2011 Теоретические основы прикладной дискретной математики №4(14)
DOI 10.17223/20710410/14/2
УДК 519.7

ЛОКАЛЬНО ОБРАТИМЫЕ БУЛЕВЫ ФУНКЦИИ[1]

С. В. Смышляев

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

E-mail: smyshsv@gmail.com

Изучается свойство локальной обратимости булевых функций. Устанавливается ряд необходимых условий локальной обратимости, позволяющих строить классы функций, соответствующие которым кодирующие устройства не допускают локального обращения. Доказывается критерий, связывающий локальную обратимость произвольной булевой функции с определенными характеристиками булевых функций с барьером.

Ключевые слова: *функции без запрета, совершенно уравновешенные функции, барьеры булевых функций, локальная обратимость, криптография.*

Введение

При исследовании кодирующих устройств, состоящих из регистра сдвига и функции усложнения [1, 2], естественным вопросом является возможность однозначного восстановления части входной последовательности кодирующего устройства по части выходной последовательности. В частности, при использовании таких кодирующих устройств в составе фильтрующих генераторов наличие возможности получения по конечному отрезку выходной последовательности достаточно большой части символов входной последовательности делает возможным нахождение секретного ключа простым решением линейной системы уравнений. Одним из возможных вариантов формализации данного свойства функций усложнения является следующий: существование таких выходных наборов, что в случае их присутствия в выходной последовательности кодирующего устройства оставшиеся символы входной последовательности можно восстанавливать однозначно по последующим символам выходной последовательности.

Данное понятие было формализовано О. А. Логачевым как понятие локальной обратимости булевой функции в работе [3], посвященной изучению соответствующих свойств функций, линейных по последней переменной. Здесь же был получен критерий локальной обратимости порождаемых такими функциями отображений, связывающий данное понятие с так называемым возвратным свойством булевой функции [4].

В настоящей работе проводится исследование свойства локальной обратимости произвольных булевых функций. Устанавливается ряд необходимых свойств локальной обратимости, в частности совершенная уравновешенность [5 – 7] и наличие барьера [8, 9]. Доказывается критерий, связывающий локальную обратимость произвольной булевой функции с описанными в работе [10] характеристиками булевых функций с барьером. Важными следствиями полученных результатов являются методы построения булевых функций с положительными криптографическими свойствами, не допускающих локального обращения. В частности, все описанные в работе [11] методы, как следует из результатов настоящей работы, позволяют строить не допускающие локального обращения совершенно уравновешенные булевы функции.

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

1. Определения и предварительные результаты

Для любого натурального n множество $\{0,1\}^n$ двоичных наборов длины n будем обозначать через V_n; множество булевых функций от n переменных — через $\mathcal{F}_n$.

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

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

Через f_l будем обозначать следующее отображение из V_{l+n-1} в V_l:

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

Легко видеть, что отображение f_l можно понимать как преобразование, производимое l тактами работы кодирующего устройства, полученного с помощью подключения входов булевой функции f к некоторым ячейкам двоичного регистра сдвига [1, 5].

Для $n, l \in \mathbb{N}$, всякого набора $(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{n-1}) \in V_{n-1}$ через $f_{R,l,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}$ будем обозначать отображение из V_l в V_l, определяемое следующим образом:

$$f_{R,l,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}(x_1, x_2, \ldots, x_l) = f_l(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{n-1}, x_1, x_2, \ldots, x_l),$$

а через $f_{L,l,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}$ — отображение из V_l в V_l вида

$$f_{L,l,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}(x_1, x_2, \ldots, x_l) = f_l(x_1, x_2, \ldots, x_l, \tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{n-1}).$$

Отображение $f_{R,l,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}$ описывает преобразование, производимое l тактами работы кодирующего устройства с функцией усложнения f на двоичных последовательностях с фиксированным началом из $n-1$ символов.

Определение 1 [5, 12]. Булева функция $f \in \mathcal{F}_n$ называется *функцией без запрета*, если соотношение $|f_l^{-1}(\mathbf{y})| > 0$ выполняется для любого $l \in \mathbb{N}$ и любого $\mathbf{y} \in V_l$.

Определение 2 [5, 12]. Булева функция $f \in \mathcal{F}_n$ называется *совершенно уравновешенной*, если соотношение $|f_l^{-1}(\mathbf{y})| = 2^{n-1}$ выполняется для любого $l \in \mathbb{N}$ и любого $\mathbf{y} \in V_l$. Множество совершенно уравновешенных функций из $\mathcal{F}_n$ обозначим через $\mathcal{PB}_n$.

Определение 3 [5, 12]. Булева функция $f \in \mathcal{F}_n$ называется *функцией без потери информации*, если при любом $l \geqslant n$ система

$$\begin{cases} f_l(x_1, x_2, \ldots, x_{l+n-1}) = f_l(z_1, z_2, \ldots, z_{l+n-1}), \\ (x_1, x_2, \ldots, x_{n-1}) = (z_1, z_2, \ldots, z_{n-1}), \\ (x_{l+1}, x_{l+2}, \ldots, x_{l+n-1}) = (z_{l+1}, z_{l+2}, \ldots, z_{l+n-1}), \\ (x_n, x_{n+1}, \ldots, x_l) \neq (z_n, z_{n+1}, \ldots, z_l) \end{cases}$$

является несовместной.

Теорема 1 [5, 12]. Пусть $f \in \mathcal{F}_n$. Следующие утверждения эквивалентны:

1) f является функцией без запрета;
2) f является совершенно уравновешенной функцией;
3) f является функцией без потери информации.

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

Определение 4 [6]. Булева функция $f \in \mathcal{F}_n$ называется функцией с правым барьером длины $b \in \mathbb{N}$, если система уравнений

$$\begin{cases} f_{R,b',n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}(x_1, x_2, \ldots, x_{b'}) = f_{R,b',n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}(z_1, z_2, \ldots, z_{b'}), \\ x_1 \neq z_1 \end{cases} \tag{2}$$

имеет решение для любого $b' \in \mathbb{N}$, $b' \leqslant b-1$, а система

$$\begin{cases} f_{R,b,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}(x_1, x_2, \ldots, x_b) = f_{R,b,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}(z_1, z_2, \ldots, z_b), \\ x_1 \neq z_1 \end{cases} \tag{3}$$

решений не имеет.

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

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

Теорема 2 [6]. Если функция имеет барьер, то она совершенно уравновешена.

