2010 Теоретические основы прикладной дискретной математики №3(9)

DOI 10.17223/20710410/9/4

УДК 519.7

ПОСТРОЕНИЕ КЛАССОВ СОВЕРШЕННО УРАВНОВЕШЕННЫХ БУЛЕВЫХ ФУНКЦИЙ БЕЗ БАРЬЕРА[1]

С. В. Смышляев

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

E-mail: smyshsv@gmail.com

Из результатов предыдущих работ, посвященных классу совершенно уравновешенных булевых функций (булевых функций без запрета), можно сделать вывод, что в данном классе особый интерес представляет подкласс функций без барьера. Ранее было доказано, что он не является пустым, тем не менее никаких оценок его мощности, отличных от тривиальных, предложено не было. В настоящей работе рассматриваются методы построения совершенно уравновешенных булевых функций без барьера, основанные на специального вида операции композиции булевых функций и на важных свойствах данной операции. Как следствие применения одного из методов получена нижняя оценка числа совершенно уравновешенных функций без барьера n переменных: $2^{2^{n-3}-n+2}$.

Ключевые слова: *булевы функции без запрета, совершенно уравновешенные функции, барьеры булевых функций, фильтрующий генератор, криптография.*

Введение

Понятие функции без запрета (совершенно уравновешенной функции) было рассмотрено в работах [1, 2], в тех же работах был получен ряд важных критериев для данного класса функций. В частности, из результатов [1, 2], а также работы [3] следует отсутствие у определенного класса преобразований двоичных последовательностей, построенных с помощью совершенно уравновешенных функций, некоторых криптографических слабостей.

В работе [4] было введено понятие свойства наличия у булевой функции барьера, достаточного для совершенной уравновешенности; были доказаны некоторые утверждения о данном классе функций. В частности, был получен результат о существовании совершенно уравновешенных функций без барьера, однако каких-либо нетривиальных оценок числа таких функций получено не было.

Изучение свойств функций с барьером было продолжено в [5, 6], и из результатов данных работ (а также работы [7]) следует наличие определенных криптографических слабостей у таких функций. Ввиду этих результатов особый интерес стала представлять задача построения широких классов совершенно уравновешенных функций без барьера.

Благодаря результатам работ [8, 9] некоторые примеры таких классов удалось получить [5, 10, 11], однако общих методов построения предложено не было, так же как и каких-либо оценок мощности таких классов.

В настоящей работе на основе общей схемы построения совершенно уравновешенных функций без барьера по определенным классам функций с барьером (классам функций с левым барьером без правого барьера) приводится важный для теорети-

[1]Работа поддержана РФФИ (проект № 09-01-00653-а).

ческих исследований класс таких функций, явно заданных в полиномиальной форме (очень узким подклассом которого является представленный в [5] класс).

В основной части работы вводится ряд понятий, позволяющих формализовать и в полной мере описать метод построения классов совершенно уравновешенных функций без барьера с помощью помеченных графов специального вида. С помощью данного метода строится широкий класс функций с левым барьером без правого барьера.

В заключительной части работы приводится ряд новых результатов о совершенно уравновешенных функциях, в частности доказывается существование при произвольном n не менее $2^{2^{n-3}-n+2}$ совершенно уравновешенных булевых функций n переменных без барьера.

1. Основные определения и обозначения

Для множества двоичных наборов длины n будем использовать обозначение $V_n = \{0,1\}^n$. Через $\mathcal{F}_n$ будем обозначать множество булевых функций от n переменных.

Пусть $n, m \in \mathbb{N}$, $f \in \mathcal{F}_n$. Рассмотрим систему булевых уравнений:

$$f(x_s, x_{s+1}, \ldots, x_{s+n-1}) = y_s,\ s = 1, 2, \ldots, m. \tag{1}$$

Обозначим для $f \in \mathcal{F}_n$ через f_m следующее отображение из V_{m+n-1} в V_m:

$$f_m(x_1, x_2, \ldots, x_{m+n-1}) = (f(x_1, \ldots, x_n), f(x_2, \ldots, x_{n+1}), \ldots, f(x_m, \ldots, x_{m+n-1})). \tag{2}$$

Отображение f_m можно понимать как порождаемое m тактами работы фильтра — кодирующего устройства, полученного с помощью подключения входов булевой функции f (называемой в таком контексте фильтрующей функцией) к некоторым ячейкам двоичного регистра сдвига.

Определение 1 [2]. Булева функция $f \in \mathcal{F}_n$ называется функцией без запрета (функцией дефекта нуль), если соотношение

$$(f_m)^{-1}(\mathbf{y}) \neq \varnothing$$

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

Определение 2 [2]. Булева функция $f \in \mathcal{F}_n$ называется совершенно уравновешенной, если соотношение

$$\sharp(f_m)^{-1}(\mathbf{y}) = 2^{n-1}$$

выполняется для любого $m \in \mathbb{N}$ и любого $\mathbf{y} \in V_m$. Множество совершенно уравновешенных функций из $\mathcal{F}_n$ обозначим через $\mathcal{PB}_n$.

