2011 Теоретические основы прикладной дискретной математики №1(11)

DOI 10.17223/20710410/11/3

УДК 519.7

О ЧИСЛЕ СОВЕРШЕННО УРАВНОВЕШЕННЫХ БУЛЕВЫХ ФУНКЦИЙ С БАРЬЕРОМ ДЛИНЫ 3[1]

С. В. Смышляев

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

E-mail: smyshsv@gmail.com

Рассматривается класс булевых функций с барьером длины 3, вложенный в множество совершенно уравновешенных булевых функций. Получены нижняя и верхняя оценки для мощности класса булевых функций с правым барьером длины 3, существенно зависящих от последней переменной, а также новая нижняя оценка логарифма числа совершенно уравновешенных булевых функций n переменных, существенно и нелинейно зависящих от крайних переменных: $2^{n-2}\left(1+\frac{\log_2 5}{4}-\mathrm{O}(1/\sqrt{n})\right)$.

Ключевые слова: *совершенно уравновешенные функции, барьеры булевых функций, криптография.*

Введение

Серьезные продвижения в исследовании свойств совершенно уравновешенных булевых функций были получены в работах [1, 2]. В частности, в них доказан критерий совершенной уравновешенности, связывающий это свойство со свойствами отсутствия запрета и отсутствия потери информации. Кроме того, в работе [2] впервые был приведен пример совершенно уравновешенной булевой функции, не являющейся линейной по первой (или последней) переменной. Ряд результатов о совершенно уравновешенных булевых функциях был получен в работах [3 – 7], в частности в [6] было выделено достаточное условие совершенной уравновешенности — наличие у булевой функции барьера. Свойства функций с барьером изучались позже в работах [8 – 10]; методы построения классов совершенно уравновешенных булевых функций без барьера рассматривались в [11, 12].

Одним из предложенных в работе [6] подходов к исследованию класса совершенно уравновешенных булевых функций является последовательное изучение множеств функций с барьерами длины $1, 2, 3, \ldots$ Множества функций с барьерами длины 1 и 2 описываются тривиальным образом и не представляют существенного интереса.

Настоящая работа посвящена получению мощностных оценок для класса функций с барьером длины 3. Производится модификация полученного в [6] критерия принадлежности произвольной булевой функции, существенно зависящей от последней переменной, данному классу. С помощью выделения независимого множества вершин большой мощности в графе де Брейна и выбора определенного класса разметок вершин данного независимого множества удается получить широкий класс функций с правым барьером длины 3. Кроме того, небольшая модификация этого построения приводит к получению нижней оценки мощности множества совершенно уравновешенных функций, существенно и нелинейно зависящих от крайних переменных, — множества, для

[1]Работа поддержана РФФИ (номер проекта 09-01-00653-а).

мощности которого ранее не было известно никаких оценок, кроме тривиальных. Вводится понятие правильной тройки разметок подграфа графа де Брейна, соответствующее набору необходимых условий, которым удовлетворяет всякая булева функция с правым барьером длины 3, существенно зависящая от последней переменной. С помощью построения подграфа специального вида и оценивания числа правильных троек его разметок получается требуемая верхняя мощностная оценка.

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, через Φ_n — множество функций из $\mathcal{F}_n$, существенно зависящих от первой и последней переменной.

Для всякой функции $f \in \mathcal{F}_n$ через $f_{(0)}, f_{(1)} \in \mathcal{F}_{n-1}$ будем обозначать функции, определяемые следующим равенством:

$$f(x_1, x_2, \ldots, x_n) = f_{(0)}(x_1, x_2, \ldots, x_{n-1}) \oplus x_n f_{(1)}(x_1, x_2, \ldots, x_{n-1}).$$

Аналогично,

$$\begin{aligned}
&f_{(0)}(x_1, x_2, \ldots, x_{n-1}) = f_{(00)}(x_1, x_2, \ldots, x_{n-2}) \oplus x_{n-1} f_{(01)}(x_1, x_2, \ldots, x_{n-2});\\
&f_{(1)}(x_1, x_2, \ldots, x_{n-1}) = f_{(10)}(x_1, x_2, \ldots, x_{n-2}) \oplus x_{n-1} f_{(11)}(x_1, x_2, \ldots, x_{n-2});\\
&f_{(00)}(x_1, x_2, \ldots, x_{n-2}) = f_{(000)}(x_1, x_2, \ldots, x_{n-3}) \oplus x_{n-2} f_{(001)}(x_1, x_2, \ldots, x_{n-3});\\
&f_{(01)}(x_1, x_2, \ldots, x_{n-2}) = f_{(010)}(x_1, x_2, \ldots, x_{n-3}) \oplus x_{n-2} f_{(011)}(x_1, x_2, \ldots, x_{n-3}).
\end{aligned}$$

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

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

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

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

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

Понятия, эквивалентные совершенной уравновешенности булевых функций, рассматривались и широко изучались в работах [1] (сюръективные эндоморфизмы символических динамических систем) и [2] (сильно равновероятные булевы функции).