Замечание 1. В работе [6] показано, что наличие барьера не является необходимым условием совершенной уравновешенности; в работе [11] приведен метод построения широких классов совершенно уравновешенных булевых функций без барьера.

Отметим, что для всех утверждений, относящихся к функциям с правым барьером, очевидным образом могут быть построены аналоги для функций с левым барьером. Далее длину правого барьера булевой функции f будем обозначать b_f^R, левого — b_f^L.

Замечание 2. Нетрудно заметить, что наличие правого барьера длины $b_f^R = 1$ (левого барьера длины $b_f^L = 1$) означает линейность функции по последнему (первому) аргументу.

Теорема 3 [10]. Для каждой функции $f \in \mathcal{F}_n$ с правым (левым) барьером можно определить величину $e_f^R \in \{0, 1, 2, \ldots, b_f^R - 1\}$ ($e_f^L \in \{0, 1, 2, \ldots, b_f^L - 1\}$), такую, что для любого $l \geqslant b_f^R - 1$ ($l \geqslant b_f^L - 1$), $\mathbf{x} \in V_{n-1}$ и любого набора $\mathbf{y} \in \mathrm{Im}(f_{R,l,n-1}^{\mathbf{x}})$ ($\mathbf{y} \in \mathrm{Im}(f_{L,l,n-1}^{\mathbf{x}})$) выполняется равенство $|{f_{R,l,n-1}^{\mathbf{x}}}^{-1}(\mathbf{y})| = 2^{e_f^R}$ ($|{f_{L,l,n-1}^{\mathbf{x}}}^{-1}(\mathbf{y})| = 2^{e_f^L}$).

Утверждение 1 [10]. Пусть $f \in \mathcal{F}_n$ имеет правый (левый) барьер. Для любых $l \geqslant b_f^R - 1$ ($l \geqslant b_f^L - 1$) и любого набора $\mathbf{x} \in V_{n-1}$ верно равенство $|\mathrm{Im}(f_{R,l,n-1}^{\mathbf{x}})| = 2^{l-e_f^R}$ ($|\mathrm{Im}(f_{L,l,n-1}^{\mathbf{x}})| = 2^{l-e_f^L}$).

Пусть $f \in \mathcal{F}_n$. Определим для всякого $m \in \mathbb{N}$ и для всякого набора $\mathbf{y} \in V_m$ следующие множества:

$$A_{\mathbf{y}}^f = \left\{\mathbf{x} \in V_{n-1} : {f_{R,m,n-1}^{\mathbf{x}}}^{-1}(\mathbf{y}) \neq \varnothing\right\}; \quad E_{\mathbf{y}}^f = \left\{\mathbf{x} \in V_{n-1} : {f_{L,m,n-1}^{\mathbf{x}}}^{-1}(\mathbf{y}) \neq \varnothing\right\}.$$

Утверждение 2 [10]. Пусть $f \in \mathcal{F}_n$ имеет правый (левый) барьер. Для любого $l \geqslant b_f^R - 1$ ($l \geqslant b_f^L - 1$) и любого набора $\mathbf{y} \in V_l$ верно равенство $|A_{\mathbf{y}}^f| = 2^{n-1-e_f^R}$ ($|E_{\mathbf{y}}^f| = 2^{n-1-e_f^L}$).

Теорема 4 [10]. Пусть $f(x_1, x_2, \ldots, x_n) \in \mathcal{F}_n$ имеет правый (левый) барьер. Тогда

1) $e_f^R = b_f^R - 1$ ($e_f^L = b_f^L - 1$) 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 $x_{b_f^L}$);
2) $e_f^R = 0$ ($e_f^L = 0$) тогда и только тогда, когда $b_f^R = 1$ ($b_f^L = 1$).

Будем обозначать через V_∞ множество всех бесконечных (вправо) двоичных последовательностей, т. е. последовательностей вида $\overline{\mathbf{z}} = (z_1, z_2, \ldots)$, где $z_i \in \{0, 1\}$, $i = 1, 2, \ldots$

Для всякой функции $f \in \mathcal{F}_n$ через f_∞ будем обозначать отображение из V_∞ в V_∞, заданное в соответствии со следующим правилом:

$$f_\infty(x_1, x_2, \ldots) = (f(x_1, x_2, \ldots, x_n), f(x_2, x_3, \ldots, x_{n+1}), \ldots).$$

Кроме того, для всякого набора $(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{n-1}) \in V_{n-1}$ введем следующее отображение из V_∞ в V_∞:

$$f_{R,\infty,n-1}^{(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_{n-1})}(x_1, x_2, \ldots) \equiv f_\infty(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{n-1}, x_1, x_2, \ldots);$$

для всякой последовательности $\overline{\mathbf{z}} \in V_\infty$ введем следующее множество:

$$A_{\overline{\mathbf{z}}}^f = \left\{\mathbf{x} \in V_{n-1} : {f_{R,\infty,n-1}^{\mathbf{x}}}^{-1}(\overline{\mathbf{z}}) \neq \varnothing\right\}.$$

Замечание 3. Легко видеть, что для любых $f \in \mathcal{F}_n$, $m, l \in \mathbb{N}$, $m < l$ и $\overline{\mathbf{z}} = (z_1, z_2, \ldots) \in V_\infty$ выполняется цепочка вложений $A_{\overline{\mathbf{z}}}^f \subseteq A_{(z_1,z_2,\ldots,z_m,\ldots,z_l)}^f \subseteq A_{(z_1,z_2,\ldots,z_m)}^f$, а также вложение $E_{(z_l,z_{l-1},\ldots,z_m,z_{m-1},\ldots,z_1)}^f \subseteq E_{(z_m,z_{m-1},\ldots,z_1)}^f$.

Определение 5 [3]. Пусть $f \in \mathcal{F}_n$. Обозначим для всякого $m \in \mathbb{N}$ через $T_f^R(m)$ множество наборов $\mathbf{y} \in \mathrm{Im}(f_m)$, для которых выполняется следующее условие: для всякой последовательности $\overline{\mathbf{z}} \in V_\infty$, такой, что $(\mathbf{y}|\overline{\mathbf{z}}) \in \mathrm{Im}(f_\infty)$, существует единственная последовательность $\overline{\mathbf{x}} \in V_\infty$, для которой множество $\{\tilde{\mathbf{x}} \in V_m : f_\infty(\tilde{\mathbf{x}}|\overline{\mathbf{x}}) = (\mathbf{y}|\overline{\mathbf{z}})\}$ непусто.

