УДК 519.7

А.Н. АЛЕКСЕЙЧУК

УЛУЧШЕННАЯ ВЕРХНЯЯ ГРАНИЦА ДЛЯ ОТНОСИТЕЛЬНОГО РАССТОЯНИЯ МЕЖДУ БУЛЕВОЙ ФУНКЦИЕЙ И МНОЖЕСТВОМ *k*-МЕРНЫХ ФУНКЦИЙ

Аннотация. Доказана теорема, улучшающая ранее известную верхнюю границу для относительного расстояния между булевой функцией от n пременных и множеством k-мерных функций, $k < n$. Доказательство базируется на применении неравенства Бонами–Бекнера.

Ключевые слова: корреляционный криптоанализ, k-мерная булева функция, бент-функция, преобразование Уолша–Адамара, неравенство Бонами–Бекнера.

Введем следующие обозначения: V_n — множество двоичных векторов длины n; $B_n = \{f \mid f : V_n \to \{0,1\}\}$ — множество булевых функций от n переменных; $\# M$ — мощность множества M; $d(f,g) = 2^{-n} \# \{x \in V_n : f(x) \neq g(x)\}$ — относительное расстояние между функциями $f, g \in B_n$; $d(f,U) = \min\limits_{g \in U} d(f,g)$ — относительное расстояние от функции $f \in B_n$ до множества $U \subseteq B_n$.

Как обычно, множество V_n отождествляется с векторным пространством размерности n над полем $F = \mathbf{GF}(2)$. При этом сумма векторов $\alpha = (\alpha_1, \ldots, \alpha_n)$, $x = (x_1, \ldots, x_n) \in V_n$ определяется по формуле $\alpha \oplus x = (\alpha_1 \oplus x_1, \ldots, \alpha_n \oplus x_n)$, а булево скалярное произведение — по формуле $\alpha x = \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n$ (здесь и далее символ $\oplus$ обозначает операцию сложения как элементов поля F, так и векторов над ним).

Обозначим $F_{n \times k}$ множество матриц размера $n \times k$ над полем F, $L_{n,k}$ — совокупность всех k-мерных подпространств векторного пространства V_n, $k = 0, 1, \ldots, n$. Для любых $f \in B_n$, $H \in L_{n,k}$ положим

$$\hat{f}(\alpha) = 2^{-n} \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha x}, \quad \alpha \in V_n, \tag{1}$$

$$\omega_f(H) = \sum_{x \in H} \hat{f}(x)^2,$$

$$l_f(H) = 2^{-k} \sum_{s \in V_k} \left| \sum_{x \in H} \hat{f}(x)(-1)^{\alpha_s x} \right|,$$

где α_s $(s \in V_k)$ — представители всех попарно различных смежных классов векторного пространства V_n по подпространству $H^{\perp}$, дуальному к H.

Числа (1) называются нормированными коэффициентами Уолша–Адамара функции f. Отметим, что согласно равенству Парсеваля $\omega_f(V_n) = 1$. Кроме того, справедливо равенство (см., например, лемму 2.40 в [1])

$$\sum_{x \in H} \hat{f}(x)(-1)^{\alpha_s x} = 2^{-(n-k)} \sum_{x \in H^{\perp}} (-1)^{f(x \oplus \alpha_s)}, \quad H \in L_{n,k}, \tag{2}$$

из которого следует, что $l_f(H) \le 1$.

Функция $g \in B_n$ называется k-мерной [2, 3], $k = 1, 2, \ldots, n-1$, если она допускает представление в виде

$$g(x) = \varphi(xA), \ x \in V_n, \tag{3}$$

где $\varphi \in B_k$, $A \in F_{n \times k}$.

Обозначим $B_{n,k}$ множество всех k-мерных функций от n переменных. Для любого $H \in L_{n,k}$ обозначим $B_{n,k}(H)$ множество всех функций $g \in B_{n,k}$, допускающих представление в виде (3), для которого столбцы матрицы A порождают подпространство H. Справедливо равенство

$$B_{n,k} = \bigcup_{H \in L_{n,k}} B_{n,k}(H). \tag{4}$$

Свойства k-мерных функций, в том числе связанные с возможностью их применения при построении корреляционных атак на поточные шифры, изучались в [2–9] и ряде других работ. Поскольку эффективность таких атак зависит от величины относительного расстояния между функцией $f \in B_n$ и множеством $B_{n,k}$ (при умеренных по сравнению с n значениях k), важной задачей является нахождение оценок данного параметра.

