УДК 519.714.3

ОБ ОДНОЙ РЕКУРСИВНОЙ КОНСТРУКЦИИ ПЛАТОВИДНЫХ УСТОЙЧИВЫХ БУЛЕВЫХ ФУНКЦИЙ С ШАГОМ ЧИСЛА ПЕРЕМЕННЫХ 3

Е. В. Хинко

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

Представлена обеспечивающая рост устойчивости рекурсивная конструкция платовидных булевых функций с шагом числа переменных 3, приведён пример начальных функций. В отличие от большинства ранее опубликованных конструкций, порождающие функции имеют пересекающиеся носители спектра.

Ключевые слова: *булевы функции, корреляционная иммунность, устойчивость, платовидность, рекурсивные конструкции.*

DOI 10.17223/20710410/31/9

ON SOME RECURSIVE CONSTRUCTION OF PLATEAUED RESILIENT BOOLEAN FUNCTIONS WITH STEP IN 3 VARIABLES

E. V. Khinko

Lomonosov Moscow State University, Moscow, Russia

E-mail: khinko-eugene@ya.ru

The recursive construction of plateaued Boolean functions with step in 3 variables that provides the growth of resilience is presented. An example of start functions is given. Generating functions have intersecting spectra in contrast to the most constructions built earlier.

Keywords: *Boolean function, correlation immunity, resilience, plateaued functions, recursive constructions.*

Введение

Вопрос корреляционной иммунности и устойчивости булевых функций имеет большое криптографическое значение и регулярно поднимается в работах многих авторов. Например, в [1, 2] затрагивается проблема устойчивости функций при максимальных значениях нелинейности, а в работах [3, 4] построены соответствующие конструкции функций. В [5] Ю. В. Таранниковым построены рекурсивные конструкции устойчивых булевых функций с высокой нелинейностью, где на каждом шаге рекурсии добавляется пара квазилинейных переменных. К относительно схожей теме в [6] также обращался К. В. Захаров, исследовавший рекурсивные конструкции бент-функций (которые можно считать подмножеством платовидных) с шагом числа переменных 2.

В настоящей работе представлена обеспечивающая рост устойчивости рекурсивная конструкция платовидных булевых функций с шагом числа переменных 3 и приведены примеры начальных функций. В большинстве из построенных ранее конструкций порождающие функции обладают непересекающимися носителями спектра. Принципиальное отличие построенной конструкции в том, что рассматривается случай порождающих функций с пересекающимися спектрами.

1. Основные определения и факты

Приведём необходимые определения и основные факты о булевых функциях в соответствии с [5].

Рассмотрим булеву функцию $f : V_n \to F_2$; множество всех таких функций обозначим B_n. Скалярным произведением двух двоичных наборов $a, b \in V_n$ называется сумма по модулю 2 их покомпонентных произведений: $\langle a, b\rangle = \bigoplus\limits_{i=1}^{n} a_i \cdot b_i$. Для каждого двоичного набора $u \in V_n$ определяется коэффициент Уолша

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x)+\langle x,u\rangle}.$$

Вес набора $u \in V_n$ (число единиц в нём) обозначается $\mathrm{wt}(u)$. *Вес функции* $f \in B_n$ (обозначение $\mathrm{wt}(f)$) — количество наборов $u \in V_n$, для которых $f(u) = 1$. Функция $f \in B_n$ называется *уравновешенной*, если $\mathrm{wt}(f) = 2^{n-1}$.

Булева функция $f \in B_n$ называется *платовидной* (с амплитудой 2^c), если $W_f(u) \in \in \{0, \pm 2^c\}$ для всех $u \in V_n$, где $c \in \mathbb{N}$.

Функция $f \in B_n$ называется *корреляционно-иммунной порядка* m, $1 \leqslant m \leqslant n$, если $\mathrm{wt}(f') = \mathrm{wt}(f)/2^m$ для любой подфункции f' от $n - m$ переменных, то есть f и любые её m переменных статистически независимы. Обозначение: $f \in \mathrm{CI}(m)$. Функция f называется *m-устойчивой*, если $f \in \mathrm{CI}(m)$ и f уравновешена. Носитель спектра функции f — множество $\{u \in V_n : W_f(u) \neq 0\}$.

Утверждение 1 (равенство Парсеваля). Для любой булевой функции f от n переменных имеет место равенство

$$\sum_{u \in V_n} W_f^2(u) = 4^n. \tag{1}$$

Равенство Парсеваля доказывается несложными преобразованиями из определения коэффициентов Уолша.

Утверждение 2 (тождество Саркара). Для произвольной функции $f \in B_n$ и любого $w \in V_n$ имеет место равенство

$$\sum_{u \in V_n, u \preccurlyeq w} W_f(u) = 2^n - 2^{\mathrm{wt}(w)+1} \cdot \mathrm{wt}(f_w), \tag{2}$$

где функция f_w получена из f подстановкой 0 вместо x_i для всех i, таких, что $w_i = 1$.

Имеет место спектральная характеризация корреляционно-иммунных функций с помощью коэффициентов Уолша, впервые полученная в [7].

Утверждение 3. Функция $f \in B_n$ является корреляционно-иммунной порядка m, $1 \leqslant m \leqslant n$, если $W_f(u) = 0$ для всех $u \in V_n$, таких, что $1 \leqslant \mathrm{wt}(u) \leqslant m$.

2. Общая постановка задачи

Пусть имеются b, $b \in \mathbb{N}$, платовидных m-устойчивых булевых функций от n переменных $f_n^i(x_1, x_2, \ldots, x_n)$, $i \in \{1, \ldots, b\}$, среди которых, возможно, есть совпадающие с точностью до взятия отрицания; добавим три переменные x_{n+1}, x_{n+2} и x_{n+3}. Новые функции от $n + 3$ переменных обозначим $f_{n+3}^s(x_1, x_2, \ldots, x_n, x_{n+1}, x_{n+2}, x_{n+3})$, $s = 1, \ldots, 8$.

