

Теорему 3 можно использовать для вычисления моментов сумм

$$v_s^*(X_1, \dots, X_n) \stackrel{\text{def}}{=} \sum_{a_1, \dots, a_n=0}^1 I \left\{ w \left(\sum_{j=1}^n a_j X_j \right) = s \right\}, s \in \{0, 1, \dots, N\},$$

где $X_1, X_2, \dots, X_n \in B_N$ — независимые случайные векторы, распределения которых инвариантны относительно перестановок координат.

Теорема 4. Пусть $X_1, \dots, X_n$ — независимые случайные векторы, имеющие равномерное распределение на B_N^s , тогда

$$\mathbf{P}\{X_1, \dots, X_n \text{ линейно зависимы}\} \leq \frac{1}{2^N} \sum_{t=0}^N C_N^t \left[\left(1 + \frac{c_{N,s,t}}{C_N^s} \right)^n - n \frac{c_{N,s,t}}{C_N^s} - 1 \right],$$

где $c_{N,s,t} = \sum_{j \geq 0} (-1)^j C_t^j C_{N-t}^{s-j}$.

ЛИТЕРАТУРА

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

УДК 519.7

ОЦЕНКИ ЧИСЛА БУЛЕВЫХ ФУНКЦИЙ, ИМЕЮЩИХ АФФИННЫЕ И КВАДРАТИЧНЫЕ ПРИБЛИЖЕНИЯ ЗАДАННОЙ ТОЧНОСТИ¹

А. М. Зубков, А. А. Серов¹

Пусть $V_n = (\text{GF}(2))^n$. Обозначим через $\mathbb{F}_2^{V_n}$ множество всех булевых функций и через $\mathbb{L}_n$, $\mathbb{A}_n$ и $\mathbb{Q}_n$ — множества всех линейных, аффинных и квадратичных функций от n булевых аргументов соответственно; тогда $\mathbb{L}_n \subset \mathbb{A}_n \subset \mathbb{Q}_n$, $|\mathbb{L}_n| = 2^n$, $|\mathbb{A}_n| = 2^{n+1}$, $|\mathbb{Q}_n| = 2^{\binom{n}{2} + n + 1}$.

Пусть $\rho(f, g) = |\{x \in V_n : f(x) \neq g(x)\}|$ — расстояние Хэмминга между булевыми функциями $f, g \in \mathbb{F}_2^{V_n}$ и $\rho(f, A) = \min_{g \in A} \rho(f, g)$ для произвольных $f \in \mathbb{F}_2^{V_n}$ и $A \subset \mathbb{F}_2^{V_n}$.

В [1–3] показано, что если $f \in \mathbb{F}_2^{V_n}$ — случайная булева функция, имеющая равномерное распределение на $\mathbb{F}_2^{V_n}$, то для каждого фиксированного $x \in \mathbb{R}$

$$\lim_{n \rightarrow \infty} \mathbf{P} \left\{ \frac{\rho(f, \mathbb{L}_n) - a_n}{b_n} < x \right\} = 1 - e^{-e^x}, \quad \lim_{n \rightarrow \infty} \mathbf{P} \left\{ \frac{\rho(f, \mathbb{A}_n) - a_n}{b_n} < x - \ln 2 \right\} = 1 - e^{-e^x},$$

$$\lim_{n \rightarrow \infty} \mathbf{P} \left\{ \frac{\rho(f, \mathbb{Q}_n) - c_n}{d_n} < x \right\} = 1 - e^{-e^x},$$

где

$$a_n = 2^{n-1} - 2^{\frac{n-1}{2}} \sqrt{n \ln 2} \left(1 - \frac{\ln \ln 2^n + \ln 4\pi}{4n \ln 2} \right), \quad b_n = \frac{2^{\frac{n-1}{2}}}{2\sqrt{n \ln 2}},$$

$$c_n = 2^{n-1} - 2^{\frac{n-2}{2}} n \sqrt{\ln 2} \left\{ 1 + \frac{1}{2n} - \frac{4 \ln(\pi n^2 \ln 2) - \ln 2}{8n^2 \ln 2} \right\}, \quad d_n = \frac{2^{\frac{n-2}{2}}}{n\sqrt{\ln 2}}.$$

¹Работа поддержана грантом РФФИ, проект № 11-01-00139.

