КИБЕРНЕТИКА

А.Н. АЛЕКСЕЙЧУК, С.Н. КОНЮШОК

УДК 519.7

АЛГЕБРАИЧЕСКИ ВЫРОЖДЕННЫЕ ПРИБЛИЖЕНИЯ БУЛЕВЫХ ФУНКЦИЙ

Аннотация. Исследуются свойства k-мерных приближений булевых функций. Одним из основных результатов является теорема о строении k-мерных функций степени d, находящихся на расстоянии не более $2^{n-d}(1-\varepsilon)$, $\varepsilon \in (0,1)$, от заданной булевой функции n переменных, $1 \le d \le k \le n$, $\varepsilon \in (0,1)$. Эта теорема существенно усиливает ранее известный результат П. Гопалана и позволяет заметно повысить эффективность предложенного им алгоритма построения всех указанных k-мерных булевых функций.

Ключевые слова: корреляционный криптоанализ, вырожденная булева функция, k-мерная функция, преобразование Уолша–Адамара, нахождение k-мерных приближений булевых функций.

ВВЕДЕНИЕ

Булева функция $g: \{0,1\}^n \to \{0,1\}$ $(0 \le k \le n)$ называется k-мерной [1, 2], если существуют функция $\varphi: \{0,1\}^k \to \{0,1\}$ и $n \times k$-матрица A над полем из двух элементов такие, что для любого $x \in \{0,1\}^n$ выполняется равенство $g(x) = \varphi(xA)$. Функция g называется алгебраически вырожденной, если она является k-мерной для некоторого $k < n$, и невырожденной — в противном случае [3–5].

Первые результаты о корреляционных свойствах алгебраически вырожденных булевых функций относятся к 70-м годам прошлого века [3]. В настоящее время интерес к исследованию этих функций обусловлен задачами криптоанализа и теории кодирования. Отметим работы [6–8], в которых описан ряд атак на генераторы гаммы поточных шифров, функции усложнения которых являются алгебраически вырожденными или близки к таковым.

Обозначим $B_{n,k}$ множество всех k-мерных булевых функций от n переменных. В [5] исследованы приближения булевых функций функциями из множества $B_{n,n-1}$; в частности, найдено расстояние между произвольной функцией $f: \{0,1\}^n \to \{0,1\}$ и множеством алгебраически вырожденных функций от n переменных, указан способ нахождения функций, ближайших к f во множестве $B_{n,n-1}$, и получены оценки их порядков (в [4, 5] порядком вырожденности функции $g \in B_{n,n-1}$ называется наибольшее число $n-k$, для которого g является k-мерной функцией).

Изучению k-мерных приближений булевых функций при всех возможных значениях k посвящены работы [1, 2, 9–11], причем в [2] рассматриваются функции над произвольным конечным полем.

В [1] предложен вероятностный алгоритм распознавания свойства k-мерности. Для любой функции $f: \{0,1\}^n \to \{0,1\}$, заданной с помощью оракула, и чисел $k \in \{0,1,\dots,n-1\}$, $\varepsilon \in (0,1)$ этот алгоритм позволяет проверить гипотезу H_0: $f \in B_{n,k}$ относительно альтернативы H_1, состоящей в том, что f находится на расстоянии не менее $2^n \varepsilon$ от множества k-мерных функций, за $O(n 2^{2k} k \varepsilon^{-1})$ двоичных операций. Более эффективный тест k-мерности, трудоемкость которого составляет $O(n\, 2^k k^2\, \varepsilon^{-1})$ двоичных операций, предложен в [10].

Для построения эффективных атак на симметричные криптосистемы необходимо находить k-мерные функции, достаточно близкие к заданной функции $f: \{0,1\}^n \to \{0,1\}$. При этом наибольший интерес представляет случай, когда f задается с помощью оракула, n велико (например, $n \ge 64$), а k — ма́ло (фиксировано или медленно увеличивается с ростом n). Эффективность решения этой задачи существенно зависит от расстояния между функцией f и ее искомыми приближениями.

Пусть g — k-мерная функция от n переменных, находящаяся от функции f на расстоянии не более $2^{n-(k+1)}(1-\varepsilon)$, $\varepsilon \in (0,1)$ (отметим, что функция g определяется этим условием однозначно). В [1] предложен вероятностный алгоритм, позволяющий находить g по заданным f, k и ε с вероятностью не менее $1-\delta$, $\delta \in (0,1)$, за $O(2^{4k} n^2 \varepsilon^{-2} \log(2^{2k} n\delta^{-1}))$ двоичных операций. В [11] представлен другой алгоритм, двоичная сложность которого равна $O(2^{2k} k^{-2} n^3 \varepsilon^{-2} \delta^{-1} \log(2^{2k} k^{-1} n\delta^{-1}\varepsilon^{-1}))$.

Задача определения всех функций $g \in B_{n,k}$, находящихся от заданной функции $f: \{0,1\}^n \to \{0,1\}$ на расстоянии, не превышающем $2^{n-k}(1-\varepsilon)$, $\varepsilon \in (0,1)$, является более трудной. Существенный вклад в ее решение сделан в работе [2], посвященной изучению k-мерных приближений функций от n переменных над произвольным конечным полем. Одним из основных результатов этой работы является теорема, описывающая строение k-мерных функций степени не выше d над полем $\mathbf{GF}(q)$, находящихся от заданной функции $f: \mathbf{GF}(q)^n \to \mathbf{GF}(q)$ на расстоянии не более $\delta_q(d)(1-\varepsilon)$, где $\delta_q(d)$ — минимальное расстояние кода Рида–Маллера $\mathbf{RM}_q(n,d)$, $1 \le d \le k$, $\varepsilon \in (0,1)$ (см. [2, п. 4]). В настоящей статье доказана теорема, существенно усиливающая этот результат для случая булевых функций. Получен также ряд утверждений о свойствах k-мерных приближений булевых функций, дополняющих и уточняющих отдельные результаты работ [5, 9].

ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ПОНЯТИЙ И НЕКОТОРЫЕ ВСПОМОГАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Обозначим V_n множество двоичных векторов длины n. Это множество является векторным пространством размерности n над полем $F = \mathbf{GF}(2)$ (при $n = 0$ полагаем $V_0 = \{0\}$). 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 ниже символ $\oplus$ обозначает операцию сложения как элементов поля F, так и векторов над этим полем).

В дальнейшем используются следующие обозначения: $\# M$ — мощность множества M; $< M >$ — подпространство, порожденное множеством $M \subseteq V_n$; $F_{n\times k}$ — множество матриц размера $n \times k$ над полем F; $C(A)$ — подпространство векторного пространства V_n, порожденное столбцами матрицы $A \in F_{n\times k}$.

