Г. А. Исаев, О множествах критерия распространения для строго мажоритарных булевых функций,
Дискрет. матем., 2023, том 35, выпуск 1, 62–70

Дискретная математика

том 35 выпуск 1 * 2023

УДК 519.716.322+519.719.2 DOI https://doi.org/10.4213/dm1756

О множествах критерия распространения для строго мажоритарных булевых функций

© 2023 г. Г. А. Исаев*

Исследуется критерий распространения для строго мажоритарных симметрических булевых функций. С помощью аппарата полиномов Кравчука доказано, что критерию распространения для строго мажоритарных функций от n переменных, где $\lfloor n/2 \rfloor$ нечётно, удовлетворяют векторы с весом Хэмминга, значение которого отличается от $n/2$ не более чем на $1/2$.

Ключевые слова: булева функция, критерий распространения, симметрическая булева функция, строго мажоритарная булева функция, полином Кравчука, спектр Уолша

1. Введение

Симметрические и, в частности, строго мажоритарные булевы функции являются одним из важных классов булевых функций с теоретической и практической точек зрения. Они представляют особый интерес для криптографии, так как позволяют эффективно реализовывать нелинейные функции от огромного числа переменных, задействуя при этом небольшой объём ресурсов системы преобразования информации ([4]). Ранее исследовались нелинейность и алгебраическая иммунность симметрических и строго мажоритарных функций. В [5] был предложен эффективный алгоритм вычисления спектра Уолша симметрических функций, основанный на свойствах полиномов Кравчука.

Говорят, что булева функция удовлетворяет критерию распространения по направлению (определяемому вектором из соответствующего n-мерного векторного пространства над полем из двух элементов), если производная данной функции по этому направлению является уравновешенной функцией. Совокупность всех таких направлений (векторов) для булевой функции называют множеством её критерия распространения. Впервые понятие критерия распространения было введено Бартом Пренелем и соавторами в [8] в целях характеризации стойкости применяемых в шифрах булевых функций относительно линейных и разностных методов криптоанализа, которые используются для получения информации о секретном ключе (подробнее об этих методах см. [3] и [4]). Необходимо отметить, что для некоторых классов булевых функций критерий распространения связан с их экстремальными свойствами. Например, количество векторов, удовлетворяющих критерию

*Место работы: МГУ им. М. В. Ломоносова, e-mail: gleb-isaev52@yandex.ru

распространения, максимально только при чётном числе переменных и для экстремального класса булевых функций, называемых бент-функциями, а минимально — у аффинных функций.

В работе исследуется критерий распространения для строго мажоритарных симметрических булевых функций. С помощью аппарата полиномов Кравчука доказано, что критерию распространения для строго мажоритарных функций от n переменных, где $\lfloor n/2 \rfloor$ нечётно, удовлетворяют векторы с весом Хэмминга, значение которого отличается от $n/2$ не более чем на $1/2$.

2. Основные определения и обозначения

Пусть $\mathbb{F}_2$ — конечное поле, состоящее из двух элементов, $V_n = \mathbb{F}_2^n$ — векторное пространство наборов длины n с компонентами из поля $\mathbb{F}_2$. *Булевой функцией* от n переменных называется отображение из V_n в $\mathbb{F}_2$. Множество всех булевых функций от n переменных обозначим через $\mathcal{F}_n$.

Операции сложения и умножения элементов поля $\mathbb{F}_2$ будем обозначать соответственно через «$\oplus$» и «$\cdot$» (далее мы часто будем опускать знак «$\cdot$»: $ab = a \cdot b$).

Определим следующие операции над векторами из V_n:

- $a \oplus b = (a_1 \oplus b_1, \ldots, a_n \oplus b_n)$ — побитовое сложение векторов $a, b \in V_n$,
- $\langle a, b \rangle = a_1 b_1 \oplus \cdots \oplus a_n b_n$ — скалярное произведение векторов $a, b \in V_n$.