Из результатов [2, 3] следует, что если $\mathbb{F}_2^{V_n, \mathbb{A}_n}(r) = \{f \in \mathbb{F}_2^{V_n} : \rho(f, \mathbb{A}_n) \leq r\}$ и $\mathbb{F}_2^{V_n, \mathbb{Q}_n}(r) = \{f \in \mathbb{F}_2^{V_n} : \rho(f, \mathbb{Q}_n) \leq r\}$ — множества булевых функций, расстояния Хэмминга от которых до множеств $\mathbb{A}_n$ и $\mathbb{Q}_n$ соответственно не превосходят r , то для любого $\varepsilon > 0$

$$\begin{aligned} \lim_{n \rightarrow \infty} 2^{-2^n} \left| \mathbb{F}_2^{V_n, \mathbb{A}_n}(r_{n,1}^{+\varepsilon}) \right| &= \lim_{n \rightarrow \infty} 2^{-2^n} \left| \mathbb{F}_2^{V_n, \mathbb{Q}_n}(r_{n,2}^{+\varepsilon}) \right| = 0, \\ \lim_{n \rightarrow \infty} 2^{-2^n} \left| \mathbb{F}_2^{V_n, \mathbb{A}_n}(r_{n,1}^{-\varepsilon}) \right| &= \lim_{n \rightarrow \infty} 2^{-2^n} \left| \mathbb{F}_2^{V_n, \mathbb{Q}_n}(r_{n,2}^{-\varepsilon}) \right| = 1, \end{aligned}$$

где $r_{n,1}^{\pm\varepsilon} = 2^{n-1} - (1 \pm \varepsilon)\sqrt{2^{n-1}n \ln 2}$; $r_{n,2}^{\pm\varepsilon} = 2^{n-1} - (1 \pm \varepsilon)n\sqrt{2^{n-2} \ln 2}$.

Теорема 1 [4]. Если $n \geq 2$, то

$$(1 - Q_1(n, r))2^{n+1} \sum_{m=0}^r C_{2^n}^m \leq |\mathbb{F}_2^{V_n, \mathbb{A}_n}(r)| \leq 2^{n+1} \sum_{m=0}^r C_{2^n}^m, \quad (1)$$

где $Q_1(n, r) = 0$ при $0 \leq r < 2^{n-2}$,

$$Q_1(n, r) < \frac{1}{15} 2^{-(c^2 - \frac{3}{2})n} \exp \left\{ \frac{2(c^2 n)^{3/2}}{2^{n/2}} \right\}$$

при $n \geq 8$, $r = 2^{n-1} - c\sqrt{2^{n-1}n \ln 2} \geq 0$ и $c > 1$.

Следствие 1. Если $r_n = 2^{n-1} - c(n)\sqrt{2^{n-1}n \ln 2} \geq 0$, $c(n) > \sqrt{3/2}$ и $n \rightarrow \infty$, то

$$Q_1(n, r_n) \rightarrow 0.$$

Теорема 2. Если $n \geq 3$, то

$$(1 - Q_2(n, r))2^{\binom{n}{2} + n + 1} \sum_{m=0}^r C_{2^n}^m \leq |\mathbb{F}_2^{V_n, \mathbb{Q}_n}(r)| \leq 2^{\binom{n}{2} + n + 1} \sum_{m=0}^r C_{2^n}^m, \quad (2)$$

где $Q_2(n, r) = 0$ при $0 \leq r < 2^{n-3}$,

$$Q_2(n, r) < \frac{2^{-n^2(c^2-3)/6+n+1}}{n^2} \exp \left\{ \frac{(cn)^3}{7 \cdot 2^{n/2}} \right\}$$

при $n \geq 15$, $r = 2^{n-1} - cn\sqrt{2^{n-2} \ln 2} \geq 0$ и $c > 1$.