Для любого множества $M \subseteq V_n$ обозначим $M^{\perp}$ подпространство, дуальное к M: $M^{\perp} = \{\alpha \in V_n \mid \forall x \in M: \alpha x = 0\}$; для любых $a, b \in \mathbf{Z}$ положим $\overline{a,b} = \{i \in \mathbf{Z}: a \le i \le b\}$.

Обозначим B_n множество булевых функций от n переменных. Относительное расстояние между функциями $f, g \in B_n$ определяется по формуле $d(f,g) = 2^{-n} \# \{x \in V_n: f(x) \ne g(x)\}$, а относительное расстояние от функции $f \in B_n$ до множества $U \subseteq B_n$ — по формуле $d(f,U) = \min\limits_{g \in U} d(f,g)$. Число $wt(f) = 2^{-n} \# \{x \in V_n: f(x) = 1\}$ называется относительным весом функции $f \in B_n$. Булева функция называется уравновешенной, если ее относительный вес равен $1/2$.

Обозначим $\deg f$ степень полинома Жегалкина функции $f \in B_n$. Доказательство следующей леммы можно найти в [12, теорема 5.5].

Лемма 1. Пусть $f \in B_n \setminus \{0\}$. Тогда $wt(f) \ge 2^{-\deg f}$.

Для любой функции $f \in B_n$ положим

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

$$D_\alpha f(x) = f(x \oplus \alpha) \oplus f(x), \; x \in V_n, \tag{2}$$

$$I_f = \{\alpha \in V_n : D_\alpha f \equiv 0\}.$$

Числа в (1) называются нормированными коэффициентами Уолша–Адамара функции f, а функция (2) — ее производной по направлению $\alpha \in V_n$ [12].

Для любого $k \in \overline{0, n}$ обозначим $\mathcal{L}_{n,k}$ множество всех k-мерных подпространств векторного пространства V_n. Положим

$$\omega_f(H) = \sum_{x \in H} \hat{f}(x)^2, \; H \in \mathcal{L}_{n,k}. \tag{3}$$

Для любого $L \in \mathcal{L}_{n,n-k}$ обозначим $L_s = L \oplus \alpha_s$, $s \in V_k$, все попарно различные смежные классы пространства V_n по подпространству L. Справедливы следующие соотношения [12, теорема 2.89, лемма 2.4]:

$$\omega_f(H) = 2^{-(n-k)} \sum_{\alpha \in H^\perp} 2^{-n} \sum_{x \in V_n} (-1)^{D_\alpha f(x)}, \; H \in \mathcal{L}_{n,k}, \tag{4}$$

$$2^{-(n-k)} \sum_{x \in L_s} (-1)^{f(x)} = \sum_{x \in L^\perp} \hat{f}(x)(-1)^{\alpha_s x}, \; L \in \mathcal{L}_{n,n-k}, \; s \in V_k. \tag{5}$$

При $k = n$ из формулы (4) вытекает равенство Парсеваля:

$$\omega_f(V_n) = \sum_{x \in V_n} \hat{f}(x)^2 = 1.$$

Определение 1 [1, 2]. Функция $g \in B_n$ называется k-мерной, $k \in \overline{0, n}$, если она допускает представление в виде

$$g(x) = \varphi(xA), \; x \in V_n, \tag{6}$$

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

Обозначим $B_{n,k}$ множество всех k-мерных функций от n переменных, положим $B_{n,-1} = \varnothing$. Справедливы соотношения

$$B_{n,0} \subseteq B_{n,1} \subseteq \ldots \subseteq B_{n,n-1} \subseteq B_{n,n};$$

при этом множество $B_{n,0}$ состоит из двух функций-констант, множество $B_{n,1}$ совпадает с классом аффинных функций, а множество $B_{n,n}$ — с совокупностью всех булевых функций от n переменных. Функции из множества $B_{n,n-1}$ называются алгебраически вырожденными, а функции из множества $B_n \setminus B_{n,n-1}$ — невырожденными [3–5].

Определение 2. Назовем функцию $g \in B_n$ строго k-мерной, если $g \in B_{n,k} \setminus B_{n,k-1}$, т.е. k является наименьшим неотрицательным целым числом, для которого существует представление функции g в виде (6). Каждое такое представление (соответствующее наименьшему возможному значению k) назовем неприводимым представлением функции g.

Следующая лемма по существу совпадает с утверждением 2 в статье [5].

Лемма 2 [5]. Функция $g \in B_n$ является строго k-мерной тогда и только тогда, когда $\dim I_g = n - k$, $k \in \overline{0, n}$.

Следствие 1. Представление (6) является неприводимым тогда и только тогда, когда $\operatorname{rank} A = k$ и $I_\varphi = \{0\}$. При этом $I_g = \{x \in V_n : xA = 0\} = C(A)^\perp$.

Отметим, что каждая k-мерная функция g допускает такое представление в виде (6), для которого $\operatorname{rank} A = k$: достаточно рассмотреть неприводимое представление $g(x) = \psi(xB)$, $x \in V_n$, где $\psi \in B_r$, $B \in F_{n \times r}$, $r = \operatorname{rank} B \le k$, дополнить матрицу B до $n \times k$-матрицы ранга k и заменить функцию ψ функцией, полученной путем введения $k - r$ фиктивных переменных.

В дальнейшем для функции $g \in B_{n,k}$, заданной по формуле (6), будем использовать обозначение $g_{\varphi, A}$, предполагая, что $\varphi \in B_k$, $A \in F_{n \times k}$ и $\operatorname{rank} A = k$.

ДОПУСТИМЫЕ ПОДПРОСТРАНСТВА. ОЦЕНКИ ОТНОСИТЕЛЬНОГО РАССТОЯНИЯ МЕЖДУ БУЛЕВОЙ ФУНКЦИЕЙ И МНОЖЕСТВОМ *k*-МЕРНЫХ ФУНКЦИЙ

Пусть $f \in B_n$, $k \in \overline{0, n-1}$, $\varepsilon \in (0,1)$.

Определение 3. Назовем пространство $H \in \mathcal{L}_{n,k}$ ε-допустимым для функции f, если существует пара $(\varphi, A) \in B_k \times F_{n\times k}$ такая, что $\operatorname{rank} A = k$, $H = C(A)$ и $d(f, g_{\varphi,A}) \le 1/2 \cdot (1-\varepsilon)$.

