2013 Теоретические основы прикладной дискретной математики №2(20)

DOI 10.17223/20710410/20/3

УДК 519.7

О СВЯЗЯХ МЕЖДУ НЕКОТОРЫМИ ПАРАМЕТРАМИ СОВЕРШЕННО УРАВНОВЕШЕННЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

С. В. Смышляев

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: smyshsv@gmail.com

Для класса совершенно уравновешенных булевых функций с барьером доказываются соотношения, связывающие между собой определённые параметры таких функций. В частности, получены общие результаты о свойствах полиномов функций с барьером, позволяющие установить новые оценки числа инверсионных функций для произвольной функции с барьером.

Ключевые слова: *совершенно уравновешенные функции, функции с барьером, криптография.*

Введение

Для обеспечения у используемых в криптографических целях кодирующих устройств, построенных на основе регистра сдвига и булевой функции усложнения [1 – 3], свойства сохранения равномерного распределения преобразуемой двоичной последовательности функции усложнения выбираются из множества совершенно уравновешенных булевых функций [2, 4, 5]. Среди таких функций особое место занимают функции с барьером [2, 6], обладающие также положительным свойством отсутствия предсказывания [2, 7]. Для функций с барьером в работе [7] введены целочисленные параметры, определённым образом характеризующие отображения, реализуемые кодирующими устройствами с такими функциями при фиксированном начале входной последовательности.

Настоящая работа посвящена вопросам о соотношениях между параметрами функций с барьером. В частности, доказано утверждение об определённых свойствах полиномиальных представлений таких функций — вопрос, результаты по которому ранее отсутствовали, за исключением частных и тривиальных.

Полученные результаты позволяют расширить область применимости утверждения о числе инверсионных функций, полученного в работе [8]. Данное утверждение представляет собой решение открытого вопроса, поставленного в работе Х. Лэя и Дж. Месси [9], и содержит выражение, позволяющее вычислить число инверсионных функций по трём параметрам функции: числу переменных, длине барьера и параметру e_f^R, описанному в [7]. С использованием полученных результатов возможно эффективное (с полиномиальной относительно длины входа сложностью) нахождение по полиномиальному представлению булевой функции нетривиальных оценок на e_f^R и, следовательно, на число инверсионных функций.

1. Определения и предварительные результаты

Будем использовать следующие обозначения. Множество двоичных наборов длины n будем обозначать через $V_n = \{0,1\}^n$, множество булевых функций n переменных — через $\mathcal{F}_n$.

[1]Работа поддержана РФФИ (проект № 12-01-00680-а).

Для всяких $n, l \in \mathbb{N}$, $f \in \mathcal{F}_n$ будем через f_l обозначать следующее отображение из V_{l+n-1} в V_l:

$$f_l(x_1, x_2, \ldots, x_{l+n-1}) \equiv (f(x_1, \ldots, x_n), f(x_2, \ldots, x_{n+1}), \ldots, f(x_l, \ldots, x_{l+n-1})).$$

Отображение f_l описывает преобразование, производимое l тактами работы кодирующего устройства, которое построено подсоединением входов реализующей булеву функцию f схемы к ячейкам двоичного регистра сдвига [1, 4].

Для всяких $n, l, p \in \mathbb{N}$, $p \leqslant l + n - 1$, $f \in \mathcal{F}_n$ и любого набора $(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p) \in V_p$ будем через $f_{R,l,p}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_p)}$ обозначать следующее отображение из $V_{l+n-1-p}$ в V_l:

$$f_{R,l,p}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_p)}(x_1, x_2, \ldots, x_{l+n-1-p}) \equiv f_l(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p, x_1, x_2, \ldots, x_{l+n-1-p}),$$

и через $f_{L,l,p}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_p)}$ — следующее отображение из $V_{l+n-1-p}$ в V_l:

$$f_{L,l,p}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_p)}(x_1, x_2, \ldots, x_{l+n-1-p}) \equiv f_l(x_1, x_2, \ldots, x_{l+n-1-p}, \tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p).$$

Отображение $f_{R,l,p}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_p)}$ описывает преобразование, производимое l тактами работы кодирующего устройства с функцией усложнения f на двоичных последовательностях с фиксированным началом $(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p)$.

