

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/7/1

УДК 519.7

О КРИПТОГРАФИЧЕСКИХ СЛАБОСТЯХ НЕКОТОРЫХ КЛАССОВ ПРЕОБРАЗОВАНИЙ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ¹

С. В. Смышляев

*Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия***E-mail:** smyshsv@gmail.com

В работе рассматривается ряд вопросов, связанных с использованием совершенно уравновешенных булевых функций в качестве фильтрующих и появлением слабостей в соответствующих криптопримитивах.

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

Введение

При изучении криптографических примитивов, состоящих из регистра сдвига и подключенной к нему реализующей некоторую булеву функцию схемы (фильтра), одним из важнейших вопросов является принципиальная возможность получить на выходе фильтра произвольную двоичную последовательность. Соответствующее свойство реализуемой булевой функции (фильтрующей) было формализовано С. Н. Сумароковым в понятии совершенной уравновешенности, им же в [1] были получены первые утверждения о классе совершенно уравновешенных функций. Исследование данного класса было продолжено в работе [2], в которой авторами было введено понятие барьера булевой функции, важное для изучения аспектов, связанных с использованием булевых функций в качестве фильтрующих, а также был доказан ряд утверждений о совершенно уравновешенных функциях с барьером. Позже [3, 4], в числе прочего, были доказаны некоторые утверждения о слабостях фильтров, построенных с помощью функций с барьером конечной длины, и построены некоторые классы совершенно уравновешенных функций без барьера. Работы [5, 6] были целиком посвящены методам построения классов совершенно уравновешенных функций, удовлетворяющих определенным наборам требований; в частности, широким классам функций без барьера [6].

В настоящей работе рассматриваются два аспекта использования совершенно уравновешенных булевых функций в качестве фильтрующих, связанные с появлением слабостей в соответствующих криптопримитивах.

В п. 1 и 2 приводятся необходимые определения и предварительные результаты. В п. 3.1 доказывается новый критерий совершенной уравновешенности функции, обосновывающий негативные криптографические качества совершенно уравновешенных булевых функций при использовании соответствующих им фильтров в ситуациях, когда на вход поступают отличные от истинно случайных последовательности — в част-

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

ности, такие, внутри которых никогда не встречаются некоторые наборы подряд идущих символов.

П. 3.2 посвящен углубленному изучению одного из поднятых в работе [4] вопросов о криптографических слабостях фильтров, построенных с использованием функций с барьером небольшой длины. Рассмотрены вопросы формального построения правил восстановления символов входной последовательности с использованием некоторых подмножеств символов выходной последовательности, доказан ряд особых свойств таких правил в терминах частично определенных булевых функций и в терминах барьеров совершенно уравновешенных булевых функций.

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:

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

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

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

Нетрудно заметить, что 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. Фильтры часто применяются в криптографических приложениях, связанных с потоковыми шифрами, — например, простейшим примитивом, с помощью которого можно выработать складываемую с битами открытого текста псевдослучайную последовательность, является фильтр, на вход которого подается некоторая линейно-рекуррентная последовательность.

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

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

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

Определение 2 [1]. Булева функция $f \in \mathcal{F}_n$ называется *совершенно уравновешенной*, если соотношение

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

выполняется для любого $m \in \mathbb{N}$ и любого $y \in V_m$. 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 [2]. Булева функция $f \in \mathcal{F}_n$ называется *функцией с правым барьером длины b* , если система уравнений

$$\begin{cases} f(y_1, y_2, \dots, y_n) = f(z_1, z_2, \dots, z_n); \\ f(y_2, y_3, \dots, y_{n+1}) = f(z_2, z_3, \dots, z_{n+1}); \\ \dots \\ f(y_{b-1}, y_b, \dots, y_{b+n-2}) = f(z_{b-1}, z_b, \dots, z_{b+n-2}); \\ y_1 = z_1; \dots; y_{n-1} = z_{n-1}; y_n = 0; z_n = 1 \end{cases} \quad (3)$$

имеет решение, а система

$$\begin{cases} f(y_1, y_2, \dots, y_n) = f(z_1, z_2, \dots, z_n); \\ f(y_2, y_3, \dots, y_{n+1}) = f(z_2, z_3, \dots, z_{n+1}); \\ \dots \\ f(y_{b-1}, y_b, \dots, y_{b+n-2}) = f(z_{b-1}, z_b, \dots, z_{b+n-2}); \\ f(y_b, y_{b+1}, \dots, y_{b+n-1}) = f(z_b, z_{b+1}, \dots, z_{b+n-1}); \\ y_1 = z_1; \dots; y_{n-1} = z_{n-1}; y_n = 0; z_n = 1 \end{cases} \quad (4)$$

решений не имеет.

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

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

Отметим важное для криптографических приложений свойство совершенно уравновешенных функций.

Теорема 1 [7]. Пусть $n \in \mathbb{N}$, $f \in \mathcal{F}_n$. Для последовательности случайных векторов $X_m = (x_1, x_2, \dots, x_{m+n-1})$, $m = 1, 2, \dots$, с распределением

$$\Pr\{X_m = (a_1, \dots, a_{m+n-1})\} = 2^{-(m+n-1)} \text{ для каждого } (a_1, \dots, a_{m+n-1}) \in V_{m+n-1}$$

случайный вектор $Y_m = f_m(X_m)$ распределен равномерно для любого $m \in \mathbb{N}$ тогда и только тогда, когда f — совершенно уравновешенная функция.