Для любого $H \in \mathcal{L}_{n,k}$ обозначим $B_{n,k}(H)$ множество всех функций $g \in B_{n,k}$, допускающих представление в виде (6) такое, что $\operatorname{rank} A = k$ и $H = C(A)$. Очевидно, что

$$B_{n,k} = \bigcup_{H \in \mathcal{L}_{n,k}} B_{n,k}(H). \tag{7}$$

При этом ε-допустимыми для функции f являются те и только те подпространства $H \in \mathcal{L}_{n,k}$, для которых $d(f, B_{n,k}(H)) \le 1/2 \cdot (1-\varepsilon)$

Для любого $H \in \mathcal{L}_{n,k}$ положим

$$l_f(H) = 2^{-n} \sum_{s\in V_k} \left| \sum_{x\in L_s} (-1)^{f(x)} \right| = 2^{-k} \sum_{s\in V_k} \left| \sum_{x\in H} \hat{f}(x)(-1)^{\alpha_s x} \right|, \tag{8}$$

где $\{L_s = L \oplus \alpha_s : s \in V_k\} = V_n / L$, $L = H^{\perp}$ (отметим, что в силу равенства (5) параметр $l_f(H)$ определен корректно).

Докажем ряд утверждений, уточняющих теоремы 4 и 5, приведенные в [9] без доказательства.

Лемма 3. Для любых $f \in B_n$, $k \in \overline{0, n-1}$, $H \in \mathcal{L}_{n,k}$ справедливо равенство

$$d(f, B_{n,k}(H)) = 1/2 \cdot (1 - l_f(H)). \tag{9}$$

При этом функция $g_{\varphi,A} \in B_{n,k}(H)$ является ближайшей к f во множестве $B_{n,k}(H)$ тогда и только тогда, когда выполняются следующие соотношения:

$$\sum_{y\in V_k} \hat{f}(Ay)(-1)^{sy} = (-1)^{\varphi(s)} \left| \sum_{y\in V_k} \hat{f}(Ay)(-1)^{sy} \right|, \ s \in V_k. \tag{10}$$

Доказательство. Пусть $g = g_{\varphi,A} \in B_{n,k}(H)$, где $C(A) = H$. Заметим, что все различные смежные классы пространства V_n по подпространству $L = H^{\perp}$ имеют следующий вид: $L_s = \{x \in V_n : xA = s\}$, $s \in V_k$. Отсюда на основании формул (5) и (8) вытекают равенства

$$2^{-(n-k)} \sum_{x\in L_s} (-1)^{f(x)} = \sum_{y\in V_k} \hat{f}(Ay)(-1)^{sy}, \ s \in V_k, \tag{11}$$

$$l_f(H) = 2^{-k} \sum_{s\in V_k} \left| \sum_{y\in V_k} \hat{f}(Ay)(-1)^{sy} \right|, \tag{12}$$

используя которые получим

$$1 - 2d(f,g) = 2^{-n} \sum_{x\in V_n} (-1)^{f(x)\oplus g(x)} =$$

$$= 2^{-n} \sum_{s\in V_k} \sum_{x\in L_s} (-1)^{f(x)\oplus g(x)} = 2^{-k} \sum_{s\in V_k} (-1)^{\varphi(s)} \left(2^{-(n-k)} \sum_{x\in L_s} (-1)^{f(x)} \right) =$$

$$= 2^{-k} \sum_{s\in V_k} (-1)^{\varphi(s)} \left(\sum_{y\in V_k} \hat{f}(Ay)(-1)^{sy} \right) \le 2^{-k} \sum_{s\in V_k} \left| \sum_{y\in V_k} \hat{f}(Ay)(-1)^{sy} \right| = l_f(H).$$

При этом последнее неравенство обращается в равенство тогда и только тогда, когда выполняются соотношения (10).

Лемма доказана.

Следствие 2. Подпространство $H \in \mathcal{L}_{n,k}$ является ε-допустимым для функции f тогда и только тогда, когда $l_f(H) \ge \varepsilon$.

Лемма 4. Для любых $f \in B_n$, $k \in \overline{0, n-1}$, $H \in \mathcal{L}_{n,k}$ справедливы неравенства

$$\omega_f(H) \le l_f(H) \le (\omega_f(H))^{1/2}, \tag{13}$$

где $\omega_f(H)$ определяется по формуле (3).

Доказательство. Обозначим A произвольную $n \times k$-матрицу, столбцы которой образуют базис векторного пространства H; положим $L = H^{\perp}$,

$$u_s = \left| \sum_{y \in V_k} \hat{f}(Ay)(-1)^{sy} \right|, \; s \in V_k.$$

На основании формул (5) и (8) справедливы равенства (11), (12), из которых следует, что $0 \le u_s \le 1$, $s \in V_k$ и

$$l_f(H) = 2^{-k} \sum_{s \in V_k} u_s.$$

Следовательно,

$$2^{-k} \sum_{s \in V_k} u_s^2 \le l_f(H) \le \left(2^{-k} \sum_{s \in V_k} u_s^2 \right)^{1/2}. \tag{14}$$

Кроме того, справедливы следующие соотношения:

$$2^{-k} \sum_{s \in V_k} u_s^2 = 2^{-k} \sum_{s \in V_k} \sum_{(y_1, y_2) \in V_k^2} \hat{f}(Ay_1)\hat{f}(Ay_2)(-1)^{s(y_1 \oplus y_2)} =$$

$$= \sum_{(y_1, y_2) \in V_k^2} \hat{f}(Ay_1)\hat{f}(Ay_2) \left(2^{-k} \sum_{s \in V_k} (-1)^{s(y_1 \oplus y_2)} \right) = \sum_{y \in V_k} \hat{f}(Ay)^2 = \omega(H). \tag{15}$$

Из формул (14), (15) получаем неравенства (13).

Лемма доказана.

Непосредственно из соотношений (7), (9), (13) вытекают следующая теорема, устанавливающая явное выражение, а также оценки относительного расстояния между булевой функцией и множеством k-мерных функций.

Теорема 1. Для любых $f \in B_n$, $k \in \overline{0, n-1}$ справедливы соотношения

$$d(f, B_{n,k}) = 1/2 \cdot \left(1 - \max_{H \in L_{n,k}} l_f(H) \right), \tag{16}$$

$$1/2 \cdot \left(1 - \max_{H \in L_{n,k}} (\omega_f(H))^{1/2} \right) \le d(f, B_{n,k}) \le 1/2 \cdot \left(1 - \max_{H \in L_{n,k}} \omega_f(H) \right), \tag{17}$$

где $l_f(H)$ определяется по формуле (8), а $\omega_f(H)$ — по формуле (3).