Введем понятие барьера булевой функции, тесно связанное с понятием совершенной уравновешенности.

Определение 3 [4]. Булева функция $f \in \mathcal{F}_n$ называется функцией с правым барьером длины b, если система уравнений

$$\begin{cases} f(x_1, x_2, \ldots, x_n) = f(z_1, z_2, \ldots, z_n), \\ f(x_2, x_3, \ldots, x_{n+1}) = f(z_2, z_3, \ldots, z_{n+1}), \\ \ldots \\ f(x_{b-1}, x_b, \ldots, x_{b+n-2}) = f(z_{b-1}, z_b, \ldots, z_{b+n-2}), \\ x_1 = z_1, \ldots, x_{n-1} = z_{n-1}, x_n = 0, z_n = 1 \end{cases} \tag{3}$$

имеет решение, а система

$$\begin{cases} f(x_1, x_2, \ldots, x_n) = f(z_1, z_2, \ldots, z_n), \\ f(x_2, x_3, \ldots, x_{n+1}) = f(z_2, z_3, \ldots, z_{n+1}), \\ \ldots \\ f(x_{b-1}, x_b, \ldots, x_{b+n-2}) = f(z_{b-1}, z_b, \ldots, z_{b+n-2}), \\ f(x_b, x_{b+1}, \ldots, x_{b+n-1}) = f(z_b, z_{b+1}, \ldots, z_{b+n-1}), \\ x_1 = z_1, \ldots, x_{n-1} = z_{n-1}, x_n = 0, z_n = 1 \end{cases} \tag{4}$$

решений не имеет.

Булева функция $f \in \mathcal{F}_n$ называется функцией с левым барьером длины b, если $f'(x_1, \ldots, x_n) \equiv f(x_n, \ldots, x_1)$ 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.

Замечание 1. Нетрудно заметить, что наличие правого (левого) барьера длины 1 означает линейность функции по последнему (первому) аргументу.

Для длины правого (левого) барьера функции f будем использовать обозначение b_f^R (b_f^L). Случай отсутствия у функции f правого (левого) барьера будем формально обозначать $b_f^R = \infty$ ($b_f^L = \infty$ соответственно).

Отметим, что для всех утверждений, в которых упоминается длина правого барьера некоторых функций, могут быть очевидным образом построены аналоги с использованием понятия левого барьера. Ввиду этого далее будем говорить только о правых барьерах функций.

2. Предварительные результаты

Утверждение 1 [2, 4]. Следующие преобразования множества $\mathcal{F}_n$ оставляют инвариантным множество $\mathcal{PB}_n$:

1°. $\gamma_0 : \ f(x_1, \ldots, x_n) \to f(x_1, \ldots, x_n) \oplus 1$;
2°. $\gamma_1 : \ f(x_1, \ldots, x_n) \to f(x_1 \oplus 1, \ldots, x_n \oplus 1)$;
3°. $\gamma_2 : \ f(x_1, \ldots, x_n) \to f(x_n, \ldots, x_1)$.

Для исследования свойств совершенно уравновешенных функций важен следующий критерий.

Теорема 1 [2, 12]. Пусть $n \in \mathbb{N}$ и $f \in \mathcal{F}_n$. Тогда следующие утверждения эквивалентны:

— f является совершенно уравновешенной;
— f является функцией без запрета;
— не существует двух различных двоичных последовательностей

$$\mathbf{x} = (x_1, x_2, \ldots, x_r), \mathbf{z} = (z_1, z_2, \ldots, z_r) \in \mathrm{V}_r, r \geqslant 2n - 1,$$

таких, что

$$x_1 = z_1, x_2 = z_2, \ldots, x_{n-1} = z_{n-1}; x_{r-n+2} = z_{r-n+2}, x_{r-n+3} = z_{r-n+3}, \ldots, x_r = z_r;$$
$$f_{r-n+1}(\mathbf{x}) = f_{r-n+1}(\mathbf{z}).$$

Теорема 2 [4]. Наличие барьера у булевой функции является достаточным условием совершенной уравновешенности функции.

Замечание 2. В работе [4], кроме того, было показано, что наличие барьера не является необходимым условием совершенной уравновешенности.

Для построения классов совершенно уравновешенных булевых функций удобно пользоваться следующей конструкцией. Пусть $g \in \mathcal{F}_m$, $h \in \mathcal{F}_n$. Тогда определим функцию $f = g[h] \in \mathcal{F}_{m+n-1}$ следующим образом:

$$f(x_1, \ldots, x_{m+n-1}) = g[h](x_1, \ldots, x_{m+n-1}) = \\ = g(h(x_1, \ldots, x_n), h(x_2, \ldots, x_{n+1}), \ldots, h(x_m, \ldots, x_{m+n-1})).$$

Для данной конструкции верны следующие два утверждения.

