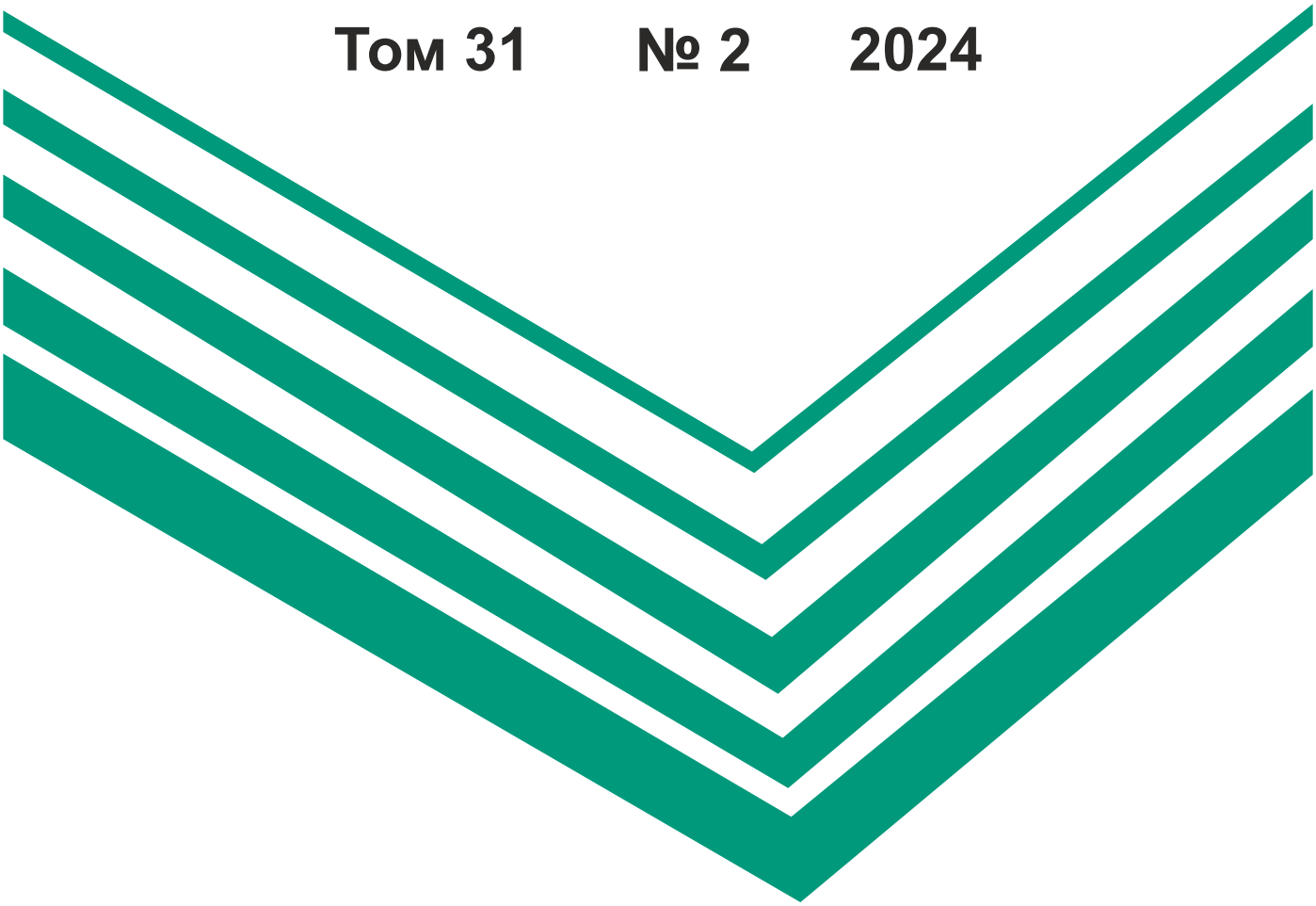
ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 31 № 2 2024



Новосибирск
Издательство Института математики

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель–июнь 2024. Т. 31, № 2. С. 108–135

УДК 519.7 DOI: 10.33048/daio.2024.31.769

РАЗНОСТИ ПО МОДУЛЮ 2^n ДЛЯ ARX-ПРЕОБРАЗОВАНИЙ, ВЕРОЯТНОСТЬ КОТОРЫХ БОЛЬШЕ 1/4

А. С. Мокроусов [a], *Н. А. Коломеец* [b]

Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия
E-mail: [a] settingx@mail.ru, [b] kolomeec@math.nsc.ru

Аннотация. Рассматриваются разностные характеристики по модулю 2^n для преобразований $x \oplus y$ и $(x \oplus y) \lll r$, где $x, y \in \mathbb{Z}_2^n$ и $1 \leqslant r < n$. Эти характеристики применяются при разностном криптоанализе шифров архитектуры ARX, использующих в качестве операций только сложение по модулю 2^n, побитовое исключающее «или» (XOR, $\oplus$) и циклический сдвиг битов на r позиций ($\lll r$). Получена полная характеризация разностей, вероятность которых больше 1/4. Возможными значениями вероятности при этом условии являются $1/3 + 4^{2-i}/6$ для обоих преобразований, где $i \in \{1, \ldots, n\}$. Описаны разности, на которых достигается каждое из значений, и подсчитано их число. Найдено общее число разностей с приведёнными вероятностями: $48n - 68$ для $x \oplus y$ и $24n - 30$ для $(x \oplus y) \lll r$, где $n \geqslant 2$. Также дано сравнение разностных характеристик в контексте рассматриваемого ограничения на вероятность. Табл. 6, библиогр. 23.

Ключевые слова: ARX-схема, разностная характеристика, сложение по модулю, XOR, циклический сдвиг битов.

Введение

Одним из подходов к построению криптографических примитивов являются ARX-схемы, комбинирующие сложение по модулю 2^n ($\boxplus$), побитовое исключающее «или» (XOR, $\oplus$) и циклический сдвиг битов в векторе $x \in \mathbb{Z}_2^n$ на r позиций в сторону старших разрядов ($x \lll r$). Приведём как примеры FEAL [1], Skein [2], Speck [3], Salsa20 [4], ChaCha [5], CHAM [6, 7], Chaskey [8]. Важно, чтобы шифр был стойким к разностному криптоанализу [9], основа которого — изучение преобразования разностей алгоритмом шифрования. Разности могут рассматриваться, например, относительно $\oplus$, $\boxplus$, какой-нибудь другой операции или вообще быть смешанными (см. [10–14]). Будем рассматривать разность по модулю 2^n,

т. е. относительно $\boxplus$. Соответствующая разностная характеристика adp^f для функции вида $f\colon \left(\mathbb{Z}_2^n\right)^k \to \mathbb{Z}_2^n$ определяется формулой

$$\mathrm{adp}^f(\alpha_1, \ldots, \alpha_k \to \alpha_{k+1}) = \\ = \Pr[f(x_1 \boxplus \alpha_1, \ldots, x_k \boxplus \alpha_k) = \alpha_{k+1} \boxplus f(x_1, \ldots, x_k)],$$

где $x_1, \ldots, x_k$ независимы и равномерно распределены на $\mathbb{Z}_2^n$. Будем называть $\alpha_1, \ldots, \alpha_{k+1} \in \mathbb{Z}_2^n$ *набором разностей,* а значение характеристики $\mathrm{adp}^f(\alpha_1, \ldots, \alpha_k \to \alpha_{k+1})$ — его *вероятностью* относительно f. Как правило, для построения атак используются цепочки разностей, в которых каждый следующий элемент максимизирует значение разностной характеристики для соответствующей базовой операции в схеме шифра. Отметим, что использование характеристик для композиций может повысить достоверность метода, так как универсальный метод их вычисления по базовым операциям неточен.

В настоящей работе достигается полная классификация наборов разностей для характеристик $\mathrm{adp}^{\oplus}$ и $\mathrm{adp}^{\mathrm{XR}}$, вероятность которых больше $\frac{1}{4}$. Это разностные характеристики для преобразований $x \oplus y$ и $(x \oplus y) \lll r$ соответственно, где $x, y \in \mathbb{Z}_2^n$ и $1 \leqslant r < n$. Отметим, что $\mathrm{adp}^{\lll}$ исследовалась, например, в [15, 16], $\mathrm{adp}^{\oplus}$ — в [17, 18], а $\mathrm{adp}^{\mathrm{XR}}$ — в [19, 20]. Известны эффективные способы их вычисления, а в некоторых случаях — и их максимумов при определённых ограничениях. Ниже доказано, что значениями $\mathrm{adp}^{\oplus}$ и $\mathrm{adp}^{\mathrm{XR}}$, превышающими $\frac{1}{4}$, являются вероятности $p_i = \frac{1}{3} + \frac{4^{2-i}}{6}$, где $i \in \{1, \ldots, n\}$. Оказалось, что все наборы разностей, на которых данные значения достигаются, можно свести к одному набору для $\mathrm{adp}^{\oplus}$ и трём наборам для $\mathrm{adp}^{\mathrm{XR}}$, используя известные преобразования разностей, сохраняющие значения характеристик. Для каждой из перечисленных вероятностей конструктивно подсчитано число наборов разностей, а также их число в целом: $48n - 68$ для $\mathrm{adp}^{\oplus}$ и $24n - 30$ для $\mathrm{adp}^{\mathrm{XR}}$ при $n \geqslant 2$. Полученные результаты показывают, что несмотря на некоторое сходство, например спектр значений, характеристика $\mathrm{adp}^{\mathrm{XR}}$ устроена сложнее даже с учётом рассматриваемого ограничения. Наличие циклического сдвига вне зависимости от значения параметра r уменьшает число наборов разностей с высокой вероятностью почти в два раза.

Работа имеет следующую структуру. Базовые определения и утверждения даны в разд. 1. В разд. 2 приведена теорема 1, согласно которой $\left\{\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \mid \alpha, \beta, \gamma \in \mathbb{Z}_2^n\right\} \cap \left(\frac{1}{4}, 1\right] = \{p_1, \ldots, p_n\}$. Более того, если $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = p_i$, то тройку-набор разностей (α, β, γ) можно привести к тройке $(2^{n-i}, 2^{n-i}, 0)$ преобразованиями из утверждения 1. Их можно назвать симметриями аргументов: для $\mathrm{adp}^{\oplus}$ это перестановки разностей в тройке, инверсия наиболее значимых битов у любых двух

элементов тройки и замена любых разностей обратными им по модулю 2^n. В разд. 3 описаны все пары, которые приводятся к данному виду (теорема 2 и табл. 1 и 2), а также подсчитано их число (следствия 2 и 3). Разд. 4 содержит дополнительные определения и утверждения, необходимые для работы с $\mathrm{adp}^{\mathrm{XR}}$, а в разд. 5 доказаны некоторые вспомогательные леммы. Наконец, в разд. 6 приводится теорема 3 о том, что спектры значений $\mathrm{adp}^{\oplus}$ и $\mathrm{adp}^{\mathrm{XR}}$, превышающих $\frac{1}{4}$, совпадают. Более того, она показывает, что если $\mathrm{adp}^{\mathrm{XR}}(\alpha, \beta \xrightarrow{r} \gamma) = p_i$, то (α, β, γ) преобразованиями из утверждения 7 приводится к одной из трёх троек. Отметим, что среди них присутствует тройка $(2^{n-i}, 2^{n-i}, 0)$ и набор, отличный от неё как минимум при $i = 2$ (утверждение 8). Тем не менее, из $3n$ битов их двоичного представления только два единичных, что, впрочем, меняется при применении симметрий аргументов. Следствие 4 и табл. 6 описывают все наборы разностей, приводимые к данным тройкам. Число наборов для каждого p_i и их общее число найдены в следствиях 5 и 6.

1. Определения

1.1. Двоичные векторы. Пусть $\mathbb{Z}_2^n$ — n-мерное линейное пространство двоичных векторов. Поскольку ARX-схемы комбинируют операции $\oplus$ и $\boxplus$, будем ассоциировать с вектором $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$ целое число

$$2^{n-1}x_1 + 2^{n-2}x_2 + \cdots + 2^0 x_n,$$

т. е. биты слева соответствуют старшим разрядам числа, а справа — младшим. Под $x + y$, где $x, y \in \mathbb{Z}_2^n$, будем подразумевать сложение соответствующих x и y целых чисел по модулю 2^n, приводя остатки к множеству $\{0, \ldots, 2^n - 1\}$. Аналогично $-x$ является противоположным к ассоциированному с x числу относительно сложения по модулю 2^n. Будем использовать как векторную, так и целочисленную нотацию. Например, вектор $(1, 0, \ldots, 0)$ и число 2^{n-1} рассматриваем как один и тот же элемент $\mathbb{Z}_2^n$.

Будем говорить, что $x \preceq y$, если $x_i \leqslant y_i$ для всех $i \in \{1, \ldots, n\}$. Обозначим через $(x, z) = (x_1, \ldots, x_n, z_1, \ldots, z_m)$ *конкатенацию* вектора $x \in \mathbb{Z}_2^n$ с вектором $z \in \mathbb{Z}_2^m$, разряды x в ней старшие. В случае $z \in \mathbb{Z}_2$ будем записывать её как xz, что в целочисленной нотации эквивалентно $xz = 2x + z$. *Вес Хэмминга* $\mathrm{wt}(x)$ вектора x — число его ненулевых координат. Положим $\overline{x} = (x_1 \oplus 1, x_2 \oplus 1, \ldots, x_n \oplus 1)$, а для $a \in \mathbb{Z}_2$ определим также $x^{[a]}$ следующим образом:

$$x^{[a]} = \begin{cases} x, & \text{если } a = 0, \\ \overline{x}, & \text{если } a = 1. \end{cases}$$

1.2. Разностные характеристики и восьмеричные слова. Рассматриваемые ниже разностные характеристики относительно сложения по модулю 2^n для преобразований $x \oplus y$ и $(x \oplus y) \lll r$, где $1 \leqslant r < n$, определяются формулами

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \frac{1}{4^n}\big|\{x, y \in \mathbb{Z}_2^n \mid (x+\alpha) \oplus (y+\beta) = \gamma + (x \oplus y)\}\big|,$$

$$\mathrm{adp}^{\mathrm{XR}}(\alpha, \beta \xrightarrow{r} \gamma) = \frac{1}{4^n}\big|\{x, y \in \mathbb{Z}_2^n \mid ((x+\alpha) \oplus (y+\beta)) \lll r = \gamma + ((x \oplus y) \lll r)\}\big|.$$

Для удобства будем представлять тройки $(\alpha, \beta, \gamma) \in \big(\mathbb{Z}_2^n\big)^3$ в виде восьмеричного слова $\omega(\alpha, \beta, \gamma) \in \mathbb{O}^n$, определив

$$\omega(\alpha, \beta, \gamma) = (4\alpha_1 + 2\beta_1 + \gamma_1, \ldots, 4\alpha_n + 2\beta_n + \gamma_n).$$

Введём и обратные преобразования: $\alpha(\omega) = \alpha$, $\beta(\omega) = \beta$ и $\gamma(\omega) = \gamma$, если $\omega = \omega(\alpha, \beta, \gamma)$. Аналогично двоичным векторам множество $\mathbb{O}$ будем рассматривать одновременно и как $\mathbb{Z}_2^3$, и как $\{0, \ldots, 7\}$. В качестве аргументов разностных характеристик будем использовать как тройки векторов, так и слова: например $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\omega(\alpha, \beta, \gamma))$.