Связь между функциями от n и $n+3$ переменных можно записать в виде совокупности восьми соотношений. Запишем кратко:

$$f^s_{n+3} = \overline{x_{n+1}} \cdot \overline{x_{n+2}} \cdot \overline{x_{n+3}} \cdot g_{s1}(x) + \overline{x_{n+1}} \cdot \overline{x_{n+2}} \cdot x_{n+3} \cdot g_{s2}(x) + \overline{x_{n+1}} \cdot x_{n+2} \cdot \overline{x_{n+3}} \cdot g_{s3}(x) + \\ + \overline{x_{n+1}} \cdot x_{n+2} \cdot x_{n+3} \cdot g_{s4}(x) + x_{n+1} \cdot \overline{x_{n+2}} \cdot \overline{x_{n+3}} \cdot g_{s5}(x) + \\ + x_{n+1} \cdot \overline{x_{n+2}} \cdot x_{n+3} \cdot g_{s6}(x) + + x_{n+1} \cdot x_{n+2} \cdot \overline{x_{n+3}} \cdot g_{s7}(x) + x_{n+1} \cdot x_{n+2} \cdot x_{n+3} \cdot g_{s8}(x), \tag{3}$$

где $g_{sj} = f^i_n$ или $g_{sj} = \overline{f^i_n}$; $s, j \in \{1, \ldots, 8\}; i \in \{1, \ldots, b\}$.

Введём обозначение

$$\sigma_{sj} g_{sj} = \begin{cases} f^i_n, \sigma_{sj} = 1, \\ \overline{f^i_n}, \sigma_{sj} = -1, \end{cases}$$

где $s = 1, \ldots, 8$. Здесь σ_{sj} выполняет роль индикатора: выбирается функция или её отрицание. Представляет интерес подбор таких соотношений индикаторов σ_{sj} и порождающих функций f^i_n, чтобы полученные новые функции от $n+3$ переменных:

а) сохраняли платовидность;

б) обеспечивали рост устойчивости функций;

в) конструкция могла воспроизводиться рекурсивно.

Пусть $a, x \in V_n$. Коэффициент Уолша новой функции выражается через коэффициенты Уолша порождающих функций следующим образом:

$$W_{f^s_{n+3}}(a a_{n+1} a_{n+2} a_{n+3}) =$$

$$= \sum_{x x_{n+1} x_{n+2} x_{n+3} \in V_{n+3}} (-1)^{f^s_{n+3}(x, x_{n+1}, x_{n+2}, x_{n+3}) \oplus \langle x x_{n+1} x_{n+2} x_{n+3}, a a_{n+1} a_{n+2} a_{n+3} \rangle} =$$

$$= W_{g_{s1}}(a) + W_{g_{s2}}(a)(-1)^{a_{n+3}} + W_{g_{s3}}(a)(-1)^{a_{n+2}} + W_{g_{s4}}(a)(-1)^{a_{n+2} \oplus a_{n+3}} + \\ + W_{g_{s5}}(a)(-1)^{a_{n+1}} + W_{g_{s6}}(a)(-1)^{a_{n+1} \oplus a_{n+3}} + \\ + W_{g_{s7}}(a)(-1)^{a_{n+1} \oplus a_{n+2}} + W_{g_{s8}}(a)(-1)^{a_{n+1} \oplus a_{n+2} \oplus a_{n+3}}. \tag{$*$}$$

Таким образом, получаем систему из восьми соотношений. Её можно кратко записать в матричном виде

$$(W_{f^s_{n+3}}(a000), \ldots, W_{f^s_{n+3}}(a111))^{\mathrm{T}} = M_3 \cdot (W_{g_{s1}}(a), W_{g_{s2}}(a), \ldots, W_{g_{s8}}(a))^{\mathrm{T}},$$

где M_3 — матрица Адамара — Сильвестра порядка 8:

$$M_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

Замечание 1. Строки матрицы M_3, а также наборы переменных $x \in V_n$ будем нумеровать в лексикографическом порядке, начиная с 1.

Замечание 2. Будем говорить, что i-й столбец матрицы M_3 соответствует функции g_{si}.

Оценим изменение коэффициентов Уолша:

$$|W_{f^s_{n+3}}(aa_{n+1}a_{n+2}a_{n+3})| \leqslant |W_{g_{s1}}(a)| + |W_{g_{s2}}(a)| + |W_{g_{s3}}(a)| + |W_{g_{s4}}(a)| + \\ + |W_{g_{s5}}(a)| + |W_{g_{s6}}(a)| + |W_{g_{s7}}(a)| + |W_{g_{s8}}(a)|.$$

Берём максимум:

$$\max_{s\in\{1,\dots,8\}} |W_{f^s_{n+3}}(aa_{n+1}a_{n+2}a_{n+3})| \leqslant 8 \max_s |W_{f^s_n}(a)|. \tag{4}$$

3. Конструкция

3.1. Постановка задачи

Соотношения (3), вообще говоря, не обеспечивают ни платовидности, ни устойчивости. Далее приведена конструкция, обеспечивающая оба эти параметра: удалось сформулировать условия, которые обеспечивают самовоспроизводимость конструкции при сохранении платовидности и росте устойчивости функций.

Рассмотрим случай восьми порождающих функций, т. е. $j = 1, \dots, 8$ для f^{ij}_n.

Из равенства Парсеваля (1) легко видеть, что если количество переменных функции увеличивается на 3 (с сохранением платовидности функции) и значения коэффициентов Уолша остаются прежними (2^c) по абсолютной величине, то мощность носителя спектра возрастает в 64 раза; если ненулевые коэффициенты становятся равными $\pm 2^{c+1}$ — в 16 раз. Ввиду (4) получаем противоречие, эти варианты невозможны.