В [9] показано, что для любых $f \in B_n$, $H \in L_{n,k}$, $k = 1, 2, \ldots, n-1$, справедливы следующие соотношения:

$$d(f, B_{n,k}(H)) = 1/2 \cdot (1 - l_f(H)), \tag{5}$$

$$1/2 \cdot (1 - (\omega_f(H))^{1/2}) \le d(f, B_{n,k}(H)), \tag{6}$$

$$d(f, B_{n,k}(H)) \le 1/2 \cdot (1 - \omega_f(H)) \tag{7}$$

(отметим, что формулы для точного значения параметра $d(f, B_{n,k}(H))$ и его нижней границы, аналогичные соотношениям (5) и (6) соответственно, приведены без доказательства в [6]). Из формул (4), (6), (7) следуют неравенства

$$1/2 \cdot \left(1 - \max_{H \in L_{n,k}} (\omega_f(H))^{1/2} \right) \le d(f, B_{n,k}) \le 1/2 \cdot \left(1 - \max_{H \in L_{n,k}} \omega_f(H) \right), \tag{8}$$

позволяющие оценивать относительное расстояние между функцией $f \in B_n$ и множеством всех k-мерных функций от n переменных.

Основным результатом настоящей статьи является теорема, существенно уточняющая верхнюю границу (8) для функций $f \in B_n$ с малым значением параметра $\max_{\alpha \in V_n} |\hat{f}(\alpha)|$.

Прежде чем сформулировать эту теорему, приведем два вспомогательных утверждения. Первое представляет собой известное неравенство Бонами–Бекнера [10].

Лемма 1. Для любых $g: V_n \to \mathbf{R}$, $\delta \in [0, 1]$ справедливо неравенство

$$\left(2^{-k} \sum_{s \in V_k} |g(s)|^{1+\delta} \right)^{\frac{2}{1+\delta}} \ge \sum_{\alpha \in V_k} \delta^{\|\alpha\|} C_g(\alpha)^2,$$

где $C_g(\alpha) = 2^{-k} \sum_{s \in V_k} g(s)(-1)^{s\alpha}$, $\|\alpha\|$ — вес Хэмминга вектора $\alpha \in V_k$.

Лемма 2. Пусть $f \in B_n$, $H \in L_{n,k}$, $k = 1, 2, \ldots, n-1$, и

$$T \overset{\text{def}}{=} k^{-1} \ln \left(\max_{\alpha \in V_n} |\hat{f}(\alpha)| \right)^{-1} - 2^{-1} \ln 2 \ge 1. \qquad (9)$$

Тогда

$$l_f(H) \ge (\omega_f(H))^{\frac{1}{2}\left(1 + \frac{\sqrt{2T-1}}{T}\right)}. \qquad (10)$$

Доказательство. Применим лемму 1 к функции $g(s) = \sum_{x \in H} \hat{f}(x)(-1)^{\alpha_s x}$, где α_s — представители всех попарно различных смежных классов векторного пространства V_n по подпространству $H^{\perp}$, $s \in V_k$.

Заметим, что на основании равенства (2) $|g(s)| \le 1$ для любого $s \in V_k$. Кроме того, если A — произвольная $n \times k$-матрица, столбцы которой образуют базис векторного пространства H, то $g(s) = \sum_{y \in V_k} \hat{f}(Ay)(-1)^{sy}$, $s \in V_k$, и, следовательно,

$$C_g(\alpha) = \sum_{y \in V_k} \hat{f}(Ay) \left(2^{-k} \sum_{s \in V_k} (-1)^{s(\alpha \oplus y)} \right) = \hat{f}(A\alpha), \ \alpha \in V_k.$$

