

УДК 519.1, 519.7

**ОЦЕНКА НЕЛИНЕЙНОСТИ КОРРЕЛЯЦИОННО-ИММУННЫХ
БУЛЕВЫХ ФУНКЦИЙ¹**

А. В. Халявин

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

Исследуется точность оценки нелинейности булевых функций от n переменных, корреляционно-иммунных порядка m : $nl(f) \leq 2^{n-1} - 2^m$. Показывается, что для всех пар значений $n \geq 512$ и $0 < m < n - 1$, кроме двух серий $m = 2^s$, $n = 2^{s+1} + 1$ и $m = 2^s + 1$, $n = 2^{s+1} + 2$ при $s \geq 0$, эту оценку можно улучшить до $nl(f) \leq 2^{n-1} - 2^{m+1}$. Справедливость результата для $n < 512$, $0 < m < n - 1$ проверена на компьютере.

Ключевые слова: булевы функции, нелинейность, корреляционная иммунность.

Введение

Булевы функции активно применяются при построении быстрых блочных и поточных шифров. Стойкость получающихся шифров напрямую зависит от характеристик этих булевых функций. Наиболее важными из них являются корреляционная иммунность, нелинейность, устойчивость, алгебраическая иммунность. Отсюда вытекает сложная задача построения функций с наилучшими значениями этих параметров. Большинство вопросов в этой области по-прежнему остаются открытыми.

В частности, не известна точная граница нелинейности для корреляционно-иммунных порядка m функций от n переменных. В работах [1–3] независимо друг от друга была доказана оценка $nl(f) \leq 2^{n-1} - 2^m$. При $0 < m \leq n/2 - 1$ лучшую оценку дает равенство Парсеваля, из которого следует $nl(f) \leq 2^{n-1} - 2^{n/2-1}$. При этом равенство $nl(f) = 2^{n-1} - 2^{n/2-1}$ достигается лишь для бент-функций, которые не бывают корреляционно-иммунными. Установлено, что при $m > n/2 - 1$ из равенства $nl(f) = 2^{n-1} - 2^m$ следует комбинаторное соотношение для n и m , которое будет дано далее. Единственными известными значениями параметров n и $\max(0, n/2 - 1) < m < n - 1$, при которых оно выполняется, являются серии $m = 2^s$, $n = 2^{s+1} + 1$ и $m = 2^s + 1$, $n = 2^{s+1} + 2$ при $s \geq 0$. Следует отметить, что для малых значений s функции с этими параметрами действительно существуют. В частности, легко построить функции для $n = 3, 5, 6$ (примеры можно найти в статье [4]), а в работе [5] построены примеры функций для $n = 9, 10$. Однако доказать отсутствие других подходящих пар значений n и m долгое время не удавалось. Ближе всего к этому вопросу удалось подобраться в работе [6], где было доказано соотношение

$$\frac{n}{2} + \frac{1}{2} \log_2 n + \frac{1}{2} \log_2 \left(\frac{\pi}{2} e^{8/9} \right) - 1 > m \geq \frac{n-1}{2} \quad \text{для } n \geq 12.$$

¹Работа поддержана грантом РФФИ (проект 08-01-00863), грантом ведущих научных школ РФ (проект НШ-4437.2010.1) и программой фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

В данной работе докажем, что при $n \geq 512$ никаких других подходящих пар, кроме указанных двух серий, не существует. Значения $n < 512$ легко проверить на компьютере.

1. Основные определения

Пусть $F_2 = \{0, 1\}$ — поле из двух элементов. Под *булевыми функциями* будем понимать отображения $f : F_2^n \mapsto F_2$. *Весом* $\text{wt}(u)$ набора $u \in F_2^n$ назовём количество единиц в нём. *Весом* $\text{wt}(f)$ булевой функции f будем называть число её единичных значений. *Расстояние* между булевыми функциями — это число наборов, значения функций на которых различаются. *Нелинейностью* $\text{nl}(f)$ булевой функции f назовём расстояние до ближайшей к ней аффинной функции. Будем говорить, что набор $x \in F_2^n$ *мажорируется* набором $y \in F_2^n$, и обозначим это $x \preceq y$, если $x_i \leq y_i$ для всех $i = 1, \dots, n$. *Подфункцией* булевой функции f назовем функцию, полученную из неё подстановкой констант вместо некоторых аргументов. Булева функция f от n переменных называется *корреляционно-иммунной порядка* m , $1 \leq m \leq n$, если для всех её подфункций f' от $n - m$ переменных выполняется соотношение $\text{wt}(f') = \text{wt}(f)/2^m$. Для изучения корреляционно-иммунных функций активно используется *преобразование Уолша*

$$W_f(u) = \sum_{x \in F_2^n} (-1)^{f(x) + (x, u)},$$

где (x, u) — скалярное произведение векторов x и u . Числа $W_f(u)$ называются коэффициентами Уолша и обладают множеством замечательных свойств. Сформулируем некоторые из них.