Отметим, что при $k = 1$ равенство (16) по существу совпадает с известной формулой для относительного расстояния между булевой функцией и множеством аффинных функций от n переменных. Действительно, если $H = \{0, \alpha\} \in \mathcal{L}_{n,1}$, где $\alpha \ne 0$, то на основании второго равенства (8)

$$l_f(H) = 1/2 \cdot (|\hat{f}(0) + \hat{f}(\alpha)| + |\hat{f}(0) - \hat{f}(\alpha)|) = \max\{|\hat{f}(0)|, |\hat{f}(\alpha)|\},$$

откуда следует

$$d(f, B_{n,1}) = 1/2 \cdot \left(1 - \max_{H \in \mathcal{L}_{n,1}} l_f(H) \right) = 1/2 \cdot \left(1 - \max_{\alpha \in V_n} |\hat{f}(\alpha)| \right).$$

Отметим также, что при $k = 1$ нижняя граница (17) достигается для любой уравновешенной функции $f \in B_n$. Кроме того, оба неравенства (17) обращаются в равенства, если f — k-мерная функция, $k \in \overline{0, n-1}$.

При $k=n-1$ формула (16) приводит к соотношению для относительного расстояния между функцией f и множеством алгебраически вырожденных функций, полученному ранее в [5].

Следствие 3 [5]. Для любой функции $f \in B_n$ выполняется равенство

$$d(f, B_{n,n-1}) = 1/2 \cdot \min_{u \in V_n \setminus \{0\}} wt(D_u f),$$

где $D_u f$ — производная функции f по направлению u.

Доказательство. Пусть $L=\{0,u\} \in \mathcal{L}_{n,1}$, где $u \neq 0$, и $V_n / L = \{L_s = L \oplus \alpha_s :\ s \in V_{n-1}\}$. Согласно первому равенству (8)

$$l_f(L^{\perp}) = 2^{-n} \sum_{s \in V_{n-1}} \left| \sum_{x \in L_s} (-1)^{f(x)} \right| = 2^{-n} \sum_{s \in V_{n-1}} \left| (-1)^{f(\alpha_s)} + (-1)^{f(\alpha_s \oplus u)} \right| =$$

$$= 2^{1-n}\ \#\{s \in V_{n-1} : f(\alpha_s) = f(\alpha_s \oplus u)\} = 2^{-n}\ \#\{x \in V_n : D_u f(x) = 0\} = 1 - wt(D_u f).$$

Следовательно, на основании формулы (16)

$$d(f, B_{n,\,n-1}) = 1/2 \cdot \left(1 - \max_{L \in \mathcal{L}_{n,1}} l_f(L^{\perp})\right) = 1/2 \cdot \left(1 - \max_{u \in V_n \setminus \{0\}} (1 - wt(D_u f))\right) =$$
$$1/2 \cdot \min_{u \in V_n \setminus \{0\}} wt(D_u f),$$

что и требовалось доказать.

СВЯЗЬ МЕЖДУ ДОПУСТИМЫМИ ПОДПРОСТРАНСТВАМИ И МЕТРИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ ПРОИЗВОДНЫХ ПО НАПРАВЛЕНИЯМ БУЛЕВЫХ ФУНКЦИЙ

Согласно определению 3 и лемме 3 нахождение k-мерных функций, расположенных от заданной функции $f \in B_n$ на расстоянии не более $1/2 \cdot (1-\varepsilon)$, $\varepsilon \in (0,1)$, сводится к построению k-мерных подпространств векторного пространства V_n, ε-допустимых для функции f. Действительно, каждой функции $g = g_{\varphi, A}$, удовлетворяющей условию $d(f,g) \le 1/2 \cdot (1-\varepsilon)$, соответствует (по крайней мере одно) ε-допустимое подпространство $H = C(A)$. При этом для каждого такого подпространства H лемма 3 позволяет построить все ближайшие к f k-мерные функции $g = g_{\varphi, A}$ такие, что $H = C(A)$ и (как следствие) $d(f,g) \le 1/2 \cdot (1-\varepsilon)$.

Ниже доказана теорема, устанавливающая способ нахождения всех ε-допустимых подпространств для заданной булевой функции.

Для любых $f \in B_n$, $\theta \in (0,1)$ обозначим

$$\mathcal{D}(f,\theta) = \{\alpha \in V_n : wt(D_\alpha f) \le \theta\}. \tag{18}$$

Теорема 2. Если подпространство $H \in \mathcal{L}_{n,k}$ является ε-допустимым для функции $f \in B_n$, то $H^{\perp} \subseteq \mathcal{D}(f, 1-\varepsilon)$. При этом если $L \in \mathcal{L}_{n,n-k}$ и $L \subseteq \mathcal{D}(f, 1/2 \cdot (1-\varepsilon))$, то $L^{\perp}$ — ε-допустимое подпространство для функции f.

Доказательство. Пусть существует пара $(\varphi, A) \in B_k \times F_{n \times k}$ такая, что $\operatorname{rank} A = k$, $H = C(A)$ и $d(f, g_{\varphi, A}) \le 1/2 \cdot (1-\varepsilon)$. Обозначим

$$g = g_{\varphi, A}\,,\ g^{(\alpha)}(x) = g(x \oplus \alpha),\ f^{(\alpha)}(x) = f(x \oplus \alpha),\ x, \alpha \in V_n\,.$$

Поскольку $H^{\perp} = C(A)^{\perp} = \{x \in V_n : xA = 0\}$, то на основании формулы (6) для любого $\alpha \in H^{\perp}$ выполняется равенство $g^{(\alpha)} = g$. Следовательно, для каждого указанного α

$$wt(D_\alpha f) = wt(f^{(\alpha)} \oplus f) = wt(f^{(\alpha)} \oplus g^{(\alpha)} \oplus g \oplus f) \le$$
$$\le wt(f^{(\alpha)} \oplus g^{(\alpha)}) + wt(g \oplus f) = 2d(f,g) \le 1 - \varepsilon,$$

откуда следует, что $H^{\perp} \subseteq \mathcal{D}(f, 1-\varepsilon)$.

Пусть далее $L \in \mathcal{L}_{n,n-k}$ и для любого $\alpha \in L$ выполняется неравенство $wt(D_\alpha f) \le 1/2 \cdot (1-\varepsilon)$. Полагая $H = L^\perp$, на основании нижней границы (13) и формулы (4) получим

$$l_f(H) \ge \omega_f(H) = 2^{-(n-k)} \sum_{\alpha \in L} 2^{-n} \sum_{x \in V_n} (-1)^{D_\alpha f(x)} = 2^{-(n-k)} \sum_{\alpha \in L} (1 - 2wt(D_\alpha f)) \ge \varepsilon.$$

Отсюда в силу следствия 2 вытекает, что подпространство H является ε-допустимым для функции f.

Теорема доказана.