Произвольную булеву функцию f из $\mathcal{F}_n$ можно представить в форме полинома от n переменных с коэффициентами из поля $\mathbb{F}_2$ (см. [3])

$$f(x_1, x_2, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \cdots \oplus a_{1\ldots n} x_1 \cdots x_n,$$

где $a_{i_1 \ldots i_j} \in \mathbb{F}_2$, $j = 1, 2, \ldots, n$. Такое представление функции называется *полиномом Жегалкина*. Если $a_{i_1 \ldots i_j} = 1$, то выражение $x_{i_1} \cdots x_{i_j}$, $j = 1, 2, \ldots, n$, называется *слагаемым в полиноме Жегалкина* функции f. Число переменных в самом длинном слагаемом полинома Жегалкина функции f называется *алгебраической степенью* функции f и обозначается через $\deg f$. Если функция имеет степень не выше 1, то она называется *аффинной*.

Преобразованием Уолша–Адамара булевой функции f из $\mathcal{F}_n$ ([3]) называют целочисленную функцию W_f, задаваемую на множестве V_n равенством

$$W_f(u) = \sum_{x \in V_n} (-1)^{\langle x, u \rangle \oplus f(x)}.$$

Вес Хэмминга $\mathrm{wt}(x)$ вектора $x = (x_1, \ldots, x_n)$ — это число ненулевых координат x_i. *Вес* $\mathrm{wt}(f)$ *булевой функции* f определяется равенством

$$\mathrm{wt}(f) = \#\{x \in V_n \colon f(x) = 1\},$$

где решётка «#» обозначает мощность соответствующего конечного множества.

Введём подмножество $U_k = \{x \in V_n \colon \mathrm{wt}(x) = k\}$. Очевидно, что пространство V_n представляет собой объединение непересекающихся подмножеств U_k, $k = 0, 1, \ldots, n$.

Булева функция $f \in \mathcal{F}_n$ называется *уравновешенной*, если $\mathrm{wt}(f) = 2^{n-1}$.

Производной по направлению $u \in V_n$ функции $f \in \mathcal{F}_n$ называется булева функция $D_u f(x) = f(x) \oplus f(x \oplus u)$, где $x \in V_n$.

Автокорреляционной функцией булевой функции $f \in \mathcal{F}_n$ называется функция $\Delta_f(u)$, имеющая вид

$$\Delta_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus f(x \oplus u)} = \sum_{x \in V_n} (-1)^{D_u f(x)}.$$

Бент-функцией называется такая булева функция $f \in \mathcal{F}_n$ (n чётно), что модуль каждого коэффициента Уолша–Адамара W_f этой функции равен $2^{\frac{n}{2}}$.

Говорят, что булева функция $f \in \mathcal{F}_n$ удовлетворяет *критерию распространения* по направлению $u \in V_n$, если производная $D_u f$ — уравновешенная функция (что эквивалентно условию $\Delta_f(u) = 0$). Множество всех таких векторов будем обозначать через $E_{\mathrm{PC}}(f) = \{u \in V_n \colon \mathrm{wt}(D_u f) = 2^{n-1}\}$ и называть *множеством критерия распространения* для функции f. Мощность этого множества обозначим через pc_f. Очевидно, что $0 \leqslant \mathrm{pc}_f \leqslant 2^n - 1$. Достижимость указанных выше границ можно продемонстрировать на примере булевых функций из известных классов. Для произвольного n и произвольной аффинной функции из $\mathcal{F}_n$ её pc_f равна 0 (так как производная аффинной функции по любому направлению является константой, см. [3]). Для чётного n и для произвольной бент-функции из $\mathcal{F}_n$ её pc_f равна $2^n - 1$ (критерий Ротхауза, см. [9]).

Характеризация векторов из множества $E_{\mathrm{PC}}(f)$ задаётся следующим утверждением.