Приведём понятия совершенно уравновешенной булевой функции, а также барьера булевой функции.

Определение 1 [6]. Булева функция $f \in \mathcal{F}_n$ называется совершенно уравновешенной, если соотношение

$$\left|f_m^{-1}(y)\right| = 2^{n-1}$$

выполняется для любого $m \in \mathbb{N}$ и любого $y \in V_m$.

Множество совершенно уравновешенных функций из $\mathcal{F}_n$ будем обозначать $\mathcal{PB}_n$.

Определение 2 [6]. Булева функция $f \in \mathcal{F}_n$ называется функцией с правым барьером длины b, $b \in \mathbb{N}$, если система уравнений

$$\begin{cases} f_{b'}(x_1, x_2, \ldots, x_{b'+n-1}) = f_{b'}(z_1, z_2, \ldots, z_{b'+n-1}), \\ x_1 = z_1, \ldots, x_{n-1} = z_{n-1}, x_n = 0, z_n = 1 \end{cases}$$

имеет решение при всяком $b' \in \mathbb{N}$, таком, что $b' \leqslant b - 1$, а система уравнений

$$\begin{cases} f_b(x_1, x_2, \ldots, x_{b+n-1}) = f_b(z_1, z_2, \ldots, z_{b+n-1}), \\ x_1 = z_1, \ldots, x_{n-1} = z_{n-1}, x_n = 0, z_n = 1 \end{cases}$$

решений не имеет.

Булева функция $f \in \mathcal{F}_n$ называется функцией с левым барьером длины b, если $\overleftrightarrow{f}(x_1, x_2, \ldots, x_n) \equiv f(x_n, x_{n-1}, \ldots, x_1)$ является функцией с правым барьером длины b.

Булева функция $f \in \mathcal{F}_n$ имеет барьер, если она имеет правый или левый барьер, или оба сразу. При этом длиной барьера функции называется соответственно длина правого барьера, левого барьера или меньшая из длин барьеров.

Длины правого и левого барьера булевой функции f будем обозначать через b_f^R и b_f^L соответственно.

Наличие правого (левого) барьера длины 1, как нетрудно заметить, означает линейность функции по последнему (первому) аргументу.

Очевидным является тот факт, что для фиксированного c проверка неравенства $b_f^R \leqslant c$ по полиному функции, содержащему N мономов, требует порядка $(2N+1)^c$ операций. Для этого требуется лишь перемножить (пользуясь только полиномиальным представлением функций) выражения вида $f(x_i, x_{i+1}, \ldots, x_{i+n-1}) \oplus \oplus f(z_i, z_{i+1}, \ldots, z_{i+n-1}) \oplus 1$ для $i = 1, 2, \ldots, c$, затем в полученное полиномиальное представление подставить $x_1 = z_1, \ldots, x_{n-1} = z_{n-1}$, $x_n = 0$, $z_n = 1$, привести подобные и сравнить полученное выражение с нулём — при равенстве, очевидно, функция имеет правый барьер длины не более c.

В работе [7] доказан ряд утверждений о свойствах прообразов выходных наборов относительно отображений $f_{R,l,p}$ и $f_{L,l,p}$ в случае наличия у функции f правого или левого барьера.