Функция $f \in \mathcal{F}_n$ называется *слабо локально обратимой вправо* (далее будем для сокращения записей использовать термин «локально обратимая функция»), если множество $T_f^R = \bigcup\limits_{i=1}^{\infty} T_f^R(i)$ непусто.

Для всякого натурального n множество локально обратимых булевых функций от n переменных будем обозначать через $\mathcal{LI}_n$.

Замечание 4. Нетрудно видеть, что для всякой функции $f \in \mathcal{F}_n$, любых $m, r \in \mathbb{N}$ и любых наборов $\mathbf{y} \in V_m$, $\mathbf{y}' \in V_r$ верно, что если $\mathbf{y} \in T_f^R$ и $(\mathbf{y}'|\mathbf{y}) \in \mathrm{Im}(f_{m+r})$, то $(\mathbf{y}'|\mathbf{y}) \in T_f^R$.

Определение 6. Функция $f \in \mathcal{F}_n$ называется *слабо локально обратимой влево*, если функция $\overleftrightarrow{f}$ является слабо локально обратимой вправо.

Определение 7. Функция $f \in \mathcal{F}_n$ называется *сильно локально обратимой вправо*, если для некоторого натурального p верно, что множество T_f^R включает в себя все наборы длины не меньше p, то есть выполняется вложение $\bigcup\limits_{i=p}^{\infty} V_i \subseteq T_f^R$.

Определение 8. Функция $f \in \mathcal{F}_n$ называется *сильно локально обратимой влево*, если функция $\overleftrightarrow{f}$ является сильно локально обратимой вправо.

Для всякого n множество сильно локально обратимых вправо (влево) булевых функций от n переменных будем обозначать через $\mathcal{PLI}_n^R$ (соответственно $\mathcal{PLI}_n^L$).

2. Основные результаты

Докажем сначала несколько вспомогательных утверждений.

Лемма 1. Пусть на множестве двоичных наборов конечной длины определен некоторый предикат $Q\colon \bigcup\limits_{i=1}^{\infty} V_i \mapsto \{\mathrm{T}, \mathrm{F}\}$, для которого выполнены следующие свойства:

1) для всяких $m \in \mathbb{N}$, $\mathbf{z} \in V_m$ и $b \in \{0,1\}$ верно, что если $Q(\mathbf{z}) = \mathrm{F}$, то $Q(\mathbf{z}|b) = \mathrm{F}$;
2) для всякого $m \in \mathbb{N}$ существует набор $\mathbf{z} \in V_m$, такой, что $Q(\mathbf{z}) = \mathrm{T}$.

Тогда существует последовательность $\overline{\mathbf{z}}^* = (z_1^*, z_2^*, \ldots) \in V_\infty$, такая, что $Q(z_1^*, z_2^*, \ldots, z_m^*) = \mathrm{T}$ для любого m.

Доказательство. Для всех $m \in \mathbb{N}$ и $\mathbf{z} \in V_m$ через $W(\mathbf{z})$ обозначим множество $\{\mathbf{z}\} \cup \{\mathbf{w} \in \bigcup\limits_{i=m+1}^{\infty} V_i : \mathbf{w} = (\mathbf{z}|\mathbf{u}), \mathbf{u} \in \bigcup\limits_{i=1}^{\infty} V_i\}$; для каждого $l \in \mathbb{N}$ рассмотрим множество $M_l = \{\mathbf{z} \in V_l : Q(\mathbf{z}) = \mathrm{T}\}$. Для каждого $m \in \mathbb{N}$ введем множество U_m, состоящее из наборов $\mathbf{z} \in V_m$, таких, что для всякого $l \geqslant m$ выполнено $W(\mathbf{z}) \cap M_l \neq \varnothing$.

Пусть $\mathbf{z} \in U_m$. Докажем, что существует $b \in \{0,1\}$, при котором $(\mathbf{z}|b) \in U_{m+1}$. Предположим противное. Если $(\mathbf{z}|0) \notin U_{m+1}$, то при некотором $l' \geqslant m+1$ выполнено $W(\mathbf{z}|0) \cap M_{l'} = \varnothing$, и тогда при любом $l \geqslant l'$, как следует из условия 1, $W(\mathbf{z}|0) \cap M_l = \varnothing$. Аналогично, если $(\mathbf{z}|1) \notin U_{m+1}$, то при некотором $l'' \geqslant m+1$ верно, что для любого $l \geqslant l''$ выполнено $W(\mathbf{z}|1) \cap M_l = \varnothing$. Таким образом, для любого $l \geqslant l''' = \max\{l', l''\}$ верно $\varnothing = (W(\mathbf{z}|0) \cup W(\mathbf{z}|1)) \cap M_l = W(\mathbf{z}) \cap M_l$, что противоречит условию $\mathbf{z} \in U_m$. Из условия 2 и аналогичных рассуждений следует, что множество U_1 непусто.

Пусть $(z_1^*) \in U_1$, $(z_1^*, z_2^*) \in U_2$, $(z_1^*, z_2^*, z_3^*) \in U_3, \ldots$ Нетрудно проверить, что построенная таким образом последовательность $\overline{\mathbf{z}}^* = (z_1^*, z_2^*, \ldots) \in V_\infty$ — искомая. ■

Утверждение 3. Пусть $f \in \mathcal{PB}_n$. Тогда для любых $m \in \mathbb{N}$, $\mathbf{y} \in V_m$, $\overline{\mathbf{z}} \in V_\infty$ выполняются следующие неравенства:

1) $f_\infty^{-1}(\mathbf{y}|\overline{\mathbf{z}}) \neq \varnothing$;
2) $E_{\mathbf{y}}^f \cap A_{\overline{\mathbf{z}}}^f \neq \varnothing$.