Теорема 1 ([3], [4])**.** *Вектор $u \in V_n$ принадлежит $E_{\mathrm{PC}}(f)$ тогда и только тогда, когда выполнено равенство*

$$\sum_{x \in V_n} (-1)^{\langle x, u \rangle} W_f^2(x) = 0.$$

3. Критерий распространения симметрических функций

Булева функция называется *симметрической*, если её значение не зависит от перестановки её переменных, т. е. оно зависит только от количества единиц во входных данных. Следовательно, любую симметрическую функцию $f \in \mathcal{F}_n$ можно задать в виде булева вектора $re_f = (re_f(0), \ldots, re_f(n))$ размерности $n + 1$, где $re_f(i) = f(x_1, \ldots, x_n)$ при $\mathrm{wt}(x_1, \ldots, x_n) = i$, $i \in \{0, 1, \ldots, n\}$.

Непосредственно из определений симметрической функции и спектра Уолша (множества значений $W_f(u)$, $u \in V_n$) следует очевидное утверждение.

Утверждение 1. *Пусть $f \in \mathcal{F}_n$ — симметрическая функция и $\alpha, \beta \in V_n$ таковы, что $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta)$. Тогда*

$$W_f(\alpha) = W_f(\beta).$$

Таким образом, спектр Уолша симметрической функции $f \in \mathcal{F}_n$ можно задать в виде вектора $rw_f = (rw_f(0), \ldots, rw_f(n))$ размерности $n + 1$, где $rw_f(i) = W_f(x)$ при $\mathrm{wt}(x) = i$, $i \in \{0, 1, \ldots, n\}$.

Для симметрических функций справедливо следующее утверждение.

Утверждение 2. *Пусть $f \in \mathcal{F}_n$ — симметрическая функция, удовлетворяющая критерию распространения по направлению $u \in V_n$, $\mathrm{wt}(u) = k$. Тогда функция f удовлетворяет критерию распространения по всем векторам веса k.*

Доказательство. Непосредственно следует из симметричности функции f. □

Следствие 1. *Пусть $f \in \mathcal{F}_n$ — симметрическая функция. Тогда*

$$E_{\mathrm{PC}}(f) = U_{k_1} \cup U_{k_2} \cup \cdots \cup U_{k_l},$$

где $\{k_1, \ldots, k_l\}$ — множество всех весов векторов, принадлежащих $E_{\mathrm{PC}}(f)$, $k_i \neq k_j$ при $i \neq j$. Более того,

$$\mathrm{pc}_f = \sum_{i=1}^{l} \binom{n}{k_i}.$$

Доказательство. Пусть $\{u^{(1)}, \ldots, u^{(l)}\} \subset E_{\mathrm{PC}}(f)$, $\mathrm{wt}(u^{(i)}) = k_i$, $i = 1, \ldots, l$. Тогда по утверждению 2 все векторы из U_{k_i} принадлежат $E_{\mathrm{PC}}(f)$ для любого $i \in \{1, \ldots, l\}$. Следовательно, $E_{\mathrm{PC}}(f) = U_{k_1} \cup \cdots \cup U_{k_l}$. Поскольку $\#U_{k_i}$ равна $\binom{n}{k_i}$, то справедлива формула для значения pc_f. □

4. Полиномы Кравчука

Полиномом Кравчука (см. [7]) называется целочисленный полином степени i, $i = 0, 1, \ldots, n$, который задаётся следующим образом:

$$K_i(k, n) = \sum_{j=0}^{i} (-1)^j \binom{k}{j} \binom{n-k}{i-j},$$

где k, n — целые неотрицательные числа.

Приведём некоторые свойства полиномов Кравчука.

Утверждение 3 ([1], [5])**.** *Для полиномов Кравчука справедливы следующие равенства.*

(1) $K_i(k, n) = \sum_{x, \mathrm{wt}(x)=i} (-1)^{\langle x, \omega \rangle}$, *где* $\omega \in V_n$, $\mathrm{wt}(\omega) = k$.
(2) $K_0(k, n) = 1$, $K_1(k, n) = n - 2k$.
(3) $K_i(k, n) = (-1)^k K_{n-i}(k, n)$ (*если n чётно и k нечётно, то* $K_{n/2}(k, n) = 0$).
(4) $K_i(k, n) = (-1)^i K_i(n - k, n)$.
(5) *Если n чётно, то* $K_i(n/2, n) = \begin{cases} 0, & i \text{ нечётно}, \\ (-1)^{i/2} \binom{n/2}{i/2}, & i \text{ чётно}. \end{cases}$
(6) $\binom{n}{k} K_i(k, n) = \binom{n}{i} K_k(i, n)$.