Теорема 1 [7]. Для каждой функции $f \in \mathcal{F}_n$ с правым барьером можно определить величину $e_f^R \in \{0, 1, 2, \ldots, b_f^R - 1\}$, $e_f^R \leqslant n-1$, такую, что для любых $p \geqslant n-1$, $l \geqslant b_f^R + p - n$, $(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p) \in V_p$ и любого набора $(y_1, y_2, \ldots, y_l) \in \mathrm{Im}\left(f_{R,l,p}^{(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p)}\right)$ выполняется равенство

$$\left| f_{R,l,p}^{(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p)^{-1}}(y_1, y_2, \ldots, y_l) \right| = 2^{e_f^R}.$$

Теорема 2 [7]. Для каждой функции $f \in \mathcal{F}_n$ с левым барьером можно определить величину $e_f^L \in \{0, 1, 2, \ldots, b_f^L - 1\}$, $e_f^L \leqslant n-1$, такую, что для любых $p \geqslant n-1$, $l \geqslant b_f^L + p - n$, $(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p) \in V_p$ и любого набора $(y_1, y_2, \ldots, y_l) \in \mathrm{Im}\left(f_{L,l,p}^{(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p)}\right)$ выполняется равенство

$$\left| f_{L,l,p}^{(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_p)^{-1}}(y_1, y_2, \ldots, y_l) \right| = 2^{e_f^L}.$$

Следствие 1 [7]. Для любой функции $f \in \mathcal{F}_n$, имеющей правый (левый) барьер, любых $l \geqslant b_f^R - 1$ ($l \geqslant b_f^L - 1$) и $x \in V_{n-1}$ верно равенство $\left|\mathrm{Im}(f_{R,l,n-1}^x)\right| = 2^{l - e_f^R}$ ($\left|\mathrm{Im}(f_{L,l,n-1}^x)\right| = 2^{l-e_f^L}$).

Лемма 1 [7]. Если у некоторой $f \in \mathcal{F}_n$ есть правый (левый) барьер, то $e_f^R = 0$ (соответственно, $e_f^L = 0$) тогда и только тогда, когда $b_f^R = 1$ ($b_f^L = 1$).

Лемма 2 [7]. Пусть $f(x_1, x_2, \ldots, x_n) \in \mathcal{F}_n$ имеет правый (левый) барьер. Тогда $e_f^R = b_f^R - 1$ (соответственно, $e_f^L = b_f^L - 1$) тогда и только тогда, когда функция f не зависит существенно от переменных $x_{n-b_f^R+2}, x_{n-b_f^R+3}, \ldots, x_n$ и линейна по переменной $x_{n-b_f^R+1}$ (не зависит существенно от переменных $x_1, x_2, \ldots, x_{b_f^L-1}$ и линейна по переменной $x_{b_f^L}$).

В работе [9] введено понятие инверсионной функции, которое в терминах функций с правым барьером может быть определено следующим образом.

Определение 3. Пусть $f \in \mathcal{F}_n$ имеет правый барьер. Тогда булева функция $\hat{f} \in \mathcal{F}_{b_f^R+n-1}$ является инверсионной для функции f, если для всякого набора $(x_1, x_2, \ldots, x_{b_f^R+n-1}) \in V_{b_f^R+n-1}$ выполняется равенство

$$\hat{f}(x_1, x_2, \ldots, x_{n-1}, f(x_1, x_2, \ldots, x_n), \ldots, f(x_{b_f^R}, x_{b_f^R+1}, \ldots, x_{b_f^R+n-1})) = x_n.$$

Исследования понятия инверсионной функции проводились в работах [10, 11]. Тем не менее оставался открытым поставленный в конце работы [9] вопрос о числе инверсионных функций для фиксированной функции с правым барьером. Из доказанных в работах [7, 8] свойств функций без предсказывания вытекает следующая теорема.

Теорема 3 [8]. Если $f \in \mathcal{F}_n$ имеет правый барьер, то для f существует в точности $2^{2^{b_f^R+n-1}\left(1-2^{-e_f^R}\right)}$ инверсионных функций.

Несмотря на полученное утверждение о числе инверсионных функций, при вычислении данной величины в случае представления функции полиномом существует серьёзная проблема. В отличие от параметров n и b_f^R, для нахождения значения параметра e_f^R (или для проверки неравенства $e_f^R \leqslant c$ для фиксированного c) по полиномиальному представлению нет известных алгоритмов полиномиальной относительно длины входа сложности. То есть нахождение числа инверсионных функций для булевой функции от n переменных, представленной полиномом длины $\mathrm{O}(n)$, требует порядка 2^n операций. Таким образом, актуальна задача нахождения соотношений между параметром e_f^R и легко вычислимыми по полиному параметрами функций, которые позволят строить эффективные алгоритмы для получения нетривиальных оценок e_f^R (а значит, и нетривиальных оценок числа инверсионных функций) по полиному функции f.