Доказательство. Зафиксируем $m \in \mathbb{N}$, $\mathbf{y} \in V_m$, $\overline{\mathbf{z}} \in V_\infty$ и рассмотрим предикат Q, принимающий на наборе $\mathbf{x} \in V_l$ значение T в том и только в том случае, когда либо $l \leqslant n-1$, либо набор $f_{l-n+1}(\mathbf{x})$ равен набору из первых $l-n+1$ символов последовательности $(\mathbf{y}|\overline{\mathbf{z}})$. Нетрудно проверить, что для предиката Q выполняются условия леммы 1 и, следовательно, существует последовательность $\overline{\mathbf{x}} = (x_1, x_2, \ldots) \in {f_\infty}^{-1}(\mathbf{y}|\overline{\mathbf{z}})$. При этом, очевидно, набор $(x_{m+1}, x_{m+2}, \ldots, x_{m+n-1})$ лежит в пересечении множеств $E_{\mathbf{y}}^f$ и $A_{\overline{\mathbf{z}}}^f$. ■

Утверждение 4. Пусть $f \in \mathcal{F}_n$, $\overline{\mathbf{y}} = (y_1, y_2, \ldots) \in V_\infty$. Тогда $A_{\overline{\mathbf{y}}}^f = \bigcap\limits_{i=1}^{\infty} A_{(y_1, y_2, \ldots, y_i)}^f$.

Доказательство. Вложение $A_{\overline{\mathbf{y}}}^f \subseteq \bigcap\limits_{i=1}^{\infty} A_{(y_1, y_2, \ldots, y_i)}^f$ следует из замечания 3.

Чтобы доказать вложение $\bigcap\limits_{i=1}^{\infty} A_{(y_1, y_2, \ldots, y_i)}^f \subseteq A_{\overline{\mathbf{y}}}^f$, рассмотрим произвольный набор $\tilde{\mathbf{x}} \in \bigcap\limits_{i=1}^{\infty} A_{(y_1, y_2, \ldots, y_i)}^f$ и предикат Q, такой, что для произвольного $\mathbf{x} \in V_l$ равенство $Q(\mathbf{x}) = \mathrm{T}$ выполняется тогда и только тогда, когда $f_{R,l,n-1}^{\tilde{\mathbf{x}}}(\mathbf{x}) = (y_1, y_2, \ldots, y_l)$. Применяя лемму 1, приходим к существованию последовательности $\overline{\mathbf{x}} \in {f_{R,\infty,n-1}^{\tilde{\mathbf{x}}}}^{-1}(\overline{\mathbf{y}})$. Таким образом, $\tilde{\mathbf{x}} \in A_{\overline{\mathbf{y}}}^f$, что завершает доказательство утверждения. ■

Лемма 2. Пусть $f \in \mathcal{F}_n$. Функция f имеет правый барьер тогда и только тогда, когда для всякого набора $\mathbf{x} \in V_{n-1}$ и для всякой последовательности $\overline{\mathbf{z}} \in \mathrm{Im}(f^{\mathbf{x}}_{R,\infty,n-1})$ выполнено равенство $|{f^{\mathbf{x}}_{R,\infty,n-1}}^{-1}(\overline{\mathbf{z}})| = 1$.

Доказательство. Необходимость очевидна. Для доказательства достаточности предположим противное: функция f не имеет правого барьера; в таком случае для любого l существуют наборы $(y_1, y_2, \ldots, y_l) \in V_l$, $(x_1, x_2, \ldots, x_{n-1}) \in V_{n-1}$, для которых выполнено

$$\begin{cases} f(x_1, x_2, \ldots, x_{n-1}, 0) = f(x_1, x_2, \ldots, x_{n-1}, 1) = y_1, \\ (x_2, x_2, \ldots, x_{n-1}, 0) \in A^f_{(y_2, y_3, \ldots, y_l)}, \\ (x_2, x_2, \ldots, x_{n-1}, 1) \in A^f_{(y_2, y_3, \ldots, y_l)}. \end{cases} \tag{4}$$

Введем предикат Q, равный T на всех наборах длины меньше n и определенный следующим образом на наборах длины $n{-}1{+}l$, $l = 1, 2\ldots$: $Q(x_1, x_2, \ldots, x_{n-1}, y_1, y_2, \ldots, y_l) =$ $=$ T тогда и только тогда, когда выполнена система (4). Можно проверить, что для определенного таким образом предиката Q выполнены все условия леммы 1 и, значит, существует набор $\mathbf{x} = (x_1, x_2, \ldots, x_{n-1}) \in V_{n-1}$ и последовательность $\overline{\mathbf{y}} = (y_1, y_2, \ldots) \in$ $\in V_\infty$, такие, что для любого l для них выполнена система (4). С учетом утверждения 4 это означает, что $|{f^{\mathbf{x}}_{R,\infty,n-1}}^{-1}(\overline{\mathbf{y}})| \geqslant 2$. Полученное противоречие завершает доказательство достаточности. ■

Следствие 1. Если $f \in \mathcal{F}_n$ не имеет правого барьера, то существует набор $\mathbf{x}^* \in V_{n-1}$ и двоичные последовательности $\overline{\mathbf{x}}', \overline{\mathbf{x}}'', \overline{\mathbf{y}}^* \in V_\infty$, для которых выполняется равенство

$$f_\infty(\mathbf{x}^*|0|\overline{\mathbf{x}}') = f_\infty(\mathbf{x}^*|1|\overline{\mathbf{x}}'') = \overline{\mathbf{y}}^*. \tag{5}$$

Докажем утверждение о необходимом условии обратимости.

Теорема 5. Если $f \in \mathcal{LI}_n$, то f имеет правый барьер.

Доказательство. Предположим противное: пусть некоторая функция f, не имеющая правого барьера, является локально обратимой.

Зафиксируем $m \in \mathbb{N}$ и $\mathbf{y} \in V_m$, такие, что $\mathbf{y} \in T^R_f$; зафиксируем также набор $\mathbf{x}^* \in V_{n-1}$ и двоичные последовательности $\overline{\mathbf{x}}', \overline{\mathbf{x}}'' \in V_\infty$, для которых выполняется условие (5) следствия 1.

Рассмотрим произвольный набор $\mathbf{x} = (x_1, x_2, \ldots, x_{m+n-1})$, лежащий в (непустом по определению) множестве $f^{-1}_m(\mathbf{y})$. Очевидно, что для последовательности $\overline{\mathbf{z}} = f_\infty(x_{m+1},$ $x_{m+2}, \ldots, x_{m+n-1}|\mathbf{x}^*|0|\overline{\mathbf{x}}')$ выполняется вложение $(\mathbf{y}|\overline{\mathbf{z}}) \in \mathrm{Im}(f_\infty)$. При этом также выполняется равенство $f_\infty(\mathbf{x}|\mathbf{x}^*|0|\overline{\mathbf{x}}') = f_\infty(\mathbf{x}|\mathbf{x}^*|1|\overline{\mathbf{x}}'') = (\mathbf{y}|\overline{\mathbf{z}})$, противоречащее, очевидно, принадлежности набора $\mathbf{y}$ множеству T^R_f. Полученное противоречие завершает доказательство теоремы. ■

Следствие 2. Для любого $n \in \mathbb{N}$ выполнено вложение $\mathcal{LI}_n \subseteq \mathcal{PB}_n$.