Утверждение 4 ([1], [5])**.** *Полиномы Кравчука связаны следующими рекуррентными соотношениями.*

(1) $(i+1)K_{i+1}(k, n) = (n - 2k)K_i(k, n) - (n - i + 1)K_{i-1}(k, n)$.
(2) $(n - k)K_i(k + 1, n) = (n - 2i)K_i(k, n) - kK_i(k - 1, n)$.
(3) $(n - i + 1)K_i(k, n + 1) = (3n - 2i - 2k + 1)K_i(k, n) - 2(n - k)K_i(k, n - 1)$.

Утверждение 5 ([6]). *Для полиномов Кравчука справедливы соотношения Паскаля.*

(1) $K_i(k,n) + K_{i-1}(k,n) = K_i(k,n+1)$.
(2) $K_i(k,n) - K_{i-1}(k,n) = K_i(k+1,n+1)$.

5. Критерий распространения для строго мажоритарных функций

Обозначим через $\lfloor a \rfloor$ и $\lceil a \rceil$ округления числа a до целых соответственно в меньшую и большую сторону и рассмотрим функцию $f \in \mathcal{F}_n$, которая задаётся следующим образом:

$$f(x) = \begin{cases} 0, \text{ если } \mathrm{wt}(x) \leqslant \lfloor \frac{n}{2} \rfloor, \\ 1, \text{ если } \mathrm{wt}(x) > \lfloor \frac{n}{2} \rfloor. \end{cases} \tag{1}$$

Такая функция называется *строго мажоритарной* (strict majority function, см. [4]). Легко заметить, что $f(x)$, определяемая равенством (1), является симметрической функцией. В случае нечётного n функция f удовлетворяет свойству уравновешенности.

Приведём некоторые утверждения о спектре Уолша строго мажоритарной функции.

Теорема 2 ([5]). *Пусть $f \in \mathcal{F}_n$ — строго мажоритарная функция.*

(1) *Если k чётно, то* $rw_f(k) = \begin{cases} K_{n/2}(k,n), & n \text{ чётно}, \\ 0, & n \text{ нечётно}. \end{cases}$
(2) *Если k нечётно, то* $rw_f(k) = 2\sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} K_i(k,n)$.
(3) $rw_f(1) = 2\binom{n-1}{\lfloor n/2 \rfloor}$.
(4) $rw_f(n) = \begin{cases} (-1)^{n/2}\binom{n}{n/2}, & n \text{ чётно}, \\ (-1)^{(n-1)/2} \cdot 2\binom{n-1}{(n-1)/2}, & n \text{ нечётно}. \end{cases}$
(5) *Если n чётно, то* $rw_f(n/2) = \begin{cases} (-1)^{n/4}\binom{n/2}{n/4}, & n/2 \text{ чётно}, \\ 2\sum_{i=0}^{\frac{n-2}{4}} (-1)^i \binom{n/2}{i}, & n/2 \text{ нечётно}. \end{cases}$

Теорема 3 ([10]). *Для нечётных n и k справедливо равенство*

$$\sum_{i=0}^{\frac{n-1}{2}} K_i(k,n) = (-1)^{\frac{k-1}{2}} \frac{(k-1)!\frac{n-k}{2}!}{\frac{n-1}{2}!\frac{k-1}{2}!} \binom{n-k}{\frac{n-k}{2}} = (-1)^{\frac{k-1}{2}} \frac{(k-1)!(n-k)!}{\frac{n-1}{2}!\frac{k-1}{2}!\frac{n-k}{2}!}.$$

Перейдём непосредственно к изучению критерия распространения для строго мажоритарных функций.

