УДК 519.212.2, 519.214 DOI 10.17223/2226308X/11/15

# УЛУЧШЕННЫЕ АСИМПТОТИЧЕСКИЕ ОЦЕНКИ ДЛЯ ЧИСЛА КОРРЕЛЯЦИОННО-ИММУННЫХ ДВОИЧНЫХ ФУНКЦИЙ И ОТОБРАЖЕНИЙ

К. Н. Панков

Уточнена локальная предельная теорема для распределения части вектора весов подфункций линейных комбинаций координатных функций случайного двоичного отображения из векторного пространства $V_n$ двоичных $n$-мерных векторов в векторное пространство $V_m$. С помощью этой теоремы получена асимптотическая формула для $|K(m,n,k)|$ — числа корреляционно-иммунных порядка $k$ двоичных отображений в случае $n \to \infty$, $m \in \{2,3,4\}$ и $k(5+2\log_2 n)+6m \leqslant n\left(\frac{5}{18}-\gamma'\right)$ для произвольного $0<\gamma'<5/18$, $k=\mathrm{O}(n/\ln n)$:

$$\log_2 |K(m,n,k)| \sim m2^n + \left(\frac{n+1+\log_2 \pi}{2} - k\right)(2^m-1) - m2^{m-1} -$$
$$-(2^m-1)\left(\frac{n-k}{2}\binom{n}{k} + \log_2\sqrt{\frac{\pi}{2}}\sum_{s=0}^{k}\binom{n}{s}\right) + \left(2\cdot 3^{m-2}-1\right)\sum_{s=0}^{k}\binom{n}{s}.$$

Найдена улучшенная асимптотическая оценка для $|K(n,1,k)|$ в случае $n \to \infty$, $k < \frac{n}{\ln n}\left(\frac{\ln 2}{4}-\varepsilon\right)$ для произвольного $0<\varepsilon<\ln 2/4$:

$$\log_2 |K[n,1,k]| \sim 2^n - \frac{1}{2}\left((n-k)\binom{n}{k} - n\right) - k -$$
$$-\left(\frac{n-k}{2}\binom{n}{k} + \sum_{s=0}^{k}\binom{n}{s}\log_2\sqrt{\frac{\pi}{2}} - 1\right)\log_2\sqrt{\pi/2}.$$

**Ключевые слова:** *случайное двоичное отображение, локальная предельная теорема, веса подфункций, корреляционно-иммунные функции.*

К классам вектор-функций, изучения которых требуют задачи криптографического синтеза и анализа, относятся, в частности, корреляционно-иммунные отображения. Такие отображения могут использоваться при реализации шифрсистем, предназначенных для защиты информации в закрытых и гибридных сетях распределённых реестров [1].

Обозначим через $V_n$ множество двоичных векторов размерности $n$. В [2] доказано, что такое свойство двоичного отображения $f(\alpha)=(f_1(\alpha), f_2(\alpha), \ldots, f_m(\alpha)) : V_n \to V_m$, как корреляционная иммунность, сводится к обладанию этим свойством всеми ненулевыми линейными комбинациями координатных функций $f(\alpha)$, называемыми в [3] компонентными функциями или компонентами. Свойства компонент могут быть выражены в терминах весов их подфункций (в обозначениях [4]):

$$w_I^J(f) = \left\| \left(\psi_m(J), f\right)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1} \right\|,$$

где $f=(f_1,\ldots,f_m)$; $\|f_1\|$ — вес булевой функции $f_1$; $|J|$ — мощность множества $J=\{j_1,\ldots,j_{|J|}\} \subset \{1,\ldots,m\}$; $I=\{i_1,\ldots,i_{|I|}\} \subset \{1,\ldots,n\}$; $\psi_m(J)$ — двоичный вектор длины $m$, у которого на $j_1,\ldots,j_{|J|}$ координатах стоят единицы, а на остальных нули (в [5] $\psi_m(J)$ называется индикаторным вектором множества $J$); $(a,b)=a_1b_1 \oplus \ldots \oplus \oplus a_nb_n$ — скалярное произведение векторов $a$ и $b$ из $V_m$; $\left(\psi_m(J), f\right)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1}$ — подфункция

компоненты $(\psi_m(J), f)$ отображения $f$, получаемая, если у аргумента компоненты $(\psi_m(J), f)$ значения координат с номерами $i_1, \ldots, i_{|I|}$ положить равными единице.