Равенство Парсеваля:

$$\sum_{u \in F_2^n} W_f^2(u) = 2^{2n}.$$

Равенство Саркара:

$$\sum_{u \in F_2^n, u \preceq w} W_f(u) = 2^n - 2^{\text{wt}(w)+1} \text{wt}(f_w),$$

где f_w — подфункция f , полученная подстановкой нулей вместо аргументов x_i для всех таких i , что $w_i = 1$.

Многие свойства булевой функции f могут быть выражены в терминах коэффициентов Уолша. В частности, уравновешенность равносильна $W_f(0) = 0$, а корреляционная иммунность порядка m — условию $W_f(u) = 0$ при $1 \leq \text{wt}(u) \leq m$ [7]. Кроме того, нелинейность булевой функции выражается равенством $\text{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |W_f(u)|$.

Корреляционно-иммунную порядка $m > 0$ функцию f от n переменных будем называть *экстремальной*, если $\text{nl}(f) = 2^{n-1} - 2^m$.

2. Строение спектра экстремальных функций

Рассмотрим корреляционно-иммунную порядка m , $0 < m < n - 1$, булеву функцию f от n переменных. Известно [1, 4], что все её коэффициенты Уолша $W_f(u)$ делятся на 2^{m+1} .

Отсюда следует, что найдется коэффициент Уолша, по модулю не меньший 2^{m+1} , а значит, $\text{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |W_f(u)| \leq 2^{n-1} - 2^m$. Кроме того, если неравенство строгое, то есть коэффициент Уолша, который по модулю не меньше чем 2^{m+2} , а значит, выполнено $\text{nl}(f) \leq 2^{n-1} - 2^{m+1}$.

Если $m < (n-1)/2$, то, с учётом равенства Парсеваля, имеем $\text{nl}(f) \leq 2^{n-1} - 2^{n/2-1} \leq 2^{n-1} - 2^m$. Равенство $\text{nl}(f) = 2^{n-1} - 2^{n/2-1}$ возможно только на бент-функциях, которые не обладают свойством корреляционной иммунности. Значит, экстремальные функции могут существовать только при $m \geq (n-1)/2$. Изучим строение спектра таких функций более подробно.

Теорема 1. Если корреляционно-иммунная порядка m булева функция f от n переменных, $m \leq n-2$, имеет нелинейность $2^{n-1} - 2^m$, то для всех $u \in F_2^n$ выполнено условие

$$W_f(u) \equiv \pi_{\text{wt}(u)} 2^{m+1} \pmod{2^{m+2}},$$

где $\pi_0 = 1$, $\pi_1 = \pi_2 = \dots = \pi_m = 0$, $\pi_i = \sum_{j=0}^{i-1} \pi_j \binom{i}{j} \pmod{2}$ при $i > m$.

Доказательство. В силу корреляционной иммунности функции f имеет место $W_f(u) = 0$ при $0 < \text{wt}(u) \leq m$.

Как уже отмечено, $W_f(0)$ делится на 2^{m+1} . Предположим, что $W_f(0)$ делится на 2^{m+2} . Докажем индукцией по $\text{wt}(u)$, что в таком случае все коэффициенты $W_f(u)$ также делятся на 2^{m+2} . База для $\text{wt}(u) \leq m$ очевидна. Докажем переход. Пусть $\text{wt}(u) > m$. По равенству Саркара $\sum_{v \preceq u} W_f(v) = 2^n - 2^{\text{wt}(u)+1} \text{wt}(f_u)$. Правая часть делится на 2^{m+2} . Кроме того, все слагаемые в сумме, кроме $W_f(u)$, делятся на 2^{m+2} по предположению индукции. Значит, и $W_f(u)$ делится на 2^{m+2} . Переход доказан. Из того, что все коэффициенты Уолша делятся на 2^{m+2} , получаем противоречие: $\text{nl}(f) = 2^{n-1} - \frac{1}{2} \max_u |W_f(u)| \leq 2^{n-1} - 2^{m+1}$. Следовательно, $W_f(0) \equiv 2^{m+1} \pmod{2^{m+2}}$.