Теорема 3 [8]. Пусть $g \in \mathcal{F}_m$, $h \in \mathcal{F}_n$. Функция $f = g[h] \in \mathcal{F}_{m+n-1}$ совершенно уравновешена тогда и только тогда, когда функции g и h совершенно уравновешены.

Теорема 4 [9]. Пусть $g \in \mathcal{F}_m$, $h \in \mathcal{F}_n$, $f = g[h]$. Тогда выполнено соотношение $\max\{b_h^R, b_g^R\} \leqslant b_f^R \leqslant b_h^R + b_g^R - 1$.

3. Основные результаты

С учетом теорем 3, 4 легко получить следующее утверждение, позволяющее строить классы совершенно уравновешенных булевых функций без барьера с помощью совершенно уравновешенных булевых функций без правого барьера.

Лемма 1. Пусть g, h совершенно уравновешены и принадлежат некоторому классу функций без правого барьера или получены из них с помощью преобразования γ_1. Тогда функции $g[h^{\gamma_2}]$ и $g^{\gamma_2}[h]$ являются совершенно уравновешенными функциями без барьера.

В следующем утверждении представлен класс совершенно уравновешенных функций без правого барьера, явно заданных в полиномиальной форме. Доказательство не отличается существенно от доказательства аналогичного утверждения для узкого подмножества данного класса, приведенного в работе [5].

Теорема 5. Пусть

$$f = x_1 \oplus x_{m_1} x_{m_1+1} \cdot h^{(1)}(x_{m_1+2}, x_{m_1+3}, \ldots, x_n) \oplus \\ \oplus x_{m_2} x_{m_2+1} \cdot h^{(2)}(x_{m_2+2}, x_{m_2+3}, \ldots, x_n) \oplus \ldots \oplus \\ \oplus x_{m_k} x_{m_k+1} \cdot h^{(k)}(x_{m_k+2}, x_{m_k+3}, \ldots, x_n),$$

где $h^{(i)} \in \mathcal{F}_{n-m_i-1}$, $i = 1, 2, \ldots, k$, — произвольные булевы функции; $m_{i+1} \geqslant m_i + 2$, $i = 1, 2, \ldots, k-1$; $m_1 \geqslant 2; m_k \leqslant n-1$. Тогда если среди функций $h^{(i)}$, $i = 1, 2, \ldots, k$, нечетное число функций принимает на единичном наборе значение 1, то f является совершенно уравновешенной функцией без правого барьера.

Для изложения метода, позволяющего строить значительно более широкие классы совершенно уравновешенных булевых функций без правого барьера, нам понадобится понятие графа сдвигов булевой функции. Данное понятие было введено в [4]; здесь приведем его в несколько другой форме, более удобной для требуемых построений.

Определение 4. Дополненным графом сдвигов функции $f \in \mathcal{F}_n$ называется ориентированный граф $\Gamma_f = (V, E)$, $\#V = 2^{2n-2}$ (без кратных ребер, с петлями), вершины которого поставлены во взаимно однозначное соответствие упорядоченным парам двоичных наборов длины $n-1$, причем для всяких x_1, …, x_{n-1}, z_1, …, z_{n-1}, u_1, …, u_{n-1}, v_1, …, v_{n-1} верно, что дуга

$$\left(\begin{pmatrix} x_1, \ldots, x_{n-1} \\ z_1, \ldots, z_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} u_1, \ldots, u_{n-1} \\ v_1, \ldots, v_{n-1} \end{pmatrix} \right)$$

присутствует в графе тогда и только тогда, когда выполнено следующее условие:

$$\begin{cases}(x_2,\ldots,x_{n-1}) = (u_1,\ldots,u_{n-2}),\\ (z_2,\ldots,z_{n-1}) = (v_1,\ldots,v_{n-2}).\end{cases}$$

При этом каждая дуга $\left(\begin{pmatrix} x_1,\ldots,x_{n-1}\\ z_1,\ldots,z_{n-1}\end{pmatrix} \longrightarrow \begin{pmatrix} x_2,\ldots,x_n\\ z_2,\ldots,z_n\end{pmatrix}\right)$ помечается значением $f(x_1,x_2,\ldots,x_{n-1},x_n)\oplus f(z_1,z_2,\ldots,z_{n-1},z_n)$. Каждому ориентированному пути в дополненном графе сдвигов Γ_f естественным образом соответствует пара двоичных последовательностей, составленных из меток вершин.

Через $I_f\subset\Gamma_f$ обозначим подграф дополненного графа сдвигов, отвечающий множеству пар равных наборов длины $n-1$; через Γ_f^* — граф, полученный из графа Γ_f удалением всех ребер, лежащих внутри I_f. Γ_f^* называется графом сдвигов функции f.

С использованием теоремы 1 легко доказать следующее утверждение.

Лемма 2. Функция f совершенно уравновешена и не имеет правого барьера в том и только в том случае, когда выполнены следующие условия:

1) в Γ_f^* нет пути ненулевой длины по дугам, помеченным нулем, с началом и концом в подграфе I_f;
2) в Γ_f^* существует путь по дугам, помеченным нулем, ведущий из I_f в некоторый ориентированный цикл, проходящий также исключительно через помеченные нулем дуги в графе Γ_f^*.

