ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.714.5 DOI 10.17223/20710410/71/1

ДВОИЧНЫЕ ПОРОГОВЫЕ ПОДСТАНОВКИ

А. И. Зобов, И. В. Чередник

РТУ МИРЭА, г. Москва, Россия

E-mail: zobowai@gmail.com, icherednick@mail.ru

Продолжается исследование двоичных пороговых подстановок — биективных преобразований множества двоичных векторов, координатные функции которых являются пороговыми. Доказано, что семейство всех двоичных пороговых подстановок множества $\{0,1\}^n$ порождает импримитивную группу, которая действует на множестве 2^{n-1} блоков $\{\mathbf{a},\overline{\mathbf{a}}\}$ подстановочно подобно сплетению $S_2 \wr S_{2^{n-1}}$. Показано, что в классе $\{0,1\}$-матриц лишь подстановочные матрицы реализуют пороговые подстановки. Предложен рекурсивный способ построения класса полноцикловых пороговых подстановок, исследована возможность практического применения таких подстановок.

Ключевые слова: *двоичные пороговые функции, двоичные биективные преобразования, пороговые подстановки.*

BINARY TRESHOLD SUBSTITUTIONS

A. I. Zobov, I. V. Cherednik

RTU MIREA, Moscow, Russia

We continue the study of binary threshold substitutions — bijective transformations of the set of binary vectors whose coordinate functions are threshold functions. It is proven that the set of binary threshold substitutions generates an imprimitive group, which acts on the set of 2^{n-1} blocks $\{\mathbf{a},\overline{\mathbf{a}}\}$ permutationally similar to the wreath product $S_2 \wr S_{2^{n-1}}$. It is shown that, within the class of $\{0,1\}$-matrices, only permutation matrices realize threshold substitutions. A recursive method for constructing a class of full-cycle threshold substitutions is proposed. The possibility of practical applications of such substitutions is investigated.

Keywords: *binary threshold functions, binary bijective transformations, threshold substitutions.*

Введение

Пороговые булевы функции $f\colon \{0,1\}^n \to \{0,1\}$, определяемые линейными неравенствами с действительными коэффициентами

$$f(x_1,\ldots,x_n)=1 \iff a_1x_1+\ldots+a_nx_n \geqslant b,$$

давно являются классическими объектами исследований [1–3], а их практическая привлекательность обуславливается простотой реализации в модели нейросетевых вычислений. В последнее время различные представители научной школы В. Г. Никонова ведут активные исследования [4–10] в области синтеза в базисе пороговых функций таких дискретных отображений, которые допускают эффективную реализацию в модели нейросетевых вычислений и/или на альтернативной элементной базе, а также пригодны к использованию в узлах защиты информации. Однако результаты работ [4–8] по существу позволяют построить лишь штучные примеры новых пороговых подстановок, а в [9, 10] исследуются не стандартные пороговые функции, а задаваемые квадратичными неравенствами. В данной работе предлагается способ построения нового семейства двоичных полноцикловых биективных преобразований, координатные функции которых являются пороговыми.

Всюду далее, если не оговорено иное, мы будем исследовать пороговые двоичные функции в псевдобулевом представлении $f\colon \{\pm1\}^n \to \{\pm1\}$ с естественным сохранением стандартной терминологии (сбалансированность, двойственность и пр.). Такой «центрально-симметричный» подход к представлению пороговых двоичных отображений действительно в ряде случаев удобнее классического булевого представления [3].

Определение 1. Псевдобулева функция $f\colon \{\pm1\}^n \to \{\pm1\}$ называется

— *пороговой*, если существуют $a_1, \ldots, a_n, b \in \mathbb{R}$, для которых выполняется условие

$$f(x_1, \ldots, x_n) = 1 \iff a_1x_1 + \ldots + a_nx_n \geqslant b; \tag{1}$$

— *сбалансированной*, если $|f^{-1}(1)| = |f^{-1}(-1)|$;

— *самодвойственной*, если $f(-\mathbf{x}) = -f(\mathbf{x})$ для каждого $\mathbf{x} = (x_1, \ldots, x_n) \in \{\pm1\}^n$.

Утверждение 1. Пусть $a_1, \ldots, a_n, b \in \mathbb{R}$ и пороговая функция f, определяемая условием (1), является сбалансированной. Тогда пороговая функция f также может быть задана центрально-симметричным условием

$$f(x_1, \ldots, x_n) = 1 \iff a_1x_1 + \ldots + a_nx_n \geqslant 0$$

и при этом множество $\{\pm1\}^n$ не содержит решений уравнения $a_1x_1 + \ldots + a_nx_n = 0$.

Доказательство. Пусть неравенство $a_1x_1 + \ldots + a_nx_n \geqslant 0$ задаёт пороговую функцию g. Тогда, как нетрудно видеть,

$$g^{-1}(-1) = \{\mathbf{b}_1, \ldots, \mathbf{b}_t\}, \quad g^{-1}(1) = \{-\mathbf{b}_1, \ldots, -\mathbf{b}_t\} \cup \{\mathbf{c}_1, \ldots, \mathbf{c}_{2^n-2t}\}, \quad t \leqslant 2^{n-1},$$

где наборы $\mathbf{c}_i = (c_1^{(i)}, \ldots, c_n^{(i)}) \in \{\pm1\}^n$ удовлетворяют условию $a_1c_1^{(i)} + \ldots + a_nc_n^{(i)} = 0$ при всех $i \in \{1, \ldots, 2^n - 2t\}$. Во введённых обозначениях:

— при $b > 0$ выполняется соотношение $\big(\{\mathbf{b}_1, \ldots, \mathbf{b}_t\} \cup \{\mathbf{c}_1, \ldots, \mathbf{c}_{2^n-2t}\}\big) \subset f^{-1}(-1)$;

— при $b \leqslant 0$ имеет место $\big(\{-\mathbf{b}_1, \ldots, -\mathbf{b}_t\} \cup \{\mathbf{c}_1, \ldots, \mathbf{c}_{2^n-2t}\}\big) \subset f^{-1}(1)$.

В обоих случаях из условия сбалансированности $|f^{-1}(-1)| = 2^{n-1} = |f^{-1}(1)|$ необходимо следует, что $t = 2^{n-1}$ и соответственно

$$g^{-1}(-1) = \{\mathbf{b}_1, \ldots, \mathbf{b}_{2^{n-1}}\} = f^{-1}(-1), \quad g^{-1}(1) = \{-\mathbf{b}_1, \ldots, -\mathbf{b}_{2^{n-1}}\} = f^{-1}(1).$$

Утверждение 1 доказано. ■

Итак, согласно утверждению 1, любую сбалансированную пороговую функцию $f\colon \{\pm1\}^n \to \{\pm1\}$ можно задать неравенством $a_1x_1 + \ldots + a_nx_n \geqslant 0$ и при этом множество $\{\pm1\}^n$ не содержит решений уравнения $a_1x_1 + \ldots + a_nx_n = 0$. Значит, произвольную

сбалансированную пороговую функцию f можно записать формулой

$$f(x_1, \ldots, x_n) = \operatorname{sgn}(a_1 x_1 + \ldots + a_n x_n)$$

или кратко в векторной форме записи $f(\mathbf{x}) = \operatorname{sgn}(\mathbf{a}\mathbf{x}^{\downarrow})$, где

$$\operatorname{sgn}(y) = \begin{cases} -1, & y < 0, \\ 0, & y = 0, \\ 1, & y > 0. \end{cases}$$

Следствие 1. Пороговая функция $f\colon \{\pm 1\}^n \to \{\pm 1\}$ является самодвойственной тогда и только тогда, когда она является сбалансированной.

Доказательство. Необходимость очевидна, а достаточность следует из центрально-симметричного определения сбалансированной пороговой функции $f(\mathbf{x})$ в виде $f(\mathbf{x}) = \operatorname{sgn}(\mathbf{a}\mathbf{x}^{\downarrow})$. ■

Замечание 1. Поскольку множество $\mathbb{Q}$ всюду плотно в $\mathbb{R}$, а линейные функции непрерывны, нетрудно понять, что в задании произвольной пороговой функции в виде (1) коэффициенты $a_1, \ldots, a_n, b$ всегда могут быть выбраны рациональными и, более того, целочисленными [3]. Поэтому в некоторых случаях для удобства (как, например, далее в теореме 3) без ограничения общности можно полагать, что неравенства, определяющие пороговые функции, имеют целочисленные коэффициенты.

Центральным объектом исследования данной работы являются биективные преобразования $F(\mathbf{x}) = \big(f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})\big)$ множества $\{\pm 1\}^n$, у которых все координатные функции являются пороговыми:

$$f_i(\mathbf{x}) = 1 \iff \mathbf{a}_i \mathbf{x}^{\downarrow} \geqslant b_i, \quad i \in \{1, \ldots, n\}.$$

Кратко такие преобразования будем называть *пороговыми подстановками*. Практическая значимость пороговых подстановок обуславливается максимальной простотой их реализации в базисе пороговых функций; теоретическая значимость состоит в том, что связанные с данными преобразованиями проблемы по существу являются фундаментальными задачами теории целочисленных линейных неравенств.

Каждая координатная функция пороговой подстановки $F(\mathbf{x}) = \big(f_1(\mathbf{x}), \ldots, f_n(\mathbf{x})\big)$ является сбалансированной и, согласно утверждению 1, может быть задана условием

$$f_i(\mathbf{x}) = 1 \iff \mathbf{a}_i \mathbf{x}^{\downarrow} \geqslant 0,$$

а также кратко в виде $f_i(\mathbf{x}) = \operatorname{sgn}(\mathbf{a}_i \mathbf{x}^{\downarrow})$, $i \in \{1, \ldots, n\}$. Таким образом, для пороговой подстановки $F(\mathbf{x})$ можно использовать краткую функциональную форму записи $F(\mathbf{x}) = \operatorname{sgn}\big(A\mathbf{x}^{\downarrow}\big)$, где $A = \begin{pmatrix} \mathbf{a}_1 \\ \ldots \\ \mathbf{a}_n \end{pmatrix}$ — матрица, которую будем называть *матрицей пороговой подстановки* $F(\mathbf{x})$.

Очевидно, что матрица $A \in \mathbb{R}_{n,n}$ определяет пороговую подстановку $\operatorname{sgn}\big(A\mathbf{x}^{\downarrow}\big)$ в том и только в том случае, когда гиперплоскости $\mathbf{a}_1\mathbf{x}^{\downarrow} = 0$, …, $\mathbf{a}_n\mathbf{x}^{\downarrow} = 0$ разбивают пространство $\mathbb{R}^n$ на 2^n частей, каждая из которых содержит единственный набор из множества $\{\pm 1\}^n$. Отсюда, согласно классическому результату Шлефли, следует, что если матрица $A \in \mathbb{R}_{n,n}$ определяет пороговую подстановку $F(\mathbf{x}) = \operatorname{sgn}\big(A\mathbf{x}^{\downarrow}\big)$, то данная матрица A обязательно является обратимой.