Следствие 4. Если множество $\mathcal{D}(f, 1-\varepsilon)$ не содержит подпространств размерности $n-k$, то $d(f, B_{n,k}) > 1/2 \cdot (1-\varepsilon)$. Если существует $(n-k)$-мерное подпространство, содержащееся во множестве $\mathcal{D}(f, 1/2 \cdot (1-\varepsilon))$, то $d(f, B_{n,k}) \le 1/2 \cdot (1-\varepsilon)$.

Полученная теорема позволяет предложить следующий алгоритм.

Алгоритм нахождения всех k-мерных подпространств, ε-допустимых для функции $f \in B_n$, заданной таблицей истинности.

1. Вычислив значения автокорреляционной функции

$$\Delta_f(\alpha) = \sum_{x \in V_n} (-1)^{D_\alpha f(x)}, \ \alpha \in V_n,$$

с помощью алгоритма быстрого преобразования Адамара (см. например, [12, с. 217]), построить множество $\mathcal{D}(f, 1-\varepsilon)$.

2. Если это множество не содержит подпространств размерности $n-k$, то для функции f не существует ε-допустимых k-мерных подпространств. В противном случае построить множество, состоящее из всех подпространств $L^\perp$ таких, что $L \in \mathcal{L}_{n,n-k}$ и либо $L \subseteq \mathcal{D}(f, 1/2 \cdot (1-\varepsilon))$, либо $L \subseteq \mathcal{D}(f, 1-\varepsilon) \setminus \mathcal{D}(f, 1/2 \cdot (1-\varepsilon))$ и $l_f(L^\perp) \ge \varepsilon$.

Все указанные подпространства и только они являются искомыми.

Отметим, что возможность применения этого алгоритма на практике определяется строением множеств (18). Ниже изложены результаты, позволяющие предложить более эффективный алгоритм нахождения ряда высоковероятных k-мерных приближений булевых функций.

УСИЛЕНИЕ ТЕОРЕМЫ ГОПАЛАНА ДЛЯ БУЛЕВЫХ ФУНКЦИЙ

В работе [2, п. 4] доказана теорема, описывающая строение определенных k-мерных приближений функций от n переменных над произвольным конечным полем. Применительно к булевым функциям эта теорема имеет следующий вид.

Теорема 3 [2]. Пусть $f \in B_n$, $g \in B_{n,k}$, $\deg g \le d$ и $d(f,g) \le 2^{-d}(1-\varepsilon)$, где $1 \le d \le k$, $\varepsilon \in (0,1)$. Тогда

$$I_g^\perp = \left\langle \left\{ \alpha \in I_g^\perp : \ |\hat{f}(\alpha)| \ge \frac{1}{8\sqrt{2}} 2^{-k/2-d} \varepsilon^2 \right\} \right\rangle.$$

Из теоремы 3 следует, что каждая функция g, удовлетворяющая ее условию, допускает такое представление (6), в котором столбцы матрицы A принадлежат множеству

$$S_f(\mu) = \{\alpha \in V_n : |\hat{f}(\alpha)| \ge \mu\} \tag{19}$$

при $\mu = \mu_1 = \dfrac{1}{8\sqrt{2}} 2^{-k/2-d} \varepsilon^2$. Поскольку $|S_f(\mu)| \le \mu^{-2}$ для любых $f \in B_n$, $\mu \in (0,1)$, то число указанных функций g ограничено сверху величиной

$$\mu_1^{-2k} N(k,d) = 2^{k^2 + k(2d+7)} \varepsilon^{-4k} N(k,d), \tag{20}$$

где $N(k,d) = 2^{\sum_{i=0}^{d} \binom{k}{i}}$ — число булевых функций степени не выше d от k переменных. Таким образом, для нахождения всех указанных функций достаточно перебрать всевозможные наборы $(\alpha_1, \dots, \alpha_k, \varphi)$, где $\alpha_1, \dots, \alpha_k \in S_f(\mu_1)$, $\varphi \in B_k$,

$\deg\varphi \le d$, задать функцию g по формуле $g(x)=\varphi(\alpha_1 x,\dots,\alpha_k x)$, $x\in V_n$, и проверить условие $d(f,g)\le 2^{-d}(1-\varepsilon)$. Если каждую такую проверку принять за одну операцию, то трудоемкость описанного алгоритма построения всех функций g по заданному множеству $S_f(\mu)$ (см. [2, п. 4]) оценивается сверху по формуле (20).

Основным результатом настоящего раздела является теорема, усиливающая теорему 3 и (как следствие) верхнюю оценку (20). Прежде чем сформулировать эту теорему, дадим одно определение и установим ряд вспомогательных результатов.

Для любой функции $g\in B_n$ положим $\Delta(g)=1/2\cdot\min\limits_{\alpha\notin I_g} wt(D_\alpha g)$.

Отметим, что если g — строго k-мерная функция и (6) — ее неприводимое представление, то $wt(D_\alpha g)=wt(D_{\alpha A}\varphi)$ для любого $\alpha\in V_n$, откуда в силу следствий 1 и 3 вытекает, что

$$\Delta(g)=1/2\cdot\min_{a\in V_k\setminus\{0\}} wt(D_a\varphi)=d(\varphi,B_{k,\,k-1}).$$

Определение 4. Назовем функцию $g\in B_{n,\,k}$ специальным (k,ε)-приближением функции $f\in B_n$, если g — строго k-мерная функция и

$$d(f,g)\le\Delta(g)(1-\varepsilon),\ \ \varepsilon\in(0,1).$$

Как показывает следующая лемма, класс специальных приближений включает функции, удовлетворяющие условию теоремы 3.

Лемма 5. Пусть $f\in B_n$, $g\in B_{n,\,k}$ — строго k-мерная функция, $\deg g\le d$ и $d(f,g)\le 2^{-d}(1-\varepsilon)$, где $1\le d\le k$, $\varepsilon\in(0,1)$. Тогда g является специальным (k,ε)-приближением функции f.

Доказательство. Если $\alpha\notin I_g$, то $D_\alpha g\ne 0$. Поскольку при этом $\deg(D_\alpha g)\le d-1$, то на основании леммы 1 справедливо соотношение $\Delta(g)=1/2\cdot\min\limits_{\alpha\notin I_g} wt(D_\alpha g)\ge 2^{-d}$, что и требовалось доказать.

Следующая лемма играет ключевую роль в доказательстве основной теоремы настоящего раздела.