Если ненулевые коэффициенты Уолша новых функций f^s_{n+3} равны $\pm 2^{c+2}$ или $\pm 2^{c+3}$, мощности носителей спектров возрастают в 4 и 1 раз соответственно, т. е. эти варианты возможны.

Таким образом, задача разбивается на два случая в зависимости от значений ненулевых коэффициентов Уолша новых функций f^s_{n+3}. Второй случай (2^{c+3}) относительно тривиален (добавление линейных переменных и т. п.), поэтому рассмотрим первый случай (увеличение мощности носителя спектра и максимума коэффициентов Уолша $W_{f^{ij}_n}$ в 4 раза).

Порождающие функции могут иметь как пересекающиеся, так и непересекающиеся носители спектра. Рассмотрим первый случай: считаем, что существуют наборы $u \in V_n$, по которым пересекаются носители спектра всех или некоторых из порождающих функций. Нам интересен случай, когда порождающих функций f^{ij}_n, $j = 1, \dots, 8$, больше одной.

3.2. Идея конструкции

Идея конструкции заключается в следующем.

Рассмотрим восемь порождающих функций от n переменных, среди которых k, $k \leqslant 8$, различных. Построим k различных функций от $n + 3$ переменых. В нашем случае $k = 4$.

Потребуем от порождающих функций m-устойчивость, платовидность и соблюдение условий (К1)–(К3) (см. ниже). Все эти свойства мы хотим сохранить и у новых функций от большего числа переменных, для того чтобы обеспечить рекурсивность конструкции.

Опишем общую схему конструкции, которая строится с помощью матрицы M_3. Возьмём в качестве набора индикаторов для построения f^s_{n+3} по формуле (3) некоторую строку матрицы M_3 или противоположную ей, т. е. если i-й элемент строки матрицы M_3 равен 1, положим $\sigma_{si} = 1$, а если -1, то $\sigma_{si} = -1$, или наоборот: если

i-й элемент строки матрицы M_3 равен 1, то $\sigma_{si} = -1$, а если -1, то $\sigma_{si} = 1$. Таким образом, с помощью строки матрицы M_3 и восьми функций от n переменных зададим функцию от $n+3$ переменных.

3.3. Описание конструкции

Рассмотрим восемь порождающих функций f_n^{ij}, $j = 1, \ldots, 8$, среди которых четыре пары совпадающих с точностью до взятия отрицания. Другими словами, рассмотрим четыре функции (обозначим их f_n^1, f_n^2, f_n^3, f_n^4), удовлетворяющие следующим условиям:

(К1) каждый двоичный набор $u \in V_n$ содержится в носителе спектра в точности нуля, двух или всех четырёх функций;

(К2) мощности всевозможных попарных пересечений носителей спектров порождающих функций f_n^i, $i = 1, \ldots, 4$, совпадают, а мощность пересечения носителей спектров всех четырёх функций равна четверти мощности носителя спектра каждой функции;

(К3) для каждого набора $u \in V_n$, содержащегося в носителе спектра всех четырёх функций f_n^i, $i = 1, \ldots, 4$, коэффициенты Уолша трёх функций одного знака, а четвёртой — другого знака.

В системе (3) порождающих функций восемь; в конструкции они объединены в четыре пары совпадающих функций следующим образом: функции f_n^{ij} соответствует f_n^1 при $j = 1, 2$; f_n^2 при $j = 3, 4$; f_n^3 при $j = 5, 6$ и f_n^4 при $j = 7, 8$.

Определение 1. Строки индикаторов σ_{sj}, определяющие конструкцию, назовём *базовыми* для данной конструкции и будем нумеровать S^1–S^4.

Зададим функции с помощью строк индикаторов. Базовые строки S^1 и S^2 соответствуют строкам 2 и 6 матрицы M_3, взятым со знаком плюс, а базовые строки S^3 и S^4 — строкам 4 и 8, взятым со знаком минус:

$f_{n+3}^1 : S^1 = (+-+-+-+-)$ (строка 2, знаки элементов),
$f_{n+3}^2 : S^2 = (+-+--+-+)$ (строка 6),
$f_{n+3}^3 : S^3 = (-++--++-)$ (строка 4, умноженная на (-1)),
$f_{n+3}^4 : S^4 = (-++-+--+)$ (строка 8, умноженная на (-1)).

В явном виде эти функции записываются так (здесь $x \in V_n$):

$$
\begin{aligned}
f_{n+3}^1(x, x_{n+1}, x_{n+2}, x_{n+3}) &= f_n^1(x)(x_{n+1}x_{n+2} + x_{n+1} + x_{n+2} + 1) + f_n^2(x)(x_{n+1}x_{n+2} + x_{n+2}) + \\
&\quad + f_n^3(x)(x_{n+1}x_{n+2} + x_{n+1}) + f_n^4(x)x_{n+1}x_{n+2} + x_{n+3};\\
f_{n+3}^2(x, x_{n+1}, x_{n+2}, x_{n+3}) &= f_{n+3}^1(x, x_{n+1}, x_{n+2}, x_{n+3}) + x_{n+1};\\
f_{n+3}^3(x, x_{n+1}, x_{n+2}, x_{n+3}) &= f_{n+3}^1(x, x_{n+1}, x_{n+2}, x_{n+3}) + x_{n+2} + 1;\\
f_{n+3}^4(x, x_{n+1}, x_{n+2}, x_{n+3}) &= f_{n+3}^1(x, x_{n+1}, x_{n+2}, x_{n+3}) + x_{n+1} + x_{n+2} + 1.
\end{aligned}
$$

Заметим, что в записи всех функций присутствует линейная переменная x_{n+3}, что может казаться плохим свойством построенных конструкций с точки зрения криптографии, однако на следующем шаге рекурсии эта переменная уже линейной не будет, так что на каждом шаге линейна только одна новая переменная. После построения функции от достаточно большого числа переменных линейную переменную последнего шага можно отбросить, при этом получится функция уже без линейной переменной, с устойчивостью на 1 меньше, т. е. такой же, как на предыдущем шаге конструкции, и на 1 меньшим числом переменных.