Утверждение 2 (теорема Шлефли). Максимальное число n-мерных открытых многогранных конусов, возникающих при разбиении пространства $\mathbb{R}^n$ гиперплоскостями $\mathbf{a}_1\mathbf{x}^{\downarrow} = 0, \ldots, \mathbf{a}_t\mathbf{x}^{\downarrow} = 0$, равно $2\sum\limits_{i=0}^{n-1}\binom{t-1}{i}$, и этот максимум достигается в том и только в том случае, если гиперплоскости находятся в общем положении.

Доказательство. См., например, в [3]. ■

К сожалению, на данный момент более не известно ничего содержательного относительно свойств матрицы A, определяющей пороговую подстановку $\operatorname{sgn}\left(A\mathbf{x}^{\downarrow}\right)$ [3]. Так, например, неизвестно точное количество пороговых подстановок на множестве $\{\pm 1\}^n$ при произвольном n, и похоже, что даже задача определения «задаёт ли конкретная матрица A пороговую подстановку» является трудной. Поясним последнее утверждение: для того чтобы отображение $\operatorname{sgn}\left(A\mathbf{x}^{\downarrow}\right)$ было биективным, согласно критерию Хаффмана [11], необходимо и достаточно, чтобы для любого подмножества $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ система неравенств

$$\begin{cases} \mathbf{a}_{i_1}\mathbf{x}^{\downarrow} > 0, \\ \ldots \\ \mathbf{a}_{i_k}\mathbf{x}^{\downarrow} > 0 \end{cases}$$

имела ровно 2^{n-k} решений из множества $\{\pm 1\}^n$. Однако уже при $k = 1$ мы имеем известную NP-полную задачу: неравенство

$$a_1x_1 + \ldots + a_nx_n > 0$$

имеет 2^{n-1} решений из $\{\pm 1\}^n$ тогда и только тогда, когда уравнение

$$a_1x_1 + \ldots + a_nx_n = 0$$

не имеет $\{\pm 1\}$-решений или, что то же самое, уравнение

$$|a_1|x_1 + \ldots + |a_n|x_n = 0$$

не имеет $\{\pm 1\}$-решений; последнее условие равносильно тому, что для любого разбиения $\{1, \ldots, n\} = \{s_1, \ldots, s_r\} \sqcup \{s_{r+1}, \ldots, s_n\}$ выполняется неравенство

$$|a_{s_1}| + \ldots + |a_{s_r}| \neq |a_{s_{r+1}}| + \ldots + |a_{s_n}|$$

— известная NP-полная задача о разбиении [12]. При этом стоит отметить, что NP-полной является лишь массовая задача о разбиении, в то время как для некоторых частных случаев данная задача может иметь даже тривиальные решения. Так, например, в случае, когда $a_1, \ldots, a_n \in \mathbb{Z}$ и $a_1 + \ldots + a_n$ — нечётное число, решение задачи вполне очевидно.

Отметим ещё одну насущную практическую проблему, связанную с пороговыми подстановками: будет ли обратная к пороговой подстановке также пороговой и как, в случае положительного ответа, построить матрицу, которая задаёт обратную пороговую подстановку? В настоящий момент относительно данной проблемы не известно ничего содержательного. Однако пример ортогональной матрицы

$$A = \begin{pmatrix} \dfrac{4}{\sqrt{41}} & \dfrac{3}{\sqrt{41}} & \dfrac{4}{\sqrt{41}} \\ \dfrac{11}{\sqrt{11562}} & \dfrac{80}{\sqrt{11562}} & \dfrac{-71}{\sqrt{11562}} \\ \dfrac{-13}{\sqrt{282}} & \dfrac{8}{\sqrt{282}} & \dfrac{7}{\sqrt{282}} \end{pmatrix},$$

которая задаёт пороговую подстановку, при том, что обратная к ней A^{T} вообще не задаёт пороговую подстановку, наводит на мысль, что едва ли обозначенная проблема допускает решение в терминах классической линейной алгебры [5, 6].

В заключение рассмотрим простой, но чрезвычайно полезный класс пороговых подстановок, который в дальнейшем будем неоднократно использовать.

Пример 1. Преобразование множества $\{\pm 1\}^n$, определённое по правилу

$$(x_1, \ldots, x_n) \mapsto (\varepsilon_1 x_{\pi(1)}, \ldots, \varepsilon_n x_{\pi(n)}),$$

где $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$; π — перестановка из симметрической группы S_n, может быть реализовано в качестве пороговой подстановки с матрицей

$$\begin{array}{c} \begin{array}{ccccccc} & \pi(1) & & \pi(n) & & \pi(2) & \end{array} \\ \begin{pmatrix} \ldots & \varepsilon_1 & 0 & \ldots & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & 0 & \varepsilon_2 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \varepsilon_n & 0 & \ldots & 0 \end{pmatrix} \end{array}$$

(матрицы данного вида будем называть $\{\pm 1\}$-подстановочными).

Множество всех таких преобразований образует группу относительно композиции отображений. По аналогии с булевым случаем, данную группу будем называть группой Джевонса и обозначать $\mathfrak{Q}_n$. Напомним, что группа Джевонса совпадает с множеством всех изометрий пространства $\{\pm 1\}^n$ относительно метрики Хэмминга [13]. На текущий момент группа Джевонса $\mathfrak{Q}_n$ — единственная алгебраическая структура, которая обнаружена в множестве всех пороговых подстановок.

1. Строение группы, порождённой пороговыми подстановками

Согласно следствию 1, координатные функции пороговой подстановки являются самодвойственными, а следовательно, произвольная пороговая подстановка реализует самодвойственное преобразование с блоками $[\mathbf{a}] = \{\pm \mathbf{a}\}$, $\mathbf{a} \in \{\pm 1\}^n$. Значит, группа $\mathfrak{G}_n$, порождаемая множеством всех пороговых подстановок, заведомо является импримитивной с системой блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$.

Любая группа подстановок с системой импримитивности $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$, содержится в группе подстановок $\mathfrak{S}_n$, которая подобна сплетению $S_2 \wr S_{2^{n-1}}$ и действует на множестве 2^{n-1} блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$, следующим образом: все 2^{n-1} блоков переставляются свободным образом, а внутри блоков осуществляются независимые биективные преобразования (тождественное или инвертирование). Итак, $\mathfrak{G}_n \subset \mathfrak{S}_n$. Однако на самом деле справедлив следующий результат:

Теорема 1. $\mathfrak{G}_n = \mathfrak{S}_n$.

Доказательство. Включение $\mathfrak{G}_n \subset \mathfrak{S}_n$ отмечено ранее. Для доказательства обратного включения $\mathfrak{S}_n \subset \mathfrak{G}_n$ сделаем предварительно несколько примечаний.

1. Пороговая подстановка с матрицей

$$\begin{pmatrix} n-2 & -1 & \ldots & -1 \\ -1 & n-2 & \ldots & -1 \\ \vdots & & \ddots & \vdots \\ -1 & \ldots & -1 & n-2 \end{pmatrix}$$

определяет транспозицию T_1, которая действует нетождественным образом только внутри класса $[(1,\dots,1)]$:

$$(1,\dots,1) \leftrightarrow (-1,\dots,-1).$$

2. Аналогично, транспозиция, которая переставляет векторы в произвольном блоке $[(\varepsilon_1,\dots,\varepsilon_n)]$, $(\varepsilon_1,\dots,\varepsilon_n) \in \{\pm 1\}^n$, может быть реализована как пороговая подстановка с матрицей

$$\begin{pmatrix} \varepsilon_1 & 0 & \dots & 0 \\ 0 & \varepsilon_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & \varepsilon_n \end{pmatrix} \begin{pmatrix} n-2 & -1 & \dots & -1 \\ -1 & n-2 & \dots & -1 \\ \vdots & & \ddots & \vdots \\ -1 & \dots & -1 & n-2 \end{pmatrix} \begin{pmatrix} \varepsilon_1 & 0 & \dots & 0 \\ 0 & \varepsilon_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & \varepsilon_n \end{pmatrix}$$

(фактически — это сопряжение транспозиции T_1 подстановкой трансляции

$$(x_1,\dots,x_n) \mapsto (\varepsilon_1 x_1,\dots,\varepsilon_n x_n)$$

из группы Джевонса).

3. Пороговая подстановка T_2 с матрицей

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & n-3 & -1 & \dots & -1 \\ 0 & -1 & n-3 & \dots & -1 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & -1 & \dots & -1 & n-3 \end{pmatrix}_{n\times n}$$

действует нетождественным образом исключительно на четырёх элементах:

$$\begin{gathered} (1,1,\dots,1) \leftrightarrow (1,-1,\dots,-1), \\ (-1,-1,\dots,-1) \leftrightarrow (-1,1,\dots,1), \end{gathered}$$

значит, она определяет транспозицию блоков

$$[(1,1,\dots,1)] \;\leftrightarrow\; [(-1,1,\dots,1)].$$

4. Сопрягая транспозицию блоков T_2 подстановкой из группы Джевонса

$$(x_1,x_2,x_3,\dots,x_n) \mapsto (-x_2,x_1,x_3,\dots,x_n),$$

получаем транспозицию блоков

$$[(-1,1,1,\dots,1)] \;\leftrightarrow\; [(-1,-1,1,\dots,1)].$$

Аналогичным образом можно построить пороговые подстановки, реализующие транспозиции блоков

$$\begin{gathered} [(-1,-1,1,\dots,1)] \;\leftrightarrow\; [(-1,-1,-1,\dots,1)], \\ \dots \\ [(-1,\dots,-1,1,1)] \;\leftrightarrow\; [(-1,\dots,-1,-1,1)], \end{gathered}$$

а также все возможные транспозиции блоков, которые имеют представителями соседние векторы.

Итак, согласно примечанию 4, существует набор пороговых подстановок-транспозиций блоков, который обеспечивает «связность» всех возможных блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$, а следовательно, ввиду известной теоремы Пойа, является системой образующих симметрической группы подстановок на множестве блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$. Кроме того, согласно примечанию 2, существуют пороговые подстановки, которые реализуют транспозиции внутри каждого из блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$. Значит, справедливо включение $\mathfrak{S}_n \subset \mathfrak{G}_n$. ■

Из доказательства теоремы 1 нетрудно вывести верхнюю оценку ширины группы $\mathfrak{S}_n$ относительно множества пороговых подстановок.

Следствие 2. Произвольная подстановка из группы $\mathfrak{S}_n$ представляется в виде произведения не более чем $n2^n$ пороговых подстановок.