При дальнейших построениях будет использован известный критерий равенства алгебраической степени булевой функции числу её переменных.

Лемма 3 [2]. Пусть $f \in \mathcal{F}_n$. Функция f имеет алгебраическую степень n тогда и только тогда, когда её вес нечётен.

2. Основные результаты

Обозначим для произвольной функции $f \in \mathcal{F}_n$ через t_f^R наибольшее целое t', такое, что в полиноме функции f присутствует моном, который содержит все переменные $x_n, x_{n-1}, \ldots, x_{n-t'+1}$, через t_f^L — наибольшее целое t'', такое, что в полиноме функции f присутствует моном, который содержит все переменные $x_1, x_2, \ldots, x_{t''}$.

Теорема 4. Пусть функция $f \in \mathcal{F}_n$ имеет правый барьер, $b_f^R \geqslant 2$. Тогда выполняется соотношение $e_f^R + t_f^R \leqslant b_f^R - 1$.

Доказательство. Если $t_f^R = 0$, то утверждение непосредственно следует из теоремы 1, поэтому далее предполагаем $t_f^R \geqslant 1$. Так как функция f имеет барьер, то она совершенно уравновешена, а следовательно, и уравновешена, откуда по лемме 3 получаем $t_f^R \leqslant n-1$. Введём обозначение $t = \min\{t_f^R, b_f^R - 1\}$ и рассмотрим набор $(a_1^*, a_2^*, \ldots, a_{n-t}^*) \in V_{n-t}$, такой, что функция $f'(x_{n-t+1}, x_{n-t+2}, \ldots, x_n) \equiv \equiv f(a_1^*, a_2^*, \ldots, a_{n-t}^*, x_{n-t+1}, x_{n-t+2}, \ldots, x_n)$ имеет алгебраическую степень t.

Пусть $a^* = (0, 0, \ldots, 0, a_1^*, a_2^*, \ldots, a_{n-t}^*)$. Рассмотрим отображение $f^{a^*}_{R,b_f^R-1,n-1}$. Оно представимо в следующем виде:

$$f^{a^*}_{R,b_f^R-1,n-1}(x_n, x_{n+1}, \ldots, x_{b_f^R+n-2}) \equiv$$

$$\equiv \left(g^{(1)}(x_n), g^{(2)}(x_n, x_{n+1}), \ldots, g^{(t)}(x_n, x_{n+1}, \ldots, x_{n+t-1}), \ldots, g^{(b_f^R-1)}(x_n, x_{n+1}, \ldots, x_{n+b_f^R-2})\right).$$

Заметим, что функция $g^{(t)}$ в точности равна функции f'. Введя для функции $g^{(t)}$ фиктивные переменные в количестве $b_f^R - 1 - t$, перейдём к рассмотрению $\tilde{g}(x_1, x_2, \ldots, x_{b_f^R-1}) \equiv g^{(t)}(x_1, x_2, \ldots, x_t)$.

С одной стороны, $\mathrm{wt}(\tilde{g}) = 2^{b_f^R-1-t} \cdot \mathrm{wt}(g^{(t)})$. Так как $g^{(t)} \equiv f'$ имеет алгебраическую степень t, то в соответствии с леммой 3 значение $\mathrm{wt}(g^{(t)})$ нечётно, поэтому $\mathrm{wt}(\tilde{g})$ не делится на $2^{b_f^R-t}$.