Записывать слова $\omega \in \mathbb{O}^n$ будем коротко: например 030^{n-2} вместо $(0, 3, 0, \ldots, 0)$. В некоторых случаях запись может содержать *шаблонные символы* `e`, `d` и `*`, т. е. являться *шаблоном*. Например $\omega = *0^{n-1}$ означает, что ω_1 может быть любым, а $\omega_2 = \omega_3 = \cdots = \omega_n = 0$. Аналогично при $\omega = \mathtt{e}0^{n-1}$ требуем, чтобы $\omega_1 \in \{0, 3, 5, 6\}$, т. е. чётность $\mathrm{wt}(\omega_1) = \mathrm{wt}(\alpha_1, \beta_1, \gamma_1)$. И наоборот, $\omega_1 \in \{1, 2, 4, 7\}$ при $\omega = \mathtt{d}0^{n-1}$. Как и в примерах, будем использовать шаблонные символы только в старшем разряде. Отметим, что подобные сокращения не будут использоваться для двоичных векторов.

1.3. Преобразования слов и троек. Определим следующие преобразования на тройках $(\alpha, \beta, \gamma) \in \big(\mathbb{Z}_2^n\big)^3$.

• $\mathcal{T}_{\alpha\beta}\colon (\alpha, \beta, \gamma) \mapsto (\beta, \alpha, \gamma)$. Аналогично задаются $\mathcal{T}_{\alpha\gamma}$ и $\mathcal{T}_{\beta\gamma}$, будем обозначать их через $\mathcal{T}_*$.

• $\mathcal{I}_{\alpha\beta}\colon (\alpha, \beta, \gamma) \mapsto (\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1}, \gamma)$. Аналогично задаются $\mathcal{I}_{\alpha\gamma}$ и $\mathcal{I}_{\beta\gamma}$, будем обозначать их через $\mathcal{I}_*$.

• $\mathcal{S}_{\alpha}\colon (\alpha, \beta, \gamma) \mapsto (-\alpha, \beta, \gamma)$. Аналогично задаются $\mathcal{S}_{\beta}$, $\mathcal{S}_{\gamma}$ и их композиции $\mathcal{S}_{\alpha\beta}$, $\mathcal{S}_{\alpha\gamma}$, $\mathcal{S}_{\beta\gamma}$ и $\mathcal{S}_{\alpha\beta\gamma}$. Будем обозначать их через $\mathcal{S}_*$.

Множество всех композиций преобразований вида $\mathcal{T}_*$, $\mathcal{I}_*$, $\mathcal{S}_*$ обозначим через $\mathcal{E}$, а через id — тождественное преобразование. Для $\mathcal{A} \subseteq \mathcal{E}$

$$\mathcal{A}(\alpha, \beta, \gamma) = \{\xi(\alpha, \beta, \gamma) \mid \xi \in \mathcal{A}\}.$$

Поскольку все «именованные» преобразования являются инволюциями, то $\mathcal{E}$ — группа. Отметим, что элементы этой группы сохраняют значение

$\mathrm{adp}^{\oplus}$. Будем применять описанные выше преобразования как к тройкам (α, β, γ), так и к соответствующим им словам $\omega(\alpha, \beta, \gamma) \in \mathbb{O}^n$.

1.4. Необходимые теоремы для работы с $\mathrm{adp}^{\oplus}$. Для подсчёта $\mathrm{adp}^{\oplus}$ будем использовать три факта. Во-первых, очевидное в случае $\alpha, \beta, \gamma \in \mathbb{Z}_2$ утверждение:

$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \begin{cases} 1, & \text{если } \mathrm{wt}(\alpha, \beta, \gamma) \text{ чётный}, \\ 0 & \text{иначе.} \end{cases} \tag{1}$$

Во-вторых, преобразования, описанные в [21, утверждения 1–3].

Утверждение 1 [21]**.** *Для любых $\xi \in \mathcal{E}$, $\omega \in \mathbb{O}^n$ справедливо равенство* $\mathrm{adp}^{\oplus}(\omega) = \mathrm{adp}^{\oplus}(\xi(\omega))$.

В-третьих, рекуррентные формулы, доказанные в [21, теорема 3]. Приведём соответствующее утверждение в более компактном виде, используя введённые ранее обозначения.

Утверждение 2 [21]**.** *Пусть $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$ и $e \in \mathbb{Z}_2^3$. Тогда при чётном* $\mathrm{wt}(e)$ *справедливо*

$$\mathrm{adp}^{\oplus}(\alpha e_1, \beta e_2 \to \gamma e_3) = \frac{1}{2^{\mathrm{wt}(e)}} \sum_{q \in \mathbb{Z}_2^3,\, q \preceq e} \mathrm{adp}^{\oplus}(\alpha^{[q_1]}, \beta^{[q_2]} \to \gamma^{[q_3]}).$$

Если $\mathrm{wt}(e)$ *нечётный, то* $\mathrm{adp}^{\oplus}(\alpha e_1, \beta e_2 \to \gamma e_3) = 0$.

Использовать его будем следующим образом. Во-первых,

$$\mathrm{adp}^{\oplus}(\alpha 0, \beta 0 \to \gamma 0) = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma). \tag{2}$$

Во-вторых, $e_1 \oplus e_2 \oplus e_3 = 1$ равносильно нечётности $\mathrm{wt}(e)$ и влечёт

$$\mathrm{adp}^{\oplus}(\alpha e_1, \beta e_2 \to \gamma e_3) = 0. \tag{3}$$

В третьих,

$$\mathrm{adp}^{\oplus}(\alpha 0, \beta 1 \to \gamma 1) = \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \overline{\gamma}) + \\ + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \overline{\beta} \to \gamma) + \frac{1}{4}\mathrm{adp}^{\oplus}(\alpha, \beta \to \overline{\gamma}). \tag{4}$$

Более того, как минимум два из четырёх слагаемых выше нулевые. Действительно,

$$\alpha_n \oplus \beta_n \oplus \gamma_n = \alpha_n \oplus \overline{\beta}_n \oplus \overline{\gamma}_n = \alpha_n \oplus \overline{\beta}_n \oplus \gamma_n \oplus 1 = \alpha_n \oplus \beta_n \oplus \overline{\gamma}_n \oplus 1,$$

что по предыдущему пункту зануляет либо два первых слагаемых, либо два последних. Также в силу утверждения 1 все оставшиеся случаи $\mathrm{wt}(e) = 2$ можно получить из описанного выше перестановкой аргументов.

2. Значения $\mathrm{adp}^{\oplus}$, превышающие $1/4$

В этом разделе рассматриваются наборы разностей $(\alpha, \beta, \gamma) \in \left(\mathbb{Z}_2^n\right)^3$ и их вероятности $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma)$ такие, что $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > \frac{1}{4}$. Начнём с определения последовательности, элементы которой и будут искомыми вероятностями.

Определение 1. Определим бесконечную последовательность рациональных чисел $\{p_i\}$ следующим образом:

$$p_i = \frac{1}{3} + \frac{4^{2-i}}{6}, \quad i \geqslant 1.$$

Сразу отметим её важные свойства.

Утверждение 3. *Элементы последовательности $\{p_i\}$ обладают следующими свойствами:*

1) $p_1 = 1$, $p_2 = \frac{1}{2}$, $p_3 = \frac{3}{8}$, $p_4 = \frac{11}{32}$, $p_5 = \frac{43}{128}$;

2) *при $i \geqslant 2$ справедливо*

$$p_i = \frac{1}{4} + \cdots + \frac{1}{4^{i-1}} + \frac{1}{4^{i-1}};$$

3) $p_{i+1} = \frac{1}{4} + \frac{1}{4} p_i$ *для всех* $i \geqslant 1$;

4) *последовательность p_i строго убывает и сходится к $\frac{1}{3}$, при этом $p_i > \frac{1}{3}$ для всех $i \geqslant 1$.*

Доказательство. Значения p_1, p_2, p_3, p_4 и p_5 нетрудно вычислить по определению. Для доказательства п. 2 достаточно применить формулу суммы членов геометрической прогрессии. Действительно,

$$\frac{1}{4} + \cdots + \frac{1}{4^{i-1}} + \frac{1}{4^{i-1}} = \frac{4}{3}\left(\frac{1}{4} - \frac{1}{4^i}\right) + \frac{1}{4^{i-1}} = \frac{1}{3} + \frac{3-1}{3 \cdot 4^{i-1}} = \frac{1}{3} + \frac{4^{2-i}}{6}.$$

П. 3 следует из второго, а п. 4 очевидно следует из определения. Утверждение 3 доказано.

Далее докажем несколько лемм, задающих ограничения на аргументы $\mathrm{adp}^{\oplus}$, при которых значение этой характеристики больше $\frac{1}{4}$. Следующее утверждение можно найти в [17]. Приведём его с доказательством, демонстрируя удобство использования рекуррентных формул.

Лемма 1. *Если $\omega \in \mathbb{O}^n$, то $\mathrm{adp}^{\oplus}(\omega) = 1$ тогда и только тогда, когда $\omega = \mathsf{e}0^{n-1}$. Более того, не существует $\omega \in \mathbb{O}^n$ таких, что $\frac{1}{2} < \mathrm{adp}^{\oplus}(\omega) < 1$.*

Доказательство. Предположим, напротив, что $n > 1$, $\omega_n \neq 0$ и при этом $\mathrm{adp}^{\oplus}(\omega) = 1$. Если $\mathrm{wt}(\omega_n)$ нечётный, то $\mathrm{adp}^{\oplus}(\omega) = 0$ в силу (3). Таким образом, остаётся только случай $\mathrm{wt}(\omega_n) = 2$, и можно применить (4):

$$\mathrm{adp}^{\oplus}(\omega) \leqslant \frac{1}{4} \cdot 1 + \frac{1}{4} \cdot 1 + \frac{1}{4} \cdot 0 + \frac{1}{4} \cdot 0 = \frac{1}{2};$$

противоречие. Значит, $n = 1$ или $\omega_n = 0$. Далее, применяя формулу (2), получаем, что только ω_1 может быть ненулевой. Равенство (1) завершает доказательство. Лемма 1 доказана.

Лемма 2. *Пусть* $1 \leqslant i \leqslant n$. *Тогда* $\mathrm{adp}^{\oplus}(0^{i-1}30^{n-i}) = p_i$.

Доказательство. В силу (2) $\mathrm{adp}^{\oplus}(0^{i-1}30^{n-i}) = \mathrm{adp}^{\oplus}(0^{i-1}3)$. Далее воспользуемся индукцией по i.

База индукции $i = 1$: $\mathrm{adp}^{\oplus}(3) = \mathrm{adp}^{\oplus}(0) = 1 = p_1$ по (1).

Шаг индукции: предположим, что утверждение справедливо для i, и докажем его для $i + 1$. Используя (4), получаем

$$\mathrm{adp}^{\oplus}(0^i3) = \frac{1}{4}\mathrm{adp}^{\oplus}(0^i) + \frac{1}{4}\mathrm{adp}^{\oplus}(3^i) + \\ + \frac{1}{4}\mathrm{adp}^{\oplus}(2^i) + \frac{1}{4}\mathrm{adp}^{\oplus}(1^i) = \frac{1}{4} + \frac{1}{4}\mathrm{adp}^{\oplus}(3^i),$$

так как $\mathrm{wt}(1) = \mathrm{wt}(2) = 1$ (см. (3)). В то же время $\mathcal{S}_{\beta\gamma}(3^i) = 0^{i-1}3$. Таким образом, $\mathrm{adp}^{\oplus}(3^i) = \mathrm{adp}^{\oplus}(0^{i-1}3) = p_i$ по утверждению 1 и индукционному предположению. При этом утверждение 3 гарантирует, что $\frac{1}{4} + \frac{1}{4}p_i = p_{i+1}$. Лемма 2 доказана.

Лемма 3. *Пусть* $\omega \in \mathbb{O}^n$, $\omega \neq *0^{n-1}$ *и* $\mathrm{adp}^{\oplus}(\omega) > 0$. *Тогда существует* $\xi \in \mathcal{E}$ *такое, что* $\xi(\omega) = 0u30^{n-m-2}$, *где* $u \in \mathbb{O}^m$ *для некоторого* $m \geqslant 0$.

Доказательство. Поскольку $\omega \neq *0^{n-1}$, хотя бы одно из α, β, γ не лежит в множестве $\{0, 2^{n-1}\}$. Без ограничения общности положим, что $\gamma \notin \{0, 2^{n-1}\}$.

Далее, используя преобразования $\mathcal{I}_*$, можно привести ω_1 к значению 0 или 1, не изменяя $\omega_2, \ldots, \omega_n$. Если получим $\omega_1 = 1$, то дополнительное применение $\mathcal{S}_\gamma$ приведёт к $\omega_1 = 0$ в силу $\gamma \notin \{0, 2^{n-1}\}$.

Заметим, что $\gamma \notin \{0, 2^{n-1}\}$ гарантирует существование t такого, что $2 \leqslant t \leqslant n$, $\omega_t \neq 0$ и $\omega_{t+1} = \omega_{t+2} = \cdots = \omega_n = 0$. По утверждению 2 нечётный $\mathrm{wt}(\omega_t)$ означает, что $\mathrm{adp}^{\oplus}(\omega) = 0$, поэтому остаётся только $\mathrm{wt}(\omega_t) = 2$, т. е. $\omega_t \in \{3, 5, 6\}$. Применяя к ω преобразования $\mathcal{T}_*$, легко привести ω к виду $0u30^{n-t}$, где $u \in \mathbb{O}^{t-2}$. Лемма 3 доказана.

Лемма 4. *Если* $k \geqslant 0$ *и* $u \in \mathbb{O}^m$, *то* $\mathrm{adp}^{\oplus}(0u30^k) > \frac{1}{4}$ *тогда и только тогда, когда* $u \in \{0^m, 3^m\}$.