Учитывая результат теоремы 5, далее при изучении класса локально обратимых функций будем рассматривать только функции с правым барьером. Как следует из утверждения 3, для любой функции f с правым барьером, любого набора $\mathbf{y}$ и любой последовательности $\overline{\mathbf{z}}$ выполняется неравенство $|E^f_{\mathbf{y}} \cap A^f_{\overline{\mathbf{z}}}| \geqslant 1$.

Лемма 3. Пусть $f \in \mathcal{F}_n$ имеет правый барьер. Для всяких $m \in \mathbb{N}$ и $\mathbf{y} \in V_m$ верно, что $\mathbf{y} \in T^R_f$ тогда и только тогда, когда для любой последовательности $\overline{\mathbf{z}} \in V_\infty$ выполняется равенство $|E^f_{\mathbf{y}} \cap A^f_{\overline{\mathbf{z}}}| = 1$.

Доказательство. Необходимость очевидна. Докажем достаточность. Пусть для набора $\mathbf{y} \in V_m$ и любой последовательности $\overline{\mathbf{z}} \in V_\infty$ выполнено $|E^f_{\mathbf{y}} \cap A^f_{\overline{\mathbf{z}}}| = 1$. Зафиксируем $\overline{\mathbf{z}} \in V_\infty$ и тот единственный набор $\mathbf{x}$, который лежит в множестве $E^f_{\mathbf{y}} \cap A^f_{\overline{\mathbf{z}}}$. По лемме 2 выполнено равенство $|{f^{\mathbf{x}}_{R,\infty,n-1}}^{-1}(\overline{\mathbf{z}})| = 1$. Таким образом, $\mathbf{y} \in T^R_f$. ■

Лемма 4. Пусть $f \in \mathcal{F}_n$ имеет правый барьер. Для всякого $m \in \mathbb{N}$ и $\mathbf{y} \in V_m$ верно, что $\mathbf{y} \in T^R_f$ тогда и только тогда, когда существует $M \in \mathbb{N}$, такое, что для любого набора $\mathbf{z} \in V_M$ выполняется равенство $|E^f_{\mathbf{y}} \cap A^f_{\mathbf{z}}| = 1$.

Доказательство. Достаточность очевидным образом следует из леммы 3, так как для всякой последовательности $\overline{\mathbf{z}} = (z_1, z_2, \ldots) \in V_\infty$ выполняется вложение $A^f_{\overline{\mathbf{z}}} \subseteq$ $\subseteq A^f_{(z_1,z_2,\ldots,z_M)}$ и, следовательно, для всякого набора $\mathbf{y}$ выполняется $|E^f_{\mathbf{y}} \cap A^f_{\overline{\mathbf{z}}}| \leqslant$ $\leqslant |E^f_{\mathbf{y}} \cap A^f_{(z_1,z_2,\ldots,z_M)}| = 1$.

Докажем необходимость. Предположим противное: существует набор $\mathbf{y} \in T^R_f$, такой, что для сколь угодно большого M найдется $\mathbf{z} \in V_M$, для которого $|E^f_{\mathbf{y}} \cap A^f_{\mathbf{z}}| \geqslant 2$. Рассмотрим предикат Q, определенный на всех наборах $\mathbf{z}$ конечной длины следующим образом: $Q(\mathbf{z}) = \mathrm{T}$ тогда и только тогда, когда $|E^f_{\mathbf{y}} \cap A^f_{\mathbf{z}}| \geqslant 2$.

Нетрудно убедиться, что для всякого $\mathbf{z}$ выполнено: если $Q(\mathbf{z}) = \mathrm{F}$, то $Q(\mathbf{z}|0) =$ $= Q(\mathbf{z}|1) = \mathrm{F}$. Кроме того, учитывая выбор набора $\mathbf{y}$, для всякого M найдется $\mathbf{z}^* \in V_M$, такой, что $Q(\mathbf{z}^*) = \mathrm{T}$. По лемме 1 из этого следует существование последовательности $\overline{\mathbf{z}} = (z_1, z_2, \ldots)$, такой, что для всякого M выполняется $|E^f_{\mathbf{y}} \cap A^f_{(z_1,z_2,\ldots,z_M)}| \geqslant 2$ и, учитывая замечание 3 и утверждение 4, $|E^f_{\mathbf{y}} \cap A^f_{\overline{\mathbf{z}}}| \geqslant 2$. Как следует из леммы 3, последнее неравенство противоречит $\mathbf{y} \in T^R_f$. ■

Пример 1. Рассмотрим функцию $f(x_1, x_2, x_3, x_4) = x_1x_2x_4 \oplus x_2x_4 \oplus x_3$. Можно проверить, что f имеет правый барьер длины 3. Покажем, что $f \in LI_4$. С учетом леммы 4 достаточно показать, что для $\mathbf{y} = (0,0,0) \in V_3$ и для любого $\mathbf{z} = (z_1) \in V_1$ выполняется $|E^f_{\mathbf{y}} \cap A^f_{\mathbf{z}}| = 1$:

$$E^f_{\mathbf{y}} = \{(0,0,0),(0,0,1)\}; \quad E^f_{\mathbf{y}} \cap A^f_{(0)} = \{(0,0,0)\}; \quad E^f_{\mathbf{y}} \cap A^f_{(1)} = \{(0,0,1)\}.$$

Из утверждения 2 и замечания 3 очевидным образом вытекает следующее утверждение.

Лемма 5. Пусть $f \in \mathcal{F}_n$ имеет правый (левый) барьер. Для любого $l \geqslant b^R_f - 1$ (любого $l \geqslant b^L_f - 1$) и любого набора $(y_1, y_2, \ldots, y_l) \in V_l$ верно равенство $A^f_{(y_1,y_2,\ldots,y_l)} =$ $= A^f_{(y_1,y_2,\ldots,y_{b^R_f-1})}$ (соответственно $E^f_{(y_l,y_{l-1},\ldots,y_1)} = E^f_{(y_{b^L_f-1},y_{b^L_f-2},\ldots,y_1)}$).