Другими словами, если биты двоичной последовательности, поступающей на вход фильтра, распределены равномерно и независимо, то биты выходной двоичной последовательности обладают этим свойством тогда и только тогда, когда фильтрующая функция совершенно уравновешена.

Для исследования класса совершенно уравновешенных функций часто удобно использовать следующую теорему.

Теорема 2 [1, 7]. 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

$$x = (x_1, x_2, \dots, x_r), z = (z_1, z_2, \dots, z_r) \in V_r, r \geq 2n - 1,$$

таких, что

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

Связь совершенной уравновешенности с наличием у функции барьера описывается следующим утверждением.

Теорема 3 [2]. Наличие барьера у булевой функции является достаточным, но не необходимым условием совершенной уравновешенности функции.

3. Основные результаты

3.1. Критерий совершенной уравновешенности

Следующее утверждение представляет собой критерий совершенной уравновешенности, суть которого заключается в существовании для каждого фиксированного набора длины k такой выходной последовательности, которая не может быть получена с помощью фильтрующей функции f ни на какой входной последовательности, не содержащей внутри себя этого набора. Иными словами, из запрета на присутствие любого фиксированного набора символов во входной последовательности кодирующего устройства указанного типа в случае совершенно уравновешенной фильтрующей функции незамедлительно следует уменьшение мощности множества возможных выходных последовательностей.

Теорема 4. Функция является совершенно уравновешенной, если и только если для любых $k > 0$, $(y_1, \dots, y_k) \in V_k$ существуют такие $r \geq \max\{1, 1 - n + k\}$ и $z = (z_1, \dots, z_r) \in V_r$, что выполняются следующие условия:

- 1) $\exists (x_1, \dots, x_{r+n-1}) \in V_{r+n-1} (f_r(x_1, \dots, x_{r+n-1}) = (z_1, \dots, z_r));$
- 2) $\forall (x_1, \dots, x_{r+n-1}) \in V_{r+n-1} (f_r(x_1, \dots, x_{r+n-1}) = (z_1, \dots, z_r) \Rightarrow \Rightarrow \exists i (1 \leq i \leq r + n - k \ \& \ (x_i, \dots, x_{i+k-1}) = (y_1, \dots, y_k))).$

Доказательство.

Необходимость. Для произвольной $f \in \mathcal{PB}_n$ предположим противное: существуют $k > 0$ и $(y_1, \dots, y_k) \in V_k$, такие, что для любого $r \geq \max\{1, 1 - n + k\}$ и любого $z = (z_1, \dots, z_r) \in V_r$ выполнено хотя бы одно из двух условий:

- а) $\nexists (x_1, \dots, x_{r+n-1}) \in V_{r+n-1} (f_r(x_1, \dots, x_{r+n-1}) = (z_1, \dots, z_r));$
- б) $\exists (x_1, \dots, x_{r+n-1}) \in V_{r+n-1} (f_r(x_1, \dots, x_{r+n-1}) = (z_1, \dots, z_r) \ \& \ \forall i (1 \leq i \leq r + n - k \Rightarrow (x_i, \dots, x_{i+k-1}) \neq (y_1, \dots, y_k))).$

Покажем, что условие «б» не может выполняться для всех r и z . Представим любой набор $x \in V_{r+n-1}$ в виде

$$x = ((x_1^1, \dots, x_k^1), (x_1^2, \dots, x_k^2), \dots, (x_1^p, \dots, x_k^p), x_1^{p+1}, \dots, x_m^{p+1}) \in V_{r+n-1},$$

где $0 \leq m < k$, $p = \left\lceil \frac{r+n-1}{k} \right\rceil$. Всего таких x , что $(x_1^j, \dots, x_k^j) \neq (y_1, \dots, y_k)$ для всех $j = 1, \dots, p$ (что, очевидно, необходимо для выполнения соотношения

$$\forall i (1 \leq i \leq r + n - k \Rightarrow (x_i, \dots, x_{i+k-1}) \neq (y_1, \dots, y_k))$$

из условия «б»), для каждого r существует не более чем $(2^k - 1)^p \cdot 2^{k-1}$.

Верно соотношение $\frac{(2^k - 1)^p 2^{k-1}}{2^{r+n-1}} \leq \left(\frac{2^k - 1}{2^k} \right)^p 2^{k-1} \xrightarrow{r \rightarrow +\infty} 0$. Поэтому существует столь большое r' , что число последовательностей $x \in V_{r'+n-1}$, не содержащих $(y_1, \dots, y_k)$, не превосходит $2^{r'+n-1} 2^{-n} = 2^{r'-1}$. Всего возможных последовательностей $z \in V_{r'}$ ровно $2^{r'}$, поэтому хотя бы для одного $z \in V_{r'}$ будет выполнено условие а, противоречащее определению совершенно уравновешенной функции. Полученное противоречие завершает доказательство необходимости.