Доказательство. Так как $\mathrm{adp}^{\oplus}(0u30^k) = \mathrm{adp}^{\oplus}(0u3)$ в силу (2), можно полагать, что $k = 0$. Пусть также $u = \omega(\alpha, \beta, \gamma)$ для некоторых $\alpha, \beta, \gamma \in \mathbb{Z}_2^m$. По рекуррентной формуле (4) получаем

$$\mathrm{adp}^{\oplus}(0u3) = \frac{1}{4}\mathrm{adp}^{\oplus}(0u) + \frac{1}{4}\mathrm{adp}^{\oplus}(3u_1) + \frac{1}{4}\mathrm{adp}^{\oplus}(2u_2) + \frac{1}{4}\mathrm{adp}^{\oplus}(1u_3),$$

где $u_1 = \omega(\alpha, \overline{\beta}, \overline{\gamma})$, $u_2 = \omega(\alpha, \overline{\beta}, \gamma)$ и $u_3 = \omega(\alpha, \beta, \overline{\gamma})$. Рассмотрим четыре значения из формулы: $\mathrm{adp}^{\oplus}(0u)$, $\mathrm{adp}^{\oplus}(3u_1)$, $\mathrm{adp}^{\oplus}(2u_2)$ и $\mathrm{adp}^{\oplus}(1u_3)$. Как минимум два из них нулевые по (3) и (1), поэтому для $\mathrm{adp}^{\oplus}(0u3) > \frac{1}{4}$ необходимо, чтобы хотя бы одно из оставшихся значений было равно 1. Действительно, в противном случае по лемме 1 имеем

$$\mathrm{adp}^{\oplus}(0u3) \leqslant \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} + \frac{1}{4} \cdot 0 + \frac{1}{4} \cdot 0 = \frac{1}{4}.$$

Проверим все возможные варианты, пользуясь леммой 1:

- $\mathrm{adp}^{\oplus}(0u) = 1$, тогда $u = 0^m$ и $3u_1 = 33^m$, т. е. $\mathrm{adp}^{\oplus}(0u3) > \frac{1}{4}$;
- $\mathrm{adp}^{\oplus}(3u_1) = 1$, тогда $u_1 = 0^m$, $u = 3^m$ и $0u = 03^m$, что влечёт $\mathrm{adp}^{\oplus}(0u3) > \frac{1}{4}$;
- $\mathrm{adp}^{\oplus}(1u_2) \neq 1$ и $\mathrm{adp}^{\oplus}(2u_3) \neq 1$, поскольку $1, 2 \notin \{0, 3, 5, 6\}$.

Таким образом, подходит либо $u = 0^m$, либо $u = 3^m$. Лемма 4 доказана.

Лемма 5. *Если $\omega \in \mathbb{O}^n$, то $\mathrm{adp}^{\oplus}(\omega) > \frac{1}{4}$ тогда и только тогда, когда $\omega = \xi(0^{i-1}30^{n-i})$ для некоторых $i \in \{1, \ldots, n\}$ и $\xi \in \mathcal{E}$.*

Доказательство. Если $\omega = s0^{n-1}$, $s \in \mathbb{O}$, то $\mathrm{adp}^{\oplus}(\omega) = 1$ при $s \in \{0, 3, 5, 6\}$ и $\mathrm{adp}^{\oplus}(\omega) = 0$ иначе (см. лемму 1 и равенства (1), (2)), причём

$$\mathcal{I}_{\beta\gamma}(00^{n-1}) = \mathcal{I}_{\alpha\beta}(50^{n-1}) = \mathcal{I}_{\alpha\gamma}(60^{n-1}) = 30^{n-1},$$

что означает верность утверждения леммы для данного ω.

Теперь в силу леммы 3 можно полагать, что $\omega = 0u30^{n-m-2}$, где $u \in \mathbb{O}^m$ и $m \geqslant 0$. По лемме 4 неравенство $\mathrm{adp}^{\oplus}(\omega) > \frac{1}{4}$ эквивалентно $u \in \{0^m, 3^m\}$, т. е. $\omega = 00^m30^{n-m-2}$ или $\omega = 03^m30^{n-m-2}$. Осталось заметить, что

$$00^m30^{n-m-2} \xrightarrow{\mathcal{I}_{\beta\gamma}} 30^m30^{n-m-2} \xrightarrow{\mathcal{S}_{\beta\gamma}} 03^m30^{n-m-2}.$$

Таким образом, $\omega = \xi(0^{m+1}30^{n-m-2})$ для некоторого $\xi \in \mathcal{E}$. Лемма 5 доказана.

Перейдём к теореме о значениях $\mathrm{adp}^{\oplus}$, превышающих $\frac{1}{4}$.

Теорема 1. *Пусть $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$ и $P = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > \frac{1}{4}$. Тогда $P \in \{p_1, \ldots, p_n\}$. Более того, $P = p_i$, $1 \leqslant i \leqslant n$, тогда и только тогда, когда $(\alpha, \beta, \gamma) = \xi(0, 2^{n-i}, 2^{n-i})$ для некоторого $\xi \in \mathcal{E}$.*

Доказательство. По лемме 5 любое $\omega \in \mathbb{O}^n$ с $\mathrm{adp}^{\oplus}(\omega) > \frac{1}{4}$ можно привести к $0^{i-1}30^{n-i}$, $i \in \{1, \ldots, n\}$, преобразованием из $\mathcal{E}$, что соответствует тройке $(0, 2^{n-i}, 2^{n-i})$. Осталось заметить, что $\mathrm{adp}^{\oplus}(0^{i-1}30^{n-i}) = p_i$ (см. лемму 2) и применить утверждение 1. Теорема 1 доказана.

Замечание 1. Вместо набора $(0, 2^{n-i}, 2^{n-i})$ из теоремы 1 удобно использовать тройку $(2^{n-i}, 2^{n-i}, 0)$, полученную преобразованием $\mathcal{T}_{\alpha\gamma}$, так как $\mathrm{adp}^{\mathrm{XR}}$ на ней будет также равна p_i (см. теорему 3).

Следствие 1. *Не существует таких* $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, *что*

$$\frac{1}{4} < \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \leqslant \frac{1}{3}.$$

Доказательство очевидно следует из теоремы 1 и утверждения 3. Следствие 1 доказано.

Известно [21], что $\max\limits_{\beta,\gamma \in \mathbb{Z}_2^n} \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \alpha \to 0)$. Таким образом, тройки $(2^{n-i}, 2^{n-i}, 0)$ максимизируют $\mathrm{adp}^{\oplus}$ при фиксации первого или второго аргумента. Отметим, что задачу, связанную со значениями $\mathrm{adp}^{\oplus}(\alpha, \alpha \to 0)$, можно найти в [22] (см. также первую олимпиаду [23]).

3. Разности, значение $\mathrm{adp}^{\oplus}$ на которых больше $1/4$

Шаблоны восьмеричных слов являются наиболее удобным способом описания разностей для $\mathrm{adp}^{\oplus}$ с вероятностью p_i.

Таблица 1

Шаблоны $\omega \in \mathbb{O}^n$ **таких, что** $\mathrm{adp}^{\oplus}(\omega) = p_i$, $3 \leqslant i \leqslant n$

	id	$\mathcal{T}_{\alpha\beta}$	$\mathcal{T}_{\alpha\gamma}$
id	$\mathtt{e}0^{i-2}30^{n-i}$	$\mathtt{e}0^{i-2}50^{n-i}$	$\mathtt{e}0^{i-2}60^{n-i}$
$\mathcal{S}_\gamma$	$\mathtt{d}1^{i-2}30^{n-i}$	$\mathtt{d}1^{i-2}50^{n-i}$	$\mathtt{d}4^{i-2}60^{n-i}$
$\mathcal{S}_\beta$	$\mathtt{d}2^{i-2}30^{n-i}$	$\mathtt{d}4^{i-2}50^{n-i}$	$\mathtt{d}2^{i-2}60^{n-i}$
$\mathcal{S}_{\beta\gamma}$	$\mathtt{e}3^{i-1}0^{n-i}$	$\mathtt{e}5^{i-1}0^{n-i}$	$\mathtt{e}6^{i-1}0^{n-i}$

Таблица 2

Шаблоны $\omega \in \mathbb{O}^n$ **таких, что** $\mathrm{adp}^{\oplus}(\omega) \in \{p_1, p_2\}$

$\mathrm{adp}^{\oplus}(\omega)$	Шаблоны ω
p_1	$\mathtt{e}0^{n-1}$
p_2	$*30^{n-2}$, $*50^{n-2}$, $*60^{n-2}$

Теорема 2. *Если* $\omega \in \mathbb{O}^n$ *и* $i \in \{1, \ldots, n\}$, *то* $\mathrm{adp}^{\oplus}(\omega) = p_i$ *тогда и только тогда, когда* ω *удовлетворяет одному из шаблонов, представленных в табл.* 1 *при* $i \geqslant 3$ *или табл.* 2 *при* $i \leqslant 2$.

Доказательство. Начнём с табл. 1, т. е. со случаев $i \geqslant 3$. Согласно теореме 1 любую тройку $(\alpha, \beta, \gamma) \in \left(\mathbb{Z}_2^n\right)^3$ преобразованиями из $\mathcal{E}$ можно привести к тройке $(0, 2^{n-i}, 2^{n-i})$, которая в восьмеричном виде представляется как $0^{i-1}30^{n-i}$.

Докажем, что слова, удовлетворяющие шаблонам из табл. 1, преобразованиями из $\mathcal{E}$ приводятся к слову $0^{i-1}30^{n-i}$. Применяя к нему $\mathcal{I}_*$,

получим любой символ $x \in \mathbb{O}$ с чётным $\mathrm{wt}(x)$ в старшем разряде, т. е. слово $0^{i-1}30^{n-i}$ можно заменить шаблоном $\mathtt{e}0^{i-2}30^{n-i}$, и далее говорить о шаблонах.

Нетрудно видеть, что шаблон в строке, помеченной $\mathcal{S}$, и столбце, помеченном $\mathcal{T}$, равен $\mathcal{T}(\mathcal{S}(\mathtt{e}0^{i-2}30^{n-i}))$: достаточно заметить, что

$$-(2^{n-i} + c \cdot 2^{n-1}) = 2^n - 2^{n-i} - c \cdot 2^{n-1} = (c \oplus 1, 1, \ldots, 1, \underbrace{0, \ldots, 0}_{n-i}), \quad c \in \mathbb{Z}_2.$$

После преобразований $\mathcal{S}_\gamma$ или $\mathcal{S}_\beta$ старший символ $\mathtt{e}$ превратится в $\mathtt{d}$, так как инвертируем ровно одну позицию символа-элемента $\mathbb{Z}_2^3$. Кроме того, $\mathcal{T}_{\alpha\beta}(3) = 5$, $\mathcal{T}_{\alpha\gamma}(3) = 6$, $\mathcal{T}_{\alpha\beta}(1) = 1$, $\mathcal{T}_{\alpha\gamma}(1) = 4$, $\mathcal{T}_{\alpha\beta}(2) = 4$ и $\mathcal{T}_{\alpha\gamma}(2) = 2$.

Осталось доказать полноту множества описанных шаблонов. Действительно, применение $\mathcal{S}_*$ к любому шаблону не выводит за пределы столбца, применение $\mathcal{T}_*$ не выводит за пределы строки, а $\mathcal{I}_*$ уже учтено в самом шаблоне. Таким образом, множество описанных в таблице шаблонов замкнуто относительно $\mathcal{E}$. Очевидно также, что все описанные шаблоны порождают различные слова.

В заключение обратимся к табл. 2. Нетрудно видеть, что её элементы порождают замкнутые относительно $\mathcal{E}$ множества слов, среди которых есть 30^{n-1} и 030^{n-2}. Теорема 2 доказана.

Замечание 2. Табл. 1 можно использовать и для $i \in \{1, 2\}$, игнорируя шаблоны с 1^{i-2} и т. п. при отрицательных $i - 2$. Однако, в этих случаях шаблоны не обеспечат уникальности порождаемых слов.

Следствие 2. *Если* $C_i = \left|\left\{(\alpha, \beta, \gamma) \in \left(\mathbb{Z}_2^n\right)^3 \mid \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = p_i\right\}\right|$, $i \in \{1, \ldots, n\}$, *то* $C_1 = 4$, $C_2 = 24$, $C_3 = C_4 = \cdots = C_n = 48$.

Доказательство. Все шаблоны, описанные в табл. 1, при $i \geqslant 3$ порождают различные слова. Каждый шаблон порождает ровно 4 слова, таким образом, имеется $4 \cdot 4 \cdot 3 = 48$ различных слов, для которых $\mathrm{adp}^{\oplus}$ равна p_i. Из табл. 2 очевидно, что $C_1 = 4$ и $C_2 = 8 \cdot 3 = 24$. Следствие 2 доказано.

Нетрудно подсчитать и общее число троек.

Следствие 3. *При* $n \geqslant 2$ *имеется ровно* $48n - 68$ *троек* $(\alpha, \beta, \gamma) \in \left(\mathbb{Z}_2^n\right)^3$ *таких, что* $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) > \frac{1}{4}$.

4. Необходимые утверждения для работы с $\mathrm{adp}^{\mathrm{XR}}$

Здесь приведём необходимые для работы с $\mathrm{adp}^{\mathrm{XR}}$ понятия и утверждения из [20].

4.1. «Неполные» характеристики и симметрии их аргументов. Разобьём $\mathrm{adp}^{\oplus}$ на неотрицательные «неполные» характеристики $\mathrm{adp}^{\oplus}_{c}$ и $\mathrm{adp}^{\oplus}_{a,b}$, $a, b, c \in \mathbb{Z}_2$:

$$\sum_{c\in\mathbb{Z}_2} \mathrm{adp}^{\oplus}_{c}(\alpha, \beta \to \gamma) = \sum_{(a,b)\in\mathbb{Z}_2^2} \mathrm{adp}^{\oplus}_{a,b}(\alpha, \beta \to \gamma) = \mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma). \quad (5)$$

Значения введённых величин при $\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) \neq 0$ для $\alpha, \beta, \gamma \in \mathbb{Z}_2$ (случай $n = 1$) даны в табл. 3, её можно найти в [20, табл. 1].

Таблица 3

Значения $\mathrm{adp}^{\oplus}_{a,b}(\alpha, \beta \to \gamma)$ **и** $\mathrm{adp}^{\oplus}_{c}(\alpha, \beta \to \gamma)$ **для** $\alpha, \beta, \gamma \in \mathbb{Z}_2$

$\alpha\beta\gamma$	$\omega(\alpha, \beta, \gamma)$	$\mathrm{adp}^{\oplus}_{0,0}$	$\mathrm{adp}^{\oplus}_{0,1}$	$\mathrm{adp}^{\oplus}_{1,0}$	$\mathrm{adp}^{\oplus}_{1,1}$	$\mathrm{adp}^{\oplus}_{0}$	$\mathrm{adp}^{\oplus}_{1}$
000	0	1	0	0	0	1	0
011	3	1/2	1/2	0	0	1/2	1/2
101	5	1/2	0	1/2	0	1/2	1/2
110	6	1/4	1/4	1/4	1/4	1	0

Для подсчёта значений $\mathrm{adp}^{\oplus}_{a,b}$ и $\mathrm{adp}^{\oplus}_{c}$ на аргументах из $\mathbb{Z}_2^{n+1}$ будем пользоваться рекуррентными формулами, аналогичными приведённым в утверждении 2 [20, теорема 3].