Учитывая данное утверждение, опишем общую схему метода построения булевых функций из $\mathcal{PB}_n$ без правого барьера. Рассмотрим граф $\Gamma_{(n)}^*$, представляющий собой граф сдвигов произвольной булевой функции из $\mathcal{F}_n$ без пометок дуг; аналогично введем графы $\Gamma_{(n)}$ и $I_{(n)}$. Для построения множества графов сдвигов Γ_f^* некоторого класса совершенно уравновешенных булевых функций без правого барьера производятся следующие действия:

1) выделяется некоторый цикл в графе $\Gamma_{(n)}^*$;
2) выделяется некоторая вершина в графе $I_{(n)}$ и выбирается некоторый путь из этой вершины в выделенный цикл по дугам графа $\Gamma_{(n)}^*$;
3) выделяется некоторое сечение графа $\Gamma_{(n)}^*$, пересекающее все пути ненулевой длины, имеющие начало и конец в подграфе $I_{(n)}$;
4) производится частичная разметка дуг $\Gamma_{(n)}^*$ таким образом, что:
   - все дуги выделенного цикла становятся помечены нулями;
   - все дуги выбранного пути от выделенной вершины в цикл становятся помечены нулями;
   - все дуги выбранного сечения становятся помечены единицами;
   - остается возможной корректная разметка оставшихся дуг графа до графа сдвигов некоторой булевой функции.

Выбор и соответствующая разметка цикла в графе $\Gamma_{(n)}^*$ и пути до этого цикла гарантируют отсутствие правого барьера у любой функции f, до графа сдвигов которой разметкой оставшихся дуг можно достроить получившийся граф; разметка сечения гарантирует совершенную уравновешенность любой такой функции.

Таким образом, центральным вопросом становится возможность разметить оставшиеся дуги графа $\Gamma_{(n)}^*$ так, чтобы получить граф сдвигов некоторой булевой функции f.

Определение 5. Пусть $\Gamma^*_{(n)} = (V, E^*)$. Разметка дуг графа $\Gamma^*_{(n)}$ $\varphi\colon E^* \mapsto \{0,1\}$ называется корректной, если она удовлетворяет следующим условиям:

1) для любых $x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_n$ верно равенство

$$\varphi\left(\begin{pmatrix} x_1, \ldots, x_{n-1} \\ z_1, \ldots, z_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} x_2, \ldots, x_n \\ z_2, \ldots, z_n \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} z_1, \ldots, z_{n-1} \\ x_1, \ldots, x_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} z_2, \ldots, z_n \\ x_2, \ldots, x_n \end{pmatrix}\right);$$

2) при любых $x_1, x_2, \ldots, x_n, u_1, u_2, \ldots, u_n, z_1, z_2, \ldots, z_n$ верно равенство

$$\varphi\left(\begin{pmatrix} x_1, \ldots, x_{n-1} \\ z_1, \ldots, z_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} x_2, \ldots, x_n \\ z_2, \ldots, z_n \end{pmatrix}\right) =$$

$$= \varphi\left(\begin{pmatrix} z_1, \ldots, z_{n-1} \\ u_1, \ldots, u_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} z_2, \ldots, z_n \\ u_2, \ldots, u_n \end{pmatrix}\right) \oplus \varphi\left(\begin{pmatrix} x_1, \ldots, x_{n-1} \\ u_1, \ldots, u_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} x_2, \ldots, x_n \\ u_2, \ldots, u_n \end{pmatrix}\right).$$

Нетрудно доказать следующее утверждение.

Лемма 3. Граф $\Gamma^*_{(n)}$ с пометками на дугах, соответствующими разметке φ, является графом сдвигов некоторой булевой функции f (а точнее, ровно двух, отличающихся только свободными членами их полиномов) тогда и только тогда, когда φ — корректная разметка.

Таким образом, по корректной разметке φ графа $\Gamma^*_{(n)}$ мы можем однозначно (если, например, дополнительно потребуем $f(0,0,\ldots,0) = 0$, т. е. $f \in T_0$) восстановить функцию f, такую, что Γ^*_f совпадает с размеченным в соответствии с φ графом $\Gamma^*_{(n)}$.

Чтобы выделять просто устроенные классы корректных разметок, будем использовать следующее понятие.