Достаточность. Предположим противное: $f \notin \mathcal{PB}_n$. Тогда, как следует из теоремы 2, $\exists k > 2n \exists (y'_1, \dots, y'_k), (y''_1, \dots, y''_k) \in V_k$ ($y'_1 = y''_1, \dots, y'_n = y''_n; y'_{k-n+1} = y''_{k-n+1}, \dots, y'_k = y''_k; f_{k-n+1}(y'_1, y'_2, \dots, y'_k) = f_{k-n+1}(y''_1, y''_2, \dots, y''_k)$), причем $(y'_1, \dots, y'_k) \neq (y''_1, \dots, y''_k)$.

Положим $(y_1, \dots, y_k) = (y'_1, \dots, y'_k)$. Если существуют $r > 0$ и $z = (z_1, \dots, z_r) \in V_r$, такие, что

$$\begin{cases} f(x_1, \dots, x_n) = z_1; \\ \dots \\ f(x_r, \dots, x_{r+n-1}) = z_r \end{cases} \quad (5)$$

для какого-то $(x_1, \dots, x_{r+n-1})$, где $(x_{i^*}, \dots, x_{i^*+k-1}) = (y'_1, \dots, y'_k)$ при некотором i^* , то, просматривая $(x_1, \dots, x_{r+n-1})$ слева направо и заменяя все вхождения $(y'_1, \dots, y'_k)$ на $(y''_1, \dots, y''_k)$, получим решение системы (5), не содержащее внутри себя $(y_1, \dots, y_k)$. Получаем противоречие с условием, т. е. f совершенно уравновешена. Достаточность доказана. ■

Замечание 2. Логично задаться вопросом: а для всякой ли выходной последовательности $z = (z_1, \dots, z_r) \in V_r$ существует набор $y = (y_1, \dots, y_k) \in V_k$, входящий (в указанном смысле) в любую входную последовательность $x = (x_1, \dots, x_{r+n-1})$ из прообраза z , в случае совершенно уравновешенной функции? Ответ на этот вопрос, вообще говоря, отрицательный. Достаточно рассмотреть функцию $f(x_1, x_2) = x_1 \oplus x_2$ и состоящую из одних нулей выходную последовательность z — в этом случае в прообраз z будет входить как последовательность из единиц, так и последовательность из нулей. Очевидно, ни одного y , входящего в оба эти решения, не существует.

Свойство совершенно уравновешенных функций, доказанное в теореме 4, означает следующее. Важное свойство, благодаря которому при преобразовании двоичных последовательностей с помощью кодирующего устройства с совершенно уравновешенной фильтрующей функцией f в выходных последовательностях сохраняются хорошие свойства близких к истинно случайным входных последовательностей, никаким положительным образом не переносится на случай далеких от истинно случайных входных последовательностей. Если входная последовательность порождена некоторым детерминированным устройством с конечной памятью и имеет явные зависимости между некоторыми битами, то эти зависимости, а точнее, непосредственно следующие из них запреты на появление некоторых наборов внутри входной последовательности, кодирующим устройством с совершенно уравновешенной фильтрующей функцией всегда будут явно отражены в появлении запретов в выходных последовательностях. То есть совершенная уравновешенность фильтрующей функции делает теоретически возможным распознавание по выходной последовательности структурных особенностей входной последовательности, если она была порождена с помощью некоторого конечного автомата. Например, если на вход фильтрующего устройства с совершенно уравновешенной функцией подавать линейно-рекуррентную последовательность, то по выходу теоретически возможно восстановление рекурренты.

Утверждение теоремы 4 можно переформулировать следующим образом: фильтрующая функция сохраняет запреты (в соответствующем смысле) тогда и только тогда, когда она совершенно уравновешена. Нетрудно заметить, что из данного критерия совершенной уравновешенности непосредственно следует, например, утверждение о совершенной уравновешенности булевой функции, полученной из некоторых двух совершенно уравновешенных функций с помощью описанной в работе [5] специально определенной операции композиции фильтрующих функций.

Случай отсутствия у фильтрующей функции совершенной уравновешенности и соответствующая ему способность кодирующего устройства с этой функцией не сохранять некоторые запреты могут быть проиллюстрированы следующим простым примером.

Рассмотрим $f(x_1, x_2) = x_1 x_2 \in \mathcal{F}_2 \setminus \mathcal{PB}_2$ и соответствующее ей фильтрующее устройство. Предположим, что на вход данного устройства могут поступать любые последовательности, за исключением содержащих внутри себя набор $(0, 1, 0)$. Покажем, что появление такого запрета на входе не породит запрета на выходе. Для этого заметим, что равенство

$$f_r(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{i-1}, 0, 1, 0, \varepsilon_{i+3}, \dots, \varepsilon_{r+1}) = f_r(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{i-1}, 0, 0, 0, \varepsilon_{i+3}, \dots, \varepsilon_{r+1})$$

выполняется для любых $r \in \mathbb{N}$, $i = 1, \dots, r-1$, и любых значений ε_j , то есть удаление в произвольной входной последовательности всех наборов $(0, 1, 0)$ и подстановка на их места наборов $(0, 0, 0)$ никак не скажется на выходной последовательности.