Доказательство. Приведённая оценка вытекает из следующих очевидных соображений. Для построения произвольной подстановки из $\mathfrak{S}_n$ необходимо построить соответствующую перестановку блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$, а также выполнить не более 2^{n-1} инвертирований в блоках. Построение произвольной перестановки блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$, требует не более $2^{n-1}-1$ транспозиций блоков произвольного вида $([\mathbf{a}], [\mathbf{b}])$, каждую из которых можно вычислить с использованием не более $2n-3$ транспозиций из примечания 4 доказательства теоремы 1. Поясним подробнее: произвольные наборы $\mathbf{a}$, $\mathbf{b}$ всегда можно соединить цепочкой $\mathbf{a} = \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k = \mathbf{b}$ длины $k \leqslant n-1$, в которой подряд идущие наборы являются соседними, а значит, для транспозиции $([\mathbf{a}], [\mathbf{b}])$ справедливо следующее представление в виде произведения транспозиций:

$$([\mathbf{a}], [\mathbf{b}]) = ([\mathbf{a}_1], [\mathbf{a}_2]) \ldots ([\mathbf{a}_{k-2}], [\mathbf{a}_{k-1}])([\mathbf{a}_{k-1}], [\mathbf{a}_k])([\mathbf{a}_{k-1}], [\mathbf{a}_{k-2}]) \ldots ([\mathbf{a}_2], [\mathbf{a}_1]).$$

Итого требуется не более $2^{n-1} + (2^{n-1}-1)(2n-3) \leqslant n2^n$ пороговых подстановок. ■

Геометрическое представление пороговых функций подсказывает, что при $n \geqslant 3$ группа $\mathfrak{S}_n$ обязательно содержит подстановки, которые не являются пороговыми.

Следствие 3. При любом $n \geqslant 3$ класс всех пороговых подстановок множества $\{\pm 1\}^n$ не замкнут относительно операции композиции.

Доказательство. При $n \geqslant 3$ группа $\mathfrak{S}_n$ содержит подстановку g, действие которой удовлетворяет следующим условиям:

$$\begin{array}{ll}
g(1,1,\ldots,1) = (-1,-1,\ldots,-1), & g(-1,-1,\ldots,-1) = (1,1,\ldots,1), \\
g(-1,1,\ldots,1) = (1,-1,1,\ldots,1), & g(1,-1,\ldots,-1) = (-1,1,-1,\ldots,-1), \\
g(1,-1,\ldots,1) = (1,1,-1,\ldots,1), & g(-1,1,\ldots,-1) = (-1,-1,1,\ldots,-1), \\
\multicolumn{2}{c}{\ldots} \\
g(1,1,\ldots,-1,1) = (1,1,\ldots,1,-1), & g(-1,-1,\ldots,1,-1) = (-1,-1,\ldots,-1,1), \\
g(1,1,\ldots,1,-1) = (1,-1,\ldots,-1,-1), & g(-1,-1,\ldots,-1,1) = (-1,1,\ldots,1,1)
\end{array}$$

(на множестве всех остальных блоков допустимо любое взаимно однозначное соответствие). Если предположить, что первая координатная функция подстановки g допускает пороговую реализацию с определяющим неравенством $a_1x_1 + a_2x_2 + \ldots + a_nx_n > 0$, то из условий, определяющих действие g, необходимо вытекает следующее противоречие:

$$\begin{cases} a_1 + a_2 + a_3 + \ldots + a_n < 0, \\ -a_1 + a_2 + a_3 + \ldots + a_n > 0, \\ a_1 - a_2 + a_3 + \ldots + a_n > 0, \\ \ldots \\ a_1 + a_2 + \ldots - a_{n-1} + a_n > 0, \\ a_1 + a_2 + \ldots + a_{n-1} - a_n > 0 \end{cases} \quad \Longrightarrow \quad \begin{cases} a_1 + a_2 + a_3 + \ldots + a_n < 0, \\ (n-2)(a_1 + a_2 + a_3 + \ldots + a_n) > 0. \end{cases}$$

Следствие 3 доказано. ■

В заключение приведём пример, который опровергает наивное предположение, что множество всех пороговых подстановок действует симметрическим образом хотя бы на множестве блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^n$.

Пример 2. Рассмотрим подстановку на множестве блоков $[\mathbf{a}]$, $\mathbf{a} \in \{\pm 1\}^4$:

$$\begin{gathered} [(1,1,1,1)] \mapsto [(1,1,1,1)], \\ [(1,1,-1,-1)] \mapsto [(1,1,1,-1)], \\ [(1,-1,-1,1)] \mapsto [(1,1,-1,1)], \\ [(1,-1,1,-1)] \mapsto [(1,1,-1,-1)], \\ [(-1,1,1,1)] \mapsto [(1,-1,1,1)], \\ [(1,-1,1,1)] \mapsto [(1,-1,1,-1)], \\ [(1,1,-1,1)] \mapsto [(1,-1,-1,1)], \\ [(1,1,1,-1)] \mapsto [(1,-1,-1,-1)]. \end{gathered}$$

Если предположить, что такая подстановка может быть реализована некоторой пороговой подстановкой g, то для действия g возможны 256 вариантов:

$$\begin{gathered} g(1,1,1,1) = \varepsilon_1(1,1,1,1), \\ g(1,1,-1,-1) = \varepsilon_2(1,1,1,-1), \\ g(1,-1,-1,1) = \varepsilon_3(1,1,-1,1), \\ g(1,-1,1,-1) = \varepsilon_4(1,1,-1,-1), \\ g(-1,1,1,1) = \varepsilon_5(1,-1,1,1), \\ g(1,-1,1,1) = \varepsilon_6(1,-1,1,-1), \\ g(1,1,-1,1) = \varepsilon_7(1,-1,-1,1), \\ g(1,1,1,-1) = \varepsilon_8(1,-1,-1,-1), \end{gathered}$$

при $\varepsilon_1, \ldots, \varepsilon_8 \in \{\pm 1\}$. В каждом из 256 предполагаемых вариантов коэффициенты линейных неравенств, определяющих первые две координатные функции указанной подстановки g:

$$\begin{aligned} g_1(x_1,x_2,x_3,x_4) = 1 &\iff a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \geqslant 0, \\ g_2(x_1,x_2,x_3,x_4) = 1 &\iff b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \geqslant 0, \end{aligned}$$

необходимо должны удовлетворять системе неравенств

$$\begin{cases}
\varepsilon_1(a_1+a_2+a_3+a_4)>0,\\
\varepsilon_2(a_1+a_2-a_3-a_4)>0,\\
\varepsilon_3(a_1-a_2-a_3+a_4)>0,\\
\varepsilon_4(a_1-a_2+a_3-a_4)>0,\\
\varepsilon_5(-a_1+a_2+a_3+a_4)>0,\\
\varepsilon_6(a_1-a_2+a_3+a_4)>0,\\
\varepsilon_7(a_1+a_2-a_3+a_4)>0,\\
\varepsilon_8(a_1+a_2+a_3-a_4)>0,\\
\varepsilon_1(b_1+b_2+b_3+b_4)>0,\\
\varepsilon_2(b_1+b_2-b_3-b_4)>0,\\
\varepsilon_3(b_1-b_2-b_3+b_4)>0,\\
\varepsilon_4(b_1-b_2+b_3-b_4)>0,\\
\varepsilon_5(-b_1+b_2+b_3+b_4)<0,\\
\varepsilon_6(b_1-b_2+b_3+b_4)<0,\\
\varepsilon_7(b_1+b_2-b_3+b_4)<0,\\
\varepsilon_8(b_1+b_2+b_3-b_4)<0,
\end{cases}$$

которая не имеет решений при любых $\varepsilon_1,\ldots,\varepsilon_8\in\{\pm1\}$ (проверка выполнена в системе Mathematica).

2. Пороговые подстановки, реализуемые $\{0,1\}$-матрицами

Согласно теореме 1, пороговые подстановки порождают достаточно обширный класс подстановок $\mathfrak{S}_n$. Однако результаты теоремы 1, выраженные в следствии 2, обескураживают ожидания относительно простоты получения произвольной подстановки из множества $\mathfrak{S}_n$ в виде композиции пороговых подстановок. Между тем практический интерес заключается в построении классов эффективно реализуемых пороговых подстановок, которые также обладают цикловой структурой, пригодной для использования в узлах защиты информации. Поэтому вполне естественно намерение изучить пороговые подстановки, которые могут быть определены максимально простыми матрицами, состоящими только из 0 и 1.

Теорема 2. $\{0,1\}$-матрица $A_{n\times n}$ задаёт пороговую подстановку $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$ в том и только в том случае, когда A — подстановочная матрица.

Доказательство. Достаточность очевидна, докажем необходимость методом «от противного». Предположим, что матрица A не является подстановочной и, не ограничивая общности, её первые две строки имеют следующий вид:

$$(\underbrace{1,\ldots,1}_{k},\underbrace{1,\ldots,1}_{s\geqslant1},\underbrace{0,\ldots,0}_{m},0,\ldots,0),$$
$$(\underbrace{0,\ldots,0}_{k},\underbrace{1,\ldots,1}_{s\geqslant1},\underbrace{1,\ldots,1}_{m},0,\ldots,0).$$

Указанные строки определяют две первые координатные функции порогового отображения $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$:

$$f_1(x_1,\ldots,x_n)=\operatorname{sgn}(x_1+\ldots+x_k+x_{k+1}+\ldots+x_{k+s}),$$
$$f_2(x_1,\ldots,x_n)=\operatorname{sgn}(x_{k+1}+\ldots+x_{k+s}+x_{k+s+1}+\ldots+x_{k+s+m}).$$

Здесь стоит отметить, что сбалансированность координатных функций f_1 и f_2 необходимо влечёт условие нечётности $k+s$ и $s+m$.

Для получения противоречия рассчитаем и сравним мощности множеств

$$M_{1,1} = \big\{\mathbf{x} \in \{\pm 1\}^n : (f_1(\mathbf{x}), f_2(\mathbf{x})) = (1,1)\big\},$$
$$M_{1,-1} = \big\{\mathbf{x} \in \{\pm 1\}^n : (f_1(\mathbf{x}), f_2(\mathbf{x})) = (1,-1)\big\}.$$

При перечислении векторов из $M_{1,1}$ нетрудно установить равенство

$$|M_{1,1}| = 2^{n-k-s-m} \sum_{t=0}^{s} \binom{s}{t} \sum_{i \geqslant (k+s+1)/2-t} \binom{k}{i} \sum_{j \geqslant (m+s+1)/2-t} \binom{m}{j},$$

где в перечисляемых наборах t обозначает количество единиц, расположенных на местах с $k+1$ по $k+s$; i — количество единиц на местах с 1 по k; j — количество единиц на местах с $k+s+1$ по $k+s+m$ (здесь и далее значение биномиального коэффициента $\binom{x}{y}$ стандартно полагается равным нулю при $x < y$, а также при $y < 0$). Аналогично

$$|M_{1,-1}| = 2^{n-k-s-m} \sum_{t=0}^{s} \binom{s}{t} \sum_{i \geqslant (k+s+1)/2-t}^{k} \binom{k}{i} \sum_{j \geqslant (m-s+1)/2+t} \binom{m}{j}.$$

Теперь рассмотрим величину

$$\frac{|M_{1,1}| - |M_{1,-1}|}{2^{n-k-s-m}} = \sum_{t=0}^{s} \binom{s}{t} \sum_{i \geqslant (k+s+1)/2-t} \binom{k}{i} \underbrace{\left[\sum_{j \geqslant (m+s+1)/2-t} \binom{m}{j} - \sum_{j \geqslant (m-s+1)/2+t} \binom{m}{j} \right]}_{N_{m,s,t}}$$