Определение 6. Пусть $n \in \mathbb{N}$; $G = (V', E')$ — неориентированный граф (без кратных ребер и петель) на 2^n вершинах, вершины которого поставлены во взаимно однозначное соответствие наборам из V_n и ребрам которого приписаны значения 0 и 1 в соответствии с функцией $\psi\colon E' \mapsto \{0,1\}$. Через $\tilde{\varphi}_{(G,\psi)}$ будем обозначать частичную разметку графа $\Gamma^*_{(n)}$, полученную в соответствии со следующим правилом: для любых $x_1, x_2, \ldots, x_n, z_1, z_2, \ldots, z_n$, таких, что в графе G есть ребро $\mathbf{e}$ между вершинами $(x_1, \ldots, x_n)$ и $(z_1, \ldots, z_n)$, выполнено

$$\tilde{\varphi}_{(G,\psi)}\left(\begin{pmatrix} x_1, \ldots, x_{n-1} \\ z_1, \ldots, z_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} x_2, \ldots, x_n \\ z_2, \ldots, z_n \end{pmatrix}\right) = \psi(\mathbf{e}).$$

Лемма 4. Пусть $G = (V', E')$ — неориентированный граф без петель и кратных ребер на 2^n вершинах, вершинам которого поставлены во взаимно однозначное соответствие наборы из V_n. Частичная разметка $\tilde{\varphi}_{(G,\psi)}$ при любом выборе функции $\psi\colon E' \mapsto \{0,1\}$ однозначным образом дополнима до корректной разметки графа $\Gamma^*_{(n)}$ (в таком случае будем обозначать ее через $\varphi_{(G,\psi)}$) тогда и только тогда, когда G является деревом.

Следствие 1. С учетом лемм 3 и 4 легко получить, что если граф $G = (V', E')$ удовлетворяет условиям леммы 4, то при любом выборе функции $\psi\colon E' \mapsto \{0,1\}$ пара (G, ψ) однозначно определяет пару булевых функций $\{f, f \oplus 1\}$.

Замечание 3. Так как свойства булевых функций f и $f \oplus 1$ с точки зрения совершенной уравновешенности и наличия барьеров идентичны, ниже для определенности будем рассматривать только функции, принимающие значение 0 на нулевом наборе

(т. е. лежащие в классе T_0), и считать, что пара (G, ψ) в условиях следствия 1 однозначно определяет функцию f. Таким образом, фиксированный граф G, удовлетворяющий условиям леммы 4, определяет взаимно однозначное соответствие между 2^{2^n-1} функциями ψ, определяющими разметку графа G, и функциями $f \in \mathcal{F}_n$, лежащими в классе T_0.

Замечание 4. Пусть G удовлетворяет условиям леммы 4. Исходя из определений 4–6, легко построить алгоритм вычисления значений функции f по паре (G, ψ). Для вычисления $f(\mathbf{x})$ требуется

1) найти в графе G путь (единственный, так как G — дерево) из вершины $(0, 0, \ldots, 0)$ в вершину $\mathbf{x}$;
2) вычислить значения функции ψ на всех ребрах данного пути;
3) положить значение $f(\mathbf{x})$ равным сумме по mod 2 всех вычисленных на предыдущем шаге значений.

Будем описывать классы булевых функций в следующих терминах. Построим граф G (являющийся деревом) на вершинах, соответствующих элементам множества V_n, и частичную разметку $\tilde{\psi}$ графа G. Таким образом мы определим класс $S_{(G,\tilde{\psi})}$ булевых функций, соответствующих всем возможным доопределениям $\tilde{\psi}$ до полной разметки ребер G. Покажем, как построить граф G и его частичную разметку $\tilde{\psi}$ так, чтобы в множество $S_{(G,\tilde{\psi})}$ входили только совершенно уравновешенные функции без правого барьера.

Теорема 6. Для всякого n существует граф G, удовлетворяющий условиям теоремы 4, и частичная разметка $\tilde{\psi}$ этого графа, такие, что множество $S_{(G,\tilde{\psi})} \cup \{f : f \oplus 1 \in \in S_{(G,\tilde{\psi})}\}$ состоит из $2^{2^{n-1}-n}$ совершенно уравновешенных функций n переменных без правого барьера.

