — симплектическая группа, имеющая прядок $|\mathbf{Sp}(2r, 2)| = 2^{r^2} \prod\limits_{i=1}^{r}(2^{2i} - 1)$.

При $1 \leqslant r \leqslant n/2 - 1$ справедливо соотношение

$$\frac{Q_r(n)}{Q_{r+1}(n)} = \frac{4}{(2^{n-2r} - 1)(2^{n-2r-1} - 1)} \left(1 - \frac{1}{2^{2r+2}}\right).$$

Поэтому числа $Q_r(n)$, $1 \leqslant r \leqslant n/2$, образуют монотонно возрастающую последовательность.

Оценим вероятность максимальности ранга.

При $n = 2k$ имеем

$$p_{2k}(2k) = \left(1 - \frac{1}{2^{2k-1}}\right)\left(1 - \frac{1}{2^{2k-3}}\right)\ldots\left(1 - \frac{1}{2}\right). \tag{1}$$

Аналогично при $n = 2k + 1$ имеем

$$p_{2k}(2k+1) = \left(1 - \frac{1}{2^{2k+1}}\right)\left(1 - \frac{1}{2^{2k-1}}\right)\ldots\left(1 - \frac{1}{2^3}\right).$$

В частности, $p_{2k-2}(2k-1) = 2p_{2k}(2k)$ при $k \geqslant 2$.

Верхнюю оценку вероятности $p_{2k}(2k)$ с наперёд заданной точностью можно получить путём перемножения только части сомножителей в произведении (1):

$$p_{2k}(2k) = \prod_{i=1}^{k}\left(1 - \frac{1}{2^{2i-1}}\right) < \prod_{i=1}^{14}\left(1 - \frac{1}{2^{2i-1}}\right) < 0{,}4194224428.$$

Нижнюю оценку вероятности $p_{2k}(2k)$ можно получить, используя подход из работы [4]:

$$\ln p_{2k}(2k) = \sum_{i=1}^{k}\ln\left(1 - \frac{1}{2^{2i-1}}\right) = -\sum_{i=1}^{k}\sum_{m=1}\frac{1}{m}\left(\frac{1}{2^{2i-1}}\right)^m =$$
$$= -\sum_{m=1}\frac{2^m}{m}\sum_{i=1}^{k}\left(\frac{1}{2^{2m}}\right)^i = -\sum_{m=1}\frac{2^{-m}}{m}\frac{1 - 1/(2^{2m})^k}{1 - 1/2^{2m}}.$$

При $k > s$ можно воспользоваться приближённой формулой

$$\ln p_{2k}(2k) > -\frac{2^{2m}}{2^{2m}-1}\ln 2 - \sum_{m=1}^{s-1}\frac{2^{-m}}{m}\left(\frac{1}{2^{2m}-1} - \frac{1}{2^{2r}-1}\right).$$

В частности, полагая $s = 8$, получаем, что при $k > 8$ имеет место нижняя оценка $p_{2k}(2k) > 0{,}41942244$. Поэтому при больших чётных $n = 2k$

$$0{,}4194224428 > p_{2k}(2k) > 0{,}41942244.$$

При больших нечетных $n = 2k+1$ получаем

$$0{,}8388448856 > p_{2k}(2k+1) = 2p_{2k+2}(2k+2) > 0{,}83884488.$$

Теорема 1. Пусть $k = [n/2]$, $n = 2k + \varepsilon$ и $0 \leqslant c \leqslant 1$. При $n \to \infty$ доля квадратичных форм от n переменных ранга меньшего, чем $2k - 2\left\lceil\sqrt{(\log_2 k)/2} + (c + (-1)^{\varepsilon})/2\right\rceil$, стремится к нулю. Поэтому для ранга почти всех квадратичных форм q от n переменных при $n \to \infty$ справедлива нижняя оценка:

$$r(q) \geqslant 2k - 2\left\lceil\sqrt{\frac{1}{2}\log_2 k} + \frac{c + (-1)^{\varepsilon}}{2}\right\rceil + 2.$$

Для математического ожидания ранга случайной квадратичной формы от n переменных можно привести следующую оценку.