Теорема 4. (1) *Пусть $n \in \mathbb{N}$ — нечётное, $\lfloor n/2 \rfloor$ — нечётное, $f \in \mathcal{F}_n$ — строго мажоритарная функция. Тогда множеству $E_{\mathrm{PC}}(f)$ принадлежат все векторы из V_n весов $\lfloor n/2 \rfloor$ и $\lceil n/2 \rceil$.*
(2) *Пусть $n \in \mathbb{N}$ — чётное, $n/2$ — нечётное, $f \in \mathcal{F}_n$ — строго мажоритарная функция. Тогда множеству $E_{\mathrm{PC}}(f)$ принадлежат все векторы веса $n/2$.*

Доказательство. Пусть n — нечётное, $\lfloor n/2 \rfloor$ — тоже нечётное. Выберем такой вектор $\omega \in V_n$, что $\mathrm{wt}(\omega) = k$, $k \in \{\lfloor n/2 \rfloor, \lceil n/2 \rceil\}$ и докажем, что $\omega \in E_{\mathrm{PC}}(f)$, воспользовавшись теоремой 1. По утверждению 1 и п. 1 утверждения 3 справедлива следующая цепочка равенств:

$$\begin{aligned}\sum_{x\in V_n} (-1)^{\langle x,\omega\rangle} W_f^2(x) &= rw_f^2(0) + rw_f^2(1)\cdot \sum_{x,\mathrm{wt}(x)=1} (-1)^{\langle x,\omega\rangle} + \cdots \\ &\quad + rw_f^2(n-1)\cdot \sum_{x,\mathrm{wt}(x)=n-1} (-1)^{\langle x,\omega\rangle} + (-1)^{\mathrm{wt}(\omega)} rw_f^2(n) \\ &= rw_f^2(0) + rw_f^2(1)\cdot K_1(k,n) + \cdots + rw_f^2(n-1)\cdot K_{n-1}(k,n) + (-1)^k rw_f^2(n). \quad (2)\end{aligned}$$

Заметим, что по п. 1 теоремы 2 для чётных i значения $rw_f(i) = 0$, а по п. 2 той же теоремы для нечётных i значения $rw_f(i) = 2\sum_{i=0}^{\frac{n-1}{2}} K_i(k,n)$. Подставляя эти величины в соотношение (2), получаем

$$\begin{aligned}rw_f^2(1)\cdot K_1(k,n) + rw_f^2(3)\cdot K_3(k,n) + \cdots + rw_f^2(n-2)\cdot K_{n-2}(k,n) + (-1)^k rw_f^2(n) \\ = 4(K_1(k,n)\cdot Q_1^2 + K_3(k,n)\cdot Q_3^2 + \cdots + (-1)^k Q_n^2), \quad (3)\end{aligned}$$

где $Q_p = \sum_{i=0}^{\frac{n-1}{2}} K_i(p,n)$. Следовательно, согласно теореме 1, чтобы доказать принадлежность вектора ω множеству $E_{\mathrm{PC}}(f)$, достаточно показать, что сумма внутри скобок в выражении (3) равна нулю. Обозначим эту сумму через Ф.

Заметим, что по теореме 3

$$|Q_p| = |Q_{n-p+1}|, \quad 1 \leqslant p \leqslant n. \quad (4)$$

Тогда по пп. 2 и 3 утверждения 3 и тождеству (4) сумма Ф принимает вид

$$\begin{aligned}\Phi &= Q_1^2\big(K_1(k,n) + (-1)^k\big) + Q_3^2(K_3(k,n) + K_{n-2}(k,n)) + \cdots \\ &\quad + Q_{\lfloor \frac{n}{2}\rfloor}^2\big(K_{\lfloor \frac{n}{2}\rfloor}(k,n) + K_{\lceil \frac{n}{2}\rceil+1}(k,n)\big) \\ &= Q_1^2\big(n-2k+(-1)^k\big) + Q_3^2\big(K_3(k,n) + (-1)^k K_2(k,n)\big) + \cdots \\ &\quad + Q_{\lfloor \frac{n}{2}\rfloor}^2\big(K_{\lfloor \frac{n}{2}\rfloor}(k,n) + (-1)^k K_{\lfloor \frac{n}{2}\rfloor-1}(k,n)\big).\end{aligned}$$