С другой стороны, как следует из теоремы 1,

$$\mathrm{wt}(\tilde{g})=\left|\tilde{g}^{-1}(1)\right|=\sum_{\substack{y_1,y_2,\dots,y_{t-1},\\ y_{t+1},\dots,y_{b_f^R-1}\in\{0,1\}}}\left|{f^{x^*}_{R,b_f^R-1,n-1}}^{-1}(y_1,y_2,\dots,y_{t-1},1,y_{t+1},\dots,y_{b_f^R-1})\right|=C\cdot 2^{e_f^R},$$

где C — некоторое целое положительное число.

Таким образом, $2^{e_f^R}$ не делится на $2^{b_f^R-t}$, откуда получаем $e_f^R\leqslant b_f^R-t-1$. Если $t=\min\{t_f^R,b_f^R-1\}=b_f^R-1$, то получим $e_f^R\leqslant 0$, то есть, с учётом леммы 1, $b_f^R=1$, что противоречит условию. Таким образом, $t=t_f^R$ и $e_f^R\leqslant b_f^R-t_f^R-1$, что завершает доказательство теоремы. ■

Данное утверждение означает, что при наличии в полиномиальном представлении булевой функции n переменных монома, содержащего одновременно переменные $x_n,x_{n-1},\dots,x_{n-t+1}$ (то есть при $t_f^R\geqslant t$), выполнено $e_f^R\leqslant b_f^R-1-t$, что, с учётом теоремы 3, означает, что данная функция имеет не более $2^{2^{b_f^R+n-1}\left(1-2^{t+1-b_f^R}\right)}$ инверсионных функций.

Замечание 1. Заметим, что неравенство $e_f^R+t_f^R\leqslant b_f^R-1$ может обращаться, а может и не обращаться в равенство. Например, для функции $f^{(1)}(x_1,x_2,x_3,x_4)=$ $=x_3\oplus x_2x_4\oplus x_1x_2x_4$ верно, что $b^R_{f^{(1)}}=3$, $e^R_{f^{(1)}}=1$, $t^R_{f^{(1)}}=1$, то есть $e^R_{f^{(1)}}+t^R_{f^{(1)}}=b^R_{f^{(1)}}-1$; для функции $f^{(2)}(x_1,x_2,x_3,x_4,x_5)=x_4\oplus x_1x_5\oplus x_1x_2x_3x_5$ верно, что $b^R_{f^{(2)}}=4$, $e^R_{f^{(2)}}=1$, $t^R_{f^{(2)}}=1$, то есть $e^R_{f^{(2)}}+t^R_{f^{(2)}}<b^R_{f^{(2)}}-1$.

Абсолютно аналогично теореме 4 доказывается следующее утверждение.

Теорема 5. Пусть функция $f\in\mathcal{F}_n$ имеет левый барьер, $b_f^L\geqslant 2$. Тогда выполняется соотношение $e_f^L+t_f^L\leqslant b_f^L-1$.

Следствие 2. Пусть функция $f\in\mathcal{F}_n$ имеет правый барьер, $2\leqslant b_f^R\leqslant n$. Тогда в полиноме функции $f(x_1,x_2,\dots,x_n)$ нет мономов, содержащих одновременно переменные $x_n,x_{n-1},\dots,x_{n-b_f^R+2}$.

Доказательство. Как следует из теоремы 1 и леммы 1, для функции f верно $e_f^R\geqslant 1$. По теореме 4 верно $e_f^R+t_f^R\leqslant b_f^R-1$, откуда $t_f^R\leqslant b_f^R-2$, то есть в полиноме функции $f(x_1,x_2,\dots,x_n)$ не может быть мономов, содержащих одновременно переменные $x_n,x_{n-1},\dots,x_{n-b_f^R+2}$. ■

Для произвольной функции $f\in\mathcal{F}_n$ с правым барьером длины 3 с помощью следствия 2 можно получить, что в разложении $f(x_1,x_2,\dots,x_n)=f_{(00)}(x_1,x_2,\dots,x_{n-2})\oplus$ $\oplus x_{n-1}f_{(01)}(x_1,x_2,\dots,x_{n-2})\oplus x_nf_{(10)}(x_1,x_2,\dots,x_{n-2})\oplus x_nx_{n-1}f_{(11)}(x_1,x_2,\dots,x_{n-2})$ функция $f_{(11)}$ тождественно равна нулю. Таким образом, полученное в работе [6] необходимое условие барьера длины 3 является тривиальным частным следствием полученного общего утверждения.