Теорема 2. Пусть $k = [n/2]$. При $n \to \infty$ математическое ожидание ранга случайной квадратичной формы q от n переменных оценивается следующим образом:

1) при $n = 2k$ имеем

$$2k - 0{,}60196883564 < \mathrm{E}\, r(q) < 2k - 0{,}6019688356\,(1 - 1/2^n)\,;$$

2) при $n = 2k+1$ имеем

$$2k - 0{,}1625309417 < \mathrm{E}\, r(q) < 2k - 0{,}1625309415\,(1 - 1/2^n)\,.$$

2. Оценка уровня аффинности квадратичной формы

Уровень аффинности $\mathrm{la}(f)$ двоичной функции f определяется как минимальное число переменных, произвольная фиксация значений которых делает функцию аффинной. Обобщённый уровень аффинности $\mathcal{L}a(f)$ двоичной функции f определяется как минимальное число линейных комбинаций переменных, некоторая фиксация значений которых делает функцию аффинной. Эти параметры связаны неравенством [5] $\mathcal{L}a(f) \leqslant \mathrm{la}(f)$. Квадратичную форму от n переменных ранга $2r$ можно линейным преобразованием аргументов привести к виду

$$q(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2r-1}x_{2r} \oplus l(x_1, \ldots, x_n),$$

где $l(x_1, \ldots, x_n)$ — некоторая аффинная функция.

Поскольку обобщенный уровень аффинности квадратичной формы ранга $2r$ равен r, то из приведённых выше асимптотических оценок ранга вытекает

Следствие 1. Пусть $0 \leqslant c \leqslant 1$. При $n \to \infty$, $n = 2k + \varepsilon$, $0 \leqslant \varepsilon \leqslant 1$, доля квадратичных форм от n переменных, имеющих обобщённый уровень аффинности меньший, чем $k - \left\lceil \sqrt{(\log_2 k)/2} + (c + (-1)^{\varepsilon})/2 \right\rceil$, стремится к нулю. Для обобщённого уровня аффинности почти всех квадратичных форм от n переменных при $n \to \infty$ справедлива нижняя оценка:

$$\mathrm{la}(f) \geqslant \mathcal{L}a(f) \geqslant k - \left\lceil \sqrt{\frac{1}{2}\log_2 k} + \frac{c + (-1)^{\varepsilon}}{2} \right\rceil + 1.$$

Отсюда следует, что оценки уровня аффинности почти всех квадратичных форм из работы [5] не являются точными.

Следствие 2. Пусть $k = [n/2]$. При $n \to \infty$ математическое ожидание обобщённого уровня аффинности $\mathcal{L}a(q)$ случайной квадратичной формы q от n переменных оценивается следующим образом:

1) при чётных n

$$k - 0{,}30098441782 < \mathrm{E}\,\mathcal{L}a(q) < k - 0{,}3009844178\,(1 - 1/2^n)\,;$$

2) при нечётных n

$$k - 0{,}8126547085 < \mathrm{E}\,\mathcal{L}a(q) < k - 0{,}8126547075\,(1 - 1/2^n)\,.$$

ЛИТЕРАТУРА

1. *Dixon L. E.* Linear Groups with an Expositions to the Galois Field Theory. Leipzig: Publ. by B. G. Teubner, 1901.
2. *Дьедонне Ж.* Геометрия классических групп. М.: Мир, 1974.
3. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
4. *Рязанов Б. В., Чечета С. И.* О приближении булевой функции множеством случайных квадратичных форм // Дискретная математика. 1995. Т. 7. Вып. 3. С. 129–145.
5. *Буряков М. Л.* Асимптотические оценки уровня аффинности для почти всех булевых функций // Дискретная математика. 2008. Т. 20. Вып. 3. С. 73–79.