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 $f'(x_1, \ldots, x_n) \equiv f(x_n, \ldots, x_1)$ 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. Заметим также, что для всяких $n, b \in \mathbb{N}$, $b \leqslant n$, верно, что любая функция из $\mathcal{F}_n$, линейно зависящая от x_{n-b+1} (линейно зависящая от x_b) и не зависящая от переменных x_{n-b+2}, x_{n-b+3}, $\ldots, x_n$ (не зависящая от переменных x_1, x_2, $\ldots$, x_{b-1}), имеет правый (левый) барьер длины b.

Замечание 2. 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

Теорема 1 [6]. Наличие барьера у булевой функции является достаточным условием совершенной уравновешенности функции.

Замечание 3. В работе [6] было установлено, что наличие барьера не является необходимым условием совершенной уравновешенности. Позже в работах [5, 8, 12] был предложен ряд методов построения совершенно уравновешенных булевых функций без барьера.

Теорема 2 [6]. Функция $f \in \mathcal{F}_n$, такая, что $f_{(1)} \not\equiv 0$, имеет правый барьер длины 3 тогда и только тогда, когда для любых $x_1, x_2, \ldots, x_{n-1}$ выполнены следующие условия:

1) $f_{(11)}(x_1, \ldots, x_{n-2}) = 0$;
2) если $f_{(10)}(x_1, \ldots, x_{n-2}) = 1$, то

$$\begin{aligned}
&f_{(10)}(x_2, \ldots, x_{n-2}, 0) = f_{(10)}(x_2, \ldots, x_{n-2}, 1) = 0,\\
&f_{(10)}(0, x_1 \ldots, x_{n-3}) = f_{(10)}(1, x_1, \ldots, x_{n-3}) = 0,\\
&f_{(011)}(x_2, \ldots, x_{n-2}) = 0,\\
&f_{(001)}(x_2, \ldots, x_{n-2}) \oplus f_{(01)}(x_1, \ldots, x_{n-2}) f_{(01)}(x_2, \ldots, x_{n-2}, 0) = 1;
\end{aligned}$$

3) если $f_{(10)}(x_1, \ldots, x_{n-2}) = f_{(10)}(x_2, \ldots, x_{n-1}) = 0$, то

$$f_{(01)}(x_2, \ldots, x_{n-1}) = 1.$$

Через GB_m будем обозначать граф де Брейна порядка m: ориентированный граф на 2^m вершинах, поставленных в соответствие элементам множества V_m и соединенных дугами так, что дуга из вершины, соответствующей набору $(a_1, a_2, \ldots, a_m) \in V_m$, в вершину, соответствующую набору $(b_1, b_2, \ldots, b_m) \in V_m$, присутствует в графе GB_m в том и только в том случае, когда $(a_2, a_3, \ldots, a_m) = (b_1, b_2, \ldots, b_{m-1})$ (см. [13]). Обозначим через GB_m^* неориентированный граф на тех же вершинах, что и граф GB_m, получаемый из него заменой всех дуг на (неориентированные) ребра и удалением петель.

Обозначим через ω отображение из V_m в множество вершин графа GB_m и графа GB_m^*, переводящее двоичные наборы в соответствующие им вершины. Через Ω будем обозначать аналогично определяемое отображение из множества всех подмножеств V_m в множество всех подмножеств вершин графов GB_m и GB_m^*.