Следствие 3. Пусть функция $f\in\mathcal{F}_n$ имеет левый барьер, $2\leqslant b_f^L\leqslant n$. Тогда в полиноме функции $f(x_1,x_2,\dots,x_n)$ нет мономов, содержащих одновременно переменные $x_1,x_2,\dots,x_{b_f^L-1}$.

Теорема 6. Пусть $n\geqslant 2$. Если для некоторой функции $f\in\mathcal{F}_n$, отличной от x_1 и $x_1\oplus 1$, верно $b_f^R\geqslant n$, то $e_f^R\leqslant b_f^R-3$.

Доказательство. Будем доказывать индукцией по n. В случае $n\leqslant 2$ утверждение очевидно, так как все функции из $\mathcal{F}_2$ с правым барьером длины 2 — это функции x_1 и $x_1\oplus 1$, а функций двух переменных с барьером большей длины не существует.

Пусть $n \geqslant 3$. Предположим противное: существует функция $f \in \mathcal{F}_n$, не равная x_1 и $x_1 \oplus 1$, такая, что $b_f^R \geqslant n$, $e_f^R \geqslant b_f^R - 2$. При этом, с учётом теоремы 1 и леммы 2, $e_f^R \leqslant n-1$, $e_f^R < b_f^R - 1$, поэтому необходимо рассмотреть только такие функции f, что $b_f^R = n$, $e_f^R = b_f^R - 2 = n-2$. Если при этом f не зависит существенно от x_n, то для функции $f'(x_1, x_2, \ldots, x_{n-1}) \equiv f(x_1, x_2, \ldots, x_{n-1}, 0)$, $f' \in \mathcal{F}_{n'}$, $n' = n-1$, верно $b_{f'}^R = b_f^R - 1 = n'$, $e_{f'}^R = e_f^R - 1 = n' - 2$ и противоречие следует из предположения индукции. Пусть теперь f существенно зависит от x_n. В соответствии с теоремой 4 $t_f^R \leqslant (b_f^R - 1) - (b_f^R - 2) = 1$. Таким образом:

1) для всякого набора констант $(a_1, a_2, \ldots, a_{n-2}) \in V_{n-2}$ функция $f(a_1, a_2, \ldots, a_{n-2}, x_{n-1}, x_n)$ либо линейна по x_n, либо не зависит существенно от x_n;
2) существует набор констант $(a_1^*, a_2^*, \ldots, a_{n-2}^*) \in V_{n-2}$, такой, что функция $f(a_1^*, a_2^*, \ldots, a_{n-2}^*, x_{n-1}, x_n)$ существенно зависит от x_n.

Отсюда следует, что функция $f(a_1^*, a_2^*, \ldots, a_{n-2}^*, x_{n-1}, x_n)$ линейна по переменной x_n, а значит, функции $f(a_1^*, a_2^*, \ldots, a_{n-2}^*, 0, x_n)$ и $f(a_1^*, a_2^*, \ldots, a_{n-2}^*, 1, x_n)$ также линейны по x_n. При этом, так как $b_f^R = n$ и $e_f^R = n-2$, то, по следствию 1,

$$\left|\mathrm{Im}\left(f_{R,n-1,n-1}^{(a_1^*,a_2^*,\ldots,a_{n-2}^*,0)}\right)\right| = \left|\mathrm{Im}\left(f_{R,n-1,n-1}^{(a_1^*,a_2^*,\ldots,a_{n-2}^*,1)}\right)\right| = 2. \tag{1}$$