Утверждение 4 [20]. *Если* $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, $e \in \mathbb{Z}_2^3$, $a, b, c \in \mathbb{Z}_2$, *то при чётном* $\mathrm{wt}(e)$

$$\mathrm{adp}^{\oplus}_{c}(\alpha e_1, \beta e_2 \to \gamma e_3) = \frac{1}{2^{\mathrm{wt}(e)}} \sum_{q\in\mathbb{Z}_2^3,\, q\preceq e} \mathrm{adp}^{\oplus}_{c\oplus q_3}(\alpha^{[q_1]}, \beta^{[q_2]} \to \gamma^{[q_3]}),$$

$$\mathrm{adp}^{\oplus}_{a,b}(\alpha e_1, \beta e_2 \to \gamma e_3) = \frac{1}{2^{\mathrm{wt}(e)}} \sum_{q\in\mathbb{Z}_2^3,\, q\preceq e} \mathrm{adp}^{\oplus}_{a\oplus q_1, b\oplus q_2}(\alpha^{[q_1]}, \beta^{[q_2]} \to \gamma^{[q_3]}),$$

при нечётном $\mathrm{wt}(e)$

$$\mathrm{adp}^{\oplus}_{c}(\alpha e_1, \beta e_2 \to \gamma e_3) = \mathrm{adp}^{\oplus}_{a,b}(\alpha e_1, \beta e_2 \to \gamma e_3) = 0.$$

Аналогично $\mathrm{adp}^{\oplus}$ подсчёт $\mathrm{adp}^{\oplus}_{a,b}$ и $\mathrm{adp}^{\oplus}_{c}$ можно упростить, используя симметрии аргументов [20, теорема 4].

Утверждение 5 [20]. *Пусть* $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, $a, b, c \in \mathbb{Z}_2$ *и* $\omega = \omega(\alpha, \beta, \gamma)$. *Тогда*

- $\mathrm{adp}^{\oplus}_{a,b}(\omega) = \mathrm{adp}^{\oplus}_{a,b}(\mathcal{S}_\gamma(\omega))$,
- $\mathrm{adp}^{\oplus}_{c}(\omega) = \mathrm{adp}^{\oplus}_{c}(\mathcal{S}_\alpha(\omega)) = \mathrm{adp}^{\oplus}_{c}(\mathcal{S}_\beta(\omega)) = \mathrm{adp}^{\oplus}_{c}(\mathcal{S}_{\alpha\beta}(\omega))$,
- $\mathrm{adp}^{\oplus}_{c}(\omega) = \mathrm{adp}^{\oplus}_{c}(\mathcal{T}_{\alpha\beta}(\omega)) = \mathrm{adp}^{\oplus}_{c}(\mathcal{I}_{\alpha\beta}(\omega))$.

Некоторые преобразования работают вместе с изменением параметров:

- $\mathrm{adp}^{\oplus}_{a,b}(\omega) = \mathrm{adp}^{\oplus}_{b,a}(\mathcal{T}_{\alpha\beta}(\omega))$,
- $\mathrm{adp}^{\oplus}_{a,b}(\omega) = \mathrm{adp}^{\oplus}_{\overline{a},b}(\mathcal{S}_{\alpha}(\omega))$ *при* $\alpha \neq 0$,
- $\mathrm{adp}^{\oplus}_{a,b}(\omega) = \mathrm{adp}^{\oplus}_{a,\overline{b}}(\mathcal{S}_{\beta}(\omega))$ *при* $\beta \neq 0$,
- $\mathrm{adp}^{\oplus}_{c}(\omega) = \mathrm{adp}^{\oplus}_{\overline{c}}(\mathcal{S}_{\gamma}(\omega))$ *при* $\gamma \neq 0$.

В контексте $\mathrm{adp}^{\oplus}_{a,b}$ *и* $\mathrm{adp}^{\oplus}_{c}$ *будем обозначать их через* $\mathcal{T}^{!}_{\alpha\beta}$, $\mathcal{S}^{!}_{\alpha}$, $\mathcal{S}^{!}_{\beta}$ *и* $\mathcal{S}^{!}_{\gamma}$ *соответственно, подчёркивая, что они действуют на* ω *и тройке* (a, b, c).

4.2. Подсчёт $\mathrm{adp}^{\mathrm{XR}}$ и симметрии её аргументов. Будем подсчитывать $\mathrm{adp}^{\mathrm{XR}}$ способом, предложенным в [20, следствие 2], используя «неполные» характеристики.

Утверждение 6 [20]**.** *Пусть* $\alpha, \beta, \gamma \in \mathbb{Z}_2^{n-r}$, $\alpha', \beta', \gamma' \in \mathbb{Z}_2^r$, $a = \alpha_{n-r} \oplus \beta_{n-r} \oplus \gamma_{n-r}$, $a' = \alpha'_r \oplus \beta'_r \oplus \gamma'_r$, *т. е.* $a, a' \in \mathbb{Z}_2$. *Тогда*

$$\begin{aligned}\mathrm{adp}^{\mathrm{XR}}((\alpha', \alpha), (\beta', \beta) \xrightarrow{r} (\gamma, \gamma')) = \\ = \mathrm{adp}^{\oplus}_{a',0}(\alpha, \beta \to \gamma^{[a]})\mathrm{adp}^{\oplus}_{a}({\alpha'}^{[a']}, \beta' \to \gamma') + \\ + \mathrm{adp}^{\oplus}_{\overline{a}',1}(\alpha, \beta \to \gamma^{[a]})\mathrm{adp}^{\oplus}_{a}({\overline{\alpha}'}^{[a']}, \overline{\beta}' \to \gamma').\end{aligned}$$

Симметрий аргументов у $\mathrm{adp}^{\mathrm{XR}}$ меньше, чем у $\mathrm{adp}^{\oplus}$ [20, теорема 5]. Аналогично $\mathcal{E}$ обозначим через $\mathcal{E}'$ множество всевозможных композиций преобразований $\mathcal{T}_{\alpha\beta}$, $\mathcal{I}_{\alpha\beta}$ и $\mathcal{S}_{*}$. Для него верно

Утверждение 7 [20]**.** *Если* $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$, $\xi \in \mathcal{E}'$, $(\alpha', \beta', \gamma') = \xi(\alpha, \beta, \gamma)$, *то* $\mathrm{adp}^{\mathrm{XR}}(\alpha, \beta \xrightarrow{r} \gamma) = \mathrm{adp}^{\mathrm{XR}}(\alpha', \beta' \xrightarrow{r} \gamma')$.

5. Вспомогательные леммы о значениях $\mathrm{adp}^{\oplus}_{a,b}$ и $\mathrm{adp}^{\oplus}_{c}$

Этот раздел содержит вспомогательные утверждения о «неполных» характеристиках. Пользуясь результатами разд. 2 и 3, далее будем работать только со словами, представленными в табл. 1. Начнём с подсчёта значений $\mathrm{adp}^{\oplus}_{a,b}$ и $\mathrm{adp}^{\oplus}_{c}$ с помощью рекуррентных формул.

Лемма 6. *Если* $a, b, c \in \mathbb{Z}_2$, $s \in \{0, 3, 5, 6\}$, $t \in \{3, 5, 6\}$, *то*

$$\mathrm{adp}^{\oplus}_{a,b}(st^{k-1}0^{n-k}) = \left(p_k - \frac{1}{4^{k-1}}\right)\mathrm{adp}^{\oplus}_{a\oplus t_1, b\oplus t_2}(s \oplus t) + \frac{1}{4^{k-1}}\mathrm{adp}^{\oplus}_{a,b}(s),$$

$$\mathrm{adp}^{\oplus}_{c}(st^{k-1}0^{n-k}) = \left(p_k - \frac{1}{4^{k-1}}\right)\mathrm{adp}^{\oplus}_{c\oplus t_3}(s \oplus t) + \frac{1}{4^{k-1}}\mathrm{adp}^{\oplus}_{c}(s),$$

определяющие значения $\mathrm{adp}^{\oplus}_{a,b}$ *и* $\mathrm{adp}^{\oplus}_{c}$ *пары будем обозначать через*

$$\rho_{a,b}(s,t) = (\mathrm{adp}^{\oplus}_{a\oplus t_1, b\oplus t_2}(s \oplus t),\ \mathrm{adp}^{\oplus}_{a,b}(s)),$$
$$\rho_{\mathrm{c}}(s,t) = (\mathrm{adp}^{\oplus}_{\mathrm{c}\oplus t_3}(s \oplus t),\ \mathrm{adp}^{\oplus}_{\mathrm{c}}(s)).$$

Доказательство. Воспользуемся индукцией по k. Ясно, что при $k = 1$ равенства верны. Предположим, что для всех $k < n$ равенства верны. Докажем, что они верны и для $k+1$. Пусть $s' = s \oplus t$. Согласно утверждению 4 (см. также пояснения к утверждению 2) имеем

$$\mathrm{adp}^{\oplus}_{a,b}(st^k0^{n-k-1}) = \mathrm{adp}^{\oplus}_{a,b}(st^k) = \frac{1}{4}\mathrm{adp}^{\oplus}_{a,b}(st^{k-1}) + \\ + \frac{1}{4}\mathrm{adp}^{\oplus}_{a\oplus t_1,b\oplus t_2}(s'0^{k-1}) = \frac{1}{4}\mathrm{adp}^{\oplus}_{a,b}(st^{k-1}) + \frac{1}{4}\mathrm{adp}^{\oplus}_{a\oplus t_1,b\oplus t_2}(s').$$

Согласно утверждению 3 $p_k - \frac{1}{4^{k-1}} = \frac{1}{4} + \cdots + \frac{1}{4^{k-1}}$. Воспользуемся индукционным предположением:

$$\frac{1}{4}\mathrm{adp}^{\oplus}_{a,b}(st^{k-1}) = \frac{1}{4}\Big(p_k - \frac{1}{4^{k-1}}\Big)\mathrm{adp}^{\oplus}_{a\oplus t_1,b\oplus t_2}(s') + \frac{1}{4^k}\mathrm{adp}^{\oplus}_{a,b}(s) = \\ = \Big(\frac{1}{4^2} + \cdots + \frac{1}{4^k}\Big)\mathrm{adp}^{\oplus}_{a\oplus t_1,b\oplus t_2}(s') + \frac{1}{4^k}\mathrm{adp}^{\oplus}_{a,b}(s),$$

при этом $\frac{1}{4} + \big(\frac{1}{4^2} + \cdots + \frac{1}{4^k}\big) = p_{k+1} - \frac{1}{4^k}$, т. е. формула для $\mathrm{adp}^{\oplus}_{a,b}$ доказана. Равенство для $\mathrm{adp}^{\oplus}_{c}$ доказывается аналогично. Лемма 6 доказана.

Рассмотрим значения выражений из леммы 6, заменив пары $\rho_{a,b}$ и ρ_c неизвестными.

Лемма 7. *Если* $f_i(x,y) = \big(p_i - \frac{1}{4^{i-1}}\big)x + \frac{1}{4^{i-1}}y$, $i \geqslant 2$, *и* $x, y \in \mathbb{Q}$, *то*

1) $f_i(x,y) \leqslant \frac{1}{4}$ *при* $x, y \leqslant \frac{1}{2}$ *для* $i = 2$ *и при* $x \leqslant \frac{1}{2}$, $y \leqslant 1$ *для* $i \geqslant 3$;

2) $f_i(1, p_k) = p_{i+k-1}$, *в частности,*

$$f_i(1,1) = p_i, \quad f_i\Big(1, \frac{1}{2}\Big) = p_{i+1}, \quad f_i\Big(1, \frac{1}{4} + \frac{1}{4}p_k\Big) = p_{i+k}.$$

3) $f_2\big(\frac{1}{2}, 1\big) = p_3$.

Доказательство. 1, 3) При $x, y \leqslant \frac{1}{2}$ справедливо $f_i(x,y) \leqslant \frac{1}{2}p_i$, что в силу $i \geqslant 2$ и утверждения 3 означает, что $f_i(x,y) \leqslant \frac{1}{4}$. Кроме того, $\frac{1}{2}\big(p_i - \frac{1}{4^{i-1}}\big) + \frac{1}{4^{i-1}} = \frac{1}{2}p_i + \frac{1}{2\cdot 4^{i-1}}$, что равно $\frac{1}{6} + \frac{1}{12\cdot 4^{i-2}} + \frac{1}{2\cdot 4^{i-1}}$ по утверждению 3, или $\frac{1}{6} + \frac{5}{6\cdot 4^{i-1}}$. Данное выражение равно p_3 при $i = 2$ и меньше $\frac{1}{4}$ при $i \geqslant 3$.

2) Имеем $f_i(1, p_k) = p_i - \frac{1}{4^{i-1}} + \frac{1}{4^{i-1}}p_k$, что в силу утверждения 3 равно

$$\frac{1}{4} + \cdots + \frac{1}{4^{i-1}} + \frac{1}{4^i} + \cdots + \frac{1}{4^{i+k-2}} + \frac{1}{4^{i+k-2}} = p_{i+k-1}.$$

Осталось заметить, что $1 = p_1$, $\frac{1}{2} = p_2$, $\frac{1}{4} + \frac{1}{4}p_k = p_{k+1}$. Лемма 7 доказана.

Опишем все слова, на которых значение $\mathrm{adp}_c^{\oplus}$ больше $\frac{1}{4}$.

Лемма 8. *Справедливы равенства*

$$\mathrm{adp}_0^{\oplus}(6^i0^{m-i}) = p_i, \quad 1 \leqslant i \leqslant m,$$
$$\mathrm{adp}_1^{\oplus}(3^{i-1}0^{m-i+1}) = p_i, \quad 2 \leqslant i \leqslant m+1.$$

Более того, если $\omega \in \mathbb{O}^m$ и $c \in \mathbb{Z}_2$ не приводятся к перечисленным словам композициями преобразований $\mathcal{T}_{\alpha\beta}$, $\mathcal{I}_{\alpha\beta}$, $\mathcal{S}_\alpha$, $\mathcal{S}_\beta$ и $\mathcal{S}_\gamma^!$ (учитывая возможное изменение параметра c (см. утверждение 5)), то $\mathrm{adp}_c^{\oplus}(\omega) \leqslant \frac{1}{4}$.