В силу однозначной связи $w_I^J$ с коэффициентами статистической структуры, приведёнными в [6], их можно по аналогии назвать весовыми коэффициентами двоичного отображения. Из результатов работы [6] следует

**Определение 1.** Отображение $f$ из множества $B_n^m$ всех $m$-мерных двоичных функций от $n$ переменных называется корреляционно-иммунным порядка $k$, если для любого $J$, $\varnothing \neq J \subset \{1, \ldots, m\}$, существует такая величина $r_J \in \{-2^{n-k-1}, \ldots, 2^{n-k-1}\}$, что для любого $I \subset \{1, \ldots, n\}$, $|I| \leqslant k$, выполняется $w_I^J(f) = 2^{n-|I|-1} + r_J 2^{k-|I|}$.

Пусть функция $f$ выбирается случайно и равновероятно из множества $B_n^m$. Рассмотрим для этой функции вектор весов подфункций

$$\overline{W}_k(f) = \left(w_I^J(f) : \varnothing \neq J \subset \{1, \ldots, m\}, I \subset \{1, \ldots, n\}, |I| \leqslant k\right)$$

длины $N = N(n, m, k) = (2^m - 1) \sum\limits_{s=0}^{k} \binom{n}{s}$. Для упрощения записи введём следующие обозначения: $\exp_2 x = 2^x$; $\mathsf{E}\xi$ — математическое ожидание случайной величины $\xi$;

$$T = T(n, m, k) = \frac{n-k}{2}\binom{n}{k}(2^m - 1) + N(n, m, k)\log_2\sqrt{\frac{\pi}{2}}.$$

**Теорема 1.** Пусть при всех достаточно больших $n$ для произвольного $0<\gamma<1/3$ выполняется $k(5 + 2\log_2 n) + 6m \leqslant n(1/3 - \gamma)$, $Q = Q(n, m, k)$ — ковариационная матрица случайного вектора $(\overline{w} - \mathsf{E}\overline{w})\, 2^{-n/2-m+2}$, $z(n)\, 2^{n/2+m-2}$ — последовательность целочисленных вектор-столбцов размерности $N$, такая, что координаты векторов из последовательности $\mathsf{E}\overline{w} + z2^{n/2+m-2}$ удовлетворяют сравнениям из работы [4]

$$\sum_{\varnothing \neq S \subset J} (-1)^{|S|} w_I^S \equiv 0 \left(\mathrm{mod} 2^{|J|-1}\right).$$

Тогда равномерно относительно $z(n)$ верно равенство

$$\mathsf{P}\left(\overline{w} - \mathsf{E}\overline{w} = z2^{n/2+m-2}\right) = \theta_{15}(z)\exp\left(-0{,}1 \cdot 2^{-2^{n\gamma+m-\log_2 n}}\right) + \exp_2\left(-T(n, m, k)\right) \times$$

$$\times\left(\exp\left(-2^{2m-3}\sum_{\varnothing \neq J \subset \{1,\ldots,m\}}\ \sum_{I \subset \{1,\ldots,n\}, |I| \leqslant k}\left(\sum_{K \subset I}(-1)^{|K|}2^{|K|}z_K^J\right)^2\right)\left(1 + \theta_{12}(z)\, n^{-3/2}2^{-4m}\right) + \right.$$

$$\left. + \theta_{14}(z)\exp\left(-0{,}12 \cdot 2^{n\gamma+3k-\log_2 n}\right)\right)|\mathfrak{R}^{**}(m, N)|,$$