С учётом линейной зависимости первых компонент значений векторных отображений $f_{R,n-1,n-1}^{(a_1^*,a_2^*,\ldots,a_{n-2}^*,0)}$ и $f_{R,n-1,n-1}^{(a_1^*,a_2^*,\ldots,a_{n-2}^*,1)}$ от переменной x_n имеем

$$\left|\mathrm{Im}\left(f_{R,1,n-1}^{(a_1^*,a_2^*,\ldots,a_{n-2}^*,0)}\right)\right| = \left|\mathrm{Im}\left(f_{R,1,n-1}^{(a_1^*,a_2^*,\ldots,a_{n-2}^*,1)}\right)\right| = 2. \tag{2}$$

Из равенств (1) и (2) получаем

$$\left|\mathrm{Im}\left(f_{R,n-2,n-1}^{(a_2^*,a_3^*,\ldots,a_{n-2}^*,d_1,d_2)}\right)\right| = 1 \tag{3}$$

для любых $d_1, d_2 \in \{0,1\}$.

Из (3) следует, что при всяких $d_1, d_2 \in \{0,1\}$ после фиксации начальных $n-1$ переменных отображения f_{n-2} значениями $a_2^*, a_3^*, \ldots, a_{n-2}^*, d_1, d_2$ получаем постоянный вектор: $f_{n-2}(a_2^*, a_3^*, \ldots, a_{n-2}^*, d_1, d_2, x_1, x_2, \ldots, x_{n-2}) \equiv (q_1^{d_1,d_2}, q_2^{d_1,d_2}, \ldots, q_{n-2}^{d_1,d_2}) \in V_{n-2}$. Следовательно, при произвольной фиксации первых двух переменных d_1 и d_2 функция f обращается в константную: $f(d_1, d_2, x_1, x_2, \ldots, x_{n-2}) \equiv q_{n-2}^{d_1,d_2}$. Следовательно, f зависит существенно только от первых двух переменных, что противоречит существенной зависимости от последней переменной. Полученное противоречие завершает доказательство утверждения. ■

Теорема 7. Пусть $n \geqslant 2$. Если для некоторой функции $f \in \mathcal{F}_n$, отличной от x_n и $x_n \oplus 1$, верно $b_f^L \geqslant n$, то $e_f^L \leqslant b_f^L - 3$.

ЛИТЕРАТУРА

1. *Preparata F. P.* Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties // IEEE Trans. Electron. Comput. 1966. V. 15. No. 6. P. 898–909.
2. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012.
3. *Golić J. Dj.* On the security of nonlinear filter generators // LNCS. 1996. V. 1039. P. 173–188.

4. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики. 1994. Т. 1. Вып. 1. С. 33–55.
5. *Smyshlyaev S. V.* Perfectly balanced Boolean functions and Golić conjecture // J. Cryptology. 2012. No. 25(3). P. 464–483.
6. *Логачев О. А., Смышляев С. В., Ященко В. В.* Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. Т. 21. Вып. 2. С. 51–74.
7. *Смышляев С. В.* Булевы функции без предсказывания // Дискретная математика. 2011. Т. 23. Вып. 1. С. 102–118.
8. *Смышляев С. В.* О свойствах булевых функций без предсказывания // Материалы Шестой Междунар. науч. конф. по проблемам безопасности и противодействия терроризму (МГУ им. М. В. Ломоносова, Москва, 11–12 ноября 2010). М.: МЦНМО, 2011. С. 47–56.
9. *Lai X. and Massey J.* Some connections between scramblers and invertible automata // Proc. 1988 Beijing Int. Workshop on Info. Theory. Beijing, China, July 4–8, 1988. P. DI-5.1–DI-5.5.
10. *Смышляев С. В.* О преобразовании двоичных последовательностей с помощью совершенно уравновешенных булевых функций // Материалы Пятой Междунар. науч. конф. по проблемам безопасности и противодействия терроризму (МГУ им. М. В. Ломоносова, Москва, 29–30 октября 2009). М.: МЦНМО, 2010. С. 31–41.
11. *Смышляев С. В.* О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. 2010. № 1(7). С. 5–15.