(1) Если $k = \lfloor n/2 \rfloor = (n-1)/2$ (т. е. k нечётно), то, воспользовавшись вторым соотношением Паскаля (п. 2 утверждения 5), получим

$$\begin{aligned}\Phi &= Q_1^2(n-1-2k) + Q_3^2 K_3(k+1,n+1) + \cdots + Q_{\lfloor \frac{n}{2}\rfloor}^2 K_{\lfloor \frac{n}{2}\rfloor}(k+1,n+1) \\ &= Q_3^2 K_3\left(\frac{n+1}{2}, n+1\right) + \cdots + Q_{\lfloor \frac{n}{2}\rfloor}^2 K_{\lfloor \frac{n}{2}\rfloor}\left(\frac{n+1}{2}, n+1\right).\end{aligned}$$

По п. 5 утверждения 3 все слагаемые суммы Ф обращаются в нуль. Следовательно, $\Phi = 0$ и $\omega \in E_{\mathrm{PC}}(f)$. И наконец, согласно утверждению 2 все векторы из V_n веса $\lfloor n/2 \rfloor$ удовлетворяют критерию распространения для функции f.

(2) Если $k = \lceil n/2 \rceil = (n+1)/2$ (т. е. k чётно), то, воспользовавшись первым соотношением Паскаля (п. 1 утверждения 5), получим

$$\Phi = Q_1^2(n+1-2k) + Q_3^2 K_3(k,n+1) + \cdots + Q_{\lfloor \frac{n}{2}\rfloor}^2 K_{\lfloor \frac{n}{2}\rfloor}(k,n+1).$$

Проведя аналогичные предыдущему пункту рассуждения, заключаем, что все векторы из V_n веса $\lceil n/2 \rceil$ тоже удовлетворяют критерию распространения для функции f.

Теперь рассмотрим случай, когда n — чётное и $n/2$ — нечётное. Выберем $\omega \in E_{\mathrm{PC}}(f)$ так, чтобы $\mathrm{wt}(\omega) = n/2$, и при помощи теоремы 1 докажем, что $\omega \in E_{\mathrm{PC}}(f)$. Как и в случае с нечётным n, справедливо равенство

$$\sum_{x \in V_n} (-1)^{\langle x,\omega \rangle} W_f^2(x) = rw_f^2(0) + rw_f^2(1) \cdot K_1\left(\frac{n}{2}, n\right) + \cdots + rw_f^2(n-1) \cdot K_{n-1}\left(\frac{n}{2}, n\right) + (-1)^{\frac{n}{2}} rw_f^2(n). \quad (5)$$

Сгруппируем слагаемые по коэффициентам Уолша–Адамара от векторов с чётными и нечётными весами и обозначим эти группы через Φ_1 и Φ_2. Тогда, согласно пп. 1 и 2 теоремы 2 выражение (5) примет вид

$$\Phi_1 + \Phi_2 = \left(\binom{n}{\frac{n}{2}}^2 + K_{\frac{n}{2}}^2(2,n) \cdot K_2\left(\frac{n}{2}, n\right) + \cdots + K_{\frac{n}{2}}^2(n-2,n) \cdot K_{n-2}\left(\frac{n}{2}, n\right) + (-1)^{\frac{n}{2}} \binom{n}{\frac{n}{2}}^2\right) + \left(4\widetilde{Q}_1^2 \cdot K_1\left(\frac{n}{2}, n\right) + 4\widetilde{Q}_3^2 \cdot K_3\left(\frac{n}{2}, n\right) + \cdots + 4\widetilde{Q}_{n-1}^2 \cdot K_{n-1}\left(\frac{n}{2}, n\right)\right),$$

где $\widetilde{Q}_p = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} K_i(p,n)$.