С учетом леммы 5 легко получить следующую эквивалентную формулировку леммы 4.

Лемма 6. Пусть $f \in \mathcal{F}_n$ имеет правый барьер. Для всякого $m \in \mathbb{N}$ и $\mathbf{y} \in V_m$ верно, что $\mathbf{y} \in T^R_f$ тогда и только тогда, когда для любого набора $\mathbf{z} \in V_{b^R_f-1}$ выполняется $|E^f_{\mathbf{y}} \cap A^f_{\mathbf{z}}| = 1$.

Лемма 7. Пусть $f \in \mathcal{F}_n$ имеет правый и левый барьер. Тогда $f \in \mathcal{LI}_n$, если и только если множество $T^R_f(b^L_f - 1)$ непусто.

Доказательство. Достаточность очевидна. Для доказательства необходимости заметим, что из лемм 5 и 6 вытекает: для любых $l \in \mathbb{N}$, $\mathbf{y} \in V_{b^L_f-1}$, $\mathbf{y}' \in V_l$ верно, что $(\mathbf{y}'|\mathbf{y}) \in T^R_f$ тогда и только тогда, когда $\mathbf{y} \in T^R_f$. Таким образом, если множество $T^R_f(b^L_f - 1)$ пусто, то и T^R_f пусто. ■

Обозначим $r_f = \min\limits_{m\geqslant 1}\min\limits_{\mathbf{y}\in V_m}|E^f_{\mathbf{y}}|$.

Лемма 8. Пусть $f\in\mathcal{F}_n$ имеет левый барьер. Тогда $r_f = 2^{n-1-e^L_f}$.

Доказательство. Из утверждения 2 следует, что при $m\geqslant b^L_f-1$ для любого $\mathbf{y}\in V_m$ верно равенство $|E^f_{\mathbf{y}}| = 2^{n-1-e^L_f}$, и поэтому $r_f = \min\{2^{n-1-e^L_f}, \min\limits_{m'\leqslant b^L_f-2}\min\limits_{\mathbf{y}\in V_{m'}}|E^f_{\mathbf{y}}|\}$. С другой стороны, из замечания 3 следует неравенство $\min\limits_{m'\leqslant b^L_f-2}\min\limits_{\mathbf{y}\in V_{m'}}|E^f_{\mathbf{y}}|\geqslant\min\limits_{\mathbf{y}\in V_{b^L_f-1}}|E^f_{\mathbf{y}}|$, откуда $r_f = 2^{n-1-e^L_f}$. ■

Пусть $f\in\mathcal{F}_n$, $m\in\mathbb{N}$, $\mathbf{y}\in V_m$, $\tilde{\mathbf{x}}\in V_{n-1}$. Введем следующее обозначение:

$$\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}}) = \{(x_{m+1},x_{m+2},\ldots,x_{m+n-1})\in V_{n-1}:$$
$$\exists(x_n,x_{n+1},\ldots,x_m)\ \big(f^{\tilde{\mathbf{x}}}_{R,m,n-1}(x_n,x_{n+1},\ldots,x_{m+n-1}) = \mathbf{y}\big)\}.$$

Лемма 9. Пусть $f\in\mathcal{F}_n$ имеет правый барьер. Тогда для любых $m\geqslant b^R_f-1$, $\mathbf{y}\in V_m$ и $\tilde{\mathbf{x}}\in A^f_{\mathbf{y}}$ выполняется равенство $|\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})| = 2^{e^R_f}$.

Доказательство. Зафиксируем произвольным образом $m\geqslant b^R_f-1$, $\mathbf{y}\in V_m$ и $\tilde{\mathbf{x}}\in A^f_{\mathbf{y}}$. По теореме 3 верно равенство $|{f^{\tilde{\mathbf{x}}}_{R,l,n-1}}^{-1}(\mathbf{y})| = 2^{e^R_f}$ и поэтому, очевидно, $|\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})|\leqslant 2^{e^R_f}$. С другой стороны, как следует из теоремы 1, любой набор множества ${f^{\tilde{\mathbf{x}}}_{R,l,n-1}}^{-1}(\mathbf{y})$ определяется последними $n-1$ символами однозначно, поэтому $|\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})| = 2^{e^R_f}$. ■

Лемма 10. Пусть $f\in\mathcal{F}_n$ имеет правый барьер. Тогда $r_f\geqslant 2^{e^R_f}$.

Доказательство. Пусть для набора $\mathbf{y}\in V_m$ выполнено $|E^f_{\mathbf{y}}| = r_f$. Учитывая замечание 3, можно считать, что $m\geqslant b^R_f-1$.

Зафиксируем произвольный набор $\tilde{\mathbf{x}}\in A^f_{\mathbf{y}}$. Как следует из леммы 9, множество $\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})$ имеет мощность $2^{e^R_f}$. Ввиду вложения $\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})\subseteq E^f_{\mathbf{y}}$ приходим к требуемому неравенству. ■

Из лемм 8 и 10 вытекает следующее утверждение.

Следствие 3. Пусть $f\in\mathcal{F}_n$ имеет правый и левый барьер. Тогда $e^R_f+e^L_f\leqslant n-1$.

Теорема 6. Пусть $f\in\mathcal{F}_n$ имеет правый барьер. Тогда если $r_f = 2^{e^R_f}$, то $f\in\mathcal{LI}_n$, причем любой набор $\mathbf{y}$, такой, что $|E^f_{\mathbf{y}}| = 2^{e^R_f}$, принадлежит множеству T^R_f.

Доказательство. Достаточно показать, что если для некоторого числа $m\in\mathbb{N}$ и набора $\mathbf{y}\in V_m$ выполнено равенство $|E^f_{\mathbf{y}}| = 2^{e^R_f}$, то $\mathbf{y}\in T^R_f$.

Пусть сначала $m\geqslant\max\{b^R_f-1,n\}$. Выберем любой набор $\tilde{\mathbf{x}}\in A^f_{\mathbf{y}}$. Нетрудно видеть, что для такого набора, с одной стороны, выполняется вложение $\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})\subseteq E^f_{\mathbf{y}}$, а с другой стороны, по лемме 9, $|\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})| = 2^{e^R_f}$. Следовательно, $\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}}) = E^f_{\mathbf{y}}$.