Доказательство. Если $\mathrm{adp}_c^{\oplus}(\omega) > \frac{1}{4}$, то и $\mathrm{adp}^{\oplus}(\omega) > \frac{1}{4}$. Это означает, что для доказательства леммы достаточно рассматривать только ω, удовлетворяющие одному из шаблонов, описанному в табл. 1 (или в табл. 2 при $m \in \{1,2\}$ (см. теорему 2)). Более того, любое такое ω можно привести к виду $st^{i-1}0^{m-1}$, где $t \in \{3,5,6\}$, $s \in \{0,3,5,6\}$ и $1 \leqslant i \leqslant m$. Действительно, каждый столбец табл. 1 содержит соответствующий данному слову шаблон. Все остальные элементы столбца получаются из заданного преобразованиями вида $\mathcal{S}_*$. Эти преобразования согласуются с указанными в условии, а также с утверждением 5 (при применении $\mathcal{S}_\gamma^!$ и ненулевом $\gamma(\omega)$ инвертируем c). Далее, в силу леммы 6 имеем

$$\mathrm{adp}_c^{\oplus}(st^{i-1}0^{m-1}) = \left(p_i - \frac{1}{4^{i-1}}\right)\mathrm{adp}_{c\oplus t_3}^{\oplus}(s \oplus t) + \frac{1}{4^{i-1}}\mathrm{adp}_c^{\oplus}(s),$$

или $\mathrm{adp}_c^{\oplus}(st^{i-1}0^{m-1}) = f_i(x,y)$ в обозначениях леммы 7, где $(x,y) = \rho_c(s,t)$ (см. лемму 6). Для начала рассмотрим случай $i \geqslant 2$.

Таблица 4

Значения $\rho_c(s,t)$, $s,t \in \{0,3,5,6\}$, $t \neq 0$

st	03	05	06	33	35	36	53	55	56	63	65	66
ρ_0	$\frac{1}{2}$ 1	$\frac{1}{2}$ 1	1 1	0 $\frac{1}{2}$	0 $\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$	0 $\frac{1}{2}$	0 $\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$	$\frac{1}{2}$ 1	$\frac{1}{2}$ 1	1 1
ρ_1	$\frac{1}{2}$ 0	$\frac{1}{2}$ 0	0 0	1 $\frac{1}{2}$	1 $\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$	1 $\frac{1}{2}$	1 $\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$	$\frac{1}{2}$ 0	$\frac{1}{2}$ 0	0 0
✓	∘	∘	∗	•	•		•	•		∘	∘	∗

В табл. 4 с использованием табл. 3 подсчитаны все возможные значения (x,y). Более того, одинаковые столбцы сгруппированы, группы отмечены ∘, • и ∗. Неотмеченные столбцы содержат пары, у которых $x,y \leqslant \frac{1}{2}$, т. е. для них $f_i(x,y) \leqslant \frac{1}{4}$ по лемме 7. При разборе случаев все такие пары также будем игнорировать (они присутствуют в каждом столбце).

Случай 1. Группа ∘, т. е. $(x,y) = \left(\frac{1}{2},1\right)$, $c = 0$ и $st \in \{03,05,63,65\}$. По лемме 7 $f_2(x,y) = p_3$ и $f_i(x,y) \leqslant \frac{1}{4}$ при $i \geqslant 3$. Таким образом, подходят

слова $03 = \mathcal{S}^!_\gamma(\mathcal{S}_\beta(33))$, $05 = \mathcal{T}_{\alpha\beta}(03)$, $63 = \mathcal{I}_{\alpha\beta}(03)$ и $65 = \mathcal{T}_{\alpha\beta}(63)$, т. е. все они приводятся к $\mathrm{adp}^{\oplus}_1(3^i0^{m-i}) = p_{i+1}$ при $i = 2$.

Случай 2. Группа $\bullet$, т. е. $(x, y) = \left(1, \frac{1}{2}\right)$, $c = 1$ и $st \in \{33, 35, 53, 55\}$. По лемме 7 $f_i(x, y) = p_{i+1}$. Все слова подходят и приводятся к виду $\mathrm{adp}^{\oplus}_c(3^{j-1}0^{m-j+1}) = p_j$ преобразованиями $\mathcal{T}_{\alpha\beta}$ и $\mathcal{I}_{\alpha\beta}$ для всех $j = i + 1$, т. е. при $3 \leqslant j \leqslant m + 1$.

Случай 3. Группа $*$, т. е. $(x, y) = (1, 1)$, $c = 0$ и $st \in \{06, 66\}$. По лемме 7 $f_i(x, y) = p_i$. Все слова подходят и имеют вид $\mathrm{adp}^{\oplus}_0(6^i0^{m-i}) = p_i$, где $2 \leqslant i \leqslant m$, с точностью до преобразования $\mathcal{I}_{\alpha\beta}$.

Осталось рассмотреть случай $i = 1$, при котором $\mathrm{adp}^{\oplus}_c(\omega) = \mathrm{adp}^{\oplus}_c(s)$. Согласно табл. 3 при $c = 0$ подходят $s = 0$ и $s = 6$, что соответствует $\mathrm{adp}^{\oplus}_0(6^i0^{m-i}) = p_i$ при $i = 1$ с точностью до $\mathcal{I}_{\alpha\beta}$. При $c = 1$ подходят $s = 3$ и $s = 5$, что соответствует $\mathrm{adp}^{\oplus}_1(3^{i-1}0^{m-i+1}) = p_i$ при $i = 2$ с точностью до $\mathcal{T}_{\alpha\beta}$. Лемма 8 доказана.

Схожий результат нам потребуется и для $\mathrm{adp}^{\oplus}_{a,b}$.

Лемма 9. *Если* $h^r_{a,b}(\omega) = \mathrm{adp}^{\oplus}_{a,b}(\omega) + p_r\mathrm{adp}^{\oplus}_{\overline{a},\overline{b}}(\omega)$, $a, b \in \mathbb{Z}_2$, $\omega \in \mathbb{O}^m$, *то* $h^r_{0,0}(0^m) = p_1$, $h^r_{1,1}(0^m) = p_r$ *и для* $1 \leqslant i \leqslant m$

$$h^r_{1,0}(5^i0^{m-i}) = h^1_{1,0}(3^i0^{m-i}) = h^1_{0,0}(6^i0^{m-i}) = p_{i+1}, \quad h^r_{1,1}(6^i0^{m-i}) = p_{i+r}.$$

Более того, если $\omega \in \mathbb{O}^m$ *и* $a, b \in \mathbb{Z}_2$ *не приводятся к перечисленным словам и параметрам композициями преобразований* $\mathcal{T}^!_{\alpha\beta}$, $\mathcal{S}^!_\alpha$, $\mathcal{S}^!_\beta$ *и* $\mathcal{S}_\gamma$ (*учитывая возможное изменение параметров* a *и* b (*см. утверждение* 5)), *то* $h^r_{a,b}(\omega) \leqslant \frac{1}{4}$.

Доказательство. Как и в доказательстве леммы 8, рассматриваем $h^r_{a,b}(\omega) > \frac{1}{4}$, $a, b \in \mathbb{Z}_2$, так что $h^1_{a,b}(\omega) > \frac{1}{4}$, откуда $\mathrm{adp}^{\oplus}(\omega) > \frac{1}{4}$. Следовательно, ω можно привести к виду $st^{i-1}0^{m-1}$ композициями преобразований $\mathcal{S}^!_\alpha$, $\mathcal{S}^!_\beta$ и $\mathcal{S}_\gamma$, где $t \in \{3, 5, 6\}$, $s \in \{0, 3, 5, 6\}$ и $1 \leqslant i \leqslant m$ (см. теорему 2 и табл. 1). При этом в соответствии с преобразованиями $\mathcal{S}^!_\alpha$ и $\mathcal{S}^!_\beta$ параметры a и b у $h^r_{a,b}$ будут меняться так же, как и у соответствующих $\mathrm{adp}^{\oplus}_{a,b}$. Таким образом, достаточно рассматривать значения $h^r_{a,b}(st^{i-1}0^{m-1})$ при всех $a, b \in \mathbb{Z}_2$.

Воспользуемся леммой 6:

$$h^r_{a,b}(st^{i-1}0^{m-1}) = \left(p_i - \frac{1}{4^{i-1}}\right)h^r_{a\oplus t_1,b\oplus t_2}(s \oplus t) + \frac{1}{4^{i-1}}h^r_{a,b}(s). \qquad (6)$$

Чтобы применять лемму 7, рассмотрим случай $i \geqslant 2$, в котором используем обозначения

$$x = h^r_{a\oplus t_1,b\oplus t_2}(s \oplus t), \quad y = h^r_{a,b}(s),$$

тогда $f_i(x,y) = h^r_{a,b}(st^{i-1}0^{m-1})$. Напомним, что

$$\rho_{a,b}(s,t) = (\mathrm{adp}^{\oplus}_{a\oplus t_1, b\oplus t_2}(s\oplus t), \mathrm{adp}^{\oplus}_{a,b}(s)).$$

Таким образом, если $\rho_{a,b}(s,t) = (u,v)$ и $\rho_{\overline{a},\overline{b}}(s,t) = (u',v')$, то

$$x = u + p_r u', \quad y = v + p_r v'.$$

Согласно табл. 3 $u, v, u', v' \in \left\{0, \frac{1}{4}, \frac{1}{2}, 1\right\}$. Более того, если $u \in \left\{\frac{1}{2}, 1\right\}$, то $u' = 0$. Данное утверждение справедливо и для пар (u', u), (v, v'), (v', v). Таким образом, если $u, u', v, v' < 1$, то $x, y \leqslant \frac{1}{2}$, что в силу леммы 7 даёт $h^r_{a,b}(st^{i-1}0^{m-1}) \leqslant \frac{1}{4}$. Далее будем рассматривать случаи, когда хотя бы одно из u, u', v и v' равно 1.

Таблица 5

Значения $\rho_{a,b}(s,t)$, $s,t \in \{0,3,5,6\}$, $t \neq 0$

st	03	05	06	33	35	36	53	55	56	63	65	66
$\rho_{0,0}$	$\frac{1}{2}$ 1	$\frac{1}{2}$ 1	$\frac{1}{4}$ 1	0 $\frac{1}{2}$	$\frac{1}{4}$ $\frac{1}{2}$	0 $\frac{1}{2}$	$\frac{1}{4}$ $\frac{1}{2}$	0 $\frac{1}{2}$	0 $\frac{1}{2}$	0 $\frac{1}{4}$	0 $\frac{1}{4}$	0 $\frac{1}{4}$
$\rho_{1,1}$	0 0	0 0	$\frac{1}{4}$ 0	0 0	$\frac{1}{4}$ 0	$\frac{1}{2}$ 0	$\frac{1}{4}$ 0	0 0	$\frac{1}{2}$ 0	$\frac{1}{2}$ $\frac{1}{4}$	$\frac{1}{2}$ $\frac{1}{4}$	1 $\frac{1}{4}$
1✓	✓	✓	✓									✓
$\rho_{0,1}$	$\frac{1}{2}$ 0	0 0	$\frac{1}{4}$ 0	1 $\frac{1}{2}$	$\frac{1}{4}$ $\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$	$\frac{1}{4}$ 0	0 0	0 0	$\frac{1}{2}$ $\frac{1}{4}$	0 $\frac{1}{4}$	0 $\frac{1}{4}$
$\rho_{1,0}$	0 0	$\frac{1}{2}$ 0	$\frac{1}{4}$ 0	0 0	$\frac{1}{4}$ 0	0 0	$\frac{1}{4}$ $\frac{1}{2}$	1 $\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$	0 $\frac{1}{4}$	$\frac{1}{2}$ $\frac{1}{4}$	0 $\frac{1}{4}$
1✓				✓				✓				

В табл. 5 с использованием табл. 3 подсчитаны все возможные значения (u,v) и (u',v'). Более того, в ней отмечены колонки, в которых хотя бы одно из u, u', v и v' равно 1. Далее по значениям пар из табл. 5 будем подсчитывать x, y и применять лемму 7, оставляя только значения $f_i(x,y) > \frac{1}{4}$.

Случай 1: $(s,t) \in \{(0,3),(0,5)\}$, $a = b$, $(u,v),(u',v') \in \left\{\left(\frac{1}{2},1\right),(0,0)\right\}$.

Случай 1.1: $a = 0$. Тогда $x = \frac{1}{2}$, $y = 1$ и $f_i(x,y) = p_3$ только при $i = 2$, в остальных случаях она не превосходит $\frac{1}{4}$, т. е. подходят только слова $030^{m-2} = \mathcal{S}_\gamma(\mathcal{S}^!_\beta(\mathcal{T}^!_{\alpha\beta}(5^20^{m-2})))$ и $050^{m-2} = \mathcal{T}^!_{\alpha\beta}(030^{m-2})$, значение $h^r_{0,0}$ на которых равно p_3.

Случай 1.2: $a = 1$. Тогда $x = \frac{1}{2}p_r$, $y = p_r$. В этом случае условие $f_i(x,y) > \frac{1}{4}$ может быть выполнено только при $p_r > \frac{1}{2}$, или $r = 1$, что соответствует $x = \frac{1}{2}$, $y = 1$, как в случае 1.1, т. е. подходят только слова $030^{m-2} = \mathcal{S}_\gamma(\mathcal{S}^!_\beta(3^20^{m-2}))$ и $050^{m-2} = \mathcal{T}^!_{\alpha\beta}(030^{m-2})$, значение $h^1_{1,1}$ на которых равно p_3.

Случай 2: $(s,t) = (0,6)$, $a = b$, $(u,v),(u',v') \in \left\{\left(\frac{1}{4},1\right),\left(\frac{1}{4},0\right)\right\}$.

Случай 2.1: $a = 0$. Тогда $x = \frac{1}{4} + \frac{1}{4}p_r$, $y = 1$. Поскольку $x = p_{r+1}$ (см. утверждение 3), аналогично вышесказанному $f_i(x, y) = p_3$ только при $r = 1$ и $i = 2$, т. е. подходит только слово $060^{m-2} = \mathcal{S}^!_\alpha(\mathcal{S}^!_\beta(6^2 0^{m-2}))$, значение $h^1_{0,0}$ на котором равно p_3.

Случай 2.2: $a = 1$. Тогда $x = \frac{1}{4} + \frac{1}{4}p_r$, $y = p_r$. Аналогично случаю 2.1 $f_i(x, y) = p_3$ только при $r = 1$ и $i = 2$, т. е. подходит только слово $060^{m-2} = \mathcal{S}^!_\alpha(\mathcal{S}^!_\beta(6^2 0^{m-2}))$, значение $h^1_{1,1}$ на котором равно p_3.

Случай 3: $(s, t) = (6, 6)$, $a = b$, $(u, v), (u', v') \in \left\{\left(0, \frac{1}{4}\right), \left(1, \frac{1}{4}\right)\right\}$.

Случай 3.1: $a = 0$. Тогда $x = p_r$, $y = \frac{1}{4} + \frac{1}{4}p_r = p_{r+1}$. По лемме 7 $f_i(x, y) > \frac{1}{4}$ только при $r = 1$, причём $f_i(x, y) = p_{i+r}$, т. е. подходит только слово $6^i 0^{m-i}$, значение $h^1_{0,0}$ на котором равно p_{i+1}.