и заметим, что $N_{m,s,t} = -N_{m,s,s-t}$ при любых m и $t \leqslant s/2$ (в частности, $N_{m,s,s/2} = 0$ при чётном s). Продолжим:

$$\frac{|M_{1,1}| - |M_{1,-1}|}{2^{n-k-s-m}} = \sum_{t<s/2} \binom{s}{t} \sum_{i \geqslant (k+s+1)/2-t} \binom{k}{i} N_{m,s,t} + \sum_{t>s/2} \binom{s}{t} \sum_{i \geqslant (k+s+1)/2-t} \binom{k}{i} N_{m,s,t} =$$
$$= \sum_{t<s/2} \binom{s}{t} N_{m,s,t} \sum_{i \geqslant (k+s+1)/2-t} \binom{k}{i} - \sum_{t<s/2} \binom{s}{t} N_{m,s,t} \sum_{i \geqslant (k-s+1)/2+t} \binom{k}{i} =$$
$$= \sum_{t<s/2} \binom{s}{t} N_{m,s,t} \underbrace{\left[\sum_{i \geqslant (k+s+1)/2-t} \binom{k}{i} - \sum_{i \geqslant (k-s+1)/2+t} \binom{k}{i} \right]}_{N_{k,s,t}} = \sum_{t<s/2} \binom{s}{t} N_{m,s,t} N_{k,s,t}.$$

Заметим, что при любых $m \in \mathbb{N}_0$, $s \in \mathbb{N}$ и $t < s/2$ имеет место

$$\begin{cases} (m-s+1)/2 + t < (m+s+1)/2 - t, \\ (m-s+1)/2 + t \leqslant m, \\ (m+s+1)/2 - t > 0 \end{cases} \implies N_{m,s,t} = -\sum_{j=(m-s+1)/2+t}^{(m+s+1)/2-t-1} \binom{m}{j} < 0.$$

Итак, показали, что при $s \geqslant 1$ всегда выполняется строгое неравенство

$$\frac{|M_{1,1}| - |M_{1,-1}|}{2^{n-k-s-m}} > 0,$$

что противоречит независимости сбалансированных координатных функций f_1 и f_2. ■

Следствие 4. Если для матрицы $A \in \mathbb{R}_{n,n}$ линейное отображение $\mathbf{x}^{\downarrow} \mapsto A\mathbf{x}^{\downarrow}$ задаёт перестановку на множестве $\{\pm 1\}^n$, то A является $\{\pm 1\}$-подстановочной матрицей.

Доказательство. Не ограничивая общности, для удобства будем полагать, что $A\mathbf{1}^{\downarrow} = \mathbf{1}^{\downarrow}$ (при необходимости можно домножить соответствующие строки матрицы A на -1). В таком случае легко видеть, что столбец

$$2A_1^{\downarrow} = A\left(\mathbf{1}^{\downarrow} - (-1, 1, \ldots, 1)^{\mathrm{T}}\right) = A\mathbf{1}^{\downarrow} - A(-1, 1, \ldots, 1)^{\mathrm{T}} = \mathbf{1}^{\downarrow} - (\varepsilon_1, \ldots, \varepsilon_n)^{\mathrm{T}}$$

состоит только из 0 и 2 и, следовательно, $A_1^{\downarrow}$ — $\{0, 1\}$-столбец. Аналогично показывается, что все остальные столбцы матрицы A также являются $\{0, 1\}$-столбцами.

Таким образом, A — $\{0, 1\}$-матрица, которая задаёт пороговую подстановку (на самом деле, действует точным образом), и, согласно теореме 2, A — подстановочная матрица. ■

Замечание 2. Из следствия 4 вытекает интересное наблюдение. Оказывается, что $\{\pm 1\}$-подстановочные матрицы описывают все изометрии множества $\{\pm 1\}^n$ не только относительно метрики Хэмминга, но и относительно метрики Евклида, поскольку в последнем случае изометрия обязательно является линейным отображением и попадает под условие следствия 4. Это вполне закономерно, поскольку на множестве $\{\pm 1\}^n$ метрики Евклида и Хэмминга эквивалентны.

В заключение данного пункта отметим, что описание $\{0, \pm 1\}$-матриц, которые определяют пороговые подстановки, представляется весьма сложной задачей. В настоящий момент не существует никаких решений для построения бесконечных классов $\{0, \pm 1\}$-матриц, определяющих пороговые подстановки. Так, например, в работах [4–6] приведены лишь частные примеры псевдоадамаровых матриц и конференц-матриц размеров 4×4, 6×6, 8×8 и 10×10, которые задают пороговые подстановки; при этом обоснование биективности рассматриваемых пороговых отображений также носит частный характер и не позволяет делать каких-либо выводов о существовании/построении псевдоадамаровых матриц и конференц-матриц, определяющих пороговые подстановки произвольной размерности.

3. Рекурсивное построение полноцикловых пороговых подстановок

Результаты п. 2 носят отрицательный характер в том смысле, что не удалось обнаружить вообще никаких новых пороговых подстановок, не говоря уже о классах пороговых подстановок. Здесь в терминах определяющих матриц исследуем возможность рекурсивного построения пороговых подстановок. Начнём с простейшего варианта рекурсивного продолжения существующих матриц.

Утверждение 3. Если матрица

$$B = \begin{pmatrix} b_{11} & * \\ 0^{\downarrow} & A_{n\times n} \end{pmatrix}_{(n+1)\times(n+1)}$$

задаёт пороговую подстановку $\operatorname{sgn}(B\mathbf{x}^{\downarrow})$ на множестве $\{\pm 1\}^{n+1}$, то данная пороговая подстановка также может быть задана матрицей

$$\begin{pmatrix} b_{11} & 0\ldots 0 \\ 0^{\downarrow} & A_{n\times n} \end{pmatrix}_{(n+1)\times(n+1)},$$

и при этом матрица A необходимо задаёт пороговую подстановку на множестве $\{\pm 1\}^n$.

Доказательство. Если система линейных неравенств

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n+1}x_{n+1} > 0, \\ a_{11}x_2 + \ldots + a_{1n}x_{n+1} > 0, \\ \ldots \\ a_{n1}x_2 + \ldots + a_{nn}x_{n+1} > 0 \end{cases}$$

задаёт пороговую подстановку, то при любых $\varepsilon_2, \ldots, \varepsilon_{n+1} \in \{\pm 1\}$ неравенство

$$b_{11}x_1 + (b_{12}\varepsilon_2 + \ldots + b_{1n+1}\varepsilon_{n+1}) > 0$$

необходимо задаёт сбалансированную псевдобулеву функцию от переменной x_1 и, как нетрудно видеть, может быть заменено более простым неравенством $b_{11}x_1 > 0$ или вовсе тривиальным $\operatorname{sgn}(b_{11})x_1 > 0$. Остаётся заметить, что система

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n > 0, \\ \ldots \\ a_{n1}x_1 + \ldots + a_{nn}x_n > 0 \end{cases}$$

необходимо задаёт пороговую подстановку на множестве $\{\pm 1\}^n$. ■

Из утверждения 3 следует, что простейший способ продолжения существующей пороговой подстановки множества $\{\pm 1\}^n$ до пороговой подстановки множества $\{\pm 1\}^{n+1}$ посредством добавления ещё одной пороговой координатной функции допускает лишь тривиальные варианты.

Следствие 5. Не существует нетривиальных «треугольных» пороговых подстановок, отличных от подстановок вида $(x_1, \ldots, x_n) \mapsto (\varepsilon_1 x_1, \ldots, \varepsilon_n x_n)$.

Теперь приступим к изложению более продвинутого (по сравнению с утверждением 3) способа рекурсивного продолжения пороговой подстановки множества $\{\pm 1\}^n$ до пороговой подстановки множества $\{\pm 1\}^{n+1}$. В конечном итоге этот метод позволит построить целое семейство полноцикловых пороговых подстановок. Для удобства изложения здесь и далее наборы $\mathbf{a} \in \{\pm 1\}^n$ будем записывать в виде столбцов $\mathbf{a}^{\downarrow}$, при этом набор $-\mathbf{a}^{\downarrow}$ будем обозначать через $\overline{\mathbf{a}}^{\downarrow}$.

Утверждение 4. Если пороговая подстановка $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$ на множестве $\{\pm 1\}^n$ реализует полный цикл, то указанный цикл имеет вид

$$\left(\mathbf{a}_1^{\downarrow}, \mathbf{a}_2^{\downarrow}, \ldots, \mathbf{a}_{2^{n-1}}^{\downarrow}, \overline{\mathbf{a}}_1^{\downarrow}, \overline{\mathbf{a}}_2^{\downarrow}, \ldots, \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\right). \tag{2}$$

Доказательство. Рассмотрим полный цикл пороговой подстановки $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$, начиная с произвольного элемента $\mathbf{a}_1^{\downarrow}$:

$$\left(\mathbf{a}_1^{\downarrow}, \mathbf{a}_2^{\downarrow}, \ldots\right).$$

Так как подстановка $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$ является полноцикловой, то цикл содержит набор $\overline{\mathbf{a}}_1^{\downarrow}$:

$$\left(\mathbf{a}_1^{\downarrow}, \mathbf{a}_2^{\downarrow}, \ldots, \mathbf{a}_t^{\downarrow}, \overline{\mathbf{a}}_1^{\downarrow}, \ldots\right),$$

а поскольку она является самодвойственной, то её полный цикл имеет вид

$$\left(\mathbf{a}_1^{\downarrow}, \mathbf{a}_2^{\downarrow}, \ldots, \mathbf{a}_t^{\downarrow}, \overline{\mathbf{a}}_1^{\downarrow}, \overline{\mathbf{a}}_2^{\downarrow}, \ldots, \overline{\mathbf{a}}_t^{\downarrow}, \mathbf{a}_1^{\downarrow}, \ldots\right).$$

Легко видеть, что полный цикл подстановки $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$ на самом деле имеет вид (2). ■

Следующее утверждение раскрывает детали одного возможного рекурсивного построения полноцикловой пороговой подстановки.

Утверждение 5. Пусть матрица $A_{n\times n}$ определяет полноцикловую пороговую подстановку $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$ на множестве $\{\pm1\}^n$:

$$\left(\mathbf{a}_1^{\downarrow},\ldots,\mathbf{a}_{2^{n-1}}^{\downarrow},\overline{\mathbf{a}}_1^{\downarrow},\ldots,\overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\right).$$

Тогда матрица

$$B=\begin{pmatrix} b & b_{11} & \ldots & b_{1n}\\ b_{11} & & & \\ \vdots & & A_{n\times n} & \\ b_{n1} & & & \end{pmatrix}_{(n+1)\times(n+1)}$$

может реализовать полноцикловую пороговую подстановку $\operatorname{sgn}(B\mathbf{x}^{\downarrow})$ вида

$$\left(\begin{pmatrix}*\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}*\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}*\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}*\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}*\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}*\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}*\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}*\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$$

только одного из следующих четырёх типов:

1) $\left(\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$;

2) $\left(\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$;

3) $\left(\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$;

4) $\left(\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$.