Заметим, что в сумме Φ_2 по п. 5 утверждения 3 все полиномы Кравчука $K_i(n/2, n)$, $i \in \{1, 3, \ldots, n-1\}$, равны нулю. Следовательно, $\Phi_2 = 0$.

Теперь рассмотрим сумму Φ_1. По пп. 3 и 4 утверждения 3 справедливы равенства $K_{n/2}^2(i,n) = K_{n/2}^2(n-i,n)$ и $K_i(n/2,n) = -K_{n-i}(n/2,n)$ при любом i, $0 \leqslant i \leqslant n$. Тогда

$$\begin{aligned}\Phi_1 &= \binom{n}{\frac{n}{2}}^2 \left(1 + (-1)^{\frac{n}{2}}\right) + K_{\frac{n}{2}}^2(2,n)\left(K_2\left(\frac{n}{2}, n\right) + K_{n-2}\left(\frac{n}{2}, n\right)\right) + \cdots \\ &\quad + K_{\frac{n}{2}}^2\left(\frac{n}{2} - 1, n\right)\left(K_{\frac{n}{2}-1}\left(\frac{n}{2}, n\right) + K_{\frac{n}{2}+1}\left(\frac{n}{2}, n\right)\right) \\ &= K_{\frac{n}{2}}^2(2,n)\left(K_2\left(\frac{n}{2}, n\right) - K_2\left(\frac{n}{2}, n\right)\right) + \cdots \\ &\quad + K_{\frac{n}{2}}^2\left(\frac{n}{2} - 1, n\right)\left(K_{\frac{n}{2}-1}\left(\frac{n}{2}, n\right) - K_{\frac{n}{2}-1}\left(\frac{n}{2}, n\right)\right) = 0.\end{aligned}$$

Таким образом, согласно теореме 1 вектор ω с весом $\mathrm{wt}(\omega) = n/2$ принадлежит множеству $E_{\mathrm{PC}}(f)$. И наконец, на основании утверждения 2 все векторы из V_n веса $n/2$ удовлетворяют критерию распространения для функции f. Теорема доказана. □

Остаются открытыми вопросы, связанные с критерием распространения для строго мажоритарных функций.

(1) Существуют ли векторы с весом Хэмминга, отличающимся от указанных в теореме 4, которые принадлежат множеству критерия распространения для строго мажоритарной функции от n переменных, где $\lfloor n/2 \rfloor$ нечётно?
(2) Обладают ли критерием распространения строго мажоритарные функции от n переменных в случае, когда $\lfloor n/2 \rfloor$ чётно? Если да, то векторы каких весов принадлежат множеству критерия распространения для строго мажоритарной функции такого типа и при каком именно n?

Пример 1. Пусть $f \in \mathcal{F}_7$ — строго мажоритарная функция. По теореме 4 ясно, что векторы из V_7 весов 3 и 4 удовлетворяют критерию распространения. Проверим, принадлежат ли множеству критерия распространения векторы с весом, не равным 3 и 4, воспользовавшись теоремой 1.

По доказательству теоремы 4 имеем следующую сумму:

$$\Phi = Q_1^2\big(7-2k+(-1)^k\big) + Q_3^2\big(K_3(k,7)+(-1)^k K_2(k,7)\big) = 400\big(7-2k+(-1)^k\big) + 16\big(K_3(k,7)+(-1)^k K_2(k,7)\big)$$

Теперь рассмотрим два случая, когда k чётно или нечётно.