Доказательство. Соединим в G попарно все вершины вида $(0, a_2, \ldots, a_n)$ и $(1, a_2, \ldots, a_n)$ с помощью 2^{n-1} ребер. Значения $\tilde{\psi}$ на данных ребрах выберем равными 1, обеспечив линейность всех функций из $S_{(G,\tilde{\psi})}$ по первой переменной. Далее соединим в G ребром вершины $(0, 1, 0, 1, \ldots, 0, 1)$ и $(1, 0, 1, 0, \ldots, 1, 0)$, соответствующее значение ψ положим равным 0, обеспечив таким образом существование в графах сдвига Γ_f^* всех функций из $S_{(G,\tilde{\psi})}$ циклов по дугам с пометкой 0. Для обеспечения отсутствия у всех функций из $S_{(G,\tilde{\psi})}$ правого барьера осталось создать пути по нулевым дугам из графов I_f в полученные циклы в Γ_f^*. Для этого соединим в G пары вершин $((0, 0, 0, \ldots, 0, 0), (0, 0, 0, \ldots, 0, 1))$, $((0, 0, 0, \ldots, 0, 0), (0, 0, 0, \ldots, 0, 1, 1))$, $((0, 0, 0, \ldots, 0, 1), (0, 0, 0, \ldots, 0, 1, 1, 0))$, а затем пары $((0, 0, 0, \ldots, 0, 1, 0), (0, 0, 0, \ldots, 0, 1, 1, 0, 1))$, $((0, 0, 0, \ldots, 0, 1, 0, 1), (0, 0, 0, \ldots, 0, 1, 1, 0, 1, 0))$, $((0, 0, 0, \ldots, 0, 1, 0, 1, 0), (0, 0, 0, \ldots, 0, 1, 1, 0, 1, 0, 1))$ и так далее до пары $((0, 0, 0, 1, 0, 1, 0, 1, \ldots, 0, 1, 0, 1, 0), (0, 1, 1, 0, 1, 0, 1, 0, 1, \ldots, 0, 1, 0, 1, 0))$. Все соответствующие значения $\tilde{\psi}$ положим также нулями. При этом пометка в графе сдвигов любой функции из $S_{(G,\tilde{\psi})}$ на паре $((0, 0, 1, 0, 1, 0, 1, 0 \ldots, 0, 0), (1, 1, 0, 1, 0, 1, 0, 1, \ldots, 0, 1))$ станет нулевой автоматически, обеспечив путь из I_f в созданный цикл Γ_f^*. Легко проверить, что в G циклов не появилось, причем, чтобы достроить его до дерева, требуется в точности $(2^n - 1) - (2^{n-1} + n) = 2^{n-1} - n - 1$ ребер, пометки на которых в частичной разметке $\tilde{\psi}$ фиксировать не будем.

Таким образом, все функции из $S_{(G,\tilde{\psi})}$ не имеют правого барьера и имеют левый барьер длины 1, то есть являются совершенно уравновешенными. С учетом того, что для доопределения $\tilde{\psi}$ требуется задать (независимым образом) $2^{n-1} - n - 1$ значений,

получим, что мощность класса $S_{(G,\tilde{\psi})}$ в точности равна $2^{2^{n-1}-n-1}$, откуда и следует требуемое утверждение. ■

Замечание 5. Для простоты при доказательстве теоремы 6 для обеспечения отсутствия правого барьера у всех функций из порождаемого класса мы явно задавали в графе сдвигов каждой функции из данного класса цикл $\begin{pmatrix} 0,1,0,1,0,1,\ldots,0,1,\ldots \\ 1,0,1,0,1,0,\ldots,1,0,\ldots \end{pmatrix}$, проходимый по помеченным нулями дугам. Пользуясь аналогичными приемами, нетрудно доказать, что для произвольной пары периодических последовательностей, таких, что для наименьшего общего кратного T их минимальных периодов выполняются неравенства $2 \leqslant T \leqslant n-3-2\log_2((n-3)(n-5)+1)$, можно построить класс $S_{(G,\tilde{\psi})}$ из $2^{2^{n-1}-n}$ совершенно уравновешенных функций без правого барьера, каждая из которых в графе сдвигов содержит цикл (по помеченным нулями дугам), образованный выбранной парой, и путь к нему из подграфа I_f по помеченным нулями дугам.

Рассмотрим некоторые свойства описанной выше операции композиции специального вида ($f = g[h]$).

Лемма 5. Пусть $n \in \mathbb{N}$, $h \in \mathcal{F}_n$. Тогда $h \in \mathcal{PB}_n$ тогда и только тогда, когда ни при каком $m \in \mathbb{N}$ не существует двух различных функций $g^{(1)}, g^{(2)} \in \mathcal{F}_m$, для которых выполняется $g^{(1)}[h] = g^{(2)}[h]$.

Доказательство. Если $h \notin \mathcal{PB}_n$, то, как следует из теоремы 1, при некотором $m^* \in \mathbb{N}$ существует набор $\mathbf{z} \in V_{m^*}$, не принадлежащий образу отображения h_{m^*}. Положим $m = m^*$ и рассмотрим произвольную пару функций $g^{(1)}, g^{(2)} \in \mathcal{F}_m$, совпадающих на всех наборах, за исключением набора $\mathbf{z}$. Нетрудно заметить, что $g^{(1)} \neq g^{(2)}$ и $g^{(1)}[h] = g^{(2)}[h]$.

Пусть теперь $h \in \mathcal{PB}_n$, $m \in \mathbb{N}$, $g^{(1)}, g^{(2)}$ — произвольная пара различных функций из $\mathcal{F}_m$, $f^{(1)} = g^{(1)}[h], f^{(2)} = g^{(2)}[h]$. Зафиксируем набор $\mathbf{z} \in V_m$, такой, что $g^{(1)}(\mathbf{z}) \neq g^{(2)}(\mathbf{z})$. Так как функция h совершенно уравновешена, то найдется $\mathbf{x} \in V_{m+n-1}$, такой, что $h_m(\mathbf{x}) = \mathbf{z}$. Отсюда $f^{(1)}(\mathbf{x}) = g^{(1)}(h_m(\mathbf{x})) = g^{(1)}(\mathbf{z}) \neq g^{(2)}(\mathbf{z}) = g^{(2)}(h_m(\mathbf{x})) = f^{(2)}(\mathbf{x})$ и $f^{(1)} \neq f^{(2)}$. ■