Доказательство. Ввиду утверждения 4, полный цикл подстановки $\operatorname{sgn}(B\mathbf{x}^{\downarrow})$ должен иметь вид

$$\left(\begin{pmatrix}a_1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}a_{2^{n-1}}\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}b_1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}b_{2^{n-1}}\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}\overline{a}_1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}\overline{a}_{2^{n-1}}\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}\overline{b}_1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}\overline{b}_{2^{n-1}}\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right).$$

Поскольку все наборы в этом цикле должны быть различны, то на самом деле $a_1=b_1$, $\ldots$, $a_{2^{n-1}}=b_{2^{n-1}}$:

$$\left(\begin{pmatrix}a_1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}a_{2^{n-1}}\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}a_1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}a_{2^{n-1}}\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}\overline{a}_1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}\overline{a}_{2^{n-1}}\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}\overline{a}_1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\ldots,\begin{pmatrix}\overline{a}_{2^{n-1}}\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right).$$

Обозначим $\mathbf{b}=(b_{11},\ldots,b_{1n})$. Наблюдая первую координату в наборах, составляющих полный цикл пороговой подстановки $\operatorname{sgn}(B\mathbf{x}^{\downarrow})$, нетрудно заметить равенства

$$\operatorname{sgn}(ba_i+\mathbf{b}\mathbf{a}_i^{\downarrow})=a_{i+1}=\operatorname{sgn}(ba_i-\mathbf{b}\mathbf{a}_i^{\downarrow}),\quad 1\leqslant i<2^{n-1}.$$

Из этих равенств следует, что $a_{i+1}=\operatorname{sgn}(ba_i)$ при всех $1\leqslant i<2^{n-1}$, и значит, возможны два варианта при $b>0$:

1) $a_1 = a_2 = \ldots = a_{2^{n-1}} = 1$;
2) $a_1 = a_2 = \ldots = a_{2^{n-1}} = -1$,

а также два варианта при $b < 0$:

1) $a_1 = -a_2 = a_3 = \ldots = -a_{2^{n-1}} = 1$;
2) $a_1 = -a_2 = a_3 = \ldots = -a_{2^{n-1}} = -1$.

Утверждение 5 доказано. ■

Покажем, что при некоторых ограничениях на полноцикловое пороговое преобразование $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$ множества $\{\pm 1\}^n$ возможно построить продолжение $\operatorname{sgn}(B\mathbf{x}^{\downarrow})$ каждого из четырёх возможных типов, перечисленных в утверждении 5.

Определение 2. Будем называть набор $\mathbf{c} \in \{\pm 1\}^n$ точкой *абсолютного минимума* для порогового отображения $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$, если выполняется условие

$$\forall \mathbf{a} \in \{\pm 1\}^n \quad |A\mathbf{c}^{\downarrow}| \leqslant |A\mathbf{a}^{\downarrow}|,$$

где знак $\leqslant$ означает покоординатное неравенство; $|\mathbf{x}| = \big(|x_1|, \ldots, |x_n|\big)$ — покоординатное вычисление абсолютных значений.

Нетрудно видеть, что для любого $\mathbf{c} \in \{\pm 1\}^n$ выполняется равенство

$$|A\mathbf{c}^{\downarrow}| = |A\overline{\mathbf{c}}^{\downarrow}|.$$

Таким образом, $\mathbf{c} \in \{\pm 1\}^n$ является точкой абсолютного минимума для порогового отображения $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$ в том и только в том случае, когда $\overline{\mathbf{c}}$ является точкой абсолютного минимимума для порогового отображения $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$.

Наборы $\mathbf{c}, \overline{\mathbf{c}} \in \{\pm 1\}^n$ будем называть точками *строгого абсолютного минимума* для порогового отображения $\operatorname{sgn}(A\mathbf{x}^{\downarrow})$, если выполняется условие

$$\forall \mathbf{a} \in \{\pm 1\}^n \setminus \{\mathbf{c}, \overline{\mathbf{c}}\} \quad |A\mathbf{c}^{\downarrow}| < |A\mathbf{a}^{\downarrow}|,$$

где знак $<$ означает строгое неравенство в каждой координате сравниваемых наборов.

Теорема 3. Пусть A_n — целочисленная матрица размера $n \times n$, которая определяет полноцикловую пороговую подстановку $\operatorname{sgn}(A_n\mathbf{x}^{\downarrow})$ на множестве $\{\pm 1\}^n$

$$\big(\mathbf{a}_1, \ldots, \mathbf{a}_{2^{n-1}}, \overline{\mathbf{a}}_1, \ldots, \overline{\mathbf{a}}_{2^{n-1}}\big)$$

с двумя строгими абсолютными минимумами в точках $\mathbf{a}_{2^{n-1}}$ и $\overline{\mathbf{a}}_{2^{n-1}}$:

$$\forall \mathbf{a} \notin \{\mathbf{a}_{2^{n-1}}, \overline{\mathbf{a}}_{2^{n-1}}\} \quad |A_n\mathbf{a}^{\downarrow}| > |A_n\mathbf{a}^{\downarrow}_{2^{n-1}}| = \mathbf{1}^{\downarrow}.$$

Тогда выполняются следующие свойства:

1) матрица $A_{n+1} = \begin{pmatrix} 2n-1 & 2\mathbf{a}_{2^{n-1}} \\ 4\overline{\mathbf{a}}_1^{\downarrow} & 3A_n \end{pmatrix}$ задаёт полноцикловую пороговую подстановку $\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})$

$$\left(\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$$

с двумя строгими абсолютными минимумами в точках $\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}$ и $\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}$, при которых $\left|A_{n+1}\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \left|A_{n+1}\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \mathbf{1}^{\downarrow}$;

2) матрица $A_{n+1} = \begin{pmatrix} 2n-1 & 2\overline{\mathbf{a}}_{2^{n-1}} \\ 4\mathbf{a}_1^{\downarrow} & 3A_n \end{pmatrix}$ задаёт полноцикловую пороговую подстановку $\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})$

$$\left(\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$$

с двумя строгими абсолютными минимумами в точках $\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}$ и $\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}$, при которых $\left|A_{n+1}\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \left|A_{n+1}\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \mathbf{1}^{\downarrow}$;

3) матрица $A_{n+1} = \begin{pmatrix} -2n+1 & 2\mathbf{a}_{2^{n-1}} \\ 4\mathbf{a}_1^{\downarrow} & 3A_n \end{pmatrix}$ задаёт полноцикловую пороговую подстановку $\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})$

$$\left(\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$$

с двумя строгими абсолютными минимумами в точках $\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}$ и $\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}$, при которых $\left|A_{n+1}\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \left|A_{n+1}\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \mathbf{1}^{\downarrow}$;

4) матрица $A_{n+1} = \begin{pmatrix} -2n+1 & 2\overline{\mathbf{a}}_{2^{n-1}} \\ 4\overline{\mathbf{a}}_1^{\downarrow} & 3A_n \end{pmatrix}$ задаёт полноцикловую пороговую подстановку $\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})$

$$\left(\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix},\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix},\dots,\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$$

с двумя строгими абсолютными минимумами в точках $\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}$ и $\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}$, при которых $\left|A_{n+1}\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \left|A_{n+1}\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right| = \mathbf{1}^{\downarrow}$.

Доказательство. Заметим, что из целочисленности матрицы A_n и условия

$$\forall \mathbf{a} \notin \{\mathbf{a}_{2^{n-1}}, \overline{\mathbf{a}}_{2^{n-1}}\} \quad |A_n\mathbf{a}^{\downarrow}| > |A_n\mathbf{a}_{2^{n-1}}^{\downarrow}| = (1,\dots,1)^{\mathrm{T}}$$

следует, что

$$\forall \mathbf{a} \notin \{\mathbf{a}_{2^{n-1}}, \overline{\mathbf{a}}_{2^{n-1}}\} \quad |A_n\mathbf{a}^{\downarrow}| \geqslant (2,\dots,2)^{\mathrm{T}}, \quad A_n\mathbf{a}_{2^{n-1}}^{\downarrow} = \overline{\mathbf{a}}_1^{\downarrow}.$$

Теперь доказательство всех свойств проводится непосредственной проверкой:
1)

$$A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix} = \begin{pmatrix}\pm(2n-1) + 2\mathbf{a}_{2^{n-1}}\mathbf{a}_i^{\downarrow}\\ \pm 4\overline{\mathbf{a}}_1^{\downarrow} + 3A_n\mathbf{a}_i^{\downarrow}\end{pmatrix} \Rightarrow \begin{cases} \operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right) = \begin{pmatrix}\pm 1\\ \mathbf{a}_{i+1}^{\downarrow}\end{pmatrix}, \\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right| \geqslant (3,2,\dots,2)^{\mathrm{T}}, \end{cases} \quad 1 \leqslant i < 2^{n-1},$$

$$A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}=\begin{pmatrix}\pm(2n-1)+2\mathbf{a}_{2^{n-1}}\overline{\mathbf{a}}_i^{\downarrow}\\ \pm 4\overline{\mathbf{a}}_1^{\downarrow}+3A_n\overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\Rightarrow\begin{cases}\operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right)=\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_{i+1}^{\downarrow}\end{pmatrix},\\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right|\geqslant(3,2,\ldots,2)^{\mathrm{T}},\end{cases}\quad 1\leqslant i<2^{n-1},$$

$$A_{n+1}\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}4n-1\\ 7\overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-4n+1\\ 7\mathbf{a}_1^{\downarrow}\end{pmatrix},$$

$$A_{n+1}\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}.$$

2)

$$A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}=\begin{pmatrix}\pm(2n-1)+2\overline{\mathbf{a}}_{2^{n-1}}\mathbf{a}_i^{\downarrow}\\ \pm 4\mathbf{a}_1^{\downarrow}+3A_n\mathbf{a}_i^{\downarrow}\end{pmatrix}\Rightarrow\begin{cases}\operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right)=\begin{pmatrix}\pm 1\\ \mathbf{a}_{i+1}^{\downarrow}\end{pmatrix},\\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right|\geqslant(3,2,\ldots,2)^{\mathrm{T}},\end{cases}\quad 1\leqslant i<2^{n-1},$$

$$A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}=\begin{pmatrix}\pm(2n-1)+2\overline{\mathbf{a}}_{2^{n-1}}\overline{\mathbf{a}}_i^{\downarrow}\\ \pm 4\mathbf{a}_1^{\downarrow}+3A_n\overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\Rightarrow\begin{cases}\operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right)=\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_{i+1}^{\downarrow}\end{pmatrix},\\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right|\geqslant(3,2,\ldots,2)^{\mathrm{T}},\end{cases}\quad 1\leqslant i<2^{n-1},$$

$$A_{n+1}\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-4n+1\\ 7\overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}4n-1\\ 7\mathbf{a}_1^{\downarrow}\end{pmatrix},$$

$$A_{n+1}\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}.$$

3)