Из всего вышесказанного можно сделать заключение о том, что использование совершенно уравновешенных функций в качестве фильтрующих предпочтительно в тех и только в тех случаях, когда им на вход будут поступать близкие к истинно случайным двоичные последовательности, не обладающие явными зависимостями между битами. В противном случае лучше использовать функции, которые не переносят некоторые возникающие во входных последовательностях запреты в выходные последовательности, а следовательно, не позволяют по выходам кодирующего устройства узнавать дополнительную информацию о структуре входных последовательностей.

3.2. Восстановление символов входной последовательности

Рассмотрим вопрос, связанный с восстановлением символов входной последовательности фильтрующего устройства. Пусть булева функция $f \in \mathcal{F}_n$ имеет правый барьер длины $b < +\infty$. В случае $b = 1$ f представима в виде $f(x_1, \dots, x_n) = g(x_1, \dots, x_{n-1}) \oplus x_n$, поэтому при использовании этой функции как фильтрующей в кодирующем устройстве упомянутого типа каждый входной бит последовательности однозначно определяется по предыдущим $n-1$ входным и соответствующему выходному биту: $x_i = \hat{f}(x_{i-n+1}, \dots, x_{i-1}, y_{i-n+1}) = g(x_{i-n+1}, \dots, x_{i-1}) \oplus y_{i-n+1}$, $i = n, n+1, \dots$. Возникает вопрос: можно ли для функций с правым барьером большей длины построить аналог локально обратной функции $\hat{f}$?

Определим для произвольной функции с барьером длины $b < +\infty$ частично определенную булеву функцию $\hat{f}(x_1, \dots, x_{n-1}, y_1, \dots, y_b)$ следующим образом:

$$\begin{aligned} \hat{f}(x_1, \dots, x_{n-1}, y_1, \dots, y_b) = \\ = \begin{cases} 0, & \exists (t_2, \dots, t_b) \in V_{b-1} : f_b(x_1, \dots, x_{n-1}, 0, t_2, \dots, t_b) = (y_1, \dots, y_b); \\ 1, & \exists (t_2, \dots, t_b) \in V_{b-1} : f_b(x_1, \dots, x_{n-1}, 1, t_2, \dots, t_b) = (y_1, \dots, y_b); \\ *, & \nexists (t_1, \dots, t_b) \in V_b : f_b(x_1, \dots, x_{n-1}, t_1, \dots, t_b) = (y_1, \dots, y_b). \end{cases} \quad (6) \end{aligned}$$

Чтобы доказать корректность такого задания функции, покажем, что условие

$$\exists (t_2, \dots, t_b) \in V_{b-1} : f_b(x_1, \dots, x_{n-1}, t_1, t_2, \dots, t_b) = (y_1, \dots, y_b)$$

может быть выполнено не более чем для одного $t_1 \in \{0, 1\}$. Предположим противное:

$$\begin{aligned} \exists (t'_2, \dots, t'_b) \in V_{b-1} (f_b(x_1, \dots, x_{n-1}, 0, t'_2, \dots, t'_b) = (y_1, \dots, y_b)), \\ \exists (t''_2, \dots, t''_b) \in V_{b-1} (f_b(x_1, \dots, x_{n-1}, 1, t''_2, \dots, t''_b) = (y_1, \dots, y_b)). \end{aligned}$$

В таком случае выполнена система

$$\begin{cases} f(z'_1, z'_2, \dots, z'_n) = y_1 = f(z''_1, z''_2, \dots, z''_n); \\ f(z'_2, z'_3, \dots, z'_{n+1}) = y_2 = f(z''_2, z''_3, \dots, z''_{n+1}); \\ \dots \\ f(z'_b, z'_{b+1}, \dots, z'_{b+n-1}) = y_b = f(z''_b, z''_{b+1}, \dots, z''_{b+n-1}); \\ z'_1 = z''_1 = x_1, \dots, z'_{n-1} = z''_{n-1} = x_{n-1}, z'_n = 0, z''_n = 1; \\ z'_{n+1} = t'_2, \dots, z'_{b+n-1} = t'_b; \\ z''_{n+1} = t''_2, \dots, z''_{b+n-1} = t''_b, \end{cases}$$

что противоречит определению правого барьера длины b . Следовательно, функция $\widehat{f}$ определена корректным образом и является функцией, которая однозначно восстанавливает символ входной последовательности по $n - 1$ предшествующим входным и b последующим выходным символам.

Логично предположить, что частично определенная булева функция, действие которой, в некотором смысле, обратно действию некоторой совершенно уравновешенной функции, сама должна быть сбалансированной.

Соответствующее утверждение сформулировано в теореме 5, доказательство которой опирается на леммы 1 и 2.