Лемма 6. Пусть $n \in \mathbb{N}$, $h^{(1)}, h^{(2)}, h^{(3)} \in \mathcal{F}_n$, причем $h^{(i)} \neq h^{(j)}$ при $i \neq j$. Пусть $m \in \mathbb{N}$, $g \in \mathcal{PB}_m$, $f^{(i)} = g[h^{(i)}]$, $i = 1,2,3$. Тогда по меньшей мере две из функций $f^{(1)}, f^{(2)}, f^{(3)}$ различны.

Доказательство. Очевидно, что среди функций $h^{(1)}, h^{(2)}, h^{(3)}$ найдутся две, $h^{(i)}$ и $h^{(j)}$, $i \neq j$, совпадающие на нулевом наборе. Так как, по условию, $h^{(i)} \neq h^{(j)}$, то найдется набор $\tilde{\mathbf{x}} = (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n) \in V_n$, такой, что $h^{(i)}(\tilde{\mathbf{x}}) \neq h^{(j)}(\tilde{\mathbf{x}})$.

Рассмотрим набор $\mathbf{x} \in V_{2m+3n-4}$, $\mathbf{x} = (\underbrace{0,0,\ldots,0}_{m+n-2}, \tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n, \underbrace{0,0,\ldots,0}_{m+n-2})$. Очевидно, что для доказательства утверждения достаточно показать, что $f^{(i)}_{m+2n-2}(\mathbf{x}) \neq f^{(j)}_{m+2n-2}(\mathbf{x})$.

Предположим противное: $f^{(i)}_{m+2n-2}(\mathbf{x}) = f^{(j)}_{m+2n-2}(\mathbf{x})$. Тогда выполнена следующая система (приведем общий вид системы для случая $m \geqslant n+1$):

$$\begin{cases} g(h^{(i)}(0,0,\ldots,0),h^{(i)}(0,0,\ldots,0),\ldots,h^{(i)}(0,0,\ldots,0),h^{(i)}(0,0,\ldots,0,\tilde{x}_1)) = \\ = g(h^{(j)}(0,0,\ldots,0),h^{(j)}(0,0,\ldots,0),\ldots,h^{(j)}(0,0,\ldots,0),h^{(j)}(0,0,\ldots,0,\tilde{x}_1)), \\ g(h^{(i)}(0,0,\ldots,0),\ldots,h^{(i)}(0,0,\ldots,0,\tilde{x}_1),h^{(i)}(0,0,\ldots,0,\tilde{x}_1,\tilde{x}_2)) = \\ = g(h^{(j)}(0,0,\ldots,0),\ldots,h^{(j)}(0,0,\ldots,0,\tilde{x}_1),h^{(j)}(0,0,\ldots,0,\tilde{x}_1,\tilde{x}_2)), \\ \ldots \\ g(h^{(i)}(0,0,\ldots,0),\ldots,h^{(i)}(0,\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1}),h^{(i)}(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_n)) = \\ = g(h^{(j)}(0,0,\ldots,0),\ldots,h^{(j)}(0,\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1}),h^{(j)}(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_n)), \\ \ldots \\ g(h^{(i)}(\tilde{x}_n,0,\ldots,0),h^{(i)}(0,0,\ldots,0),\ldots,h^{(i)}(0,0,\ldots,0)) = \\ = g(h^{(j)}(\tilde{x}_n,0,\ldots,0),h^{(j)}(0,0,\ldots,0),\ldots,h^{(j)}(0,0,\ldots,0)); \\ h^{(i)}(0,0,\ldots,0) = h^{(j)}(0,0,\ldots,0), \\ h^{(i)}(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_n) \neq h^{(j)}(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_n). \end{cases} \tag{5}$$

Нетрудно видеть, что система (5) по теореме 1 не может быть выполнена в случае совершенно уравновешенной g. Полученное противоречие с условием завершает доказательство утверждения. ■

Замечание 6. Заметим, что более сильное утверждение о том, что в случае совершенно уравновешенной g из неравенства $h^{(1)} \neq h^{(2)}$ следует $g[h^{(1)}] \neq g[h^{(2)}]$, вообще говоря, верным не является. Для построения контрпримера достаточно рассмотреть функции $g(x_1,x_2) = x_1 \oplus x_2 \in \mathcal{PB}_2$ и $h^{(2)} = h^{(1)} \oplus 1$, где $h^{(1)}$ — произвольная булева функция.

Теорема 7. Пусть $n \in \mathbb{N}$; $b \in \mathbb{N}$ или $b = \infty$. Мощность множества функций из $\mathcal{PB}_{n+2}$ с левым барьером длины b без правого барьера не меньше мощности множества функций из $\mathcal{PB}_n$ с левым барьером длины b.