Случай 3.2: $a = 1$. Тогда $x = 1$, $y = \frac{1}{4} + \frac{1}{4}p_r = p_{r+1}$. По лемме 7 $f_i(x, y) > \frac{1}{4}$, причём $f_i(x, y) = p_{i+r}$, т. е. подходит слово $6^i 0^{m-i}$, значение $h^r_{1,1}$ на котором равно p_{i+r}.

Случай 4: $(s, t) = (3, 3)$, $a \neq b$, $(u, v), (u', v') \in \left\{\left(1, \frac{1}{2}\right), (0, 0)\right\}$.

Случай 4.1: $a = 0$. Тогда $x = 1$, $y = \frac{1}{2}$. По лемме 7 $f_i(x, y) > \frac{1}{4}$, причём $f_i(x, y) = p_{i+1}$, т. е. подходит только слово $3^i 0^{m-i} = \mathcal{T}^!_{\alpha\beta}(5^i 0^{m-i})$, значение $h^r_{0,1}$ на котором равно p_{i+1}.

Случай 4.2: $a = 1$. Тогда $x = p_r$, $y = \frac{1}{2}p_r$. По лемме 7 $f_i(x, y) > \frac{1}{4}$ только при $r = 1$, причём $f_i(x, y) = p_{i+1}$, т. е. подходит только слово $3^i 0^{m-i}$, значение $h^1_{1,0}$ на котором равно p_{i+1}.

Случай 5: $(s, t) = (5, 5)$, $a \neq b$, $(u, v), (u', v') \in \left\{(0, 0), \left(1, \frac{1}{2}\right)\right\}$. Этот случай симметричен предыдущему относительно перестановки a и b, т. е. подходят только слова $5^i 0^{m-i} = \mathcal{T}^!_{\alpha\beta}(3^i 0^{m-i})$, значение $h^1_{0,1}$ на котором равно p_{i+1}, и $5^i 0^{m-i}$, значение $h^r_{1,0}$ на котором также равно p_{i+1}.

Тем самым для $i \geqslant 2$ получили все перечисленные в условии слова, за исключением 0^m. Разберём случай $i = 1$, т. е. найдём значение $h^r_{a,b}(s0^{m-1})$, которое равно $h^r_{a,b}(s) = \mathrm{adp}^{\oplus}_{a,b}(s) + p_r \mathrm{adp}^{\oplus}_{\overline{a},\overline{b}}(s)$ согласно (6). Для этого достаточно воспользоваться табл. 3.

При $s = 0$ имеем $h^r_{0,0}(0^m) = 1$, $h^r_{0,0}(0^m) = p_r$ и $h^r_{1,0}(0^m) = h^r_{0,1}(0^m) = 0$. При $s = 6$ при всех a, b получаем $h^r_{a,b}(60^{m-1}) = \frac{1}{4} + \frac{1}{4}p_r$, что равно p_{r+1} по утверждению 3. Однако $\mathcal{S}^!_\alpha(60^{m-1}) = \mathcal{S}^!_\beta(60^{m-1}) = 6^i 0^{m-1}$ при $i = 1$. Кроме того, $h^1_{0,0}(6^i 0^{m-i})$ лежит в этом случае при $i = 1$.

При $s = 3$ имеем $h^r_{0,0}(30^{m-1}) = h^r_{0,1}(30^{m-1}) = \frac{1}{2} = p_2$ и $h^r_{1,0}(30^{m-1}) = h^r_{1,1}(30^{m-1}) = \frac{1}{2}p_r$, что равно p_2 только при $r = 1$ и не превосходит $\frac{1}{4}$ при других r. Однако $\mathcal{T}^!_{\alpha\beta}(30^{m-1}) = 50^{m-1}$ и $\mathcal{S}^!_\beta(30^{m-1}) = 30^{m-1}$, т. е. случаи учтены в $h^r_{1,0}(5^i 0^{m-i}) = p_{i+1}$ при $i = 1$. Оставшаяся пара аналогичными рассуждениями приводится к $h^1_{1,0}(3^i 0^{m-i}) = p_{i+1}$ при $i = 1$. Случай $s = 5$

можно не рассматривать, поскольку он соответствует применению $\mathcal{T}^{!}_{\alpha\beta}$ к $s = 3$. Лемма 9 доказана.

6. Значения $\mathrm{adp}^{\mathrm{XR}}$, превышающие $1/4$

Перейдём к описанию всех слов, значение $\mathrm{adp}^{\mathrm{XR}}$ на которых больше $\frac{1}{4}$. Отметим, что при заданном условии $\mathrm{adp}^{\mathrm{XR}}$ принимает в точности те же значения, что и $\mathrm{adp}^{\oplus}$.

Теорема 3. *Пусть $\alpha, \beta, \gamma \in \mathbb{Z}_2^n$ и $P = \mathrm{adp}^{\mathrm{XR}}(\alpha, \beta \xrightarrow{r} \gamma) > \frac{1}{4}$, где $1 \leqslant r < n$. Тогда $P \in \{p_1, \ldots, p_n\}$. Более того, $P = p_i$, $1 \leqslant i \leqslant n$, тогда и только тогда, когда тройку (α, β, γ) преобразованиями из $\mathcal{E}'$ можно привести к одной из следующих:*

1) $(2^{n-i}, 2^{n-i}, 0)$ *при* $1 \leqslant i \leqslant n$,
2) $(0, 2^{n-i+1}, 2^{r-i+1})$ *при* $2 \leqslant i \leqslant r+1$,
3) $(2^{n-r-i+1}, 0, 2^{n-i+1})$ *при* $2 \leqslant i \leqslant n-r+1$.

Доказательство. Для подсчёта $\mathrm{adp}^{\mathrm{XR}}$ используем утверждение 6, поэтому переобозначим вход, разделим его на две части: пусть теперь $\alpha, \beta, \gamma \in \mathbb{Z}_2^{n-r}$, $\alpha', \beta', \gamma' \in \mathbb{Z}_2^r$, $a = \alpha_{n-r} \oplus \beta_{n-r} \oplus \gamma_{n-r}$ и $a' = \alpha'_r \oplus \beta'_r \oplus \gamma'_r$. Тогда в силу утверждения 6

$$\begin{aligned}\mathrm{adp}^{\mathrm{XR}}((\alpha', \alpha), (\beta', \beta) \xrightarrow{r} (\gamma, \gamma')) = \\ = \mathrm{adp}^{\oplus}_{a',0}(\alpha, \beta \to \gamma^{[a]})\mathrm{adp}^{\oplus}_{a}({\alpha'}^{[a']}, \beta' \to \gamma') + \\ + \mathrm{adp}^{\oplus}_{\overline{a}',1}(\alpha, \beta \to \gamma^{[a]})\mathrm{adp}^{\oplus}_{a}(\overline{\alpha}'^{[a']}, \overline{\beta}' \to \gamma').\end{aligned}$$

Аргументами теперь являются (α', α), (β', β) и (γ, γ'), введём $\omega'_{u,v} = \omega({\alpha'}^{[u]}, {\beta'}^{[v]}, \gamma')$ для произвольных $u, v \in \mathbb{Z}_2$ и $\omega_a = \omega(\alpha, \beta, \gamma^{[a]})$, а также $\omega' = \omega'_{0,0}$ и $\omega = \omega_0$. Тогда аргументы из формулировки теоремы, на которых $\mathrm{adp}^{\mathrm{XR}}$ равно p_i, можно описать следующими парами:

$$(\omega', \omega) = (6^i 0^{r-i},\, 0^{n-r}), \quad 1 \leqslant i \leqslant r, \tag{7}$$

$$(\omega', \omega) = (6^r,\, 6^{i-r} 0^{n-i}), \quad r+1 \leqslant i \leqslant n, \tag{8}$$

$$(\omega', \omega) = (2^{i-2} 3 0^{r-i+1},\, 0^{n-r}), \quad 2 \leqslant i \leqslant r+1, \tag{9}$$

$$(\omega', \omega) = (4^r,\, 5^{i-1} 0^{n-r-i+1}), \quad 2 \leqslant i \leqslant n-r+1. \tag{10}$$

Здесь из-за деления входа на две части тройка $(2^{n-i}, 2^{n-i}, 0)$ распадается на пары (7) и (8), для удобства она приведена к виду $(-2^{n-i}, -2^{n-i}, 0)$ преобразованием $\mathcal{S}_{\alpha\beta}$. Аналогично вторая тройка преобразованием $\mathcal{S}_{\beta}$ приведена к виду $(0, -2^{n-i+1}, 2^{r-i+1})$, а третья тройка преобразованием $\mathcal{S}_{\alpha\gamma}$ — к виду $(-2^{n-r-i+1}, 0, -2^{n-i+1})$, они соответствуют (9) и (10).

Напомним, что

$$-2^{n-i} = (\underbrace{1,\dots,1}_{i},\underbrace{0,\dots,0}_{n-i}).$$

Из формулы для $\mathrm{adp}^{\mathrm{XR}}$ получаем неравенство

$$\mathrm{adp}^{\mathrm{XR}}((\alpha',\alpha),(\beta',\beta) \xrightarrow{r} (\gamma,\gamma')) \leqslant \\ \leqslant \left(\mathrm{adp}^{\oplus}_{a',0}(\omega_a) + \mathrm{adp}^{\oplus}_{\overline{a}',1}(\omega_a)\right) \max\left\{\mathrm{adp}^{\oplus}_{a}(\omega'_{a',0}),\, \mathrm{adp}^{\oplus}_{a}(\omega'_{\overline{a}',1})\right\}.$$

Таким образом, если оба множителя не превосходят $\frac{1}{2}$, то имеет неравенство $\mathrm{adp}^{\mathrm{XR}}((\alpha',\alpha),(\beta',\beta) \xrightarrow{r} (\gamma,\gamma')) \leqslant \frac{1}{4}$. Значит, как минимум один из них больше $\frac{1}{2} = p_2$, что в силу лемм 8 и 9 требует равенство p_1, т. е. единице.

Случай 1: $\mathrm{adp}^{\oplus}_{a',0}(\omega_a) + \mathrm{adp}^{\oplus}_{\overline{a}',1}(\omega_a) = 1$. В этом случае $\mathrm{adp}^{\oplus}(\omega_a) = 1$, т. е. $\omega_a = s0^{n-r-1}$ в силу теоремы 2, где $s \in \{0,3,5,6\}$. Поскольку $\mathrm{adp}^{\oplus}_{a',0}(s0^{n-r-1}) = \mathrm{adp}^{\oplus}_{a',0}(s)$ и аналогично $\mathrm{adp}^{\oplus}_{\overline{a}',1}(s0^{n-r-1}) = \mathrm{adp}^{\oplus}_{\overline{a}',1}(s)$ в силу утверждения 4, можно воспользоваться табл. 3. Из неё следует, что $a' = 0$, $\mathrm{adp}^{\oplus}_{a',0}(\omega_a) = 1$, $\mathrm{adp}^{\oplus}_{\overline{a}',1}(\omega_a) = 0$ и $\omega_a = 0^{n-r}$. Таким образом,

$$\mathrm{adp}^{\mathrm{XR}}((\alpha',\alpha),(\beta',\beta) \xrightarrow{r} (\gamma,\gamma')) = \mathrm{adp}^{\oplus}_{a}(\alpha',\beta' \to \gamma') = \mathrm{adp}^{\oplus}_{a}(\omega') > \frac{1}{4}.$$

Лемма 8 гарантирует, что $\mathrm{adp}^{\oplus}_{a}(\omega') \in \{p_1,\dots,p_{r+1}\}$, и описывает следующие два подслучая.

Случай 1.1: $\mathrm{adp}^{\oplus}_{0}(6^i0^{r-i}) = p_i$ при $1 \leqslant i \leqslant r$, т. е. $a = 0$, что влечёт $\omega = 0^{n-r}$ и соответствует (7).

Случай 1.2: $\mathrm{adp}^{\oplus}_{1}(3^{i-1}0^{r-i+1}) = p_i$ при $2 \leqslant i \leqslant r+1$, т. е. $a = 1$, что влечёт $\omega = 1^{n-r}$. Заметим, что

$$\mathcal{S}_\gamma(\omega',\omega) = \mathcal{S}_\gamma(3^{i-1}0^{r-i+1},1^{n-r}) = (2^{i-2}30^{r-i+1},0^{n-r})$$

(см. формулу ниже). Это соответствует (9).

Также лемма 8 гарантирует, что достаточно рассматривать только эти подслучаи. Действительно, $\omega_a = 0^{n-r}$, значит, что $\alpha = \beta = 0$. Поскольку $-(\alpha',0) = (-\alpha',0)$ и аналогично для β, получаем

$$\mathcal{S}_\alpha(\omega',\omega_a) = (\mathcal{S}_\alpha(\omega'),\omega_a), \quad \mathcal{S}_\beta(\omega',\omega_a) = (\mathcal{S}_\beta(\omega'),\omega_a).$$

Также если $\gamma' \neq 0$, то справедливо $-(\gamma,\gamma') = (\overline{\gamma},-\gamma')$, поэтому

$$\mathcal{S}_\gamma(\omega',\omega_a) = (\mathcal{S}_\gamma(\omega'),\omega_{\overline{a}}) \quad \text{при } \gamma(\omega') \neq 0,$$

что полностью соответствует $\mathcal{S}^!_\gamma$ для ω' и a: $\mathrm{adp}^{\oplus}_{a}(\omega') = \mathrm{adp}^{\oplus}_{\overline{a}}\big(\mathcal{S}^!_\gamma(\omega')\big)$ (см. утверждение 5). Если же $\gamma' = 0$, то $\mathcal{S}^!_\gamma(\omega') = \omega'$, т. е. ни a, ни ω' не изменяются. Таким образом, преобразования $\mathcal{T}_{\alpha\beta}$, $\mathcal{I}_{\alpha\beta}$, $\mathcal{S}_\alpha$, $\mathcal{S}_\beta$ и $\mathcal{S}^!_\gamma$ на ω' полностью соответствуют преобразованиям $\mathcal{T}_{\alpha\beta}$, $\mathcal{I}_{\alpha\beta}$, $\mathcal{S}_\alpha$, $\mathcal{S}_\beta$ и $\mathcal{S}_\gamma$ на паре (ω',ω), которая является входом $\mathrm{adp}^{\mathrm{XR}}$.