$$A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}=\begin{pmatrix}\mp(2n-1)+2\mathbf{a}_{2^{n-1}}\mathbf{a}_i^{\downarrow}\\ \pm 4\mathbf{a}_1^{\downarrow}+3A_n\mathbf{a}_i^{\downarrow}\end{pmatrix}\Rightarrow\begin{cases}\operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right)=\begin{pmatrix}\mp 1\\ \mathbf{a}_{i+1}^{\downarrow}\end{pmatrix},\\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right|\geqslant(3,2,\ldots,2)^{\mathrm{T}},\end{cases}\quad 1\leqslant i<2^{n-1},$$

$$A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}=\begin{pmatrix}\mp(2n-1)+2\mathbf{a}_{2^{n-1}}\overline{\mathbf{a}}_i^{\downarrow}\\ \pm 4\mathbf{a}_1^{\downarrow}+3A_n\overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\Rightarrow\begin{cases}\operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right)=\begin{pmatrix}\mp 1\\ \overline{\mathbf{a}}_{i+1}^{\downarrow}\end{pmatrix},\\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right|\geqslant(3,2,\ldots,2)^{\mathrm{T}},\end{cases}\quad 1\leqslant i<2^{n-1},$$

$$A_{n+1}\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}4n-1\\ 7\overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-4n+1\\ 7\mathbf{a}_1^{\downarrow}\end{pmatrix},$$

$$A_{n+1}\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}.$$

4)

$$A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}=\begin{pmatrix}\mp(2n-1)+2\overline{\mathbf{a}}_{2^{n-1}}\mathbf{a}_i^{\downarrow}\\ \pm 4\overline{\mathbf{a}}_1^{\downarrow}+3A_n\mathbf{a}_i^{\downarrow}\end{pmatrix}\Rightarrow\begin{cases}\operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right)=\begin{pmatrix}\mp 1\\ \mathbf{a}_{i+1}^{\downarrow}\end{pmatrix},\\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \mathbf{a}_i^{\downarrow}\end{pmatrix}\right|\geqslant(3,2,\ldots,2)^{\mathrm{T}},\end{cases}\quad 1\leqslant i<2^{n-1},$$

$$A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}=\begin{pmatrix}\mp(2n-1)+2\overline{\mathbf{a}}_{2^{n-1}}\overline{\mathbf{a}}_i^{\downarrow}\\ \pm 4\overline{\mathbf{a}}_1^{\downarrow}+3A_n\overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\ \Rightarrow\ \begin{cases}\operatorname{sgn}\left(A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right)=\begin{pmatrix}\mp 1\\ \overline{\mathbf{a}}_{i+1}^{\downarrow}\end{pmatrix},\\ \left|A_{n+1}\begin{pmatrix}\pm 1\\ \overline{\mathbf{a}}_i^{\downarrow}\end{pmatrix}\right|\geqslant(3,2,\ldots,2)^{\mathrm{T}},\end{cases}\quad 1\leqslant i<2^{n-1},$$

$$A_{n+1}\begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-4n+1\\ 7\overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}-1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}4n-1\\ 7\mathbf{a}_1^{\downarrow}\end{pmatrix},$$

$$A_{n+1}\begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix},\qquad A_{n+1}\begin{pmatrix}-1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}=\begin{pmatrix}-1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}.$$

Теорема 3 доказана. ■

Замечание 3. В условии теоремы 3 целочисленность матрицы A_n, а также нормированное значение абсолютного минимума $\mathbf{1}^{\downarrow}=(1,\ldots,1)^{\mathrm{T}}$ используются исключительно для лаконичности формулировки и простоты доказательства. Так, например, в общем случае для произвольной матрицы A_n размера $n\times n$, что определяет полноцикловую пороговую подстановку $\operatorname{sgn}(A_n\mathbf{x}^{\downarrow})$ на множестве $\{\pm 1\}^n$

$$\left(\mathbf{a}_1,\ldots,\mathbf{a}_{2^{n-1}},\overline{\mathbf{a}}_1,\ldots,\overline{\mathbf{a}}_{2^{n-1}}\right)$$

с двумя строгими абсолютными минимумами в точках $\mathbf{a}_{2^{n-1}}$ и $\overline{\mathbf{a}}_{2^{n-1}}$:

$$\exists\varepsilon>0\quad\forall\mathbf{a}\notin\{\mathbf{a}_{2^{n-1}},\overline{\mathbf{a}}_{2^{n-1}}\}\quad|A_n\mathbf{a}^{\downarrow}|>(1+\varepsilon)|A_n\mathbf{a}_{2^{n-1}}^{\downarrow}|,$$

при построении полноциклового продолжения $\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})$ первого типа можно использовать матрицу

$$A_{n+1}=\begin{pmatrix}2n-1 & 2\mathbf{a}_{2^{n-1}}\\ -(1+\varepsilon/2)A_n\overline{\mathbf{a}}_{2^{n-1}}^{\downarrow} & A_n\end{pmatrix}.$$

Нетрудно видеть, что предложенная в теореме 3 конструкция построения полноцикловой пороговой подстановки из полноцикловой пороговой подстановки меньшей размерности в любом из четырёх перечисленных вариантов допускает рекурсивное применение.

Следствие 6. Для любого натурального n существует полноцикловая пороговая подстановка множества $\{\pm 1\}^n$.

Доказательство. Матрица $A_1=(-1)_{1\times 1}$ задаёт полноцикловую пороговую подстановку с двумя точками строгого абсолютного минимума. Применяя к A_1 рекурсивную процедуру, описанную в теореме 3, можно для любого n построить матрицу A_n размера $n\times n$, которая задаёт полноцикловую пороговую подстановку $\operatorname{sgn}(A_n\mathbf{x}^{\downarrow})$. ■

На практике при использовании полноцикловых подстановок часто требуется, чтобы обращение данной подстановки также допускало эффективное вычисление. Оказывается, для пороговых подстановок, которые построены рекурсивным образом в соответствии с теоремой 3, обратные подстановки тоже являются пороговыми и могут быть построены рекурсивным образом.

Следствие 7. В условиях теоремы 3 пусть $\hat{A}_n$ — целочисленная матрица размера $n\times n$, которая определяет обратную к $\operatorname{sgn}(A_n\mathbf{x}^{\downarrow})$ полноцикловую пороговую подстановку

$$\left(\overline{\mathbf{a}}_{2^{n-1}}^{\downarrow},\ldots,\overline{\mathbf{a}}_1^{\downarrow},\mathbf{a}_{2^{n-1}}^{\downarrow},\ldots,\mathbf{a}_1^{\downarrow}\right)$$

с двумя строгими абсолютными минимумами в точках $\overline{\mathbf{a}}_1$ и $\mathbf{a}_1$:

$$\forall \mathbf{a} \notin \{\mathbf{a}_1, \overline{\mathbf{a}}_1\} \quad |\hat{A}_n \mathbf{a}^{\downarrow}| > |\hat{A}_n \mathbf{a}_1^{\downarrow}| = \mathbf{1}^{\downarrow}.$$

Тогда подстановка, обратная к пороговой подстановке $\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})$, также является пороговой и в каждом из четырёх перечисленных в теореме 3 случаев может быть задана соответствующей матрицей $\hat{A}_{n+1}$:

1) матрица $\hat{A}_{n+1}=\begin{pmatrix} 2n-1 & 2\overline{\mathbf{a}}_1 \\ 4\mathbf{a}^{\downarrow}_{2^{n-1}} & 3\hat{A}_n \end{pmatrix}$ задаёт подстановку $\operatorname{sgn}(\hat{A}_{n+1}\mathbf{x}^{\downarrow})=\big(\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})\big)^{-1}$ с двумя строгими абсолютными минимумами в точках $\begin{pmatrix} 1 \\ \mathbf{a}_1^{\downarrow} \end{pmatrix}$ и $\begin{pmatrix} -1 \\ \overline{\mathbf{a}}_1^{\downarrow} \end{pmatrix}$;

2) матрица $\hat{A}_{n+1}=\begin{pmatrix} 2n-1 & 2\mathbf{a}_1 \\ 4\overline{\mathbf{a}}^{\downarrow}_{2^{n-1}} & 3\hat{A}_n \end{pmatrix}$ задаёт подстановку $\operatorname{sgn}(\hat{A}_{n+1}\mathbf{x}^{\downarrow})=\big(\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})\big)^{-1}$ с двумя строгими абсолютными минимумами в точках $\begin{pmatrix} -1 \\ \mathbf{a}_1^{\downarrow} \end{pmatrix}$ и $\begin{pmatrix} 1 \\ \overline{\mathbf{a}}_1^{\downarrow} \end{pmatrix}$;

3) матрица $\hat{A}_{n+1}=\begin{pmatrix} -2n+1 & 2\mathbf{a}_1 \\ 4\mathbf{a}^{\downarrow}_{2^{n-1}} & 3\hat{A}_n \end{pmatrix}$ задаёт подстановку $\operatorname{sgn}(\hat{A}_{n+1}\mathbf{x}^{\downarrow})=\big(\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})\big)^{-1}$ с двумя строгими абсолютными минимумами в точках $\begin{pmatrix} 1 \\ \mathbf{a}_1^{\downarrow} \end{pmatrix}$ и $\begin{pmatrix} -1 \\ \overline{\mathbf{a}}_1^{\downarrow} \end{pmatrix}$;

4) матрица $\hat{A}_{n+1}=\begin{pmatrix} -2n+1 & 2\overline{\mathbf{a}}_1 \\ 4\overline{\mathbf{a}}^{\downarrow}_{2^{n-1}} & 3\hat{A}_n \end{pmatrix}$ задаёт подстановку $\operatorname{sgn}(\hat{A}_{n+1}\mathbf{x}^{\downarrow})=\big(\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})\big)^{-1}$ с двумя строгими абсолютными минимумами в точках $\begin{pmatrix} -1 \\ \mathbf{a}_1^{\downarrow} \end{pmatrix}$ и $\begin{pmatrix} 1 \\ \overline{\mathbf{a}}_1^{\downarrow} \end{pmatrix}$.

Доказательство. Согласно теореме 3, продолжение матрицы $\hat{A}_n$ до целочисленной матрицы $\hat{A}_{n+1}$ позволяет реализовать полный цикл каждого из четырёх возможных типов с двумя строгими абсолютными минимумами.

Нетрудно видеть, что для полного цикла $\operatorname{sgn}(A_{n+1}\mathbf{x}^{\downarrow})$ типа 1 (2, 3 или 4) обратной будет подстановка $\operatorname{sgn}(\hat{A}_{n+1}\mathbf{x}^{\downarrow})$, полученная в результате продолжения типа 1 (2, 4 и 3 соответственно). ■

Проиллюстрируем результаты теоремы 3 и следствий 6, 7 на примере.

Пример 3. Рассмотрим пороговую подстановку с матрицей $A_1 = (-1)_{1\times 1}$. Очевидно, подстановка $\operatorname{sgn}(A_1\mathbf{x}^{\downarrow})$ является полноцикловой с двумя точками строго абсолютного минимума, а матрица $\hat{A}_1 = (-1)_{1\times 1}$ задаёт обратную подстановку.