Отсюда на основании леммы 1 находим, что

$$l_f(H) = 2^{-k} \sum_{s \in V_k} |g(s)| \ \ge \ 2^{-k} \sum_{s \in V_k} |g(s)|^{1+\delta} \ge \left(\sum_{\alpha \in V_k} \delta^{\|\alpha\|} \hat{f}(A\alpha)^2 \right)^{\frac{1+\delta}{2}} \ge$$

$$\ge \left(\delta^k \sum_{\alpha \in V_k} \hat{f}(A\alpha)^2 \right)^{\frac{1+\delta}{2}} = (\delta^k \omega_f(H))^{\frac{1+\delta}{2}}, \ \delta \in [0, 1].$$

Полагая в приведенных соотношениях $\delta = (1+x)^{-1}$ и применяя неравенство $(1+x)^{-k} \ge e^{-kx}$, $x \ge 0$, получаем

$$l_f(H) \ge (e^{-kx} \omega_f(H))^{\frac{2+x}{2(1+x)}}, \ x \ge 0. \qquad (11)$$

Положим $\theta = \dfrac{2k}{\ln(\omega_f(H)^{-1})}$ и заметим, что в силу условия (9) справеливы соотношения $\omega_f(H) = \sum_{\alpha \in H} \hat{f}(\alpha)^2 \le 2^k \max_{\alpha \in V_n} |\hat{f}(\alpha)|^2 = e^{-2kT}$, $T \ge 1$, из которых следует, что

$$\theta \le T^{-1} \le 1. \qquad (12)$$

Далее запишем неравенство (11) в виде

$$l_f(H) \ge \exp\{-1/2 \cdot \ln(\omega_f(H)^{-1}) h(x)\}, \qquad (13)$$

где $h(x) = \left(1 + \dfrac{\theta x}{2}\right)\left(1 + \dfrac{1}{1+x}\right)$, $x \ge 0$. Заметим, что

$$h(x)=1+\frac{\theta(1+x)}{2}+\left(1-\frac{\theta}{2}\right)\cdot\frac{1}{1+x}\ \ge\ 1+2\sqrt{\frac{\theta}{2}\left(1-\frac{\theta}{2}\right)},\ x\ge 0\,;$$

при этом последнее неравенство обращается в равенство тогда и только тогда, когда $x=x_0=\sqrt{2\theta^{-1}-1}$ (отметим, что в силу (12) точка x_0 определена корректно).

Теперь, полагая в формуле (13) $x=x_0$, получаем

$$l_f(H)\ge\exp\left\{-1/2\cdot\ln(\omega_f(H)^{-1})\left(1+2\sqrt{\frac{\theta}{2}\left(1-\frac{\theta}{2}\right)}\right)\right\}.$$

Наконец, поскольку функция $1+2\sqrt{\frac{\theta}{2}\left(1-\frac{\theta}{2}\right)}=1+\sqrt{\theta(2-\theta)}$ возрастает при $\theta\in[0,1]$, на основании (12) справедливо неравенство

$$l_f(H)\ge\exp\{-1/2\cdot\ln(\omega_f(H)^{-1})(1+\sqrt{T^{-1}\,(2-T^{-1})})\}=(\omega_f(H))^{\frac{1}{2}\left(1+\frac{\sqrt{2T-1}}{T}\right)}.$$

Итак, формула (10), а вместе с ней и лемма доказаны.

Непосредственно из леммы 2 и соотношений (4)–(7) следует следующий результат.

Теорема. Для любых $f\in B_n$, $H\in L_{n,k}$, $k=1,2,\dots,n-1$, справедливы неравенства

$$1/2\cdot(1-(\omega_f(H))^{1/2})\le d(f,B_{n,k}(H))\le 1/2\cdot(1-(\omega_f(H))^{1/2\cdot(1+\nu(T))}),\quad(14)$$

где

$$T=k^{-1}\ln\left(\max_{\alpha\in V_n}|\hat f(\alpha)|\right)^{-1}-2^{-1}\ln 2,\ \nu(T)=\begin{cases}\dfrac{\sqrt{2T-1}}{T}, & \text{если } T\ge 1;\\ 1 & \text{в противном случае.}\end{cases}$$

Кроме того,

$$1/2\cdot\left(1-\max_{H\in L_{n,k}}(\omega_f(H))^{1/2}\right)\le d(f,B_{n,k})\le$$

$$\le 1/2\cdot\left(1-\max_{H\in L_{n,k}}(\omega_f(H))^{1/2(1+\nu(T))}\right).\quad(15)$$

Отметим, что $\nu(T)<1$, если $T>1$. Поэтому верхние границы параметров $d(f,B_{n,k}(H))$ и $d(f,B_{n,k})$ в выражениях (14) и (15) более точные по сравнению с оценками (7) и (8) соответственно.