С учетом леммы 6 достаточно показать: для любого набора $\mathbf{z}\in V_{b^R_f-1}$ выполняется $|\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})\cap A^f_{\mathbf{z}}| = 1$. Действительно, если предположить, что найдутся $\mathbf{z}\in V_{b^R_f-1}$, $\mathbf{x}',\mathbf{x}''\in\tilde{E}^f_{\mathbf{y}}(\tilde{\mathbf{x}})\cap A^f_{\mathbf{z}}$, $\mathbf{x}'\neq\mathbf{x}''$, то для некоторых $\mathbf{t}',\mathbf{t}''\in V_{m-n+1}$, $\mathbf{s}',\mathbf{s}''\in V_{b^R_f-1}$ разрешима следующая система уравнений:

$$f_{m+b^R_f-1}(\tilde{\mathbf{x}}|\mathbf{t}'|\mathbf{x}'|\mathbf{s}') = f_{m+b^R_f-1}(\tilde{\mathbf{x}}|\mathbf{t}''|\mathbf{x}''|\mathbf{s}'').$$

Разрешимость этой системы противоречит определению правого барьера длины b_f^R.

В случае, если при $m < \max\{b_f^R - 1, n\}$ для некоторого $\mathbf{y} = (y_1, y_2, \ldots, y_m) \in V_m$ выполняется $|E_{\mathbf{y}}^f| = 2^{e_f^R}$ (и тогда $r_f = 2^{e_f^R}$), рассмотрим набор $\mathbf{y}^* = (0, 0, \ldots, 0, y_1, y_2, \ldots, y_m) \in V_{\max\{b_f^R-1,n\}}$. Легко видеть, что тогда $|E_{\mathbf{y}^*}^f| = r_f = |E_{\mathbf{y}}^f|$ и $E_{\mathbf{y}^*}^f = E_{\mathbf{y}}^f$. Как следует из показанного выше, для любого $\mathbf{z} \in V_{b_f^R-1}$ выполнено $|\tilde{E}_{\mathbf{y}^*}^f(\tilde{\mathbf{x}}) \cap A_{\mathbf{z}}^f| = 1$ и, значит, $|E_{\mathbf{y}}^f \cap A_{\mathbf{z}}^f| = 1$. По лемме 6 это означает, что $\mathbf{y} \in T_f^R$. ■

Теорема 7. Пусть $f \in \mathcal{F}_n$ имеет правый и левый барьер. Тогда если $e_f^R + e_f^L = n-1$, то $f \in \mathcal{PLI}_n^R \cap \mathcal{PLI}_n^L$.

Доказательство. Применяя сначала лемму 8 и теорему 6, а затем утверждение 2, получим $\bigcup\limits_{m=b_f^R-1}^{\infty} V_m \subseteq T_f^R$, а это и означает, что $f \in \mathcal{PLI}_n^R$ с $p = b_f^R - 1$.

Применяя аналогичные рассуждения к функции $\overleftrightarrow{f}$, получим, что $f \in \mathcal{PLI}_n^L$ с $p = b_f^L - 1$. ■

Следствие 4. Пусть $f \in \mathcal{F}_n$ имеет правый и левый барьер. Тогда если $e_f^R + e_f^L = n - 1$, то f является локально обратимой (т. е. слабо локально обратимой вправо) и слабо локально обратимой влево.

Теорема 8. Пусть $f \in \mathcal{F}_n$ имеет правый барьер. Тогда если $f \in \mathcal{LI}_n$, то $r_f = 2^{e_f^R}$, причем равенство $|E_{\mathbf{y}}^f| = 2^{e_f^R}$ верно для всех наборов $\mathbf{y} \in T_f^R$.

Доказательство. Пусть для некоторого $m \in \mathbb{N}$ и $\mathbf{y} \in V_m$ верно $\mathbf{y} \in T_f^R$. Из леммы 6 следует, что для любого набора $\mathbf{z} \in V_{b_f^R-1}$ выполняется равенство $|E_{\mathbf{y}}^f \cap A_{\mathbf{z}}^f| = 1$. Пусть $l = m + b_f^R - 1$. Рассмотрим произвольные наборы $\mathbf{x}^* \in E_{\mathbf{y}}^f$ и $\mathbf{z} \in \mathrm{Im}(f_{R,b_f^R-1,n-1}^{\mathbf{x}^*})$. В таком случае $E_{\mathbf{y}}^f \cap A_{\mathbf{z}}^f = \{\mathbf{x}^*\}$ и множество ${f_l}^{-1}(\mathbf{y}|\mathbf{z})$ имеет следующую структуру:

$$
\begin{gathered}
{f_l}^{-1}(\mathbf{y}|\mathbf{z}) = \{(x_1, x_2, \ldots, x_{l+n-1}) \in V_{l+n-1} : (x_{m+1}, x_{m+2}, \ldots, x_{m+n-1}) = \mathbf{x}^*, \\
(x_1, x_2, \ldots, x_m) \in {f_{L,m,n-1}^{\mathbf{x}^*}}^{-1}(\mathbf{y}), (x_{m+n}, x_{m+n+1}, \ldots, x_{l+n-1}) \in {f_{R,b_f^R-1,n-1}^{\mathbf{x}^*}}^{-1}(\mathbf{z})\}.
\end{gathered}
$$

Таким образом, $|{f_l}^{-1}(\mathbf{y}|\mathbf{z})| = 2^{e_f^R} |{f_{L,m,n-1}^{\mathbf{x}^*}}^{-1}(\mathbf{y})|$. С другой стороны, $f \in \mathcal{PB}_n$, поэтому $|{f_l}^{-1}(\mathbf{y}|\mathbf{z})| = 2^{n-1}$ и, следовательно,

$$
|{f_{L,m,n-1}^{\mathbf{x}^*}}^{-1}(\mathbf{y})| = 2^{n-1-e_f^R}. \tag{6}
$$

Так как набор $\mathbf{x}^*$ из множества $E_{\mathbf{y}}^f$ был выбран произвольно, равенство (6) выполняется для любого $\mathbf{x}^* \in E_{\mathbf{y}}^f$. Но в таком случае сумма $\sum\limits_{\mathbf{x}^* \in E_{\mathbf{y}}^f} |{f_{L,m,n-1}^{\mathbf{x}^*}}^{-1}(\mathbf{y})|$, равная, с одной стороны, $|f_m^{-1}(\mathbf{y})| = 2^{n-1}$, равна также $2^{n-1-e_f^R} |E_{\mathbf{y}}^f|$, откуда следует $|E_{\mathbf{y}}^f| = 2^{e_f^R}$ и, с учетом леммы 10, $r_f = 2^{e_f^R}$. ■

Из леммы 8 и теоремы 8 вытекает следующее необходимое условие локальной обратимости функции с правым и левым барьером.