где $|\theta_{12}(z)| \leqslant 286{,}9$, $|\theta_{14}(z)| \leqslant 1$, $|\theta_{15}(z)| \leqslant 1$, $\mathbb{Z}$ — кольцо целых чисел, а множество $\mathfrak{R}^{**}(m, N)$ имеет вид

$$\mathfrak{R}^{**}(m, N) = \left\{\overrightarrow{r} \in \{0, 1, \ldots, 2^{m-1} - 1\}^N : \right.$$

$$\left.\forall I\, \forall s \in \{1, \ldots, m\}\, \forall \delta \in V_m\left(\sum_{J \subset \{1,\ldots,m\}, s \in J}(-1)^{(\delta, \psi_m(J)) \oplus 1} r_I^J \in 2^{m-1}\mathbb{Z}\right)\right\}.$$

Пусть $K(n, m, k)$ — множество всех корреляционно-иммунных порядка $k$ двоичных отображений.

**Следствие 1.** Пусть при всех достаточно больших $n$ для произвольного $0 < \gamma' < 5/18$ выполняется неравенство $k\,(5 + 2\log_2 n) + 6m \leqslant n\,(5/18 - \gamma')$. Тогда при $n \to \infty$ выполняется

$$\log_2 |K\,[n, m, k]| \sim m2^n + \left(\frac{n + 1 + \log_2 \pi}{2} - k\right)(2^m - 1) - \\ -m2^{m-1} - T\,(n, m, k) + \log_2 |\mathfrak{R}^{**}\,(m, N)|\,.$$

При $m \in \{2, 3, 4\}$ выполняется $\log_2 |\mathfrak{R}^{**}\,(m, N)| = N\,(n, 1, k)\,(2 \cdot 3^{m-2} - 1)$.

**Следствие 2.** В условиях теоремы 1 существует $n_0$, такое, что для любых $\varepsilon_1, \varepsilon_2 > 0$, $n > n_0$ верны неравенства

$$-\varepsilon_1\,(m-1)\sum_{s=0}^{k}\binom{n}{s} < \log_2 |K\,(n, m, k)| - m2^n\left(\frac{n + 1 + \log_2 \pi}{2} - k\right)(2^m - 1) + \\ +m2^{m-1} + T\,(n, m, k) < \varepsilon_2\,(m-2)\,(2^m - 1)\sum_{s=0}^{k}\binom{n}{s} + \sum_{s=0}^{k}\binom{n}{s}.$$

При $m = 1$ можно доказать более сильный результат, чем в следствии 1:

**Теорема 2.** Пусть $n \to \infty$ и при всех достаточно больших $n$ для произвольного $0 < \varepsilon < \dfrac{\ln 2}{4}$ выполняется неравенство $k < \dfrac{n}{\ln n}\left(\dfrac{\ln 2}{4} - \varepsilon\right)$. Тогда

$$|K\,[n, 1, k]| \sim \exp_2\left(2^n - \frac{1}{2}\left((n-k)\binom{n}{k} - n\right) - k - (T\,(n, 1, k) - 1)\log_2\sqrt{\pi/2}\right).$$

Полученные оценки уточняют или улучшают результаты работ [6–9], развивая результаты, анонсированные в [10].

## ЛИТЕРАТУРА


1. Развитие технологии распределенных реестров. Доклад для общественных консультаций. М.: Центральный банк Российской Федерации, 2017. `http://www.cbr.ru/analytics/ppc/Consultation_Paper_1712129(2).pdf`
2. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
3. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. N.Y.: Cambridge University Press, 2010. P. 398–472.
4. *Панков К. Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4. С. 14–30.
5. *Сачков В. Н.* Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013.
6. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82–95.
7. *Панков К. Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
8. *Панков К. Н.* Локальная предельная теорема для распределения части вектора весов подфункций компонент случайного двоичного отображения // Математические вопросы криптографии. 2014. № 3. С. 49–80.