Далее покажем, что заданные таким образом функции f_{n+3}^i, $i = 1, \ldots, 4$, сохраняют свойства (К1)–(К3), которым удовлетворяют порождающие функции f_n^i, $i = 1, \ldots, 4$.

4. Проверка выполнения условий (К1)–(К3)

4.1. Общие замечания

Заметим, что каждые две строки матрицы M_3 отличаются (и совпадают) в четырёх столбцах (свойство матриц Адамара — Сильвестра).

Лемма 1. Если $W_{f^i_{n+3}}(aa_{n+1}a_{n+2}a_{n+3}) \neq 0$, $i = 1, \ldots, 4$, то набор $aa_{n+1}a_{n+2}a_{n+3} \in V_{n+3}$ имеет чётный порядковый номер (т. е. $a_{n+3} = 1$, см. замечание 2).

Доказательство. Докажем, что на наборах с нечётными номерами $W_{f^i_{n+3}}(aa_{n+1}a_{n+2}a_{n+3}) = 0$, $i = 1, \ldots, 4$.

Рассмотрим функцию f^1_{n+3} и преобразование $(*)$ для любого набора $aa_{n+1}a_{n+2}0 \in V_{n+3}$:

$$W_{f^1_{n+3}}(aa_{n+1}a_{n+2}0) = W_{f^1_n}(a) - W_{f^1_n}(a) + W_{f^2_n}(a)(-1)^{a_{n+2}} - W_{f^2_n}(a)(-1)^{a_{n+2}} +$$
$$+W_{f^3_n}(a)(-1)^{a_{n+1}} - W_{f^3_n}(a)(-1)^{a_{n+1}} + W_{f^4_n}(a)(-1)^{a_{n+1}\oplus a_{n+2}} - W_{f^4_n}(a)(-1)^{a_{n+1}\oplus a_{n+2}} = 0.$$

Для остальных функций f^i_{n+3}, $i = 2, 3, 4$, доказательство аналогично. ■

4.2. Преобразование коэффициентов Уолша на наборах, содержащихся в носителях спектров всех четырёх порождающих функций

Рассмотрим набор $x \in V_n$, содержащийся в носителях спектров всех четырёх функций f^i_n, $i = 1, \ldots, 4$, и те восемь наборов $xx_{n+1}x_{n+2}x_{n+3} \in V_{n+3}$, которые ему соответствуют: двоичному набору от n переменных с номером k соответствуют восемь наборов с номерами от $8(k-1)+1$ до $8(k-1)+8$ от $n+3$ переменных.

Определение 2. Набор $xx_{n+1}x_{n+2}x_{n+3} \in V_{n+3}$ с номером $8(k-1)+j$ называется *родным* для функции f^i_{n+3}, $i \in \{1, \ldots, 4\}$, если эта функция задана с помощью j-й строки матрицы M_3.

Заметим, что из построения функций следует чётность числа j.

Например, строка со знаками $+ - + - + - + -$, которой задаётся f^1_{n+3}, — вторая в матрице M_3, поэтому для f^1_{n+3} родными являются наборы с номерами $8(k-1)+2$; для f^2_{n+3} — наборы с номерами $8(k-1)+6$, $k = 1, 2, \ldots, 2^n$, и т. д.

Оставшиеся наборы $xx_{n+1}x_{n+2}1 \in V_{n+3}$ (с чётными номерами) назовём для определённости *неродными* для каждой функции.

Лемма 2 (о преобразовании коэффициентов Уолша на родных наборах). На каждом родном для функции f^i_{n+3} наборе $aa_{n+1}a_{n+2}a_{n+3} \in V_{n+3}$:

а) если коэффициенты Уолша каких-то трёх из четырёх порождающих функций положительны на наборе a, то коэффициент Уолша функции f^i_{n+3} положительный при $i = 1, 2$ и отрицательный при $i = 3, 4$;

б) если коэффициенты Уолша каких-то трёх из четырёх порождающих функций отрицательны на наборе a, то коэффициент Уолша функции f^i_{n+3} отрицательный при $i = 1, 2$ и положительный при $i = 3, 4$.

Доказательство. Докажем п. а, т. е. случай, когда на наборе $a \in V_n$ коэффициент Уолша у трёх порождающих функций положительный и у одной — отрицательный.

Рассмотрим функцию f^1_{n+3} и преобразование $(*)$ для соответствующего родного набора $a001$. Запишем $(*)$, считая, что $W_{f^1_n}(a) = W_{f^2_n}(a) = W_{f^3_n}(a) = -W_{f^4_n}(a) > 0$:

$$W_{f^1_{n+3}}(a001) = W_{f^1_n}(a) - W_{f^1_n}(a)(-1)^1 + W_{f^2_n}(a)(-1)^0 - W_{f^2_n}(a)(-1)^{0\oplus 1} +$$
$$+W_{f^3_n}(a)(-1)^0 - W_{f^3_n}(a)(-1)^{0\oplus 1} + W_{f^4_n}(a)(-1)^{0\oplus 0} - W_{f^4_n}(a)(-1)^{0\oplus 0\oplus 1} = 4W_{f^1_n}(a).$$

Для остальных родных наборов, функций f^i_{n+3} и п. б доказательство аналогично. ■

Лемма 3 (о преобразовании коэффициентов Уолша на неродных наборах).