Теорема 3 [14]. В графе GB^*_m существует независимое множество вершин (т. е. множество вершин, никакие две из которых не соединены ребром), не содержащее $\omega(0,0,\ldots,0)$ и $\omega(1,1,\ldots,1)$ и имеющее следующую мощность:

$$\begin{cases} 2^{m-1} - \left(\dfrac{1}{2}\dbinom{m}{m/2} - \dbinom{m-2}{m/2-2}\right), & \text{если } m \text{ четно;} \\ 2^{m-1} - \left(\dbinom{m-1}{(m-1)/2} - 2\dbinom{m-3}{(m-1)/2-2}\right), & \text{если } m \text{ нечетно.} \end{cases}$$

3. Основные результаты

Обозначим для всяких $n, b \in \mathbb{N}$ через $W_{b,n}$ множество функций из $\mathcal{F}_n$ с правым барьером длины b, существенно зависящих от x_n.

Из результатов работы [6] вытекает, что множество $W_{2,n}$ пусто при всяком n. С учетом этого нетрудно установить, что все функции с правым барьером длины 3, не принадлежащие $W_{3,n}$, не зависят существенно от x_{n-1} и x_n и линейны по x_{n-2}. Таким образом, учитывая замечания 1 и 2, при исследовании функций с барьером длины 3 достаточно ограничиться изучением множества $W_{3,n}$.

Перепишем условия, сформулированные в теореме 2, выделив отдельно свойства каждой из функций $f_{(11)}, f_{(10)}, f_{(01)}, f_{(00)}$. Получим: $f \in W_{3,n}$ тогда и только тогда, когда для всяких $x_1, x_2, \ldots, x_{n-1}$ выполняются следующие условия:

1) $f_{(11)}(x_1,\ldots,x_{n-2}) = 0$;
2) $f_{(10)}(x_1,\ldots,x_{n-2}) f_{(10)}(x_2,\ldots,x_{n-1}) = 0$;
3) если $f_{(10)}(x_1,\ldots,x_{n-2}) = f_{(10)}(x_2,\ldots,x_{n-1}) = 0$, то $f_{(01)}(x_2,\ldots,x_{n-1}) = 1$;
   если $f_{(10)}(x_1,\ldots,x_{n-2}) = 1$, то $f_{(01)}(x_2,\ldots,x_{n-2},0) = f_{(01)}(x_2,\ldots,x_{n-2},1)$;
   если $f_{(10)}(0,x_2,\ldots,x_{n-2}) = f_{(10)}(1,x_2,\ldots,x_{n-2}) = 1$ и $f_{(01)}(x_2,\ldots,x_{n-1}) = 1$, то $f_{(01)}(0,x_2,\ldots,x_{n-2}) = f_{(01)}(1,x_2,\ldots,x_{n-2})$;
4) если $f_{(10)}(x_1,\ldots,x_{n-2}) = 1$, то $f_{(00)}(x_2,\ldots,x_{n-2},0) \oplus f_{(00)}(x_2,\ldots,x_{n-2},1) = f_{(01)}(x_1,\ldots,x_{n-2}) f_{(01)}(x_2,\ldots,x_{n-1}) \oplus 1$.

Лемма 1. Пусть S — независимое множество вершин графа GB^*_{n-2}, не содержащее вершин $\omega(0,0,\ldots,0)$ и $\omega(1,1,\ldots,1)$. Тогда любая функция $f_{(10)}$, равная нулю на всех наборах из $V_{n-2} \setminus \Omega^{-1}(S)$, удовлетворяет условию 2.

Доказательство. Так как S является независимым множеством вершин графа GB^*_{n-2} и не содержит $\omega(0,0,\ldots,0)$ и $\omega(1,1,\ldots,1)$, то в графе GB_{n-2} никакая дуга не соединяет две вершины из S. Следовательно, при указанном выборе функции $f_{(10)}$ не существует ни одного набора $(x_1,\ldots,x_{n-1}) \in V_{n-1}$, такого, что $f_{(10)}(x_1,\ldots,x_{n-2}) = f_{(10)}(x_2,\ldots,x_{n-1}) = 1$. Таким образом, для функции $f_{(10)}$ выполняется условие 2. ■

Лемма 2. В графе GB^*_m существует не содержащее $\omega(0,0,\ldots,0)$ и $\omega(1,1,\ldots,1)$ независимое множество вершин S мощности $2^{m-1} - \mathrm{O}\left(2^m/\sqrt{m}\right)$, такое, что для любых $x_2,\ldots,x_m$ вершины $\omega(0,x_2,\ldots,x_m)$ и $\omega(1,x_2,\ldots,x_m)$ входят или не входят в S одновременно.