Предварительно введем два обозначения: для функции $f \in \mathcal{F}_n$ и натурального l для всякого набора $(x_1, \dots, x_n) \in V_n$ определим величину $M'_{f_l}(x_1, \dots, x_n)$:

$$\begin{aligned} M'_{f_l}(x_1, \dots, x_n) = \\ = \sharp\{(y_1, \dots, y_l) : \exists(t_{n+1}, \dots, t_{l+n-1}) (f_l(x_1, \dots, x_n, t_{n+1}, \dots, t_{l+n-1}) = (y_1, \dots, y_l))\}; \end{aligned}$$

для всякого набора $(x_1, \dots, x_{n-1}) \in V_{n-1}$ определим величину $M''_{f_l}(x_1, \dots, x_{n-1})$:

$$\begin{aligned} M''_{f_l}(x_1, \dots, x_{n-1}) = \\ = \sharp\{(y_1, \dots, y_l) : \exists(t_n, \dots, t_{l+n-1}) (f_l(x_1, \dots, x_{n-1}, t_n, t_{n+1}, \dots, t_{l+n-1}) = (y_1, \dots, y_l))\}. \end{aligned}$$

Лемма 1. Пусть $f \in \mathcal{F}_n$ имеет правый барьер длины $b < +\infty$. Если для некоторого $l \geq b$ существует набор $(\tilde{x}_1, \dots, \tilde{x}_n) \in V_n$, такой, что

$$M'_{f_l}(\tilde{x}_1, \dots, \tilde{x}_n) \neq \frac{1}{2} M''_{f_l}(\tilde{x}_1, \dots, \tilde{x}_{n-1}),$$

то существует набор $(x'_1, \dots, x'_{m+n-2}) \in V_{m+n-2}$, для которого выполнена следующая система:

$$\begin{cases} m \geq 2; \\ (x'_m, \dots, x'_{m+n-2}) = (x'_1, \dots, x'_{n-1}); \\ M'_{f_l}(x'_j, \dots, x'_{j+n-1}) \leq M''_{f_l}(x'_j, \dots, x'_{j+n-2})/2, \quad j = 1, \dots, m-1; \\ \exists j \in \{1, 2, \dots, m-1\} \quad (M'_{f_l}(x'_j, \dots, x'_{j+n-1}) < M''_{f_l}(x'_j, \dots, x'_{j+n-2})/2). \end{cases}$$

Доказательство. Рассмотрим граф де Брейна порядка $n - 1$ (напомним, что графом де Брейна порядка k называется ориентированный граф с 2^k вершинами и 2^{k+1} ориентированными ребрами, причем вершинам взаимно однозначно сопоставляются двоичные наборы длины k ; дуга из вершины с набором $(x_1, \dots, x_k)$ в вершину с набором $(y_1, \dots, y_k)$ присутствует в графе тогда и только тогда, когда выполнены равенства $y_i = x_{i+1}$ для всех $i = 1, \dots, k - 1$). Введем дополнительные пометки на его дугах.

Дугу из вершины с набором $(x_1, \dots, x_{n-1})$ в вершину с набором $(x_2, \dots, x_n)$ пометим в соответствии со следующим правилом:

$$\begin{cases} 0, & M'_{f_l}(x_1, \dots, x_n) < M''_{f_l}(x_1, \dots, x_{n-1})/2; \\ 1, & M'_{f_l}(x_1, \dots, x_n) = M''_{f_l}(x_1, \dots, x_{n-1})/2; \\ 2, & M'_{f_l}(x_1, \dots, x_n) > M''_{f_l}(x_1, \dots, x_{n-1})/2. \end{cases}$$

Тогда условие леммы можно переформулировать следующим образом: в помеченном описанным выше способом графе де Брейна порядка $n-1$ существует хотя бы один цикл, не содержащий дуг с пометкой 2 и содержащий хотя бы одну дугу с пометкой 0.

Из существования у функции f правого барьера длины b следует: для $l \geq b$ верно, что для произвольного набора $(\bar{x}_1, \dots, \bar{x}_{n-1})$ выполняется соотношение

$$\begin{aligned} \{(y_1, \dots, y_l) : \exists (x_{n+1}, \dots, x_{l+n-1}) \in V_{l-1} \\ (f_l(\bar{x}_1, \dots, \bar{x}_{n-1}, 0, x_{n+1}, \dots, x_{l+n-1}) = (y_1, \dots, y_l))\} \cap \\ \cap \{(y_1, \dots, y_l) : \exists (x_{n+1}, \dots, x_{l+n-1}) \in V_{l-1} \\ (f_l(\bar{x}_1, \dots, \bar{x}_{n-1}, 1, x_{n+1}, \dots, x_{l+n-1}) = (y_1, \dots, y_l))\} = \emptyset. \end{aligned}$$

Так как при этом выполняется соотношение

$$\begin{aligned} \{(y_1, \dots, y_l) : \exists (x_{n+1}, \dots, x_{l+n-1}) \in V_{l-1} \\ (f_l(\bar{x}_1, \dots, \bar{x}_{n-1}, 0, x_{n+1}, \dots, x_{l+n-1}) = (y_1, \dots, y_l))\} \cup \\ \cup \{(y_1, \dots, y_l) : \exists (x_{n+1}, \dots, x_{l+n-1}) \in V_{l-1} \\ (f_l(\bar{x}_1, \dots, \bar{x}_{n-1}, 1, x_{n+1}, \dots, x_{l+n-1}) = (y_1, \dots, y_l))\} = \\ = \{(y_1, \dots, y_l) : \exists (x_n, \dots, x_{l+n-1}) \in V_l \\ (f_l(\bar{x}_1, \dots, \bar{x}_{n-1}, x_n, x_{n+1}, \dots, x_{l+n-1}) = (y_1, \dots, y_l))\}, \end{aligned}$$

то верно

$$M''_{f_l}(\bar{x}_1, \dots, \bar{x}_{n-1}) = M'_{f_l}(\bar{x}_1, \dots, \bar{x}_{n-1}, 0) + M'_{f_l}(\bar{x}_1, \dots, \bar{x}_{n-1}, 1),$$

поэтому в нашем графе сумма пометок на любой паре выходящих из одной вершины дуг равна 2.