Докажем теперь утверждение теоремы при $\text{wt}(u) > m$ индукцией по $\text{wt}(u)$. Как и раньше, получаем, что $\sum_{v \preceq u} W_f(v) \equiv 0 \pmod{2^{m+2}}$. С другой стороны, по предположению индукции

$$\sum_{v \preceq u} W_f(v) \equiv \sum_{j=0}^{\text{wt}(u)-1} \binom{\text{wt}(u)}{j} \pi_j 2^{m+1} + W_f(u) \equiv \pi_{\text{wt}(u)} 2^{m+1} + W_f(u) \pmod{2^{m+2}},$$

откуда ввиду $2^{m+1} \equiv -2^{m+1} \pmod{2^{m+2}}$ получаем требуемое. Переход доказан. ■

Заметим теперь, что из $\text{nl}(f) = 2^{n-1} - \frac{1}{2} \max_u |W_f(u)| = 2^{n-1} - 2^m$ следует $|W_f(u)| \leq 2^{m+1}$, а значит, $|W_f(u)| = \pi_{\text{wt}(u)} 2^{m+1}$. Применяя равенство Парсеваля, получаем следующую теорему.

Теорема 2. Если существует корреляционно-иммунная порядка m булева функция от n переменных, $m \leq n-2$, с нелинейностью $2^{n-1} - 2^m$, то выполнено

$$\sum_{j=0}^n \binom{n}{j} \pi_j = 2^{2n-2m-2}. \quad (1)$$

Далее покажем в лемме 7, что равенство (1) выполнено при $n = 2^{s+1} + 1$, $m = 2^s$ и $n = 2^{s+1} + 2$, $m = 2^s + 1$, где $s \geq 0$. Однако ранее оставался открытым вопрос о возможности выполнения равенства для других значений n и m . Последующие разделы посвящены доказательству того, что других подходящих пар при $n-2 \geq m \geq (n-1)/2$, $n \geq 512$ не существует.

3. Остатки биномиальных коэффициентов по модулю 2^k

Известно, что двоичная запись чисел n и m тесно связана с остатком $\binom{n}{m}$ по модулю 2^k . Покажем, как именно устроена эта связь. Обозначим $F(1) = 1$, $F(x) = \prod_{i=1}^{x-1} (2i+1)$ при $x > 1$, $F(x) = 1 / \prod_{i=x}^0 (2i+1)$ при $x \leq 0$. Поскольку все множители нечётны, то можно говорить о значении $F(x)$ по модулю 2^k для всех целых x . Кроме того, легко видеть, что $F(x) = (2x)!/x!$ при $x \geq 0$.

Лемма 1. $F(x + 2^{k-1}) \equiv cF(x) \pmod{2^k}$ для некоторого c , зависящего только от k .

Доказательство. $F(x + 2^{k-1})/F(x) \equiv \prod_{i=x}^{x+2^{k-1}-1} (2i+1) \equiv \prod_{i=0}^{2^{k-1}-1} (2i+1) \pmod{2^k}$.

Последнее равенство выполнено потому, что в обеих частях стоит произведение всех нечётных остатков по модулю 2^k . Таким образом, утверждение теоремы будет выполнено, если в качестве c взять $\prod_{i=0}^{2^{k-1}-1} (2i+1)$. ■

Введем еще одну функцию $G(x, y) = \frac{F(x)}{F(y)F(x-y)}$.

Лемма 2. $G(x, y) \pmod{2^k}$ периодична с периодом 2^{k-1} по обоим аргументам.

Доказательство.

$G(x, y + 2^{k-1}) \equiv \frac{F(x)}{F(y + 2^{k-1})F(x - y - 2^{k-1})} \equiv \frac{F(x)}{cF(y)c^{-1}F(x - y)} \equiv \frac{F(x)}{F(y)F(x - y)} \equiv G(x, y) \pmod{2^k}$. Отсюда следует периодичность по второму аргументу. Для первого аргумента выкладки аналогичны:

$G(x + 2^{k-1}, y) \equiv \frac{F(x + 2^{k-1})}{F(y)F(x - y + 2^{k-1})} \equiv \frac{cF(x)}{F(y)cF(x - y)} \equiv \frac{F(x)}{F(y)F(x - y)} \equiv G(x, y) \pmod{2^k}$. ■

Лемма 3. $\binom{2n}{2m} = \binom{n}{m} G(n, m)$.