Лемма 6. Пусть $f\in B_n$, g — специальное (k,ε)-приближение функции f и $g(x)=\psi(xA)$, $x\in V_n$, — неприводимое представление функции g. Пусть далее $g_0(x)=\varphi(xA)$, $x\in V_n$, — k-мерная функция, ближайшая к f на множестве $B_{n,\,k}(C(A))$. Для любых $a\in V_k\setminus\{0\}$, $t\in\mathbf{N}$ обозначим

$$M_t(a)=2^{-k}\sum_{s\in V_k}(u_s(-1)^{\varphi(s)}-u_{s\oplus a}(-1)^{\varphi(s\oplus a)})^{2t},$$

где

$$u_s=\left|\sum_{y\in V_k}\hat f(Ay)(-1)^{sy}\right|,\ \ s\in V_k.$$

Тогда для любого $\delta\in(0,1)$ выполняются следующие неравенства:

$$(2\delta)^{2t}\left(wt(D_a\psi)-\frac{2d(f,g)}{1-\delta}\right)\le M_t(a)\le 2^{(2t-1)k+1}\left(\max_{\substack{y\in V_k:\\ ay=1}}|\hat f(Ay)|\right)^{2t}. \qquad (21)$$

Доказательство. Убедимся в справедливости нижней границы (21). Обозначим

$$\nu_s=(-1)^{\varphi(s)\oplus\psi(s)}u_s+(-1)^{\varphi(s\oplus a)\oplus\psi(s\oplus a)}u_{s\oplus a},\ \ s\in V_k,$$

$$V(\delta)=\{s\in V_k:\ D_a\psi(s)=1,\ \nu_s\ge 2\delta\}.$$

Вначале докажем соотношения

$$d(f,g)=2^{-k}\sum_{s\in V_k}1/2\cdot(1-1/2\cdot\nu_s), \qquad (22)$$

$$2^{-k}\,\#V(\delta)\ge wt(D_a\psi)-\frac{2d(f,g)}{1-\delta}. \qquad (23)$$

Положим $H=C(A)$, $L_s=\{x\in V_n : xA=s\}$, $s\in V_k$. Поскольку функция g_0 является ближайшей к функции f на множестве $B_{n,k}(H)$, то на основании леммы 3 выполняются равенства

$$\sum_{y\in V_k}\hat f(Ay)(-1)^{sy}=(-1)^{\varphi(s)}u_s\,,\ s\in V_k\,. \tag{24}$$

Используя формулы (11) и (24), получаем

$$1-2d(f,g)=2^{-n}\sum_{x\in V_n}(-1)^{f(x)\oplus g(x)}=$$

$$=2^{-n}\sum_{s\in V_k}\sum_{x\in L_s}(-1)^{f(x)\oplus g(x)}=2^{-k}\sum_{s\in V_k}(-1)^{\psi(s)}\left(2^{-(n-k)}\sum_{x\in L_s}(-1)^{f(x)}\right)=$$

$$=2^{-k}\sum_{s\in V_k}(-1)^{\psi(s)}\left(\sum_{y\in V_k}\hat f(Ay)(-1)^{sy}\right)=2^{-k}\sum_{s\in V_k}(-1)^{\psi(s)\oplus\varphi(s)}u_s=2^{-k}\sum_{s\in V_k}1/2\cdot\nu_s.$$

Итак, справедливо равенство (22).

Для доказательства соотношения (23) заметим, что

$$2^{-k}\#V(\delta)=2^{-k}\#\{s\in V_k:\ D_a\psi(s)=1\}-2^{-k}\#\{s\in V_k:\ D_a\psi(s)=1,\ \nu_s<2\delta\}\geq$$

$$\geq wt(D_a\psi)-2^{-k}\#\{s\in V_k:\ \nu_s<2\delta\}=$$

$$=wt(D_a\psi)-2^{-k}\#\{s\in V_k:\ 1/2\cdot(1-1/2\cdot\nu_s)>1/2\cdot(1-\delta)\},$$

причем $1/2\cdot(1-1/2\cdot\nu_s)\geq 0$ для любого $s\in V_k$. Следовательно,

$$2^{-k}\#\{s\in V_k:\ 1/2\cdot(1-1/2\cdot\nu_s)>1/2\cdot(1-\delta)\}\leq\frac{2}{1-\delta}\left(2^{-k}\sum_{s\in V_k}1/2\cdot(1-1/2\cdot\nu_s)\right),$$

справедливость соотношения (23) вытекает из равенства (22).

Для завершения доказательства нижней границы (21) воспользуемся неравенством

$$M_t(a)\geq 2^{-k}\sum_{s\in V(\delta)}(u_s-u_{s\oplus a}(-1)^{D_a\varphi(s)})^{2t} \tag{25}$$

и заметим, что

$$|u_s-u_{s\oplus a}(-1)^{D_a\varphi(s)}|\geq 2\delta\,,\ s\in V(\delta)\,. \tag{26}$$

Действительно, если $s\in V(\delta)$ и $D_a\varphi(s)=1$, то

$$|u_s-u_{s\oplus a}(-1)^{D_a\varphi(s)}|=u_s+u_{s\oplus a}\geq\nu_s\geq 2\delta\,.$$

Если $s\in V(\delta)$ и $D_a\varphi(s)=0$, то $|u_s-u_{s\oplus a}(-1)^{D_a\varphi(s)}|=|u_s-u_{s\oplus a}|$. При этом $D_a\psi(s)=1$, $\nu_s\geq 2\delta$ и, следовательно, $(-1)^{\varphi(s)\oplus\psi(s)}=-(-1)^{\varphi(s\oplus a)\oplus\psi(s\oplus a)}$, $\nu_s=(-1)^{\varphi(s)\oplus\psi(s)}(u_s-u_{s\oplus a})\geq 2\delta$. Но тогда $|\nu_s|=|u_s-u_{s\oplus a}|\geq 2\delta$, что и требовалось доказать. Таким образом, в силу соотношений (23), (25), (26) справедлива нижняя граница (21).

Для доказательства верхней границы (21) воспользуемся равенствами (24). В результате получим, что

$$M_t(a)=2^{-k}\sum_{s\in V_k}\left(\sum_{y\in V_k}\hat f(Ay)(-1)^{sy}-\sum_{y\in V_k}\hat f(Ay)(-1)^{(s\oplus a)y}\right)^{2t}=$$

$$=2^{-k}\sum_{s\in V_k}\left(\sum_{y\in V_k}\hat f(Ay)(-1)^{sy}(1-(-1)^{ay})\right)^{2t}=2^{2t-k}\sum_{s\in V_k}\left(\sum_{\substack{y\in V_k:\\ ay=1}}\hat f(Ay)(-1)^{sy}\right)^{2t}=$$

$$= 2^{2t-k} \sum_{s \in V_k} \sum_{\substack{(y_1,\ldots,\, y_{2t}) \in V_k^{2t}: \\ ay_1 = \ldots = ay_{2t} = 1}} \hat{f}(Ay_1) \cdots \hat{f}(Ay_{2t})(-1)^{s(y_1 \oplus \cdots \oplus y_{2t})} =$$

$$= 2^{2t} \sum_{\substack{(y_1,\ldots,\, y_{2t-1}) \in V_k^{2t-1}: \\ ay_1 = \ldots = ay_{2t-1} = 1}} \hat{f}(Ay_1) \cdots \hat{f}(Ay_{2t-1}) \hat{f}(Ay_1 \oplus \cdots \oplus Ay_{2t-1}) \le$$

$$\le 2^{2t} \sum_{\substack{(y_1,\ldots,\, y_{2t-1}) \in V_k^{2t-1}: \\ ay_1 = \ldots = ay_{2t-1} = 1}} \left(\max_{\substack{y \in V_k: \\ ay = 1}} |\hat{f}(Ay)| \right)^{2t} = 2^{2t + (k-1)(2t-1)} \left(\max_{\substack{y \in V_k: \\ ay = 1}} |\hat{f}(Ay)| \right)^{2t} .$$

Лемма полностью доказана.