Удалим из графа все дуги с пометкой 2. Для завершения доказательства леммы достаточно построить в получившемся таким образом графе цикл, содержащий дугу с пометкой 0.

Начнем обход получившегося графа, начиная из вершины с набором $(\tilde{x}_1, \dots, \tilde{x}_{n-1})$. Перейдем по единственной исходящей из нее дуге (с пометкой 0). Покажем, что из текущей вершины существует путь (возможно, нулевой длины) по дугам с пометкой 1 в некоторую вершину, из которой исходит дуга с пометкой 0. Достаточно рассмотреть два возможных случая: либо из нашей вершины по дугам с пометкой 1 доступны все вершины графа (и, в том числе, подходящая нам вершина с набором $(\tilde{x}_1, \dots, \tilde{x}_{n-1})$), либо некоторая часть графа недоступна, что может произойти только из-за встреченных вершин, из которых в исходном графе исходила дуга с пометкой 2.

Итак, из исходной вершины по пути, состоящему ровно из одной дуги с пометкой 0 и, возможно, простой цепи из дуг с пометками 1, можно попасть в некоторую вершину, из которой тоже исходит дуга с пометкой 0. В случае, если эта новая вершина отлична от исходной, вновь перейдем по дуге с пометкой 0 и дугам с пометками 1 в некоторую вершину с исходящей из нее дугой с пометкой 0. Продолжая действовать таким образом, через некоторое число шагов попадем в одну из ранее встреченных вершин с исходящей дугой с пометкой 0. Искомый цикл построен, лемма доказана. ■

Лемма 2. Если $f \in \mathcal{F}_n$ имеет правый барьер длины $b < +\infty$, то равенство $M'_{f_l}(x_1, \dots, x_{n-1}, 0) = M'_{f_l}(x_1, \dots, x_{n-1}, 1) = M''_{f_l}(x_1, \dots, x_{n-1})/2$ выполняется для любого $l \geq b$ и любого $(x_1, \dots, x_{n-1}) \in V_{n-1}$.

Доказательство. С помощью вытекающего из определения правого барьера длины b равенства

$$\{(y_1, \dots, y_l) : \exists(t_{n+1}, \dots, t_{l+n-1}) (f_l(x_1, \dots, x_{n-1}, 0, t_{n+1}, \dots, t_{l+n-1}) = (y_1, \dots, y_l))\} \cap \\ \cap \{(y_1, \dots, y_l) : \exists(t_{n+1}, \dots, t_{l+n-1}) (f_l(x_1, \dots, x_{n-1}, 1, t_{n+1}, \dots, t_{l+n-1}) = (y_1, \dots, y_l))\} = \emptyset$$

и очевидного равенства

$$\{(y_1, \dots, y_l) : \exists(t_{n+1}, \dots, t_{l+n-1}) (f_l(x_1, \dots, x_{n-1}, 0, t_{n+1}, \dots, t_{l+n-1}) = (y_1, \dots, y_l))\} \cup \\ \cup \{(y_1, \dots, y_l) : \exists(t_{n+1}, \dots, t_{l+n-1}) (f_l(x_1, \dots, x_{n-1}, 1, t_{n+1}, \dots, t_{l+n-1}) = (y_1, \dots, y_l))\} = \\ = \{(y_1, \dots, y_l) : \exists(t_n, t_{n+1}, \dots, t_{l+n-1}) (f_l(x_1, \dots, x_{n-1}, t_n, t_{n+1}, \dots, t_{l+n-1}) = (y_1, \dots, y_l))\},$$

которые верны для любого $l \geq b$, легко получить, что для доказательства леммы достаточно показать невозможность существования для какого-либо $l \geq b$ набора $(\tilde{x}_1, \dots, \tilde{x}_n) \in V_n$, для которого выполняется неравенство

$$M'_{f_l}(x_1, \dots, x_n) < M''_{f_l}(x_1, \dots, x_{n-1})/2. \quad (7)$$

Предположим существование такого набора $(\tilde{x}_1, \dots, \tilde{x}_n) \in V_n$ для некоторого l , $l \geq b$, для которого выполняется (7).