Случай 2: $\max\left\{\mathrm{adp}^{\oplus}_{a}(\omega'_{a',0}),\, \mathrm{adp}^{\oplus}_{a}(\omega'_{\overline{a}',1})\right\} = 1$. Лемма 8 гарантирует, что либо $\omega'_{a',0}$, либо $\omega'_{\overline{a}',1}$ приводится к 60^{r-1}, при этом $a = 0$. Заметим, что $\mathcal{I}_{\alpha\beta}(60^{r-1}) = 0^r$, а любое из преобразований $\mathcal{S}_*$ и $\mathcal{T}_{\alpha\beta}$ оставляет слова 0^r и 60^{r-1} на месте, т. е. одно из $\omega'_{a',0}$ и $\omega'_{\overline{a}',1}$ принадлежит множеству $\{0^r, 60^{r-1}\}$. Более того, можно применить преобразования $\mathcal{I}_{\alpha\beta}$, так как эти разряды старшие для исходных аргументов $\mathrm{adp}^{\mathrm{XR}}$, поэтому можно рассматривать только случаи $\omega'_{a',0} = 0^r$ или $\omega'_{\overline{a}',1} = 0^r$. Таким образом, данный случай сводится к рассмотрению значения

$$\mathrm{adp}^{\mathrm{XR}}((\alpha',\alpha),(\beta',\beta) \xrightarrow{r} (\gamma,\gamma')) = \mathrm{adp}^{\oplus}_{u,v}(\omega) + p_r \mathrm{adp}^{\oplus}_{u,\overline{v}}(\omega) = h^r_{u,v}(\omega) > \frac{1}{4}$$

в обозначениях леммы 9, где $u = \alpha'_1$, $v = \beta'_1$, т. е. $\alpha' = (u,\ldots,u)$, $\beta' = (v,\ldots,v)$ и $\gamma' = 0$, что влечёт $\omega'_{u,v} = 0^r$ и $\omega' = x^r$, где $x = 4u+2v$. Лемма 9 также гарантирует, что $h^r_{u,v}(\omega) \in \{p_1,\ldots,p_n\}$, и описывает следующие три подслучая.

Случай 2.1. Во-первых, $h^r_{1,0}(5^i 0^{m-i}) = p_{i+1}$, так что получаем пару $\omega' = 4^r$ и $\omega = 5^i 0^{m-i}$, что соответствует (10) с учётом уменьшения i на 1.

Во-вторых, $h^1_{1,0}(3^i 0^{m-i}) = p_{i+1}$ при $r = 1$, так что получаем $\omega' = 4$ и $\omega = 3^i 0^{n-i-1}$. Однако эта пара приводится к предыдущей преобразованиями $\mathcal{T}_{\alpha\beta}$ и $\mathcal{I}_{\alpha\beta}$.

В-третьих, $h^1_{0,0}(6^i 0^{m-i}) = p_{i+1}$ также при $r = 1$, так что $\omega' = 0$ и $\omega = 6^i 0^{n-i-1}$. Эта пара приводится к виду (8) преобразованием $\mathcal{I}_{\alpha\beta}$.

Случай 2.2: $h^r_{1,1}(6^i 0^{m-i}) = p_{i+r}$, что даёт $\omega' = 6^r$, $\omega = 6^i 0^{m-i}$ и соответствует (8).

Случай 2.3: $\omega = 0^m$, что соответствует значению $\mathrm{adp}^{\oplus}$, равному 1, которое рассмотрено в случае 1.

Аналогично случаю 1 и лемме 8 лемма 9 гарантирует, что достаточно рассмотреть только перечисленные подслучаи, поскольку

$$\mathcal{S}_\alpha(\omega'_{u,v},\omega) = \left(\omega'_{\overline{u},v}, \mathcal{S}^!_\alpha(\omega)\right), \quad \mathcal{S}_\beta(\omega'_{u,v},\omega) = \left(\omega'_{u,\overline{v}}, \mathcal{S}^!_\beta(\omega)\right)$$

при $\alpha \neq 0$ и $\beta \neq 0$ соответственно, а также $\mathcal{S}_\gamma(\omega'_{u,v},\omega) = (\omega'_{u,v}, \mathcal{S}_\gamma(\omega))$ из-за $\gamma' = 0$. Очевидно также, что $\mathcal{T}_{\alpha\beta}(\omega'_{u,v},\omega) = (\omega'_{v,u}, \mathcal{T}^!_{\alpha\beta}(\omega))$. Таким образом, преобразования $\mathcal{T}^!_{\alpha\beta}$, $\mathcal{S}^!_\alpha$, $\mathcal{S}^!_\beta$ и $\mathcal{S}_\gamma$ на ω для $h^r_{u,v}$ (т. е. для $\mathrm{adp}^{\oplus}_{u,v}$) полностью соответствуют преобразованиям $\mathcal{T}_{\alpha\beta}$, $\mathcal{S}_\alpha$, $\mathcal{S}_\beta$ и $\mathcal{S}_\gamma$ на паре (ω',ω), которая является входом $\mathrm{adp}^{\mathrm{XR}}$. Теорема 3 доказана.

Утверждение 8. *Тройки из условия теоремы* 3 *с учётом ограничений на* i *не приводятся друг к другу преобразованиями из* $\mathcal{E}'$. *Более того, они не приводятся друг к другу преобразованиями из* $\mathcal{E}$, *за исключением случая* $n = 2r$, *когда тройка из п.* 2 *приводится к тройке из п.* 3.

Доказательство. Начнём со второй части. Единственный ненулевой элемент первой тройки 2^{n-i} не приводится ни отрицанием, ни прибавлением 2^{n-1} к отличной степени двойки, в том числе и к 2^{n-i+1}. Таким образом, первую тройку нельзя привести преобразованиями $\mathcal{T}_*$, $\mathcal{I}_*$ и $\mathcal{S}_*$ ни ко второй, ни к третьей. Далее, у второй и третьей элементы 0 и 2^{n-i+1} совпадают, и оставшимися являются 2^{r-i+1} и $2^{n-r-i+1}$ соответственно, причём оба отличны от 2^{n-i+1}, единственного ненулевого элемента. Тем самым единственный вариант приведения троек — $r-i+1 = n-r-i+1$, т. е. $n = 2r$.

Осталось доказать, что вторая и третья тройки не приводятся друг к другу композициями преобразований $\mathcal{T}_{\alpha\beta}$, $\mathcal{I}_{\alpha\beta}$ и $\mathcal{S}_*$. Действительно, из них только $\mathcal{S}_\gamma$ может изменять γ, при этом 2^{r-i+1} и 2^{n-i+1} — различные степени двойки. Утверждение 8 доказано.

Отметим, что $i = 2$ удовлетворяет ограничениям на все тройки (при $n \geqslant 2$). Таким образом, значение $p_2 = \frac{1}{2}$ гарантированно достигается на трёх тройках, не приводимых друг к другу преобразованиями из $\mathcal{E}'$.

Таблица 6

Множества $\mathcal{T}$, $\mathcal{I}$, $\mathcal{S}$, порождающие $\mathcal{E}'(\alpha,\beta,\gamma)$

(α,β,γ)	$\mathcal{T}$	$\mathcal{I}$	$\mathcal{S}$
$(2^{n-i}, 2^{n-i}, 0)$	$\{\mathrm{id}\}$	$\{\mathrm{id}, \mathcal{I}_{\alpha,\beta}\}$	$\{\mathrm{id}, \mathcal{S}_\alpha, \mathcal{S}_\beta, \mathcal{S}_{\alpha\beta}\}$
$(0, 2^{n-i+1}, 2^{r-i+1})$	$\{\mathrm{id}, \mathcal{T}_{\alpha,\beta}\}$	$\{\mathrm{id}, \mathcal{I}_{\alpha,\beta}\}$	$\{\mathrm{id}, \mathcal{S}_\beta, \mathcal{S}_\gamma, \mathcal{S}_{\beta\gamma}\}$
$(2^{n-r-i+1}, 0, 2^{n-i+1})$	$\{\mathrm{id}, \mathcal{T}_{\alpha,\beta}\}$	$\{\mathrm{id}, \mathcal{I}_{\alpha,\beta}\}$	$\{\mathrm{id}, \mathcal{S}_\alpha, \mathcal{S}_\gamma, \mathcal{S}_{\alpha\gamma}\}$

Следствие 4. *Пусть $(\alpha,\beta,\gamma) \in \left(\mathbb{Z}_2^n\right)^3$ — тройка из условия теоремы* 3. *Тогда множество троек $\mathcal{E}'(\alpha,\beta,\gamma)$ порождается композициями преобразований из множеств $\mathcal{T}$, $\mathcal{I}$, $\mathcal{S}$, описанных для каждого случая в табл.* 6, *при этом*

$$|\mathcal{E}'(2^{n-i}, 2^{n-i}, 0)| = \begin{cases} 2 & \text{при } i = 1, \\ 4 & \text{при } i = 2, \\ 8 & \text{при } 2 < i \leqslant n, \end{cases}$$

$$|\mathcal{E}'(0, 2^{n-i+1}, 2^{r-i+1})| = \begin{cases} 4 & \text{при } i = 2, \\ 16 & \text{при } 2 < i \leqslant r+1, \end{cases}$$

$$|\mathcal{E}'(2^{n-r-i+1}, 0, 2^{n-i+1})| = \begin{cases} 8 & \text{при } i = 2, \\ 16 & \text{при } 2 < i \leqslant n-r+1. \end{cases}$$

Доказательство. Очевидно, что все тройки $\mathcal{E}'(\alpha,\beta,\gamma)$ получаются композициями преобразований из множеств $\{\mathrm{id}, \mathcal{T}_{\alpha\beta}\}$, $\{\mathrm{id}, \mathcal{I}_{\alpha\beta}\}$ и $\{\mathrm{id}, \mathcal{S}_\alpha,$

$\mathcal{S}_\beta, \mathcal{S}_\gamma, \mathcal{S}_{\alpha\beta}, \mathcal{S}_{\alpha\gamma}, \mathcal{S}_{\beta\gamma}, \mathcal{S}_{\alpha\beta\gamma}\}$. Далее, один из элементов каждой тройки нулевой и может быть преобразован только в 2^{n-1}, который также самообратный, поэтому половина возможных вариантов ξ для каждой тройки можно отбросить. В первой тройке два ненулевых элемента равны, тем самым можно убрать $\mathcal{T}_{\alpha\beta}$.

Осталось заметить, что при $i > 2$ первая тройка не содержит ни 2^{n-1}, ни 2^{n-2}. Аналогично для второй и третьей тройки при $i > 3$. Это означает, что все значения вида $c2^{n-1} \pm 2^k$, где $c \in \mathbb{Z}_2$ и k из имеющихся в тройках, будут различны, т. е. имеем описанные в условии следствия мощности. Если $i = 3$, то у третьей тройки только третий элемент равен 2^{n-2}, от которого может быть взят обратный, а во второй тройке возможен случай $2^{n-1} - 2^{n-2} = 2^{n-2}$. Тогда и бывший нулевой элемент будет равен 2^{n-1}, поскольку инверсию старших битов делаем одновременно у двух первых элементов, т. е. и в этом случае тройки будут различными. Случай $i = 1$ для первой тройки и $i = 2$ очевидны. Следствие 4 доказано.

Следствие 5. *Если* $C_i = \left|\left\{(\alpha, \beta, \gamma) \in \left(\mathbb{Z}_2^n\right)^3 \mid \mathrm{adp}^{\mathrm{XR}}(\alpha, \beta \xrightarrow{r} \gamma) = p_i\right\}\right|$, $i \in \{1, \ldots, n\}$, *то*

$$C_i = \begin{cases} 2 & \text{при } i = 1, \\ 16 & \text{при } i = 2, \\ 40 & \text{при } 3 \leqslant i \leqslant \min\{r+1,\, n-r+1\}, \\ 24 & \text{при } \min\{r+1,\, n-r+1\} < i \leqslant \max\{r+1,\, n-r+1\}, \\ 8 & \text{при } \max\{r+1,\, n-r+1\} < i \leqslant n. \end{cases}$$

В частности, $C_3 = C_4 = \cdots = C_n = 24$ *при* $r = 1$ *и* $r = n - 1$.

Доказательство следует из утверждения 8 и следствия 4. Следствие 5 доказано.

Несложно подсчитать общее число рассматриваемых троек.

Следствие 6. *При* $n \geqslant 2$ *имеется ровно* $24n-30$ *троек* $(\alpha, \beta, \gamma) \in \left(\mathbb{Z}_2^n\right)^3$ *таких, что* $\mathrm{adp}^{\mathrm{XR}}(\alpha, \beta \xrightarrow{r} \gamma) > \frac{1}{4}$.

Это число почти в два раза меньше аналогичного для $\mathrm{adp}^{\oplus}$.

Заключение

В работе получена полная характеризация разностей по модулю 2^n для преобразований $x \oplus y$ и $(x \oplus y) \lll r$, вероятность которых больше $\frac{1}{4}$. Несмотря на то, что с учётом указанного ограничения спектры значений обеих характеристик совпадают, множества-прообразы «усложняются» после добавления циклического сдвига. Также они содержат примерно

в два раза меньше элементов. Аналогично результатам из [20] минимальные различия получаются при циклическом сдвиге на одну позицию влево или вправо ($r = 1$ и $r = n - 1$ соответственно).

Обратим внимание, что полученные результаты легко применить к более широкому классу преобразований, например к $(x \lll r) \oplus y$ или $((x \boxplus y) \lll r) \oplus z$, поскольку их разностные характеристики прямо выражаются через значения $\mathrm{adp}^{\mathrm{XR}}$.

Финансирование работы

Исследование выполнено при поддержке Математического центра в Академгородке в рамках соглашения с Министерством науки и высшего образования Российской Федерации (соглашение № 075–15–2022–282).

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Shimizu A., Miyaguch S.** Fast data encipherment algorithm FEAL // Advances in cryptology — EUROCRYPT'87. Proc. Workshop Theory and Application of Cryptographic Techniques (Amsterdam, The Netherlands, Apr. 13–15, 1987). Heidelberg: Springer, 1988. P. 267–278. (Lect. Notes Comput. Sci.; V. 304). DOI: 10.1007/3-540-39118-5_24.
2. **Ferguson N., Lucks S., Schneier B.** [et al.]. The Skein hash function family. Santa Barbara, CA: Univ. Calif., 2008. 100 p. URL: www.schneier.com/wp-content/uploads/2015/01/skein.pdf (accessed Apr. 3, 2024).
3. **Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L.** The SIMON and SPECK families of lightweight block ciphers. San Diego: Univ. California, 2013. 45 p. (Cryptol. ePrint Archive; Paper ID 2013/404), URL: eprint.iacr.org/2013/404 (accessed June 1, 2024).
4. **Bernstein D. J.** Salsa20 specification. Chicago: Univ. Ill. Chic., 2007. 9 p. URL: cr.yp.to/snuffle/spec.pdf (accessed June 1, 2024).
5. **Bernstein D. J.** ChaCha, a variant of Salsa20. Chicago: Univ. Ill. Chic., 2008. 6 p. URL: cr.yp.to/chacha/chacha-20080128.pdf (accessed June 1, 2024).
6. **Koo B., Roh D., Kim H., Jung Y., Lee D., Kwon D.** CHAM: A family of lightweight block ciphers for resource-constrained devices // Information security and cryptology — ICISC 2017. Rev. Sel. Pap. 20th Int. Conf. (Seoul, South Korea, Nov. 29 – Dec. 1, 2017). Cham: Springer, 2017. P. 3–25. (Lect. Notes Comput. Sci.; V. 10779). DOI: 10.1007/978-3-319-78556-1_1.
7. **Roh D., Koo B., Jung Y., Jeong I., Lee D., Kwon D., Kim W.** Revised version of block cipher CHAM // Information security and cryptology — ICISC 2019. Rev. Sel. Pap. 22th Int. Conf. (Seoul, South Korea, Dec. 4–6, 2019). Cham: Springer, 2020. P. 1–19. (Lect. Notes Comput. Sci.; V. 11975). DOI: 10.1007/978-3-030-40921-0_1.