Доказательство. Представляя (при четном m) разность $\left(\dfrac{1}{2}\dbinom{m}{m/2} - \dbinom{m-2}{m/2-2}\right)$ в виде $\dbinom{m-2}{m/2-1}$ и применяя формулу Стирлинга, легко показать, что из теоремы 3 следует существование множества $T' \subseteq V_{m-1} \setminus \{(0,0,\ldots,0),(1,1,\ldots,1)\}$ мощности $2^{m-2} - \mathrm{O}(2^{m-1}/\sqrt{m-1})$, такого, что $S' = \Omega(T')$ — независимое множество вершин графа GB^*_{m-1}.

Положим $T = \{(x_1, x_2, \ldots, x_m) \in V_m : (x_2, x_3, \ldots, x_m) \in T'\}$, $S = \Omega(T)$. Очевидно, что $|S| = |T| = 2^{m-1} - \mathrm{O}\,(2^m/\sqrt{m})$ и $\omega(0, 0, \ldots, 0) \notin S$, $\omega(1, 1, \ldots, 1) \notin S$. Покажем, что вершины из S образуют независимое множество в графе GB^*_m. Заметим, что две вершины $\omega(x'_1, x'_2, \ldots, x'_m), \omega(x''_1, x''_2, \ldots, x''_m)$ соединены ребром в GB^*_m тогда и только тогда, когда выполнено условие $(x'_1, x'_2, \ldots, x'_{m-1}) = (x''_2, x''_3, \ldots, x''_m)$ либо условие $(x'_2, x'_3, \ldots, x'_m) = (x''_1, x''_2, \ldots, x''_{m-1})$. Таким образом, легко видеть, что если множество вершин S не является независимым в графе GB^*_m, то и множество S' не является независимым в GB^*_{m-1}. ■

Используя приведенные утверждения, докажем следующую нижнюю оценку.

Теорема 4. $\log_2 |W_{3,n}| \geqslant 2^{n-2}\left(1 + \dfrac{\log_2 5}{4} - \mathrm{O}(1/\sqrt{n})\right)$.

Доказательство. Зафиксируем произвольную функцию $f_{(10)} \in \mathcal{F}_{n-2}$, $f_{(10)} \not\equiv 0$, удовлетворяющую условию 2. Очевидно, что произвольная функция $f_{(01)} \in \mathcal{F}_{n-2}$, удовлетворяющая при всяких $x_1, x_2, \ldots, x_{n-1}$ условию

3′) если $f_{(10)}(x_1, \ldots, x_{n-2}) = f_{(10)}(x_2, \ldots, x_{n-1}) = 0$, то $f_{(01)}(x_2, \ldots, x_{n-1}) = 1$;
если $f_{(10)}(0, x_2, \ldots, x_{n-2}) \oplus f_{(10)}(1, x_2, \ldots, x_{n-2}) = 1$, то $f_{(01)}(x_2, \ldots, x_{n-2}, 0) = f_{(01)}(x_2, \ldots, x_{n-2}, 1) = 1$;
если $f_{(10)}(0, x_2, \ldots, x_{n-2}) = f_{(10)}(1, x_2, \ldots, x_{n-2}) = 1$, то $f_{(01)}(x_2, \ldots, x_{n-2}, 0) = f_{(01)}(x_2, \ldots, x_{n-2}, 1) = 0$,

удовлетворяет также и условию 3. Оценим число функций $f_{(01)}, f_{(00)}$, удовлетворяющих условиям 3′ и 4.

Нетрудно проверить, что при любой фиксированной удовлетворяющей 2 функции $f_{(10)}$ условие 3′ однозначно определяет значение $f_{(01)}$ на тех и только тех наборах, на которых $f_{(10)}$ обращается в нуль. Таким образом, удовлетворяющих 3′ функций $f_{(01)}$ в точности $2^{\mathrm{wt}(f_{(10)})}$.

При всяких удовлетворяющих условиям 2 и 3′ функциях $f_{(10)}$ и $f_{(01)}$ условие 4 не накладывает ограничений на выбор функции $f_{(000)}$ и определяет значение функции $f_{(001)}$ на наборе $(x_1, x_2, \ldots, x_{n-3})$ тогда и только тогда, когда $f_{(10)}(0, x_1, \ldots, x_{n-3}) = 1$ или $f_{(10)}(1, x_1, \ldots, x_{n-3}) = 1$. Таким образом, удовлетворяющих 4 функций $f_{(00)}$ в точности $2^{2^{n-2} - \mathrm{wt}(f_{(10)}(0,x_1,\ldots,x_{n-3}) \vee f_{(10)}(1,x_1,\ldots,x_{n-3}))}$.