Доказательство. Если $m > n$, то обе части равны нулю. В противном случае $\binom{2n}{2m} = \frac{2n!}{2m!(2n-2m)!} = \frac{(2n)!m!(n-m)!}{n!(2m)!(2n-2m)!} \cdot \frac{n!}{m!(n-m)!} = \frac{F(n)}{F(m)F(n-m)} \binom{n}{m} = \binom{n}{m} G(n, m)$. ■

Заметим, что $\binom{2n+1}{2m} = \binom{2n}{2m} \frac{2n+1}{2n-2m+1}$, $\binom{2n}{2m+1} = \binom{2n}{2m} \frac{2n-2m}{2m+1}$, $\binom{2n+1}{2m+1} = \binom{2n}{2m} \frac{2n+1}{2m+1}$. Рассмотрев эти равенства по модулю 2^k , получаем следующую теорему.

Теорема 3. $\binom{2n+a}{2m+b} \equiv \binom{n}{m} H((2n+a) \bmod 2^k, (2m+b) \bmod 2^k) \pmod{2^k}$, где $a, b \in \{0, 1\}$, $H(2x, 2y) = G(x, y)$, $H(2x+1, 2y) = G(x, y) \frac{2x+1}{2x-2y+1}$, $H(2x, 2y+1) = G(x, y) \frac{2x-2y}{2y+1}$, $H(2x+1, 2y+1) = G(x, y) \frac{2x+1}{2y+1}$.

Обозначим M_k матрицу значений функции H по модулю 2^k :

$$M_k = \begin{bmatrix} H(0,0) \bmod 2^k & \cdots & H(0,2^k-1) \bmod 2^k \\ \vdots & \ddots & \vdots \\ H(2^k-1,0) \bmod 2^k & \cdots & H(2^k-1,2^k-1) \bmod 2^k \end{bmatrix}.$$

Элемент этой матрицы в $(i+1)$ -й строке и $(j+1)$ -м столбце будем записывать как $M_k(i,j) = H(i,j) \bmod 2^k$. Матрицы с маленькими индексами имеют следующие значения:

$$M_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 1 & 0 & 7 & 6 & 1 & 4 & 7 & 2 \\ 1 & 1 & 1 & 5 & 5 & 5 & 5 & 1 \\ 1 & 2 & 1 & 0 & 5 & 6 & 5 & 4 \\ 1 & 3 & 3 & 1 & 1 & 3 & 3 & 1 \\ 1 & 4 & 3 & 2 & 1 & 0 & 3 & 6 \\ 1 & 5 & 5 & 5 & 5 & 1 & 1 & 1 \\ 1 & 6 & 5 & 4 & 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 & 1 & 7 & 7 & 1 \end{bmatrix}.$$

Пусть $wa = a_{s-1} \dots a_1 a_0$ и $wb = b_{s-1} \dots b_1 b_0$ — два двоичных слова. Обозначим $\Pi_k(wa, wb) = \prod_{i=0}^{s-k} M_k \left(\sum_{j=0}^{k-1} a_{i+j} 2^j, \sum_{j=0}^{k-1} b_{i+j} 2^j \right)$.

Для чисел $a = \sum_{j=0}^{s-1} a_j 2^j$ и $b = \sum_{j=0}^{s-1} b_j 2^j$, последовательно применяя теорему 3 вместе с определениями M_k и Π_k , получим следующее утверждение.

Лемма 4. $\begin{pmatrix} b \\ a \end{pmatrix} \equiv \Pi_k(wb, wa) \begin{pmatrix} \sum_{j=0}^{k-2} b_{s-k+1+j} 2^j \\ \sum_{j=0}^{k-2} a_{s-k+1+j} 2^j \end{pmatrix} \pmod{2^k}.$

Для каждой матрицы $M = \{m_{ij}\}$ размера $2^k \times 2^k$ введём функцию $M(wa, wb) = m_{1+[a/2^{s-k}], 1+[b/2^{s-k}]}$. Аналогично для строки или столбца $\{m_i\}$ размера 2^k введём функцию $M(wa) = m_{1+[a/2^{s-k}]}$. Определим семейство матриц

$$M_k^* = \begin{bmatrix} \binom{0}{0} & \cdots & \binom{0}{2^k-1} \\ \vdots & \ddots & \vdots \\ \binom{2^k-1}{0} & \cdots & \binom{2^k-1}{2^k-1} \end{bmatrix}.$$