Рассмотрим для произвольных фиксированных $\hat{x}_1, \dots, \hat{x}_n$ системы, описывающие отображения $f_l(\hat{x}_1, \dots, \hat{x}_{n-1}, x_n, x_{n+1}, \dots, x_{n+l-1}), f_l(\hat{x}_1, \dots, \hat{x}_{n-1}, \hat{x}_n, x_{n+1}, \dots, x_{n+l})$:

$$\begin{cases} y_1 = f(\hat{x}_1, \dots, \hat{x}_{n-2}, \hat{x}_{n-1}, x_n); \\ y_2 = f(\hat{x}_2, \dots, \hat{x}_{n-1}, x_n, x_{n+1}); \\ \dots \\ y_l = f(x_l, \dots, x_{l+n-2}, x_{l+n-2}, x_{l+n-1}); \end{cases} \quad \begin{cases} y_1 = f(\hat{x}_1, \dots, \hat{x}_{n-2}, \hat{x}_{n-1}, \hat{x}_n); \\ y_2 = f(\hat{x}_2, \dots, \hat{x}_{n-1}, \hat{x}_n, x_{n+1}); \\ \dots \\ y_l = f(x_l, \dots, x_{l+n-2}, x_{l+n-2}, x_{l+n-1}); \\ y_{l+1} = f(x_{l+1}, \dots, x_{l+n-2}, x_{l+n-1}, x_{l+n}). \end{cases}$$

Так как $f(\hat{x}_1, \dots, \hat{x}_n)$ во второй системе определена однозначно и не зависит от $x_{n+1} \dots, x_{n+l}$, верно равенство

$$\#\{(y_1, \dots, y_{l+1}) : \exists(x_{n+1}, \dots, x_{l+n}) (f_{l+1}(\hat{x}_1, \dots, \hat{x}_n, x_{n+1}, \dots, x_{l+n}) = (y_1, \dots, y_{l+1}))\} = \\ = \#\{(y_2, \dots, y_{l+1}) : \exists(x_{n+1}, \dots, x_{l+n}) (f_l(\hat{x}_2, \dots, \hat{x}_n, x_{n+1}, \dots, x_{l+n}) = (y_2, \dots, y_{l+1}))\} = \\ = M''_{f_l}(\hat{x}_2, \dots, \hat{x}_n).$$

С другой стороны, вторая система получена из первой фиксацией аргумента x_n и добавлением одной новой строки. Поэтому выполняется неравенство

$$\#\{(y_1, \dots, y_{l+1}) : \exists(x_{n+1}, \dots, x_{l+n}) (f_{l+1}(\hat{x}_1, \dots, \hat{x}_n, x_{n+1}, \dots, x_{l+n}) = (y_1, \dots, y_{l+1}))\} \leq \\ \leq 2 \#\{(y_1, \dots, y_l) : \exists(x_{n+1}, \dots, x_{l+n-1}) (f_l(\hat{x}_1, \dots, \hat{x}_n, x_{n+1}, \dots, x_{l+n-1}) = (y_1, \dots, y_l))\} = \\ = 2M'_{f_l}(\hat{x}_1, \dots, \hat{x}_n).$$

Окончательно получим: для всякого набора $(\hat{x}_1, \dots, \hat{x}_n) \in V_n$ выполнено

$$M''_{f_l}(\hat{x}_2, \dots, \hat{x}_n) \leq 2M'_{f_l}(\hat{x}_1, \dots, \hat{x}_n). \quad (8)$$

В лемме 1 доказано, что при нашем предположении о существовании набора $(\tilde{x}_1, \dots, \tilde{x}_n) \in V_n$, для которого выполнено (7), существует набор $(x'_1, \dots, x'_{m+n-2})$, такой, что:

$$\begin{cases} m \geq 2; \\ (x'_m, \dots, x'_{m+n-2}) = (x'_1, \dots, x'_{n-1}); \\ M'_{f_l}(x'_j, \dots, x'_{j+n-1}) \leq M''_{f_l}(x'_j, \dots, x'_{j+n-2})/2, \quad j = 1, \dots, m-1; \\ \exists j \in \{1, 2, \dots, m-1\} \quad (M'_{f_l}(x'_j, \dots, x'_{j+n-1}) < M''_{f_l}(x'_j, \dots, x'_{j+n-2})/2). \end{cases} \quad (9)$$

Из (8) следует, что $M''_{f_l}(x'_{j+1}, \dots, x'_{j+n-1}) \leq 2M'_{f_l}(x'_j, \dots, x'_{j+n-1})$ для $j = 1, \dots, m-1$. Тогда, с учетом (9), верна следующая цепочка неравенств:

$$\begin{aligned} M''_{f_l}(x'_1, \dots, x'_{n-1}) &= M''_{f_l}(x'_m, \dots, x'_{m+n-2}) \leq 2M'_{f_l}(x'_{m-1}, \dots, x'_{m+n-2}) \leq \\ &\leq 2M''_{f_l}(x'_{m-1}, \dots, x'_{m+n-3})/2 = M''_{f_l}(x'_{m-1}, \dots, x'_{m+n-3}) \leq \dots \leq M''_{f_l}(x'_1, \dots, x'_{n-1}), \end{aligned}$$

причем хотя бы одно из неравенств этой цепочки — строгое.