Следствие 2. Если $r_n = 2^{n-1} - c(n)n\sqrt{2^{n-2} \ln 2} \geq 0$, $c(n) > \sqrt{3}$ и $n \rightarrow \infty$, то

$$Q_2(n, r_n) \rightarrow 0.$$

Таким образом, если выполнены условия следствия 1 (следствия 2), то левые и правые части оценок (1) (оценок (2)) асимптотически эквивалентны.

ЛИТЕРАТУРА

1. *Ryasanov B. V.* Probabilistic methods in the theory of approximation of discrete functions // 3rd International Petrozavodsk Conference. 1993. P. 403–412.
2. *Рязанов Б. В., Чечёта С. И.* О приближении случайной булевой функции множеством квадратичных форм // Дискретная математика. 1995. № 3. С. 129–145.
3. *Серов А. А.* Предельное распределение расстояния между случайной булевой функцией и множеством аффинных функций // Теория вероятн. и ее примен. 2010. № 4. С. 791–795.

4. Зубков А. М., Серов А. А. Оценки числа булевых функций, имеющих аффинные приближения заданной точности // Дискретная математика. 2010. № 4. С. 3–19.

УДК 519.7

О НЕЛИНЕЙНОСТИ НЕКОТОРЫХ БУЛЕВЫХ ФУНКЦИЙ С МАКСИМАЛЬНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ

Н. А. Коломеец

После публикации работ [1, 2] большое внимание уделяется алгебраической иммунности булевых функций. Алгебраическая иммунность булевой функции f (обозначается через $AI(f)$) — это минимальная положительная алгебраическая степень булевой функции, аннулирующей f или $f \oplus 1$, т. е.

$$AI(f) = \min_{g \neq 0} \{ \deg(g) : \forall x f(x)g(x) = 0 \text{ или } \forall x (f(x) \oplus 1)g(x) = 0 \}.$$

Известно, что для функции f от n переменных $AI(f) \leq \lceil n/2 \rceil$. Для криптографических приложений наибольший интерес представляют функции с максимально возможной алгебраической иммунностью, т. е. с $AI(f) = \lceil n/2 \rceil$ (такое значение алгебраической иммунности достижимо для любого n).

В данной работе исследуется нелинейность функций, обладающих максимально возможной алгебраической иммунностью, а именно: рассматриваются функции, построенные с помощью одной из самых простых конструкций для чётного числа переменных, которая предложена D. K. Dalai и др. в работе [3]:

$$f(x) = \begin{cases} 0, & \text{wt}(x) < n/2, \\ b \in \{0, 1\}, & \text{wt}(x) = n/2, \\ 1, & \text{wt}(x) > n/2, \end{cases} \quad (1)$$

где n — количество переменных (n чётно); $\text{wt}(x)$ — вес Хэмминга вектора x . Все такие функции обладают алгебраической иммунностью $n/2$.

Нелинейностью булевой функции f (обозначается через $nl(f)$) называется расстояние Хэмминга от функции f до класса аффинных функций (функций вида $a_1x_1 \oplus \dots \oplus a_nx_n \oplus a_0$). Это также одно из важнейших криптографических свойств булевых функций.

Получена следующая верхняя оценка нелинейности функций вида (1).

Теорема 1. Для функций f вида (1) выполняется

$$nl(f) \leq 2^{n-1} - \binom{n-1}{n/2}.$$

В той же работе [3] рассматривается нелинейность функций, полученных с помощью данной конструкции, а именно доказано

Утверждение 1 (Dalai и др. [3]). Для функции

$$f(x) = \begin{cases} 0, & \text{wt}(x) \leq n/2, \\ 1, & \text{wt}(x) > n/2 \end{cases}$$

от n переменных (n чётно) верно

$$nl(f) = 2^{n-1} - \binom{n-1}{n/2}.$$