Доказательство. Нетрудно заметить, что для доказательства утверждения достаточно построить для всякого $n \in \mathbb{N}$ отображение $\Phi_n \colon \mathcal{PB}_n \mapsto \mathcal{PB}_{n+2}$, удовлетворяющее следующим условиям:

1) для всякой $f \in \mathcal{PB}_n$ верно $b^R_{\Phi_n(f)} = \infty$;
2) для всякой $f \in \mathcal{PB}_n$ верно $b^L_{\Phi_n(f)} = b^L_f$;
3) Φ_n инъективно.

Для всякой $f \in \mathcal{PB}_n$ положим $\Phi_n(f) = f[h]$, где $h(x_1,x_2,x_3) = x_1 \oplus x_2x_3$. По теореме 3 если $f \in \mathcal{PB}_n$, то $\Phi_n(f) \in \mathcal{PB}_{n+2}$. Как следует из теоремы 5, $b^R_h = \infty$, поэтому, как следует из теоремы 4, $b^R_{\Phi_n(f)} = \infty$ для любой $f \in \mathcal{PB}_n$, и условие 1 выполнено. Функция h линейна по первой переменной, то есть $b^L_h = 1$, поэтому, по теореме 4, для всякой $f \in \mathcal{PB}_n$ выполняется соотношение $\max\{b^L_f, 1\} \leqslant b^L_{\Phi_n(f)} \leqslant b^L_f + 1 - 1$, $b^L_{\Phi_n(f)} = b^L_f$, и условие 2 выполнено. Чтобы доказать, что определенное таким образом Φ_n является инъективным, достаточно заметить, что $h \in \mathcal{PB}_3$, и применить лемму 5. ■

Следствие 2. При любом $n \in \mathbb{N}$ число функций из $\mathcal{PB}_{n+2}$ без правого барьера больше числа функций из $\mathcal{PB}_n$ с правым барьером.

Доказательство. При $n = 1, 2$ данный результат можно получить непосредственно из полученной в работе [4] классификации. Пусть теперь $n \geqslant 3$. Булевых функций с правым барьером в множестве $\mathcal{PB}_n$ ровно столько же, сколько функций

с левым барьером, каждой из которых, как показано в теореме 7, можно поставить в соответствие с помощью отображения Φ_n свою функцию с левым барьером без правого барьера из множества $\mathcal{PB}_{n+2}$. Учитывая при всяком $n \geqslant 3$ существование в множестве $\mathcal{PB}_{n+2}$ функций без барьера (которые, в соответствии с теоремой 4, не могут быть получены отображением Φ_n ни из каких функций с левым барьером), получим требуемое утверждение. ■

Непосредственно из теоремы 7 легко получить следующее утверждение.

Следствие 3. При любом $n \geqslant 5$ существует не менее $2^{2^{n-3}-n+2}$ совершенно уравновешенных булевых функций без барьера.

ЛИТЕРАТУРА

1. *Hedlund G. A.* Endomorphisms and automorphisms of the shift dynamical system // Math. Sys. Theory. 1969. No. 3. P. 320–375.
2. *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.
3. *Anderson R. J.* Searching for the Optimum Correlation Attack // LNCS. 1995. V. 1008. P. 137–143.
4. *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.
5. *Смышляев С. В.* О некоторых свойствах совершенно уравновешенных булевых функций // Материалы Четвертой Междунар. научн. конф. по проблемам безопасности и противодействия терроризму (МГУ им. М. В. Ломоносова, Москва, 30–31 октября 2008). М.: МЦНМО, 2009. С. 57–64.
6. *Смышляев С. В.* О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. 2010. №1(7). С. 5–15.
7. *Golic Dj. J.* On the Security of Nonlinear Filter Generators // LNCS. 1996. V. 1039. P. 173–188.
8. *Логачев О. А.* Об одном классе совершенно уравновешенных булевых функций // Материалы Третьей Междунар. научн. конф. по проблемам безопасности и противодействия терроризму (МГУ им. М. В. Ломоносова, Москва, 25–27 октября 2007). М.: МЦНМО, 2008. С. 137–141.
9. *Смышляев С. В.* Барьеры совершенно уравновешенных булевых функций // Дискретная математика. 2010. Т. 22. Вып. 2. С. 66–79.
10. *Смышляев С. В.* О совершенно уравновешенных булевых функциях без барьера // Материалы Восьмой Междунар. научн. конф. «Дискретные модели в теории управляющих систем» (МГУ им. М. В. Ломоносова, Москва, 6–9 апреля 2009). М.: МАКС Пресс, 2009. С. 278–284.
11. *Смышляев С. В.* О преобразовании двоичных последовательностей с помощью совершенно уравновешенных булевых функций // Материалы Пятой Междунар. научн. конференции по проблемам безопасности и противодействия терроризму (МГУ им. М. В. Ломоносова, Москва, 29–30 октября 2009). М.: МЦНМО, 2010. С. 31–41.
12. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.