С учетом равенства $\mathrm{wt}(f_{(10)}) - \mathrm{wt}(f_{(10)}(0, x_1, \ldots, x_{n-3}) \vee f_{(10)}(1, x_1, \ldots, x_{n-3})) = \mathrm{wt}(f_{(10)}(0, x_1, \ldots, x_{n-3}) f_{(10)}(1, x_1, \ldots, x_{n-3}))$ получаем: при всякой удовлетворяющей 2 функции $f_{(10)}$ не менее $2^{2^{n-2} + \mathrm{wt}(f_{(10)}(0,x_1,\ldots,x_{n-3}) f_{(10)}(1,x_1,\ldots,x_{n-3}))}$ пар функций $(f_{(01)}, f_{(00)})$ удовлетворяют условиям 3 и 4.

Пусть S — независимое множество вершин графа GB^*_{n-2}, определяемое леммой 2. Рассмотрим все возможные отличные от тождественного нуля функции $f_{(10)}$, определенные в соответствии с леммой 1. С учетом полученных выше результатов имеем

$$|W_{3,n}| \geqslant \sum_{\substack{f_{(10)} \in \mathcal{F}_{n-2} \setminus \{0\}, \\ f_{(10)}(\mathbf{x}) = 0, \omega(\mathbf{x}) \notin S}} 2^{2^{n-2} + \mathrm{wt}(f_{(10)}(0,x_1,\ldots,x_{n-3}) f_{(10)}(1,x_1,\ldots,x_{n-3}))} =$$

$$= 2^{2^{n-2}} \sum_{\substack{g\colon \Omega^{-1}(S') \mapsto V_2, \\ g \not\equiv (0,0)}} 2^{|g^{-1}(1,1)|} = 2^{2^{n-2}} \left(\sum_{i=0}^{|S'|} \left[\binom{|S'|}{i} 3^{|S'|-i} \cdot 2^i \right] - 1 \right) = \tag{2}$$

$$= 2^{2^{n-2}} \left(5^{|S'|} - 1\right) = 2^{2^{n-2} - \log_2 \left(\frac{5^{|S'|}}{5^{|S'|}-1} \right)} \cdot 5^{|S'|} = 2^{2^{n-2} - \mathrm{o}(1)} \cdot 2^{\log_2 5 \cdot \left(2^{n-4} - \mathrm{O}\left(\frac{2^{n-4}}{\sqrt{n-4}}\right)\right)} =$$

$$= 2^{2^{n-2}\left(1 + \frac{1}{4}\log_2 5 - \mathrm{O}\left(\frac{1}{4\sqrt{n-4}}\right)\right) - \mathrm{o}(1)}.$$

Логарифмируя получившееся неравенство, получаем

$$\log_2 |W_{3,n}| \geqslant 2^{n-2}\left(1+\frac{\log_2 5}{4}-\mathrm{O}(1/\sqrt{n})\right). \blacksquare$$

Через $\mathcal{L}_n^{\mathcal{L}}$ ($\mathcal{L}_n^{\mathcal{R}}$) обозначим множество функций n переменных, линейно зависящих от первой (последней) переменной. Как следует из результатов работ [3, 4, 6], наибольший интерес среди элементов $\mathcal{PB}_n$ представляют функции из $(\mathcal{PB}_n \cap \Phi_n) \setminus (\mathcal{L}_n^{\mathcal{L}} \cup \mathcal{L}_n^{\mathcal{R}})$.

Для получения нижней оценки мощности данного множества вернемся к доказательству теоремы 4. Требуя дополнительно от функции $f_{(000)}$ нелинейной существенной зависимости от x_1, получим, что при этом при всяких удовлетворяющих условиям 2 и 3′ функциях $f_{(10)}$ и $f_{(01)}$ число удовлетворяющих условию 4 функций $f_{(00)}$ в точности равно $\left(2^{2^{n-2}}-2^{2^{n-3}+2^{n-4}+1}\right)2^{-\mathrm{wt}(f_{(10)}(0,x_1,\ldots,x_{n-3})\vee f_{(10)}(1,x_1,\ldots,x_{n-3}))}$. Пользуясь цепочкой неравенств, аналогичной (2), и логарифмируя, приходим к следующему утверждению.