8. **Mouha N., Mennink B., Herrewege A., Watanabe D., Preneel B., Verbauwhede I.** Chaskey: An efficient MAC algorithm for 32-bit microcontrollers // Selected areas in cryptography — SAC 2014. Rev. Sel. Pap. 21th Int. Workshop (Montreal, Canada, Aug. 14–15, 2014). Cham: Springer, 2014. P. 306–323. (Lect. Notes Comput. Sci.; V. 8781).
9. **Biham E., Shamir A.** Differential cryptanalysis of DES-like cryptosystems // J. Cryptol. 1991. V. 4. P. 3–72.
10. **Biryukov A., Velichkov V.** Automatic search for differential trails in ARX ciphers // Topics in cryptology — CT-RSA 2014. Proc. Cryptographer's Track at the RSA Conf. (San Francisco, USA, Feb. 25–28, 2014). Cham: Springer, 2014. P. 227–250. (Lect. Notes Comput. Sci.; V. 8366). DOI: 10.1007/978-3-319-04852-9_12.
11. **Leurent G.** Analysis of differential attacks in ARX constructions // Advances in cryptology — ASIACRYPT 2012. Proc. 18th Int. Conf. Theory and Application of Cryptology and Information Security (Beijing, China, Dec. 2–6, 2012). Heidelberg: Springer, 2012. P. 226–243. (Lect. Notes Comput. Sci.; V. 7658). DOI: 10.1007/978-3-642-34961-4_15.
12. **Leurent G.** Construction of differential characteristics in ARX designs application to Skein // Advances in cryptology — CRYPTO 2013. Proc. 33rd Annu. Cryptology Conf. (Santa Barbara, CA, USA, Aug. 18–22, 2013). Pt. I. Heidelberg: Springer, 2013. P. 241–258. (Lect. Notes Comput. Sci.; V. 8042). DOI: 10.1007/978-3-642-40041-4_14.
13. **Малышев Ф. М.** Вероятностные характеристики разностных и линейных соотношений для неоднородной линейной среды // Мат. вопросы криптографии. 2019. Т. 10, № 1. С. 41–72.
14. **Малышев Ф. М.** Разностные характеристики основных операций ARX-шифров // Мат. вопросы криптографии. 2020. Т. 11, № 4. С. 97–105.
15. **Berson T. A.** Differential cryptanalysis mod 2^{32} with applications to MD5 // Advances in cryptology — EUROCRYPT'92. Proc. Workshop Theory and Application of Cryptographic Techniques (Balatonfüred, Hungary, May 24–28, 1992). Heidelberg: Springer, 1992. P. 71–80. (Lect. Notes Comput. Sci.; V. 658).
16. **Daum M. A.** Cryptanalysis of hash functions of the MD4-family: PhD Thes. Bochum: Ruhr-Univ. Bochum, 2005. 178 p.
17. **Lipmaa H., Wallén J., Dumas P.** On the additive differential probability of exclusive-or // Fast software encryption. Rev. Pap. 11th Int. Workshop (Delhi, India, Feb. 5–7, 2004). Heidelberg: Springer, 2004. P. 317–331. (Lect. Notes Comput. Sci.; V. 3017).
18. **Mouha N., Velichkov V., De Canniére C., Preneel B.** The differential analysis of S-functions // Selected areas in cryptography. Rev. Sel. Pap. 17th Int. Workshop (Waterloo, Canada, Aug. 12–13, 2010). Heidelberg: Springer, 2011. P. 36–56. (Lect. Notes Comput. Sci.; V. 6544).
19. **Velichkov V., Mouha N., De Canniére C., Preneel B.** The additive differential probability of ARX // Fast software encryption. Rev. Sel. Pap. 18th Int. Workshop (Lyngby, Denmark, Feb. 13–16, 2011). Heidelberg: Springer, 2011. P. 342–358. (Lect. Notes Comput. Sci.; V. 6733).

20. Kolomeec N. A., Sutormin I. A., Bykov D. A., Panferov M. A., Bonich T. A. On additive differential probabilities of the composition of bitwise exclusive-or and a bit rotation. Ithaca, NY: Cornell Univ., 2023. 35 p. (Cornell Univ. Libr. e-Print Archive; arXiv:2303.04097).

21. Mouha N., Kolomeec N. A., Akhtiamov D. [et al.]. Maximums of the additive differential probability of exclusive-or // IACR Trans. Symmetric Cryptol. 2021. V. 2021, No. 2. P. 292–313.

22. Gorodilova A. A., Tokareva N. N., Agievich S. V. [et al.]. An overview of the Eighth International Olympiad in Cryptography «Non-Stop University Crypto» // Сиб. электрон. мат. изв. 2022. Т. 19, № 1. С. A.9–A.37.

23. Agievich S. V., Gorodilova A. A., Kolomeec N. A. [et al.]. Problems, solutions and experience of the first international student's Olympiad in cryptography // Прикл. дискрет. математика. 2015. № 3. С. 41–62.

Мокроусов Антон Сергеевич
Коломеец Николай Александрович

Статья поступила
3 мая 2023 г.
После доработки —
16 октября 2023 г.
Принята к публикации
22 декабря 2023 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
April–June 2024. Vol. 31, No. 2. P. 108–135

UDC 519.7 DOI: 10.33048/daio.2024.31.769

ADDITIVE DIFFERENTIALS FOR ARX MAPPINGS WITH PROBABILITY EXCEEDING 1/4

A. S. Mokrousov[a] and *N. A. Kolomeec*[b]

Novosibirsk State University,
2 Pirogov Street, 630090 Novosibirsk, Russia
E-mail: [a] settingx@mail.ru, [b] kolomeec@math.nsc.ru

Abstract. We consider the additive differential probabilities of functions $x \oplus y$ and $(x \oplus y) \lll r$, where $x, y \in \mathbb{Z}_2^n$ and $1 \leqslant r < n$. The probabilities are used for the differential cryptanalysis of ARX ciphers that operate only with addition modulo 2^n, bitwise XOR ($\oplus$) and bit rotations ($\lll r$). A complete characterization of differentials whose probability exceeds 1/4 is obtained. All possible values of their probabilities are $1/3 + 4^{2-i}/6$ for $i \in \{1, \ldots, n\}$. We describe differentials with each of these probabilities and calculate the number of these values. We also calculate the number of all considered differentials. It is $48n - 68$ for $x \oplus y$ and $24n - 30$ for $(x \oplus y) \lll r$, where $n \geqslant 2$. We compare differentials of both mappings under the given constraint. Tab. 6, bibliogr. 23.

Keywords: ARX scheme, differential probabilities, modulo addition, XOR, bit rotation.

References

1. **A. Shimizu** and **S. Miyaguch,** Fast data encipherment algorithm FEAL, in *Advances in Cryptology — EUROCRYPT'87* (Proc. Workshop Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, Apr. 13–15, 1987) (Springer, Heidelberg, 1988), pp. 267–278 (Lect. Notes Comput. Sci., Vol. 304), DOI: 10.1007/3-540-39118-5_24.
2. **N. Ferguson, S. Lucks, B. Schneier,** [et al.], The Skein Hash Function Family (Univ. California, Santa Barbara, CA, 2008), URL: www.schneier.com/wp-content/uploads/2015/01/skein.pdf (accessed Apr. 3, 2024).

English transl.: *Journal of Applied and Industrial Mathematics* **18** (2), 294–311 (2024), DOI: 10.1134/S199047892402011X.

3. **R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks,** and **L. Wingers,** The SIMON and SPECK families of lightweight block ciphers (Univ. California, San Diego, 2013) (Cryptol. ePrint Archive, Paper ID 2013/404), URL: `eprint.iacr.org/2013/404` (accessed June 1, 2024).
4. **D. J. Bernstein,** Salsa20 specification (Univ. Ill. Chic., Chicago, 2007), URL: `cr.yp.to/snuffle/spec.pdf` (accessed June 1, 2024).
5. **D. J. Bernstein,** ChaCha, a variant of Salsa20 (Univ. Ill. Chic., Chicago, 2008), URL: `https://cr.yp.to/chacha/chacha-20080128.pdf` (accessed June 1, 2024).
6. **B. Koo, D. Roh, H. Kim, Y. Jung, D. Lee,** and **D. Kwon,** CHAM: A family of lightweight block ciphers for resource-constrained devices, in *Information Security and Cryptology — ICISC 2017* (Rev. Sel. Pap. 20th Int. Conf., Seoul, South Korea, Nov. 29 – Dec. 1, 2017) (Springer, Cham, 2017), pp. 3–25 (Lect. Notes Comput. Sci., Vol. 10779), DOI: `10.1007/978-3-319-78556-1_1`.
7. **D. Roh, B. Koo, Y. Jung, I. Jeong, D. Lee, D. Kwon,** and **W. Kim,** Revised version of block cipher CHAM, in *Information Security and Cryptology — ICISC 2019* (Rev. Sel. Pap. 22th Int. Conf., Seoul, South Korea, Dec. 4–6, 2019) (Springer, Cham, 2020), pp. 1–19 (Lect. Notes Comput. Sci., Vol. 11975), DOI: `10.1007/978-3-030-40921-0_1`.
8. **N. Mouha, B. Mennink, A. Herrewege, D. Watanabe, B. Preneel,** and **I. Verbauwhede,** Chaskey: An efficient MAC algorithm for 32-bit microcontrollers, in *Selected Areas in Cryptography — SAC 2014* (Rev. Sel. Pap. 21th Int. Workshop, Montreal, Canada, Aug. 14–15, 2014) (Springer, Cham, 2014), pp. 306–323 (Lect. Notes Comput. Sci., Vol. 8781).
9. **E. Biham** and **A. Shamir,** Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.* **4**, 3–72 (1991).
10. **A. Biryukov** and **V. Velichkov,** Automatic search for differential trails in ARX ciphers, in *Topics in Cryptology — CT-RSA 2014* (Proc. Cryptographer's Track at the RSA Conf., San Francisco, USA, Feb. 25–28, 2014) (Springer, Cham, 2014), pp. 227–250 (Lect. Notes Comput. Sci., Vol. 8366), DOI: `10.1007/978-3-319-04852-9_12`.
11. **G. Leurent,** Analysis of differential attacks in ARX constructions, in *Advances in Cryptology — ASIACRYPT 2012* (Proc. 18th Int. Conf. Theory and Application of Cryptology and Information Security, Beijing, China, Dec. 2–6, 2012) (Springer, Heidelberg, 2012), pp. 226–243 (Lect. Notes Comput. Sci., Vol. 7658), DOI: `10.1007/978-3-642-34961-4_15`.
12. **G. Leurent,** Construction of differential characteristics in ARX designs application to Skein, in *Advances in Cryptology — CRYPTO 2013* (Proc. 33rd Annu. Cryptology Conf., Santa Barbara, CA, USA, Aug. 18–22, 2013), Pt. I (Springer, Heidelberg, 2013), pp. 241–258 (Lect. Notes Comput. Sci., Vol. 8042), DOI: `10.1007/978-3-642-40041-4_14`.
13. **F. M. Malyshev,** Probabilistic characteristics of differential and linear relations for nonhomogeneous linear medium, *Mat. Vopr. Kriptogr.* **10** (1), 41–72 (2019) [Russian].
14. **F. M. Malyshev,** Differential characteristics of base operations in ARX-ciphers, *Mat. Vopr. Kriptogr.* **11** (4), 97–105 (2020) [Russian].

15. T. A. Berson, Differential cryptanalysis mod 2^{32} with applications to MD5, in *Advances in Cryptology — EUROCRYPT'92* (Proc. Workshop Theory and Application of Cryptographic Techniques, Balatonfüred, Hungary, May 24–28, 1992) (Springer, Heidelberg, 1992), pp. 71–80 (Lect. Notes Comput. Sci., Vol. 658).

16. M. A. Daum, Cryptanalysis of hash functions of the MD4-family, *PhD Thesis* (Ruhr-Univ. Bochum, Bochum, 2005).

17. H. Lipmaa, J. Wallén and **P. Dumas,** On the additive differential probability of exclusive-or, in *Fast Software Encryption* (Rev. Pap. 11th Int. Workshop, Delhi, India, Feb. 5–7, 2004) (Springer, Heidelberg, 2004), pp. 317–331 (Lect. Notes Comput. Sci., Vol. 3017).

18. N. Mouha, V. Velichkov, C. De Canniére and **B. Preneel,** The differential analysis of S-functions, in *Selected Areas in Cryptography* (Rev. Sel. Pap. 17th Int. Workshop, Waterloo, Canada, Aug. 12–13, 2010) (Springer, Heidelberg, 2011), pp. 36–56 (Lect. Notes Comput. Sci., Vol. 6544).

19. V. Velichkov, N. Mouha, C. De Canniére and **B. Preneel,** The additive differential probability of ARX, in *Fast Software Encryption* (Rev. Sel. Pap. 18th Int. Workshop, Lyngby, Denmark, Feb. 13–16, 2011) (Springer, Heidelberg, 2011), pp. 342–358 (Lect. Notes Comput. Sci., Vol. 6733).

20. N. A. Kolomeec, I. A. Sutormin, D. A. Bykov, M. A. Panferov, and **T. A. Bonich,** On additive differential probabilities of the composition of bitwise exclusive-or and a bit rotation (Cornell Univ., Ithaca, NY, 2023) (Cornell Univ. Libr. e-Print Archive, arXiv:2303.04097).

21. N. Mouha, N. A. Kolomeec, D. Akhtiamov, [et al.], Maximums of the additive differential probability of exclusive-or, *IACR Trans. Symmetric Cryptol.* **2021** (2), 292–313 (2021).

22. A. A. Gorodilova, N. N. Tokareva, S. V. Agievich, [et al.], An overview of the Eighth International Olympiad in Cryptography "Non-Stop University Crypto", *Sib. Elektron. Mat. Izv.* **19** (1), A.9–A.37 (2022).

23. S. V. Agievich, A. A. Gorodilova, N. A. Kolomeec, [et al.], Problems, solutions and experience of the first international student's Olympiad in cryptography, *Prikl. Diskretn. Mat.,* No. 3, 41–62 (2015).

Anton S. Mokrousov
Nikolay A. Kolomeec

Received May 3, 2023
Revised October 16, 2023
Accepted December 22, 2023