9. *Canfield E. R., Gao Z., Greenhill C., et al.* Asymptotic enumeration of correlation-immune Boolean functions // Cryptography and Communications. 2010. No. 1. P. 111–126.
10. *Панков К. Н.* Уточнённые асимптотические оценки для числа $(n, m, k)$-устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.

УДК 519.7 DOI 10.17223/2226308X/11/16

# СВЯЗЬ ОДНОРОДНЫХ БЕНТ-ФУНКЦИЙ И ГРАФОВ ПЕРЕСЕЧЕНИЙ[1]

А. С. Шапоренко

Исследуется связь однородных бент-функций и графов пересечений $\Gamma_{(n,k)}$. Граф $\Gamma_{(n,k)}$ — граф, вершины которого соответствуют $\binom{n}{k}$ неупорядоченным подмножествам размера $k$ множества $\{1, \ldots, n\}$, две вершины соединены ребром в том и только в том случае, если соответствующие им подмножества имеют в точности один общий элемент. Выделены те $n$ и $k$, для которых справедливо, что в $\Gamma_{(n,k)}$ есть клики размера $k+1$. Выдвинуто предположение о том, что для таких $n$ и $k$ клики размера $k+1$ являются максимальными. Получено, что при $n = (k+1)k/2$ количество клик размера $k+1$ в графе $\Gamma_{(n,k)}$ равно $n!/(k+1)!$. Установлено, что однородные булевы функции, полученные путём взятия дополнения к кликам максимального размера в графах $\Gamma_{(10,4)}$ и $\Gamma_{(28,7)}$, не являются бент-функциями.

**Ключевые слова:** *графы пересечений, однородные бент-функции.*

Бент-функцией называется булева функция от $n$ переменных ($n$ чётно), такая, что расстояние Хэмминга от данной функции до множества всех аффинных функций является максимально возможным. Бент-функция называется однородной, если все одночлены её АНФ имеют одинаковые степени.

В [1] определён граф пересечений $\Gamma_{(n,k)}$, вершины которого соответствуют $\binom{n}{k}$ неупорядоченным подмножествам размера $k$ множества $\{1, \ldots, n\}$. Две вершины соединены ребром в том и только в том случае, если соответствующие подмножества имеют в точности один общий элемент. Будем называть дополнением к клике графа $\Gamma_{(n,k)}$ множество всех вершин этого графа, кроме тех, которые являются вершинами рассматриваемой клики.

В графе $\Gamma_{(6,3)}$ 20 вершин вида $\{a, b, c\}$, где $a, b, c \in \{1, \ldots, 6\}$ и различны. В этом графе были выделены клики размера 4 $(k+1)$ и, как указано в [1], такой размер клики является максимальным. Всего в графе $\Gamma_{(6,3)}$ 30 таких клик.

В $\Gamma_{(6,3)}$ дополнением к клике $C$ с вершинами $\{1, 3, 6\}$, $\{1, 4, 5\}$, $\{2, 3, 5\}$ и $\{2, 4, 6\}$ будет множество, состоящее из 16 вершин. Если мы будем сопоставлять вершинам $\{\ell, m, n\}$ одночлены $x_\ell x_m x_n$, то 16 вершин дополнения к клике $C$ будут соответствовать 16 одночленам АНФ однородной бент-функции от шести переменных степени 3 [2]. Поскольку таких клик 30 (равно как и однородных бент-функций от шести переменных степени 3 [2]), справедливо, что такие функции находятся во взаимно однозначном соответствии с дополнениями клик (максимальных) $C_i$ графа $\Gamma_{(6,3)}$, $i = 1, \ldots, 30$. Встаёт вопрос о возможности классификации однородных бент-функций от большего числа переменных с помощью выделения некоторого подмножества вершин графа $\Gamma_{(n,k)}$.

[1]Работа поддержана Министерством образования и науки (задание № 1.12875.2018/12.1).