Для маленьких k получаем $M_0^* = [1]$, $M_1^* = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $M_2^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix}$. Тогда биномиальные коэффициенты можно полностью выразить через функции от их двоичных записей:

$$\begin{pmatrix} b \\ a \end{pmatrix} \equiv \Pi_k(wb, wa) M_{k-1}^*(wb, wa) \pmod{2^k}. \quad (2)$$

4. Делимость сумм биномиальных коэффициентов

Для начала выведем более простую формулу для π_i .

Лемма 5. При $i > m$ выполнено

$$\sum_{j=m}^{i-1} \binom{j}{m} \binom{i}{j} \equiv \binom{i}{m} \pmod{2}.$$

Доказательство. Из строения матрицы M_1^* видно, что биномиальный коэффициент $\binom{a}{b}$ отличен от 0 по модулю 2 тогда и только тогда, когда двоичная запись a мажорирует двоичную запись b . Поэтому если двоичная запись i не мажорирует двоичную запись m , то правая часть чётна; левая часть также чётна, поскольку в силу транзитивности мажорирования хотя бы один из множителей в каждом слагаемом будет чётным. Если же двоичная запись i мажорирует двоичную запись m и в ней на k единичных бит больше, то в левой части будет $2^k - 1$ нечётных слагаемых. Поскольку $i \neq m$, то $k > 0$; значит, левая часть будет нечётной. ■

Лемма 6. При $i > m$ выполнено

$$\pi_i \equiv \binom{i-1}{m} \pmod{2}.$$

Доказательство. Докажем это утверждение индукцией по i . База $i = m + 1$: $\pi_{m+1} = 1 = \binom{m}{m}$. Докажем переход:

$$\begin{aligned} \pi_i &= 1 + \sum_{j=m+1}^{i-1} \pi_j \binom{i}{j} \equiv 1 + \sum_{j=m+1}^{i-1} \binom{j-1}{m} \binom{i}{j} = 1 + \sum_{j=m+1}^{i-1} \binom{j-1}{m} \binom{i-1}{j} + \\ &+ \sum_{j=m+1}^{i-1} \binom{j-1}{m} \binom{i-1}{j-1} \equiv 1 + \sum_{j=m+1}^{i-2} \pi_j \binom{i-1}{j} + \binom{i-2}{m} \binom{i-1}{i-1} + \\ &+ \sum_{j=m}^{i-2} \binom{j}{m} \binom{i-1}{j} = \pi_{i-1} + \binom{i-2}{m} + \sum_{j=m}^{i-2} \binom{j}{m} \binom{i-1}{j} \equiv \binom{i-2}{m} + \binom{i-2}{m} + \\ &+ \sum_{j=m}^{i-2} \binom{j}{m} \binom{i-1}{j} \equiv \sum_{j=m}^{i-2} \binom{j}{m} \binom{i-1}{j} \equiv \binom{i-1}{m} \pmod{2}. \end{aligned}$$

Здесь последнее равенство следует из леммы 5 ввиду $i > m + 1$. ■

Используя лемму 6, условие (1) можно преобразовать к виду

$$1 + \sum_{\substack{i, \\ \binom{i}{m} \equiv 1 \pmod{2}}} \binom{n}{i+1} = 2^{2n-2m-2}. \quad (3)$$

Лемма 7. Равенства (1) и (3) верны при $n = 2^{s+1} + 1$, $m = 2^s$ и $n = 2^{s+1} + 2$, $m = 2^s + 1$, где $s \geq 0$.

Доказательство. Воспользуемся тем, что $\binom{i}{m} \equiv 1 \pmod{2}$ тогда и только тогда, когда двоичная запись i мажорирует двоичную запись m . В случае $n = 2^{s+1} + 1$, $m = 2^s$

сумма равна

$$\begin{aligned} 1 + \sum_{\substack{i, \\ \binom{i}{m} \equiv 1 \pmod{2}}} \binom{n}{i+1} &= 1 + \sum_{i=2^s+1}^{2^{s+1}} \binom{2^{s+1}+1}{i} = \\ &= \sum_{i=2^s+1}^{2^{s+1}+1} \binom{2^{s+1}+1}{i} = 2^{2^{s+1}} = 2^{2n-2m-2}. \end{aligned}$$