Соотношение положительных и отрицательных коэффициентов Уолша новых функций f^i_{n+3}, $i = 1, \ldots, 4$, на неродных для каждой функции наборах с чётными номерами, соответствующих $a \in V_n$, таково:

1) для f^1_{n+3} и f^2_{n+3} при соотношении коэффициентов Уолша порождающих функций на наборе $a \in V_n$ «три положительных — один отрицательный» и для f^3_{n+3} и f^4_{n+3} при соотношении «один положительный — три отрицательных»:

— если $W_{f^2_n}(a)$, $W_{f^3_n}(a)$ или $W_{f^4_n}(a)$ отрицательный (положительный), то на неродных наборах от $n+3$ переменных два положительных и один отрицательный коэффициент Уолша, а если $W_{f^1_n}(a) < 0$ (> 0) — три отрицательных;

2) для f^3_{n+3} и f^4_{n+3} при соотношении коэффициентов Уолша порождающих функций на наборе $a \in V_n$ «три положительных — один отрицательный» и для f^1_{n+3} и f^2_{n+3} при соотношении «один положительный — три отрицательных»:

— если $W_{f^2_n}(a)$, $W_{f^3_n}(a)$ или $W_{f^4_n}(a)$ отрицательный (положительный), то на неродных наборах от $n+3$ переменных два отрицательных и один положительный коэффициент Уолша, а если $W_{f^1_n}(a) < 0$ (> 0) — три положительных.

Доказательство. Пусть коэффициент Уолша на наборе $a \in V_n$ у трёх из четырёх порождающих функций положителен, а у одной оставшейся — отрицателен. Если имеет место обратная картина, рассмотрение аналогично. Рассмотрим для определённости f^3_{n+3}, которая порождена строкой индикаторов $(- + + - - + + -)$.

С л у ч а й I. Пусть $W_{f^2_n}(a) < 0$ (случаи $W_{f^3_n}(a) < 0$ и $W_{f^4_n}(a) < 0$ рассматриваются аналогично). Запишем преобразование $(*)$ для неродных наборов:

$$W_{f^3_{n+3}}(a001) = -W_{f^1_n}(a) + W_{f^1_n}(a)(-1)^1 + W_{f^2_n}(a)(-1)^0 - W_{f^2_n}(a)(-1)^{0\oplus 1} -$$
$$-W_{f^3_n}(a)(-1)^0 + W_{f^3_n}(a)(-1)^{0\oplus 1} + W_{f^4_n}(a)(-1)^{0\oplus 0} - W_{f^4_n}(a)(-1)^{0\oplus 0\oplus 1} = -4W_{f^1_n}(a);$$
$$W_f(a101) = -W_{f^1_n}(a) + W_{f^1_n}(a)(-1)^1 + W_{f^2_n}(a)(-1)^0 - W_{f^2_n}(a)(-1)^{0\oplus 1} -$$
$$-W_{f^3_n}(a)(-1)^1 + W_{f^3_n}(a)(-1)^{1\oplus 1} + W_{f^4_n}(a)(-1)^{1\oplus 0} - W_{f^4_n}(a)(-1)^{1\oplus 0\oplus 1} = -4W_{f^1_n}(a);$$
$$W_f(a111) = -W_{f^1_n}(a) + W_{f^1_n}(a)(-1)^1 + W_{f^2_n}(a)(-1)^1 - W_{f^2_n}(a)(-1)^{1\oplus 1} -$$
$$-W_{f^3_n}(a)(-1)^1 + W_{f^3_n}(a)(-1)^{1\oplus 1} + W_{f^4_n}(a)(-1)^{1\oplus 1} - W_{f^4_n}(a)(-1)^{1\oplus 1\oplus 1} = 4W_{f^1_n}(a).$$

С л у ч а й II, когда $W_{f^1_n}(a) < 0$, рассматривается аналогично; то же — для остальных порождающих функций. ■

Из лемм 1–3 вытекает следующая

Теорема 1. Если условие (К3) выполнено для порождающих функций f^i_n, то оно выполнено и для функций f^i_{n+3}, $i = 1, \ldots, 4$.

Обозначим $p_{n,c}$ $(m_{n,c})$ количество положительных (отрицательных) коэффициентов Уолша платовидной функции от n переменных с амплитудой 2^c. Из тождества Саркара легко можно вывести следующее утверждение о соотношении положительных и отрицательных коэффициентов Уолша платовидной функции.

Утверждение 4. Спектр каждой функции f^i_n, $i = 1, \ldots, 4$, состоит из $2^{2n-2c-1} + 2^{n-c}$ коэффициентов Уолша одного знака и $2^{2n-2c-1} - 2^{n-c}$ коэффициентов другого знака.

Доказательство. Возьмём в качестве вектора w в тождестве Саркара (2) набор из единиц (1,1,...,1):

$$\sum_{u\in V_n} W_{f_n^i}(u) = 2^n - 2^{n+1}\mathrm{wt}(f_w) = 2^n - 2^{n+1}f(0,\dots,0) = \pm 2^n,$$

то есть $2^c(p_{n,c} - m_{n,c}) = \pm 2^n$. Из равенства Парсеваля (1) имеем $2^{2c}(p_{n,c} + m_{n,c}) = 4^n$.

Отсюда получаем $p_{n,c} = 2^{2n-2c-1} \pm 2^{n-c-1}$, $m_{n,c} = 2^{2n-2c-1} \mp 2^{n-c-1}$. ■

Следствие 1. Соотношение положительных и отрицательных коэффициентов Уолша у новых функций f_{n+3}^i, $i = 1,\dots,4$, следующее:

$$p_{n+3,c+2} = 2^{2(n+3)-2(c+2)-1} \pm 2^{n+3-c-2-1} = 2^{2n-2c+1} \pm 2^{n-c},$$
$$m_{n+3,c+2} = 2^{2(n+3)-2(c+2)-1} \mp 2^{n+3-c-2-1} = 2^{2n-2c+1} \mp 2^{n-c},$$

т. е. первое слагаемое растёт в 4 раза, а второе только в 2.