Теорема 5. $\log_2 \left|(\mathcal{PB}_n \cap \Phi_n) \setminus (\mathcal{L}_n^{\mathcal{L}} \cup \mathcal{L}_n^{\mathcal{R}})\right| \geqslant 2^{n-2}\left(1+\frac{\log_2 5}{4}-\mathrm{O}(1/\sqrt{n})\right)$.

Для получения верхней оценки мощности $W_{3,n}$ введем следующее понятие.

Определение 3. Пусть H — некоторый подграф графа GB_m. Будем называть тройку $(\varphi_{(10)}, \varphi_{(01)}, \varphi_{(00)})$ разметок вершин графа H элементами множества $\{0,1\}$ правильной, если для любых трех вершин v_1, v_2, v_3 графа H выполняются следующие условия:

1) если в H есть дуга из v_1 в v_2, то $\varphi_{(10)}(v_1) = 0$ или $\varphi_{(10)}(v_2) = 0$, причем если $\varphi_{(10)}(v_1) = \varphi_{(10)}(v_2) = 0$, то $\varphi_{(01)}(v_2) = 1$;
2) если в H из v_1 в вершины v_2 и v_3 ведут дуги и $v_2 \neq v_3$, то если $\varphi_{(10)}(v_1) = 1$, то $\varphi_{(01)}(v_2) = \varphi_{(01)}(v_3)$ и $\varphi_{(00)}(v_2) \oplus \varphi_{(00)}(v_3) = \varphi_{(01)}(v_1)\varphi_{(01)}(v_2) \oplus 1$.

Непосредственно из определения 3 и теоремы 2 вытекает следующее утверждение.

Утверждение 1. Если $f \in W_{3,n}$, то тройка $(f_{(10)} * \omega^{-1}, f_{(01)} * \omega^{-1}, f_{(00)} * \omega^{-1})$ разметок вершин GB_{n-2} является правильной относительно любого подграфа GB_{n-2}, содержащего все вершины GB_{n-2}.

Опишем для всех m подграфы H_m графа де Брейна GB_m, для которых далее получим верхние оценки числа правильных троек разметок. Удалим из графа GB_m вершину $\omega(0,0,\ldots,0)$, затем выделим в получившемся подграфе остовное дерево, представляющее собой полное двоичное дерево высоты $m-1$, на i-м уровне которого $(i = 0,1,\ldots,m-1)$ находятся все вершины множества

$$\Omega\left(\{(x_1,x_2,\ldots,x_m) \in V_m : (x_1,x_2,\ldots,x_{m-1-i}) = (0,0,\ldots,0), x_{m-i} = 1\}\right).$$

Обозначим получившийся подграф через H'_m. Добавим к H'_m вершину $\omega(0,0,\ldots,0)$ и обе исходящие из нее в графе GB_m дуги; получившийся подграф обозначим H_m. На рис. 1 приведен пример такого графа для $m = 3$.

Обозначим через c_m число правильных троек разметок H_m. Пусть среди правильных троек разметок графа H'_m есть ровно $4a_m$ таких, что $\varphi_{(10)}(\omega(0,0,\ldots,0,1)) = 0$, и $4b_m$ таких, что $\varphi_{(10)}(\omega(0,0,\ldots,0,1)) = 1$.

Учитывая структуру графов H'_m и H_m, приходим к следующему утверждению.

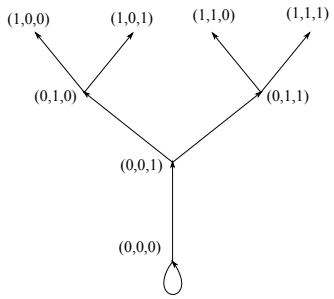

Рис. 1. Граф H_3

Утверждение 2. Значения a_m, b_m, c_m, $m = 1, 2, \ldots$, удовлетворяют следующим равенствам:

$$a_1 = b_1 = 1;$$
$$a_{m+1} = 4(a_m + 2b_m)^2,\ m = 1, 2, \ldots;$$
$$b_{m+1} = 4a_m^2,\ m = 1, 2, \ldots;$$
$$c_m = 4a_m + 8b_m,\ m = 1, 2, \ldots$$

С учетом полученных результатов докажем верхнюю оценку.

Теорема 6. Для всякого $n \geqslant 3$ верно

$$\log_2 |W_{3,n}| < 2^{n-2} \cdot 2{,}100641.$$

Доказательство. Из утверждения 1, определений графа H_m и величины c_m следует, что $|W_{3,n}| \leqslant c_{n-2}$.