Следующая теорема обобщает и одновременно усиливает теорему 3.

Теорема 4. Пусть g — специальное (k, ε)-приближение функции $f \in B_n$. Тогда

$$I_g^{\perp} = \langle \{ x \in I_g^{\perp} : \ |\hat{f}(x)| \ge \mu_0 \} \rangle , \tag{27}$$

где

$$\mu_0 = \max \left\{ 2^{1-k} \varepsilon , \ \frac{4}{3\sqrt{3}} 2^{-k/2} \varepsilon^{3/2} \Delta(g)^{1/2} \right\} . \tag{28}$$

Доказательство. Пусть $g(x) = \psi(xA)$, $x \in V_n$ — неприводимое представление функции g. Согласно следствию 1 выполняется равенство $I_g^{\perp} = C(A)$. Обозначим $W = \langle \{ x \in C(A) : \ |\hat{f}(x)| \ge \mu_0 \} \rangle$ и заметим, что существует $\varepsilon' > 0$ такое, что $W = \langle \{ x \in C(A) : \ |\hat{f}(x)| > \mu_0 - \varepsilon' \} \rangle$.

Предположим, что равенство (27) не выполняется, т.е. $W \underset{\neq}{\subset} C(A)$. Тогда $W^{\perp} \underset{\neq}{\supset} C(A)^{\perp} = \{ x \in V_n : xA = 0 \}$ и существует вектор $\beta \in W^{\perp}$ такой, что $a = \beta A \ne 0$. Отсюда следует, что для любого $y \in V_k$, удовлетворяющего условию $ay = 1$, справедливо неравенство $|\hat{f}(Ay)| \le \mu_0 - \varepsilon'$. Действительно, поскольку $1 = ay = \beta(Ay) \ne 0$ и $\beta \in W^{\perp}$, то $Ay \notin W$, а значит $|\hat{f}(Ay)| \le \mu_0 - \varepsilon'$.

Итак, имеет место неравенство

$$\max_{\substack{y \in V_k: \\ ay = 1}} |\hat{f}(Ay)| \le \mu_0 - \varepsilon' .$$

Отсюда на основании оценок (21) следует, что для любых $\delta \in (0, 1)$, $t \in \mathbf{N}$ справедливо неравенство

$$(2\delta)^{2t} \left(wt(D_a \psi) - \frac{2d(f, g)}{1-\delta} \right) \le 2^{(2t-1)k+1} (\mu_0 - \varepsilon')^{2t},$$

которое запишем в виде

$$2\delta \left(wt(D_a \psi) - \frac{2d(f, g)}{1-\delta} \right)^{\frac{1}{2t}} \le 2^{k \frac{2t-1}{2t} + \frac{1}{2t}} (\mu_0 - \varepsilon') .$$

Далее, по условию теоремы имеем $d(f, g) \le \Delta(g)(1-\varepsilon)$; кроме того, из равенства $I_g^{\perp} = C(A)$, условия $a = \beta A \ne 0$ и определения параметра $\Delta(g)$ вытекает, что $wt(D_a \psi) = wt(D_{\beta} g) \ge 2\Delta(g)$. Следовательно, для любого $\delta \in (0, \varepsilon)$

$$wt(D_a \psi) - \frac{2d(f, g)}{1-\delta} \ge 2\Delta(g) - \frac{2\Delta(g)(1-\varepsilon)}{1-\delta} = 2\Delta(g) \left(1 - \frac{1-\varepsilon}{1-\delta} \right) \ge 2\Delta(g)(\varepsilon - \delta) > 0 .$$

Итак, для любых $\delta \in (0, \varepsilon)$, $t \in \mathbf{N}$ справедливо неравенство

$$2\delta \, (2\Delta(g)(\varepsilon - \delta))^{\frac{1}{2t}} \le 2^{k \frac{2t-1}{2t} + \frac{1}{2t}} (\mu_0 - \varepsilon') . \tag{29}$$

Переходя к пределу при $t \to \infty$ в обеих частях неравенства (29), получаем, что $2\delta \le 2^k (\mu_0 - \varepsilon')$ для любого $\delta \in (0, \varepsilon)$ и, следовательно, $2^{1-k} \varepsilon \le \mu_0 - \varepsilon'$.

Наконец, полагая в (29) $t=1$, $\delta=2\varepsilon/3$, получаем

$$\frac{4}{3\sqrt{3}}2^{-k/2}\varepsilon^{3/2}\Delta(g)^{1/2}\le\mu_0-\varepsilon'.$$

Таким образом, справедливо неравенство

$$\max\{2^{1-k}\varepsilon,\ \frac{4}{3\sqrt{3}}2^{-k/2}\varepsilon^{3/2}\Delta(g)^{1/2}\}\le\mu_0-\varepsilon',$$

которое, однако, противоречит формуле (28). Таким образом, предположение о том, что $W\ne C(A)$, является ложным; следовательно, выполняется равенство (27).

Теорема доказана.

Непосредственно из теоремы 4 и леммы 5 получаем следующие утверждения.

Следствие 5. Пусть $f\in B_n$, $g\in B_{n,k}$ — строго k-мерная функция, $\deg g\le d$ и $d(f,g)\le 2^{-d}(1-\varepsilon)$, где $1\le d\le k$, $\varepsilon\in(0,1)$. Тогда функция g допускает такое представление (6), в котором столбцы матрицы A являются линейно независимыми векторами, принадлежащими множеству $S_f(\mu_0)$ вида (19), где μ_0 определяется по формуле (28).