4.3. Преобразование коэффициентов Уолша на наборах, содержащихся в носителях спектров ровно двух из четырёх порождающих функций

Пересечение носителей спектров всех четырёх порождающих функций f_n^i, $i = 1,\dots,4$, обозначим U_n. Назовём подмножество столбцов матрицы M_3 *участком*.

Лемма 4. Для каждого набора $a \in V_n \setminus U_n$, такого, что $\sum\limits_{i=1}^{4} |W_{f_n^i}(a)| \neq 0$, выполняется $|\{W_{f_{n+3}^i}(ax_{n+1}x_{n+2}x_{n+3}) : W_{f_{n+3}^i}(ax_{n+1}x_{n+2}x_{n+3}) \neq 0\}| \in \{0,2\}$.

Доказательство. Рассмотрим набор $a \in V_n \setminus U_n$, такой, что $\sum\limits_{i=1}^{4} |W_{f_n^i}(a)| \neq 0$, т. е. набор, на котором коэффициенты Уолша ровно двух из четырёх порождающих функций f_n^i, $i = 1,\dots,4$, не равны нулю. Рассмотрим участок Y строк матрицы M_3, состоящий из тех и только тех компонент, соответствующих функциям f_n^i, для которых $W_{f_n^i}(a) \neq 0$. Из свойств матриц Адамара следует, что строка X матрицы M_3 с чётным номером полностью совпадает (различается) на Y с одной из других строк с чётным номером и совпадает (различается) с двумя другими строками ровно в двух позициях из четырёх. Поэтому в точности две из четырёх базовых строк конструкции S^1–S^4 имеют четыре либо ноль совпадений со строкой X на участке Y; значит, в точности две из четырёх функций f_{n+3}^i, $i = 1,\dots,4$, на наборе $ax_{n+1}x_{n+2}x_{n+3}$ имеют ненулевой коэффициент Уолша. ■

Возможны два случая соотношений ненулевых коэффициентов Уолша порождающих функций.

С л у ч а й I. Оба ненулевых коэффициента Уолша $W_{f_n^i}(a)$, $a \in V_n$, одного знака (например, +).

а) Рассмотрим подслучай, когда строки матрицы M_3 с чётными номерами на участках, соответствующих функциям с ненулевыми на данном наборе $a \in V_n$ коэффициентами Уолша, разбиваются на две пары совпадающих, то есть на некотором наборе $a \in V_n$ выполняется $W_{f_n^{i_j}}(a) \neq 0$, $i_j \in \{1,\dots,8\}$, $j \in \{1,\dots,4\}$, и именно в этих четырёх столбцах i_1, i_2, i_3, i_4 чётные строки матрицы M_3 попарно совпадают. Значит, для каждой новой функции f_{n+3}^i, $i = 1,\dots,4$, на родном для функции наборе $aa_{n+1}a_{n+2}a_{n+3} \in V_{n+3}$ и на парном ему два коэффициента Уолша $W_{f_{n+3}^i}$ одного знака: если базовая строка S^i совпадает со строкой матрицы M_3 (f_{n+3}^1 и f_{n+3}^2), то знак

коэффициентов Уолша сохранится, если нет (f^3_{n+3} и f^4_{n+3}) — изменится на противоположный.

Пример 1. Пусть на наборе a с номером k коэффициенты Уолша $W_{f^1_n}(a) = W_{f^2_n}(a) = 8$, $W_{f^3_n}(a) = W_{f^4_n}(a) = 0$. Пары суть участки базовых строк, соответствующие строкам 2 и 6 матрицы M_3 (общий участок $+-+-$) и строкам 4 и 8 (общий участок $+--+$), столбцы с 1 по 4. У f^1_{n+3} и f^2_{n+3} на наборах с номерами $8(k-1)+2$ и $8(k-1)+6$ положительные коэффициенты и нули на оставшихся шести наборах, а у f^3_{n+3} и f^4_{n+3} на наборах с номерами $8(k-1)+4$ и $8(k-1)+8$ отрицательные коэффициенты и нули на оставшихся шести наборах.

б) Рассмотрим подслучай, когда строки матрицы M_3 с чётными номерами на участках, соответствующих функциям с ненулевыми на наборе $a \in V_n$ коэффициентами, разбиваются на две пары полностью различающихся. Значит, для каждой новой функции f^i_{n+3}, $i = 1, \ldots, 4$, на родном для функции наборе $aa_{n+1}a_{n+2}a_{n+3} \in V_{n+3}$ и парном ему коэффициенты Уолша $W_{f^i_{n+3}}$ разных знаков, причём положительный на родном наборе, соответствующем S^1 и S^2 (f^1_{n+3} и f^2_{n+3}), и отрицательный на родном наборе для S^3 и S^4 (f^3_{n+3} и f^4_{n+3}).

Пример 2. Пусть на наборе a с номером k имеет место $W_{f^1_n}(a) = W_{f^4_n}(a) = 0$, $W_{f^2_n}(a) = W_{f^3_n}(a) = 8$. Пары суть участки базовых строк, соответствующие строкам 2 и 8 матрицы M_3 (участок $+-+-$ для 2 и $-+-+$ для 8) и строкам 6 и 4 (участок $+--+$ для 6 и $-++-$ для 4), столбцы с 3 по 6. У f^1_{n+3} и f^4_{n+3} положительные коэффициенты на наборе с номером $8(k-1)+2$, отрицательные на наборе с номером $8(k-1)+8$ и нули на оставшихся шести наборах, а у f^2_{n+3} и f^3_{n+3} положительные коэффициенты на наборе с номером $8(k-1)+6$, отрицательные на наборе с номером $8(k-1)+4$ и нули на оставшихся шести наборах.

С л у ч а й II. Ненулевые коэффициенты Уолша $W_{f^i_n}(a)$, $a \in V_n$, разных знаков.