Следствие 5. Пусть $f \in \mathcal{F}_n$ имеет правый и левый барьер. Тогда если $f \in \mathcal{LI}_n$, то $e_f^R + e_f^L = n - 1$.

Следствие 6. Пусть $f \in \mathcal{F}_n$ имеет правый и левый барьер. Тогда если $f \in \mathcal{LI}_n$, то $b_f^R + b_f^L \geqslant n + 1$. Если дополнительно f существенно и нелинейно зависит от первой и последней переменной, то $b_f^R + b_f^L \geqslant n + 3$.

Доказательство. Вытекает из следствия 5, а также теорем 3 и 4. ■

С помощью теорем 5, 6 и 8 легко получить описание множества T_f^R для произвольной функции $f \in \mathcal{F}_n$.

Теорема 9. Для произвольной функции f верно

$$T_f^R = \begin{cases} \varnothing, \text{ если } f \text{ не имеет правого барьера,} \\ \left\{ \mathbf{y} \in \bigcup\limits_{m=1}^{\infty} V_m : \ |E_{\mathbf{y}}^f| = 2^{e_f^R} \right\} \text{ иначе.} \end{cases}$$

Таким образом, получен следующий критерий локальной обратимости.

Следствие 7. Функция $f \in \mathcal{F}_n$ локально обратима тогда и только тогда, когда она имеет правый барьер и $r_f = 2^{e_f^R}$.

Лемма 11. Пусть $f \in \mathcal{F}_n$ не имеет левого (правого) барьера. Тогда $f \notin \mathcal{PLI}_n^R$ (соответственно $f \notin \mathcal{PLI}_n^L$).

Доказательство. Пусть $f \in \mathcal{F}_n$ не имеет левого барьера. Достаточно рассмотреть случай, при котором у f есть правый барьер (иначе $f \notin \mathcal{LI}_n$ и, следовательно, $f \notin \mathcal{PLI}_n^R$).

Так как f не имеет левого барьера, то для любого сколь угодно большого $m \in \mathbb{N}$ существует набор $\mathbf{y} \in V_m$, для которого найдется $\mathbf{z} \in V_{b_f^R-1}$, такой, что в множестве ${f_{m+b_f^R-1}}^{-1}(\mathbf{y}|\mathbf{z})$ есть пара наборов вида $(\mathbf{x}'|0|\tilde{\mathbf{x}}), (\mathbf{x}''|1|\tilde{\mathbf{x}}) \in V_{m+b_f^R+n-2}$, где $\tilde{\mathbf{x}} \in V_{b_f^R-1}$ и $\mathbf{x}', \mathbf{x}'' \in V_{m+n-2}$. Отсюда $|E_{\mathbf{y}}^f \cap A_{\mathbf{z}}^f| \geqslant 2$ и, по лемме 6, $\mathbf{y} \notin T_f^R$.

Таким образом, для всякого $m \in \mathbb{N}$ найдется $\mathbf{y} \notin T_f^R$, поэтому $f \notin \mathcal{PLI}_f^R$.

Аналогично доказывается, что если f не имеет правого барьера, то $f \notin \mathcal{PLI}_f^L$. ■

Теорема 10. Пусть $f \in \mathcal{F}_n$. Тогда следующие утверждения эквивалентны:

1) f обладает правым и левым барьерами и $e_f^R + e_f^L = n - 1$;
2) f обладает левым барьером и является слабо локально обратимой вправо;
3) f обладает правым барьером и является слабо локально обратимой влево;
4) f является слабо обратимой вправо и слабо обратимой влево;
5) $f \in \mathcal{PLI}_n^R$, то есть f является сильно локально обратимой вправо;
6) $f \in \mathcal{PLI}_n^L$, то есть f является сильно локально обратимой влево.

Доказательство. Эквивалентность утверждений 1 и 2, 1 и 3, 1 и 4 вытекает из теоремы 5 и следствий 4 и 5. Кроме того, из теоремы 7 вытекает, что из утверждения 1 следуют утверждения 5 и 6. Чтобы доказать, что из утверждения 5 следует утверждение 1, достаточно сначала применить лемму 11, а затем, учитывая, что $\mathcal{PLI}_n^R \subseteq \mathcal{LI}_n$, теорему 5 и следствие 5. Аналогично доказывается, что из утверждения 6 следует утверждение 1. ■

Таким образом, любая локально обратимая функция является либо функцией с правым барьером и без левого барьера, либо такой функцией с правым и левым барьером, что $e_f^R + e_f^L = n - 1$ (и в таком случае она также является сильно локально обратимой вправо и влево).

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. *Golic J. Dj.* On the Security of Nonlinear Filter Generators // LNCS. 1996. V. 1039. P. 173–188.
3. *Логачев О. А.* О локальной обратимости одного класса булевых отображений // Материалы IX Междунар. семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения акад. О. Б. Лупанова, Москва, 18–23 июня 2007 года. М.: Изд-во механико-математического факультета МГУ, 2007. С. 440–442.
4. *Рысцов И. К.* Возвратные слова для разрешимых автоматов // Кибернетика и системный анализ. 1994. Т. 6. С. 21–26.
5. *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.
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. *Smyshlyaev S. V.* Perfectly Balanced Boolean Functions and Golic Conjecture // J. Cryptology (accepted, available online). DOI 10.1007/s00145-011-9100-7.
8. *Смышляев С. В.* Барьеры совершенно уравновешенных булевых функций // Дискретная математика. 2010. Т. 22. Вып. 2. С. 66–79.
9. *Смышляев С. В.* О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. 2010. № 1(7). С. 5–15.
10. *Смышляев С. В.* Булевы функции без предсказывания // Дискретная математика. 2011. Т. 23. Вып. 1. С. 102–118.
11. *Смышляев С. В.* Построение классов совершенно уравновешенных булевых функций без барьера // Прикладная дискретная математика. 2010. № 3(9). С. 41–50.
12. *Hedlund G. A.* Endomorphisms and automorphisms of the shift dynamical system // Math. Sys. Theory. 1969. No. 3. P. 320–375.