Следствие 6. Пусть $f\in B_n$, $g\in B_{n,k}$, $\deg g\le d$ и $d(f,g)\le 2^{-d}(1-\varepsilon)$, где $1\le d\le k$, $\varepsilon\in(0,1)$. Тогда функция g допускает представление (6), в котором столбцы матрицы A принадлежат множеству $S_f(\mu)$ при

$$\mu=\mu_0=\max\left\{2^{1-k}\varepsilon,\ \frac{4}{3\sqrt{3}}2^{-k/2-d/2}\varepsilon^{3/2}\right\}.$$

В частности, число указанных функций g ограничено сверху величиной

$$\mu_0^{-2k}N(k,d)<\min\{2^{2k^2-2k}\varepsilon^{-2k},\ 2^{k^2+k(d+1)}\varepsilon^{-3k}\}N(k,d),\qquad(30)$$

где $N(k,d)=2^{\sum_{i=0}^{d}\binom{k}{i}}$ — число булевых функций степени не выше d от k переменных.

Как видно из формул (20) и (30), полученная оценка количества k-мерных функций, удовлетворяющих условию теоремы 3, заметно лучше оценки из [2]. Более того, справедливо следующее утверждение.

Следствие 7. Пусть $f\in B_n$, $k\in\overline{1,n-1}$. Тогда каждая функция $g\in B_{n,k}\setminus B_{n,k-1}$, удовлетворяющая условию $d(f,g)\le 2^{-k}(1-\varepsilon)$, $\varepsilon\in(0,1)$, допускает такое представление (6), в котором столбцы матрицы A принадлежат множеству $S_f(2^{1-k}\varepsilon)$. При этом число указанных функций не превосходит $2^{2k^2-2k}\varepsilon^{-2k}(2^k+1)$.

Доказательство. Пусть $g=g_{\varphi,A}$ — строго k-мерная функция такая, что $d(f,g)\le 2^{-k}(1-\varepsilon)$. Если $g'=g'_{\varphi',A}$ и $d(f,g')\le 2^{-k}(1-\varepsilon)$, то

$$2^k d(\varphi,\varphi')=2^k d(g,g')\le 2^k(d(g,f)+d(f,g'))\le 2(1-\varepsilon)<2,$$

откуда следует, что $2^k d(\varphi,\varphi')\le 1$. Таким образом, для любой $n\times k$-матрицы A ранга k существует не более 2^k+1 функций $\varphi\in B_k$, удовлетворяющих условию $d(f,g_{\varphi,A})\le 2^{-k}(1-\varepsilon)$. Для завершения доказательства остается применить теорему 4. Отметим, что импликация

$$(d(f,g)\le 2^{-k}(1-\varepsilon), g(x)=\varphi(\alpha_1x,\dots,\alpha_kx), x\in V_n)\Rightarrow(\alpha_1,\dots,\alpha_k\in S_f(2^{1-k}\varepsilon)),$$

справедливая при выполнении условия следствия 7, преобразуется в равносильное утверждение при $k=1$: аффинная функция с вектором коэффициентов $\alpha\in V_n\setminus\{0\}$ тогда и только тогда находится от функции $f\in B_n$ на относительном расстоянии не более $1/2\cdot(1-\varepsilon)$, $\varepsilon\in(0,1)$, когда $|\hat f(\alpha)|\ge\varepsilon$. При этом оценка из теоремы 3 позволяет лишь утверждать, что $|\hat f(\alpha)|\ge 1/16\cdot\varepsilon^2$.

ЗАКЛЮЧЕНИЕ

Основными результатами статьи являются теоремы 1, 2 и 4. Первая из них содержит явное выражение, а также оценки относительного расстояния между булевой функцей и множеством k-мерных функций от n переменных. Вторая теорема устанавливает связь между k-мерными приближениями произвольной функции $f \in B_n$ и метрическими свойствами ее производных по направлениям. Теорема 4 описывает строение специальных k-мерных приближений функции $f \in B_n$, заметно усиливая ранее известный результат П. Гопалана [2].

Построение k-мерных функций, находящихся от заданной функции $f \in B_n$ на расстоянии не более $1/2 \cdot (1-\varepsilon)$, $\varepsilon \in (0,1)$, сводится к построению ε-допустимых для f k-мерных подпространств векторного пространства V_n. Для нахождения всех таких подпространств можно применять описанный в статье алгоритм, сложность которого зависит от строения множеств вида (18).

Теорема 4 и следствия из нее содержат важную информацию о строении k-мерных функций степени d, находящихся на расстоянии не более $2^{n-d}(1-\varepsilon)$ от заданной булевой функции n переменных, $1 \le d \le k \le n$, $\varepsilon \in (0,1)$. Эта информация позволяет установить нетривиальные верхние оценки количества указанных k-мерных функций и существенно повысить эффективность алгоритма их построения, преложенного в [2].

СПИСОК ЛИТЕРАТУРЫ

1. Testing Fourier dimensionality and sparsity / P. Gopalan, R. O'Donnel, A. Servedio, A. Shpilka, K. Wimmer // SIAM J. on Comput. — 2011. — **40**(4). — P. 1075–1100.
2. 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.
3. Lechner R.L. Harmonic analysis of switching functions // Recent Developments in Switching Theory. — New–York: Academic Press, 1971. — P. 122–228.
4. Dawson E., Wu C.K. Construction of correlation immune Boolean functions // Inform. and Communicat. Security, Proceedings. — Berlin: Springer–Verlag, 1997. — P. 170–180.
5. Алексеев Е.К. О некоторых мерах нелинейности булевых функций // Приклад. дискретная математика. — 2011. — № 2(12). — С. 5–16.
6. Daemen J., Govaerts R., Vandewalle J. Resynchronization weaknesses in synchronous stream ciphers // Advances in Cryptology — EUROCRYPT'93, Proceedings. — Berlin: Springer–Verlag, 1993. — P. 159–167.
7. Golić J., Morgari G. On the resynchronization attack // Fast Software Encryption. — FSE'03, Proceedings. — Berlin: Springer–Verlag, 2003. — P. 100–110.
8. Алексеев Е.К. Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной // Сб. статей молодых ученых факультета МВК МГУ. — 2011. — Вып. 8. — С. 114–123.
9. Canteaut A. On the correlations between a combining function and function of fewer variables // The 2002 IEEE Inform. Theory Workshop, Proceedings. — Berlin: Springer–Verlag, 2002. — P. 78–81.
10. Алексейчук А.Н., Конюшок С.Н. Усовершенствованный тест k-мерности для булевых функций // Кибернетика и системный анализ. — 2013. — **49**, № 2. — С. 27–35.
11. Alekseychuk A.N., Konyushok S.N. Fast algorithm for reconstruction of high-probable low-dimensional approximations for Boolean functions // Modern Stochastics: Theory and Applications III, Proceedings. — Kyiv. Taras Shevchenko National University, 2012. — P. 32.
12. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.

Поступила 05.11.2013