а) Рассмотрим подслучай, когда строки матрицы M_3 с чётными номерами на участках, соответствующих функциям с ненулевыми на данном наборе $a \in V_n$ коэффициентами (это автоматически означает, что $W_{f^1_n}(a) \neq 0$) разбиваются на пары совпадающих.

Если $W_{f^1_n}(a) > 0$, то у f^1_{n+3} и f^2_{n+3} положительные коэффициенты на наборах, в паре с которыми нет родного для данной функции, у f^3_{n+3} и f^4_{n+3} отрицательные коэффициенты также на наборах, соответствующих паре, содержащей только неродные для данной функции наборы.

Пример 3. Пусть на наборе $a \in V_n$ с номером k имеет место $W_{f^1_n}(a) = 8$, $W_{f^2_n}(a) = -8$, $W_{f^3_n}(a) = W_{f^4_n}(a) = 0$. Строки 2 и 6 и строки 4 и 8 в левой половине матрицы M_3, соответствующей f^1_n и f^2_n, попарно совпадают. Тогда у f^1_{n+3} и f^2_{n+3} положительные коэффициенты на наборах с номерами $8(k-1)+4$ и $8(k-1)+8$, у f^3_{n+3} и f^4_{n+3} отрицательные коэффициенты на наборах с номерами $8(k-1)+2$ и $8(k-1)+6$.

Если $W_{f^1_n} < 0$, то у f^1_{n+3} и f^2_{n+3} отрицательные коэффициенты на наборах, в паре с которыми нет родного для данной функции, у f^3_{n+3} и f^4_{n+3} отрицательные коэффициенты также на наборах, соответствующих паре, содержащей только неродные для данной функции наборы.

Пример 4. Пусть на наборе a с номером k имеет место $W_{f^1_n}(a) = -8$, $W_{f^4_n}(a) = 8$, $W_{f^2_n}(a) = W_{f^3_n}(a) = 0$. Строки 2 и 8 и строки 6 и 4 в части, отвечающей f^1_n и f^4_n, попарно совпадают. Тогда у f^1_{n+3} отрицательные коэффициенты на наборах с номерами $8(k-1)+4$ и $8(k-1)+6$, у f^2_{n+3} — на наборах с номерами $8(k-1)+2$ и $8(k-1)+8$; у f^4_{n+3} положительные коэффициенты на наборах с номерами $8(k-1)+4$ и $8(k-1)+6$, у f^3_{n+3} — на наборах с номерами $8(k-1)+2$ и $8(k-1)+8$.

Значит, для каждой новой функции f^i_{n+3}, $i = 1, \ldots, 4$, на родном и парном ему наборах два коэффициента Уолша одного знака, если базовая строка совпадает со строкой матрицы M_3 (f^1_{n+3} и f^2_{n+3}), и разных знаков, если не совпадает (f^3_{n+3} и f^4_{n+3}). При этом во втором случае отрицательный коэффициент Уолша будет на родном наборе.

б) Рассмотрим последний подслучай, когда строки матрицы M_3 с чётными номерами на участках, соответствующих функциям с ненулевыми на данном наборе $a \in V_n$ коэффициентами Уолша, разбиваются на две пары полностью различающихся (это автоматически значит, что $W_{f^1_n}(a) = 0$). Тогда ненулевые коэффициенты у функции, которой соответствует строка индикаторов σ_{si} из одной пары, суть на наборах, которым соответствуют строки другой пары, причём коэффициенты имеют разные знаки как у самой функции, так и у функции, которой соответствует другая строка пары.

Пример 5. Пусть на наборе a с номером k имеет место $W_{f^3_n}(a) = -8$, $W_{f^4_n}(a) = 8$, $W_{f^1_n}(a) = W_{f^2_n}(a) = 0$. Строки 2 и 6 и строки 4 и 8 в части, отвечающей третьей и четвёртой порождающим, попарно различаются. Тогда у f^1_{n+3} отрицательный коэффициент на наборе с номером $8(k-1)+4$ и положительный на наборе с номером $8(k-1)+8$; у f^2_{n+3} отрицательный на наборе с номером $8(k-1)+8$ и положительный на наборе с номером $8(k-1)+4$; у f^3_{n+3} отрицательный коэффициент на наборе с номером $8(k-1)+6$ и положительный на наборе с номером $8(k-1)+2$ и у f^4_{n+3} отрицательный коэффициент на наборе с номером $8(k-1)+2$ и положительный на наборе с номером $8(k-1)+6$.

Из вышеизложенного очевидно следует выполнение для новых функций f^i_{n+3}, $i = 1, \ldots, 4$, условия (К1) и первой части (К2). Остаётся вторая часть условия (К2). Проверяем его выполнение.

Как уже говорилось, из равенства Парсеваля (1) следует, что мощность носителя спектра каждой новой функции f^i_{n+3}, $i = 1, \ldots, 4$, в 4 раза больше мощности носителя спектра каждой из порождающих функций. У исходного множества функций f^i_n, $i = 1, \ldots, 4$, мощность пересечения U_n носителей спектров всех четырёх функций равна четверти мощности носителя спектра каждой из порождающих функций. Если $W_{f^i_n}(u) \neq 0$, $i = 1, \ldots, 4$, $u \in U_n$, то, как следует из теоремы 1, $W_{f^i_{n+3}}(u001)W_{f^i_{n+3}}(u011)W_{f^i_{n+3}}(u101)W_{f^i_{n+3}}(u111) \neq 0$, $i = 1, \ldots, 4$, т. е. $\{u001, u011, u101, u111\} \subseteq U_{n+3}$. Осталось проверить, что никакие другие наборы от $n+3$ переменных в U_{n+3} не попали. А этот факт напрямую следует из леммы 4.