Для матриц A_1 и $\hat{A}_1$ выполним рекурсивное продолжение типа 1:

$$A_2 = \begin{pmatrix} 1 & 2 \\ -4 & -3 \end{pmatrix}, \qquad \hat{A}_2 = \begin{pmatrix} 1 & -2 \\ 4 & -3 \end{pmatrix}.$$

Полученные матрицы реализуют полные циклы:

$$A_2\colon \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} -1 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} -1 \\ 1 \end{pmatrix},$$
$$\hat{A}_2\colon \begin{pmatrix} -1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} -1 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ -1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Теперь для матриц A_2 и $\hat{A}_2$ выполним рекурсивное продолжение типа 2:

$$A_3 = \begin{pmatrix} 3 & -2 & 2 \\ 4 & 3 & 6 \\ 4 & -12 & -9 \end{pmatrix}, \qquad \hat{A}_3 = \begin{pmatrix} 3 & 2 & 2 \\ -4 & 3 & -6 \\ 4 & 12 & -9 \end{pmatrix}.$$

Построенные матрицы реализуют полные циклы:

$$A_3\colon \begin{pmatrix}-1\\1\\1\end{pmatrix}\mapsto\begin{pmatrix}-1\\1\\-1\end{pmatrix}\mapsto\begin{pmatrix}-1\\-1\\-1\end{pmatrix}\mapsto\begin{pmatrix}-1\\-1\\1\end{pmatrix}\mapsto\begin{pmatrix}1\\-1\\-1\end{pmatrix}\mapsto\begin{pmatrix}1\\-1\\1\end{pmatrix}\mapsto\begin{pmatrix}1\\1\\1\end{pmatrix}\mapsto\begin{pmatrix}1\\1\\-1\end{pmatrix},$$

$$\hat{A}_3\colon \begin{pmatrix}1\\1\\-1\end{pmatrix}\mapsto\begin{pmatrix}1\\1\\1\end{pmatrix}\mapsto\begin{pmatrix}1\\-1\\1\end{pmatrix}\mapsto\begin{pmatrix}1\\-1\\-1\end{pmatrix}\mapsto\begin{pmatrix}-1\\-1\\1\end{pmatrix}\mapsto\begin{pmatrix}-1\\-1\\-1\end{pmatrix}\mapsto\begin{pmatrix}-1\\1\\-1\end{pmatrix}\mapsto\begin{pmatrix}-1\\1\\1\end{pmatrix}.$$

Для матриц A_3 и $\hat{A}_3$ выполним рекурсивное продолжение типа 3:

$$A_4=\begin{pmatrix}-5&-2&-2&2\\-4&9&-6&6\\4&12&9&18\\4&12&-36&-27\end{pmatrix},\qquad \hat{A}_4=\begin{pmatrix}-5&-2&2&2\\-4&9&6&6\\-4&-12&9&-18\\4&12&36&-27\end{pmatrix}.$$

И так далее.

4. Применение построенных полноцикловых пороговых подстановок

Исследуем строение координатных функций всех возможных полноцикловых пороговых подстановок, которые могут быть построены рекурсивным образом посредством многократного применения конструкции, предложенной в теореме 3, с тривиальным начальным условием, а также сделаем вывод о возможности применения указанных подстановок на практике. Описание координатных функций проведём в хорошо развитой терминологии линейных рекуррентных последовательностей над полем (подробно ознакомиться с этим разделом математики можно в монографии [14], ставшей мировым стандартом в данной области, а также в [15]).

Напомним, что над произвольным полем последовательность со знаками

$$\underbrace{0,\dots,0}_{k},\binom{k}{k}\alpha^0,\binom{k+1}{k}\alpha^1,\binom{k+2}{k}\alpha^2,\dots$$

называют *биномиальной последовательностью порядка k с корнем α* и обозначают через $\alpha^{[k]}$. Для знаков последовательности $\alpha^{[k]}$ удобно использовать универсальную формулу $\alpha^{[k]}(i)=\binom{i}{k}\alpha^{i-k}$, $i\in\mathbb{N}_0$, полагая $\alpha^{[k]}(i)=0$ при $i<k$. Биномиальная последовательность $\alpha^{[k]}$ является линейной рекуррентой с минимальным многочленом $(x-\alpha)^{k+1}$.

В последовательности двоичных наборов, упорядоченных лексикографически:

$$\begin{matrix}v_1\colon\\v_2\colon\\\vdots\\v_{n-1}\colon\\v_n\colon\end{matrix}\quad\begin{pmatrix}0\\0\\\vdots\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix},\begin{pmatrix}0\\0\\\vdots\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\\vdots\\1\\1\end{pmatrix},\dots\begin{pmatrix}0\\1\\\vdots\\1\\1\end{pmatrix},\begin{pmatrix}1\\0\\\vdots\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\\vdots\\0\\1\end{pmatrix},\begin{pmatrix}1\\0\\\vdots\\1\\0\end{pmatrix},\dots\begin{pmatrix}1\\1\\\vdots\\1\\1\end{pmatrix},\qquad(3)$$

координатные последовательности являются начальными отрезками биномиальных последовательностей над полем $\mathbb{F}_2$:

$$v_1=1^{[2^{n-1}]}(\overline{0,2^n-1}),v_2=1^{[2^{n-2}]}(\overline{0,2^n-1}),\dots,v_{n-1}=1^{[2^1]}(\overline{0,2^n-1}),v_n=1^{[2^0]}(\overline{0,2^n-1}).$$

Заметим, что указанные отрезки явным образом содержат всю информацию о последовательностях $1^{[2^0]}, 1^{[2^1]}, \ldots, 1^{[2^{n-2}]}, 1^{[2^{n-1}]}$ (2^n — общий период для данных последовательностей), и потому вполне естественно использовать для отрезков

$$1^{[2^0]}(\overline{0, 2^n-1}),\ 1^{[2^1]}(\overline{0, 2^n-1}),\ \ldots,\ 1^{[2^{n-2}]}(\overline{0, 2^n-1}),\ 1^{[2^{n-1}]}(\overline{0, 2^n-1})$$

лаконичные обозначения $1^{[2^0]}, 1^{[2^1]}, \ldots, 1^{[2^{n-2}]}, 1^{[2^{n-1}]}$ — это не приведёт к путанице, поскольку в данной работе рассматриваются только конечные последовательности.

Для представления координатных функций исследуемых полноцикловых пороговых подстановок в виде линейных рекуррентных последовательностей необходимо перейти к стандартному булеву представлению — для этого (-1) заменим на 0, а 1 оставим без изменений. Таким образом, предложенные в теореме 3 варианты рекурсивного продолжения полноцикловых подстановок в булевом представлении будут иметь вид

1) $\left(\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}0\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}0\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$;

2) $\left(\begin{pmatrix}0\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}0\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$;

3) $\left(\begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}0\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}0\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$;

4) $\left(\begin{pmatrix}0\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}0\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}1\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}1\\ \overline{\mathbf{a}}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\end{pmatrix}, \begin{pmatrix}1\\ \mathbf{a}_1^{\downarrow}\end{pmatrix}, \ldots, \begin{pmatrix}0\\ \mathbf{a}_{2^{n-1}}^{\downarrow}\end{pmatrix}\right)$

(черта сверху в данном случае означает стандартное отрицание в булевой логике).

Теорема 4. Пусть $u_1, \ldots, u_n$ — координатные последовательности булевого представления полноцикловой подстановки $\operatorname{sgn}(A_n\mathbf{x}^{\downarrow})$, построенной рекурсивным образом посредством $(n-1)$-кратного применения конструкций, предложенных в теореме 3. Тогда над полем $\mathbb{F}_2$ справедливы разложения

$$\begin{array}{rccccccccc}
u_1 = & 1^{[2^{n-1}]} & & + & & & + a_1 1^{[2^0]} & + b_1 1^{[0]},\\
u_2 = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & & & + a_2 1^{[2^0]} & + b_2 1^{[0]},\\
\ldots & & & & & & & & \\
u_{n-2} = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & \ldots & + 1^{[2^2]} & + a_{n-2} 1^{[2^0]} & + b_{n-2} 1^{[0]},\\
u_{n-1} = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & \ldots & + 1^{[2^2]} + 1^{[2^1]} & & + b_{n-1} 1^{[0]},\\
u_n = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & \ldots & + 1^{[2^2]} + 1^{[2^1]} & + 1^{[2^0]} & + b_n 1^{[0]},
\end{array}$$

в которых коэффициенты $a_1, \ldots, a_{n-2}, b_1, \ldots, b_n \in \mathbb{F}_2$ зависят от выбора типа рекурсивного продолжения на соответствующем шаге построения.

Доказательство. Проведём индукцию по n.

Б а з а при $n = 1$ очевидна: существует единственная полноцикловая подстановка на множестве $\{0, 1\}$ и её цикл может быть записан двумя способами: $(0, 1)$ и $(1, 0)$ — последовательности с разложениями $1^{[2^0]}$ и $1^{[2^0]} + 1^{[0]}$ соответственно.

Ш а г и н д у к ц и и при $n \geqslant 2$. Предположим, что имеется полноцикловая пороговая подстановка $\left(\mathbf{a}_1^{\downarrow}, \ldots, \mathbf{a}_{2^{n-2}}^{\downarrow}, \overline{\mathbf{a}}_1^{\downarrow}, \ldots, \overline{\mathbf{a}}_{2^{n-2}}^{\downarrow}\right)$ в булевом представлении с координатными последовательностями $u'_2, \ldots, u'_n$. Нетрудно видеть, что применение к данной подстановке какого-либо из вариантов рекурсивного продолжения, предложенных в теореме 3, приведёт к полноцикловой подстановке с координатными последовательностями

$$u_1 = 1^{[2^{n-1}]} + a\,1^{[2^0]} + b\,1^{[0]}, \quad u_2 = 1^{[2^{n-1}]} + u'_2, \quad \ldots, \quad u_n = 1^{[2^{n-1}]} + u'_n,$$

где коэффициенты $a, b \in \mathbb{F}_2$ зависят от выбранного способа рекурсивного продолжения. Здесь стоит отметить, что при $n = 2$ совпадают рекурсивные способы продолжения 1 и 3 (а также 2 и 4), поэтому коэффициент a обязательно равен 0. Для завершения шага индукции остаётся воспользоваться предположением индукции о строении координатных последовательностей $u'_2, \ldots, u'_n$. ■

Следствие 8. Рекурсивное $(n-1)$-кратное применение конструкций, предложенных в теореме 3, позволяет построить 2^{2n-3} различных полноцикловых пороговых подстановок множества $\{0,1\}^n$.