(1) Пусть k чётно. Тогда по первому соотношению Паскаля выражение Φ принимает вид
$$\Phi = 400(8-2k) + 16K_3(k,8).$$
где $K_3(k,8) = \binom{8-k}{3} - k\binom{8-k}{2} + \binom{k}{2}(8-k) - \binom{k}{3}$.
   (a) Если $k=2$, то $\Phi = 400\cdot 4 + 16\cdot(-4) = 1536 \neq 0$.
   (b) Если $k=6$, то $\Phi = 400\cdot(-4) + 16\cdot 4 = -1536 \neq 0$.
(2) Пусть k нечётно. Тогда по второму соотношению Паскаля выражение Φ принимает вид
$$\Phi = 400(6-2k) + 16K_3(k+1,8).$$
   (a) Если $k=1$, то $\Phi = 400\cdot 4 + 16\cdot(-4) = 1536 \neq 0$.
   (b) Если $k=5$, то $\Phi = 400\cdot(-4) + 16\cdot 4 = -1536 \neq 0$.
   (c) Если $k=7$, то $\Phi = 400\cdot(-8) + 16\cdot(-56) = -4096 \neq 0$.

Таким образом, не существует векторов с весом Хэмминга, не равным 3 и 4, которые удовлетворяют критерию распространения для строго мажоритарной функции $f \in \mathcal{F}_7$.

В дополнение приведём таблицу значений мощности множества критерия распространения для строго мажоритарных функций, полученных в ходе экспериментальных вычислений.

$\boldsymbol{n}$	2	3	4	5	6	7	8	9	10	11	12	13
$\mathbf{pc}_{\boldsymbol{f}}$	3	6	0	0	35	70	0	0	462	924	0	0

Таблица 1: Значения pc_f для строго мажоритарных функций.

На основании результатов, указанных в таблице, можно выдвинуть следующие гипотезы.

Гипотеза 1. *Не существует векторов, удовлетворяющих критерию распространения для строго мажоритарной функции от n переменных, где* $\lfloor n/2 \rfloor$ *чётно.*

Гипотеза 2. *Не существует векторов с весом, отличающимся от* $\lfloor n/2 \rfloor$ *и* $\lceil n/2 \rceil$, *удовлетворяющих критерию распространения для строго мажоритарной функции от* n *переменных, где* n *и* $\lfloor n/2 \rfloor$ *нечётно.*

Гипотеза 3. *Существуют векторы с весом, равным* $n/2-1$ *или* $n/2+1$, *удовлетворяющие критерию распространения для строго мажоритарной функции от* n *переменных, где* n *чётно и* $n/2$ *нечётно.*

В заключение автор выражает искреннюю признательность А. В. Тарасову за ценные замечания и предложения по тексту статьи.

Список литературы

1. Ивченко Г. И., Медведев Ю. И., Миронова В. А., “Многочлены Кравчука и их применения в задачах криптографии и теории кодирования”, *Матем. вопр. криптогр.*, **6**:1 (2015), 33–56.
2. Камловский О. В., “Суммы модулей коэффициентов Уолша–Адамара некоторых сбалансированных булевых функций”, *Матем. вопр. криптогр.*, **8**:4 (2017), 75–98.
3. Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2012, 584 с.
4. Carlet C., *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, 2020, 574 pp.
5. Dalai D. K., Maitra S., Sarkar S., “Basic theory in construction of Boolean functions with maximum possible annihilator immunity”, *Designs, Codes and Cryptography*, **40** (2006), 41–58.
6. Feinsilver P., “Sums of squares of Krawtchouk polynomials, Catalan numbers, and some algebras over the Boolean lattice”, *Int. J. Math. Comp. Sci.*, **12**:1 (2017), 65–83.
7. Krawtchouk M., “Sur une généralisation des polynômes d’Hermite”, *Comptes Rendus Math.*, **189** (1929), 620–622.
8. Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J., “Propagation characteristics of Boolean functions”, EUROCRYPT 1990, Lect. Notes Comput. Sci., **473**, 1990, 161–173.
9. Rothaus O. S., “On “Bent” Functions”, *J. Comb. Theory* (A), **20**:3 (1976), 300–305.
10. Titswort R. C., *Correlation properties of cyclic sequences*, Ph. D. dissertation, Calif. Inst. Technol., Pasadena, California, 1962, 244 pp.

Статья поступила 11.01.2023.