Приведем два следствия полученной теоремы.

Следствие 1. Пусть $f_n\in B_n$, $k_n\in\{1,2,\dots,n-1\}$, $n=2,3,\dots$, и

$$k_n=o\left(\ln\left(\max_{\alpha\in V_n}|\hat f_n(\alpha)|\right)^{-1}\right),\ n\to\infty.$$

Тогда

$$\lim_{n\to\infty}\frac{\ln(1-2d(f_n,B_{n,k_n}))}{\ln\left(\max_{H\in L_{n,k_n}}(\omega_{f_n}(H))\right)}=\frac{1}{2}.$$

Напомним, что функция $f \in B_n$ называется бент-функцией, если $|\hat{f}(\alpha)| = 2^{-n/2}$ для любого $\alpha \in V_n$ [1].

Следствие 2. Пусть f — бент-функция от n переменных, $k = 1, 2, \ldots, n-1$, и

$$T = \frac{n}{2k} - \frac{\ln 2}{2} \geq 1. \tag{16}$$

Тогда

$$1/2 \cdot (1 - 2^{(k-n)/2}) \leq d(f, B_{n,k}) \leq 1/2 \cdot \left(1 - 2^{\frac{k-n}{2}\left(1 + \frac{\sqrt{2T-1}}{T}\right)}\right). \tag{17}$$

Отметим, что неравенство (16) выполняется при $n \geq 2{,}7k$. Оценка параметра $d(f, B_{n,k})$ для бент-функции $f \in B_n$, равносильная нижней границе (17), приведена без доказательства в работе [6], где указаны также необходимые и достаточные условия, при которых эта оценка достигается. Вопрос о точном значении параметра $\max_f \{d(f, B_{n,k})\}$ при $2 \leq k \leq n-2$, где f пробегает множество всех бент-функций от n переменных, в настоящее время не решен.

СПИСОК ЛИТЕРАТУРЫ

1. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.
2. Gopalan P., O'Donnel R., Servedio A., Shpilka A., Wimmer K. Testing Fourier dimensionality and sparsity // SIAM J. on Computing. — 2011. — **40**, N 4. — P. 1075–1100.
3. Gopalan P. A Fourier-analytic approach to Reed–Muller decoding // Annual IEEE Symp. on Foundation in Computer Science. FOCS 2010, Proceedings. — Berlin: Springer-Verlag, 2010. — P. 685–694.
4. Lechner R.L. Harmonic analysis of switching functions // Recent Developments in Switching Theory. — New-York: Academic Press, 1971. — P. 122–228.
5. Dawson E., Wu C.K. Construction of correlation immune Boolean functions // Information and Communication Security, Proceedings. — Berlin: Springer-Verlag, 1997. — P. 170–180.
6. Canteaut A. On the correlations between a combining function and function of fewer variables // The 2002 IEEE Information Theory Workshop, Proceedings. — Berlin: Springer-Verlag, 2002. — P. 78–81.
7. Алексеев Е.К. О некоторых мерах нелинейности булевых функций // Прикладная дискретная математика. — 2011. — № 2(12). — С. 5–16.
8. Алексейчук А.Н., Конюшок С.Н. Усовершенствованный тест k-мерности для булевых функций // Кибернетика и системный анализ. — 2013. — № 2. — С. 27–35.
9. Алексейчук А.Н., Конюшок С.Н. Алгебраически вырожденные приближения булевых функций // Кибернетика и системный анализ. — 2014. — **50**, № 6. — С. 3–14.
10. De Wolf R. A brief introduction to Fourier analysis on the Boolean cube // Theory of Comput. Library. — 2008. — N 1. — P. 1–20.

Поступила 21.02.2015