Обозначим для всякого $m = 1, 2, \ldots$ отношение a_m/b_m через d_m. Получим выражение c_{m+1} через c_m и d_m:

$$c_{m+1} = 4a_{m+1} + 8b_{m+1} = 16a_m^2 + 64a_m b_m + 64b_m^2 + 32a_m^2 =$$
$$= c_m^2 \frac{48a_m^2 + 64a_m b_m + 64b_m^2}{16a_m^2 + 64a_m b_m + 64b_m^2} = c_m^2 \frac{3d_m^2 + 4d_m + 4}{d_m^2 + 4d_m + 4}.$$

Выражая d_{m+1} через d_m, получим $d_{m+1} = 1 + 4\dfrac{d_m + 1}{d_m^2}$. Найдем отрезок числовой оси, которому принадлежат все значения d_m, начиная с некоторого номера m^*. Покажем, что в качестве такого отрезка можно выбрать отрезок от 2,867 до 2,882. Для этого заметим, что если для некоторого m^* верно $2{,}867 \leqslant d_{m^*} \leqslant 2{,}882$, то и для всех $m \geqslant m^*$ верно $2{,}867 \leqslant d_m \leqslant 2{,}882$. Учитывая, что $d_1 = 1$ и вычисляя явно все d_m вплоть до d_{32}, получим, что указанные неравенства выполняются при $m^* = 32$. Таким образом, для любого $m \geqslant 32$ верно неравенство $c_{m+1} \leqslant 1{,}697 \cdot c_m^2$ и, следовательно, $c_m \leqslant 1{,}697^{-1}(1{,}697 \cdot c_{32})^{2^{m-32}}$, $\log_2 c_m \leqslant 2^m(\log_2 1{,}697 + \log_2 c_{32})/2^{32} - \log_2 1{,}697$. Вычисляя $\log_2 c_{32}$, получаем $\log_2 c_m < 2^m \cdot 2{,}100641$ для всех $m \geqslant 32$. Проверяя явным образом выполнение данного соотношения для всех $m = 1, 2, \ldots, 31$, приходим к требуемому утверждению. ■

Из теорем 4 и 6 окончательно получаем следующие оценки мощности $W_{3,n}$:

$$2^{n-2}\left(C_1 - \mathrm{O}(1/\sqrt{n})\right) \leqslant \log_2 |W_{3,n}| < 2^{n-2} \cdot C_2,$$

где $C_1 = 1 + (\log_2 5)/4 \approx 1{,}58048$; $C_2 = 2{,}100641$.

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. *Golic Dj. J.* On the Security of Nonlinear Filter Generators // LNCS. 1996. V. 1039. P. 173–188.
5. *Смышляев С. В.* О некоторых свойствах совершенно уравновешенных булевых функций // Материалы Четвертой Междунар. науч. конф. по проблемам безопасности и противодействия терроризму (МГУ им. М. В. Ломоносова, Москва, 30–31 октября 2008). М.: МЦНМО, 2009. С. 57–64.
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. *Логачев О. А.* Об одном классе совершенно уравновешенных булевых функций // Материалы Третьей Междунар. науч. конф. по проблемам безопасности и противодействия терроризму (МГУ им. М. В. Ломоносова, Москва, 25–27 октября 2007). М.: МЦНМО, 2008. С. 137–141.
8. *Смышляев С. В.* Барьеры совершенно уравновешенных булевых функций // Дискретная математика. 2010. Т. 22. Вып. 2. С. 66–79.
9. *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.
10. *Смышляев С. В.* О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. 2010. № 1(7). С. 5–15.
11. *Смышляев С. В.* О совершенно уравновешенных булевых функциях без барьера // Материалы Восьмой Междунар. науч. конф. «Дискретные модели в теории управляющих систем» (МГУ им. М. В. Ломоносова, Москва, 6–9 апреля 2009). М.: МАКС Пресс, 2009. С. 278–284.
12. *Смышляев С. В.* Построение классов совершенно уравновешенных булевых функций без барьера // Прикладная дискретная математика. 2010. № 3(9). С. 41–50.
13. *Холл М.* Комбинаторика. М.: Мир, 1970.
14. *Lichiardopol N.* Independence number of de Bruijn graphs // Dicrete Mathematics. 2006. V. 306(12). P. 1145–1160.