Получили $M'_{f_l}(x'_1, \dots, x'_{n-1}) < M''_{f_l}(x'_1, \dots, x'_{n-1})$. Это противоречие завершает доказательство леммы. ■

Теорема 5. Пусть $f \in \mathcal{F}_n$, f имеет правый барьер длины $b < +\infty$. Тогда функция $\hat{f}$, определенная согласно (6), является уравновешенной (в соответствующем смысле для частично определенных булевых функций):

$$\begin{aligned} \#\{(x_1, \dots, x_{n-1}, y_1, \dots, y_b) : \hat{f}(x_1, \dots, x_{n-1}, y_1, \dots, y_b) = 0\} &= \\ = \#\{(x_1, \dots, x_{n-1}, y_1, \dots, y_b) : \hat{f}(x_1, \dots, x_{n-1}, y_1, \dots, y_b) = 1\}. \end{aligned} \quad (10)$$

Доказательство. Равенство (10), согласно определению $\hat{f}$, можно переписать в следующем виде:

$$\begin{aligned} \#\{(x_1, \dots, x_{n-1}, y_1, \dots, y_b) : \exists(t_{n+1}, \dots, t_{b+n-1}) \\ (f_b(x_1, \dots, x_{n-1}, 0, t_{n+1}, \dots, t_{b+n-1}) = (y_1, \dots, y_b))\} &= \\ = \#\{(x_1, \dots, x_{n-1}, y_1, \dots, y_b) : \exists(t_{n+1}, \dots, t_{b+n-1}) \\ (f_b(x_1, \dots, x_{n-1}, 1, t_{n+1}, \dots, t_{b+n-1}) = (y_1, \dots, y_b))\}. \end{aligned}$$

По определению величины M'_{f_l} это равенство эквивалентно следующему:

$$\sum_{(x_1, \dots, x_{n-1}) \in V_{n-1}} M'_{f_l}(x_1, \dots, x_{n-1}, 0) = \sum_{(x_1, \dots, x_{n-1}) \in V_{n-1}} M'_{f_l}(x_1, \dots, x_{n-1}, 1). \quad (11)$$

Последнее равенство верно в силу леммы 2. ■

Замечание 3. Нетрудно заметить, что из леммы 2 следует и более сильное утверждение: уравновешенной (в соответствующем смысле для частично определенных булевых функций) является не только функция $\hat{f}$, но и любая ее подфункция, полученная фиксацией переменных $x_1, \dots, x_{n-1}$.

Рассмотренный в замечании 3 факт можно проинтерпретировать следующим образом: если использовать функцию $\hat{f}$ для восстановления символов входной последовательности кодирующего устройства с фильтрующей функцией f с правым барьером конечной длины, то при восстановлении очередного входного символа при известных предыдущих $n-1$ входных символах ровно половина множества возможных l -грамм последующих выходных символов будет свидетельствовать о равенстве очередного входного символа нулю, ровно половина — о равенстве единице.

Напоследок заметим, что данное свойство нельзя обобщить для произвольной ситуации, в которой возможно восстановление очередного входного символа кодирующего устройства с совершенно уравновешенной фильтрующей функцией по предшествующим $n - 1$ входным и последующим l выходным символам. Например, при $f(x_1, x_2, x_3) = x_1 \oplus x_2 x_3 \in \mathcal{PB}_3$, $n = 2$ и $l = 2$, если требуется восстановить x_3 , зная $x_1, x_2, y_1 = f(x_1, x_2, x_3) = x_1 \oplus x_2 x_3$ и $y_2 = f(x_2, x_3, x_4) = x_2 \oplus x_3 x_4$, то в ситуации, когда $x_1 = 0$ и $x_2 = 1$, символ x_3 восстановим по паре (y_1, y_2) , однако о равенстве x_3 нулю свидетельствует только одна пара — $(y_1, y_2) = (0, 1)$, тогда как о равенстве x_3 единице свидетельствуют две: $(1, 0)$ и $(1, 1)$.

Кроме того, нельзя обобщить данное свойство и на случай произвольного отображения вида $V_{n+b-1} \rightarrow V_b$, которое является уравновешенным и у которого n -й входной символ можно восстановить по предшествующим $n - 1$ входным и b последующим выходным символам. Далее приведен пример отображения F , для которого аналог функции $\hat{f}$ не является уравновешенным.

Пусть $n = b = 2$; $F : V_{n+b-1} \rightarrow V_b$; $\hat{f} : V_{n+b-1} \rightarrow \{0, 1, *\}$.

$F(x_1, x_2, x_3) = (y_1, y_2)$					$\hat{f}(x_1, y_1, y_2) = x_2$			
x_1	x_2	x_3	y_1	y_2	x_1	y_1	y_2	x_2
0	0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	1	0
0	1	0	0	0	0	1	0	1
0	1	1	1	0	0	1	1	*
1	0	0	1	1	1	0	0	1
1	0	1	1	1	1	0	1	*
1	1	0	0	0	1	1	0	1
1	1	1	1	0	1	1	1	0

ЛИТЕРАТУРА

1. Сумароков С. Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обзорение прикладной и промышленной математики. 1994. Т. 1. Вып. 1. С. 33–55.
2. Логачев О. А., Смышляев С. В., Яценко В. В. Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. Т. 21. Вып. 2. С. 51–74.
3. 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.
4. Смышляев С. В. Барьеры совершенно уравновешенных булевых функций // Дискретная математика (в печати).
5. 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.
6. 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.
7. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.