Доказательство. Существует единственная полноцикловая пороговая подстановка на множестве $\{0,1\}$. Применим к ней все возможные $(n-1)$-кратные комбинации рекурсивных продолжений, рассмотренных в теореме 3. В результате получим полноцикловые пороговые подстановки на множестве $\{0,1\}^n$, координатные функции которых обладают всеми возможными биномиальными разложениями, указанными в условии теоремы 4 — всего 2^{2n-2} различных вариантов. Однако необходимо отметить, что каждая полноцикловая пороговая подстановка, построенная в результате рекурсивных продолжений из теоремы 3, обладает двумя точками строгого абсолютного минимума и потому допускает два способа записи в соответствии с представлением из условия теоремы 3: $\left(\mathbf{a}_1^{\downarrow}, \ldots, \mathbf{a}_{2^{n-1}}^{\downarrow}, \overline{\mathbf{a}}_1^{\downarrow}, \ldots, \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}\right)$ и $\left(\overline{\mathbf{a}}_1^{\downarrow}, \ldots, \overline{\mathbf{a}}_{2^{n-1}}^{\downarrow}, \mathbf{a}_1^{\downarrow}, \ldots, \mathbf{a}_{2^{n-1}}^{\downarrow}\right)$. Значит, каждая такая подстановка может быть получена в результате применения двух $(n-1)$-кратных комбинаций рекурсивных продолжений, поэтому общее количество полноцикловых пороговых подстановок, которые возможно построить с применением результата теоремы 3, равно 2^{2n-3}. ■

В дополнение к результату следствия 8 заметим, что построенные с использованием теоремы 3 полноцикловые пороговые подстановки можно сопрягать подстановками из группы Джевонса — результатом такого действия будут полноцикловые пороговые подстановки. При этом из описания координатных функций, полученного в теореме 4, легко видеть, что перестановка координат обладает точным действием, в то время как инверсии не добавляют ни одного нового варианта (инверсия i-й координаты приводит к замене слагаемого $b_i 1^{[0]}$ в разложении i-й координатной последовательности на слагаемое $\overline{b}_i 1^{[0]}$). Значит, $n!2^{2n-3}$ — общее количество различных полноцикловых пороговых подстановок, которые можно получить в результате сопряжений элементами группы Джевонса множества всех полноцикловых пороговых подстановок, построенных в соответствии с теоремой 4. Однако, как показывает следующий результат, вся эта «арифметика» не имеет никакого смысла с точки зрения практического применения построенных подстановок.

Следствие 9. Произвольная полноцикловая пороговая подстановка, построенная рекурсивным образом посредством $(n-1)$-кратного применения конструкций, предложенных в теореме 3, в булевом представлении афинно эквивалентна полноцикловой подстановке, определяемой лексикографическим упорядочением векторов (3).

Доказательство. Пусть $u_1, \ldots, u_n$ — координатные последовательности булевого представления полноцикловой пороговой подстановки, построенной рекурсивным образом посредством $(n-1)$-кратного применения конструкций, предложенных в теореме 3. Нетрудно видеть, что система равенств

$$
\begin{array}{rllllllll}
u_1 = & 1^{[2^{n-1}]} & & + & & & + a_1 1^{[2^0]} & + b_1 1^{[0]}, \\
u_2 = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & & & + a_2 1^{[2^0]} & + b_2 1^{[0]}, \\
\dots & & & & & & & & \\
u_{n-2} = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & \dots & + 1^{[2^2]} & + a_{n-2} 1^{[2^0]} & + b_{n-2} 1^{[0]}, \\
u_{n-1} = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & \dots & + 1^{[2^2]} + 1^{[2^1]} & & + b_{n-1} 1^{[0]}, \\
u_n = & 1^{[2^{n-1}]} & + 1^{[2^{n-2}]} & + & \dots & + 1^{[2^2]} + 1^{[2^1]} & + 1^{[2^0]} & + b_n 1^{[0]}
\end{array}
$$

линейно эквивалентна над полем $\mathbb{F}_2$ системе

$$
\begin{array}{rlllll}
u'_1 = & 1^{[2^{n-1}]} & + & a_1 1^{[2^0]} & + & b_1 1^{[0]}, \\
u'_2 = & 1^{[2^{n-2}]} & + & (a_1 + a_2) 1^{[2^0]} & + & (b_1 + b_2) 1^{[0]}, \\
\dots & & & & & \\
u'_{n-2} = & 1^{[2^2]} & + & (a_{n-3} + a_{n-2}) 1^{[2^0]} & + & (b_{n-3} + b_{n-2}) 1^{[0]}, \\
u'_{n-1} = & 1^{[2^1]} & + & a_{n-2} 1^{[2^0]} & + & (b_{n-2} + b_{n-1}) 1^{[0]}, \\
u'_n = & & & 1^{[2^0]} & + & (b_{n-1} + b_n) 1^{[0]},
\end{array}
$$

которая, в свою очередь, линейно эквивалентна системе соотношений

$$
\begin{array}{rlll}
u''_1 = & 1^{[2^{n-1}]} & + & (b_1 + a_1(b_{n-1} + b_n)) 1^{[0]}, \\
u''_2 = & 1^{[2^{n-2}]} & + & (b_1 + b_2 + (a_1 + a_2)(b_{n-1} + b_n)) 1^{[0]}, \\
\dots & & & \\
u''_{n-2} = & 1^{[2^2]} & + & (b_{n-3} + b_{n-2} + (a_{n-3} + b_{n-2})(b_{n-1} + b_n)) 1^{[0]}, \\
u''_{n-1} = & 1^{[2^1]} & + & (b_{n-2} + b_{n-1} + a_{n-2}(b_{n-1} + b_n)) 1^{[0]}, \\
u''_n = & 1^{[2^0]} & + & (b_{n-1} + b_n) 1^{[0]}.
\end{array}
$$

Для завершения доказательства остаётся заметить, что биномиальная последовательность $1^{[0]}$ по существу является константой 1. ■

Итак, согласно следствию 9, все полноцикловые пороговые подстановки, которые можно получить рекурсивным образом посредством $(n-1)$-кратного применения конструкций, предложенных в теореме 3, аффинно эквивалентны счётчиковой последовательности (3) и соответственно также «провальны» по ряду важных криптографических характеристик (алгебраическая степень, нелинейность и др.) [11]. Следовательно, в криптографических приложениях указанные полноцикловые подстановки имеет смысл использовать исключительно для генерации первичных или управляющих последовательностей, к которым обязательно будет применено усложнение.

ЛИТЕРАТУРА

1. *Дертоузос М.* Пороговая логика. М.: Мир, 1967.
2. *Бутаков Е. А.* Методы синтеза релейных устройств из пороговых элементов. М.: Энергия, 1970.
3. *Зуев Ю. А.* Пороговые функции и пороговые представления булевых функций // Математические вопросы кибернетики. Вып. 5. М.: Наука, 1994.
4. *Никонов В. Г., Сидоров Е. С.* О способе построения взаимно однозначных отображений при помощи квазиадамаровых матриц // Лесной вестник. 2009. № 2. С. 155–158.
5. *Никонов В. Г., Литвиненко В. С.* Геометрический подход к доказательству биективности одного координатно-порогового отображения // Comp. Nanotechnol. 2015. No. 1. P. 26–31.
6. *Никонов В. Г., Литвиненко В. С.* О биективности преобразований, задаваемых квазиадамаровыми матрицами // Comp. Nanotechnol. 2016. No. 1. P. 6–13.

7. *Никонов В. Г., Кононов С. А.* О некоторых свойствах квазиадамаровых матриц, задающих биективные преобразования // Comp. Nanotechnol. 2022. V. 9. No. 1. P. 32–38.
8. *Никонов В. Г., Зобов А. И.* Построение обратимого полноциклового преобразования в пороговом базисе // Comp. Nanotechnol. 2023. V. 10. No. 2. P. 36–41.
9. *Шурупов А. Н.* Критерии функциональной разделимости квадратичных булевых пороговых функций // Прикладная дискретная математика. 2015. № 2(28). С. 37–45.
10. *Шурупов А. Н.* Некоторые структурные свойства квадратичных булевых пороговых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 48–51.
11. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
12. *Garey M. R. and Johnson D. S.* Computers and Intractability: A Guide to the Theory of NP-Completeness. N.Y.: W. H. Freeman and Company, 1979.
13. *MacWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Amsterdam: Elsevier, 1977.
14. *Лидл Р., Нидерайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988. 430 с.
15. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: учебник для вузов. 5-е изд. СПб.: Лань, 2024. 608 с.

REFERENCES

1. *Dertouzos M. L.* Threshold Logic. Cambridge, MIT Press, 1965.
2. *Butakov E. A.* Metody sinteza releynykh ustroystv iz porogovykh elementov [Methods of Synthesis of Relay Devices from Threshold Elements]. Moscow, Energiya, 1970. (in Russian)
3. *Zuev Yu. A.* Porogovye funktsii i porogovye predstavleniya bulevykh funktsiy [Threshold functions and threshold representations of Boolean functions]. Matematicheskie Voprosy Kibernetiki, iss. 5. Moscow, Nauka, 1994. (in Russian)
4. *Nikonov V. G. and Sidorov E. S.* O sposobe postroeniya vzaimno odnoznachnykh otobrazheniy pri pomoshchi kvaziadamarovykh matrits [On a method for constructing bijective mappings using quasi-Hadamard matrices]. Lesnoy Vestnik, 2009, no. 2, pp. 155–158. (in Russian)
5. *Nikonov V. G. and Litvinenko V. S.* Geometricheskiy podkhod k dokazatel'stvu biektivnosti odnogo koordinatno-porogovogo otobrazheniya [Geometrical approach to the argumentum of bijection of one coordinate-threshold reflection]. Comp. Nanotechnol., 2015, no. 1, pp. 26–31. (in Russian)
6. *Nikonov V. G. and Litvinenko V. S.* O biektivnosti preobrazovaniy, zadavaemykh kvaziadamarovymi matritsami [About bijectivity of transformations determined by quasi-Hadamard matrixes]. Comp. Nanotechnol., 2016, no. 1, pp. 6–13. (in Russian)
7. *Nikonov V. G. and Kononov S. A.* O nekotorykh svoystvakh kvaziadamarovykh matrits, zadayushchikh biektivnye preobrazovaniya [About some properties of quasi-hadamard matrices defining bijective transformations]. Comp. Nanotechnol., 2022, vol. 9, no. 1, pp. 32–38. (in Russian)
8. *Nikonov V. G. and Zobov A. I.* Postroenie obratimogo polnotsiklovogo preobrazovaniya v porogovom bazise [Construction of a reversible full-cycle transformation in a threshold basis]. Comp. Nanotechnol., 2023, vol. 10, no. 2, pp. 36–41. (in Russian)
9. *Shurupov A. N.* Kriterii funktsional'noy razdelimosti kvadratichnykh bulevykh porogovykh funktsiy [Functional decomposability criteria for quadratic threshold Boolean functions]. Prikladnaya Diskretnaya Matematika, 2015, no. 2(28), pp. 37–45. (in Russian)
10. *Shurupov A. N.* Nekotorye strukturnye svoystva kvadratichnykh bulevykh porogovykh funktsiy [Some structural properties of quadratic Boolean threshold functions]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2015, no. 8, pp. 48–51. (in Russian)

11. *Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2012. 584 p. (in Russian)
12. *Garey M. R. and Johnson D. S.* Computers and Intractability: A Guide to the Theory of NP-Completeness. N.Y., W. H. Freeman and Company, 1979.
13. *MacWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Amsterdam, Elsevier, 1977.
14. *Lidl R. and Niederreiter H.* Finite Fields, 2nd ed. Cambridge, Cambridge University Press, 1996.
15. *Glukhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra [Algebra]. Saint Petersburg, Lan Publ., 2024. 608 p. (in Russian)