Замечание 3. Конструкция обеспечивает рост устойчивости на 1 при добавлении трёх переменных: по лемме 1 на наборах вида $8(k-1)+1$ коэффициенты Уолша новых функций всегда нулевые. Таким образом, минимальный вес наборов в носителе спектра для f^s_{n+3}, $s = 1, \ldots, 4$, увеличится как минимум на один. Из спектральной характеризации (утверждение 3) следует, что корреляционная иммунность функций за один шаг рекурсии вырастет как минимум на один.

Из теоремы 1, леммы 4 и изложенного выше следует следующая

Теорема 2. Заданная с помощью базовых строк S^1–S^4 конструкция с шагом числа переменых 3 платовидных m-устойчивых булевых функций при выполнении начальных условий (К1)–(К3):

1) рекурсивна, т. е. сохраняет начальные условия, что позволяет применять её многократно;

2) обеспечивает рост устойчивости функций на 1.

Пример 6. Зададим функции f_n^i, $i = 1, \ldots, 4$, от $n = 3$ переменных их коэффициентами Уолша:

$$\begin{array}{llll} (0 & 4\ 4 & 0\ 4 & 0\ 0\ -4) & (f_3^1 = x_1x_2 + x_1x_3 + x_2x_3);\\ (0 & 4\ 0 & -4\ 4 & 0\ 4\ 0) & (f_3^2 = x_1x_3 + x_2x_3 + x_1);\\ (0 & 4\ 4 & 0\ 0 & -4\ 4\ 0) & (f_3^3 = x_1x_2 + x_1x_3 + x_2);\\ (0 & -4\ 0 & 4\ 0 & 4\ 0\ 4) & (f_3^4 = x_1x_2 + x_1 + x_2 + x_3). \end{array}$$

Заметим, что начальные функции платовидны, 0-устойчивы и удовлетворяют свойствам (K1)–(K3). Применение изложенной конструкции даёт следующие четыре функции от шести переменных:

$$\begin{aligned} f_6^1 &= (x_1x_2 + x_1x_3)(x_4x_6 + x_4 + x_6 + 1) + (x_2x_6 + x_2x_3)(x_4 + 1) + \\ &\quad + x_5(x_1x_2 + x_2x_4 + x_3x_4 + x_1) + x_6;\\ f_6^2 &= (x_1x_2 + x_1x_3)(x_4x_6 + x_4 + x_6 + 1) + (x_2x_6 + x_2x_3)(x_4 + 1) + \\ &\quad + x_5(x_1x_2 + x_2x_4 + x_3x_4 + x_1) + x_4 + x_6;\\ f_6^3 &= (x_1x_2 + x_1x_3)(x_4x_6 + x_4 + x_6 + 1) + (x_2x_6 + x_2x_3)(x_4 + 1) + \\ &\quad + x_5(x_1x_2 + x_2x_4 + x_3x_4 + x_1) + x_6 + 1;\\ f_6^4 &= (x_1x_2 + x_1x_3)(x_4x_6 + x_4 + x_6 + 1) + (x_2x_6 + x_2x_3)(x_4 + 1) + \\ &\quad + x_5(x_1x_2 + x_2x_4 + x_3x_4 + x_1) + x_4 + x_6. \end{aligned}$$

Из теоремы 2 следует, что новые функции платовидны, 1-устойчивы и удовлетворяют свойствам (K1)–(K3).

ЛИТЕРАТУРА

1. *Fedorova M. and Tarannikov Yu.* On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Indocrypt'2001. LNCS. 2001. V. 2247. P. 254–266.
2. *Tarannikov Yu.* On resilient Boolean functions with maximal possible nonlinearity // Indocrypt'2000. LNCS. 2000. V. 1977. P. 19–30.
3. *Pasalic E., Maitra S., Johansson T., and Sarkar P.* New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // Electronic Notes in Discr. Math. 2001. V. 6. P. 158–167.
4. *Tarannikov Yu.* New constructions of resilient boolean functions with maximal nonlinearity // FSE'2001. LNCS. 2002. V. 2355. P. 66–77.
5. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. 2002. Вып. 11. С. 91–148.
6. *Захаров К. В.* О порождении бент-функций рекурсивными конструкциями. Дипломная работа. М.: МГУ, 2008.
7. *Guo-Zhen X. and Massey J.* A spectral characterization of correlation-immune combining functions // IEEE Trans. Inform. Theory. 1998. V. 34. No. 3. P. 569–571.

REFERENCES

1. *Fedorova M. and Tarannikov Yu.* On the constructing of highly nonlinear resilient Boolean functions by means of special matrices. Indocrypt'2001, LNCS, 2001, vol. 2247, pp. 254–266.
2. *Tarannikov Yu.* On resilient Boolean functions with maximal possible nonlinearity. Indocrypt'2000, LNCS, 2000, vol. 1977, pp. 19–30.
3. *Pasalic E., Maitra S., Johansson T., and Sarkar P.* New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity. Electronic Notes in Discr. Math., 2001, vol. 6, pp. 158–167.

4. *Tarannikov Yu.* New constructions of resilient boolean functions with maximal nonlinearity. FSE'2001, LNCS, 2002, vol. 2355, pp. 66–77.
5. *Tarannikov Yu. V.* O korrelyatsionno-immunnykh i ustoychivykh bulevykh funktsiyakh [On correlation immune and resilient Boolean functions]. Matematicheskie voprosy kibernetiki, 2002, iss. 11, pp. 91–148. (in Russian)
6. *Zakharov K. V.* O porozhdenii bent-funktsiy rekursivnymi konstruktsiyami [On the recursive generation of bent functions]. Graduate work, Moscow, MSU, 2008. (in Russian)
7. *Guo-Zhen X. and Massey J.* A spectral characterization of correlation-immune combining functions. IEEE Trans. Inform. Theory, 1998, vol. 34, no. 3, pp. 569–571.