В случае же $n = 2^{s+1} + 2$, $m = 2^s + 1$ сумма равна

$$\begin{aligned} 1 + \sum_{\substack{i, \\ \binom{i}{m} \equiv 1 \pmod{2}}} \binom{n}{i+1} &= 1 + \sum_{i=2^s+2, 2|i}^{2^{s+1}} \binom{2^{s+1}+2}{i} = \\ &= \sum_{i=2^s+2, 2|i}^{2^{s+1}+2} \binom{2^{s+1}+2}{i} = \frac{1}{2} \sum_{i=0, 2|i}^{2^{s+1}+2} \binom{2^{s+1}+2}{i} = \frac{1}{2} 2^{2^{s+1}+1} = 2^{2^{s+1}} = 2^{2n-2m-2}. \end{aligned}$$

Лемма доказана. ■

Выразим теперь условие суммирования в (3) в терминах слов. Пусть $s = \lceil \log_2 \max(n, m) \rceil + 1$, wn и wt — двоичные записи длины s чисел n и m соответственно. Если $i = 2^s - 1$, то $i + 1 = 2^s > n$, а значит, $\binom{n}{i+1} = 0$. Поэтому значение $i = 2^s - 1$ можно исключить из суммирования. Используя теперь (2), получаем, что

$$\begin{aligned} 1 + \sum_{\substack{i, \\ \binom{i}{m} \equiv 1 \pmod{2}}} \binom{n}{i+1} &\equiv \\ &\equiv 1 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \leq wi}} \Pi_k(wn, wi+1) M_{k-1}^*(wn, wi+1) \pmod{2^k}, \end{aligned}$$

где под $wi + 1$ понимается слово той же длины s , представляющее двоичную запись числа $i + 1 \pmod{2^s}$. Поскольку $i < 2^s - 1$, это слово всегда представляет число $i + 1$.

Обозначим $\bar{w}$ — натуральное число, соответствующее слову w ; $|w|$ — длина слова w .

Лемма 8. Пусть $\bar{wt} < \bar{wn}$. Тогда

$$\sum_{\substack{wi \neq 11\dots 1, \\ wt \leq wi}} \Pi_1(wn, wi+1) \equiv 1 \pmod{2}.$$

Доказательство. Будем доказывать это утверждение индукцией по длине слов. Если $|wn| = 1$, то $wn = 1$, $wt = 0$. В сумме оказывается только одно слагаемое, соответствующее $wi = 0$: $\Pi_1(1, 1) = 1$. База индукции доказана. Докажем переход. Пусть утверждение верно для $|wt| = |wn| \leq k$; докажем его для $|wt| = |wn| = k + 1$.

Пусть $wt = 1w_1$, $wn = 1w_2$, $\bar{w}_1 < \bar{w}_2$. Получаем

$$\sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \leq wi}} \Pi_1(1w_2, wi+1) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \leq wi}} \Pi_1(1w_2, 1(wi+1)) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \leq wi}} \Pi_1(w_2, wi+1).$$

Последнее выражение равно 1 по модулю 2 в силу предположения индукции.

Пусть $wt = 0w_1$, $wn = 1w_2$. Получаем

$$\begin{aligned} \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_1(1w_2, wi + 1) &= \Pi_1(1w_2, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(1w_2, 0(wi + 1)) + \\ + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(1w_2, 1(wi + 1)) &= 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} (\Pi_1(w_2, wi + 1) + \Pi_1(w_2, wi + 1)) \equiv 1 \pmod{2}. \end{aligned}$$

Пусть $wt = 0w_1$, $wn = 0w_2$, $\overline{w_1} < \overline{w_2}$. Получаем

$$\begin{aligned} \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_1(0w_2, wi + 1) &= \Pi_1(0w_2, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(0w_2, 0(wi + 1)) + \\ + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(0w_2, 1(wi + 1)) &= 0 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} (\Pi_1(w_2, wi + 1) + \Pi_1(w_2, wi + 1) \cdot 0) = \\ &= \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \equiv 1 \pmod{2}. \end{aligned}$$

Последнее сравнение верно в силу предположения индукции. Переход доказан. ■

Лемма 9. Пусть $\overline{wt} < \overline{wn}$. Тогда

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} (wn) + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (wn, wi + 1) \equiv 1 \pmod{2}.$$

Доказательство. Если длина слов wt и wn равна 1, то $wn = 1$, $wt = 0$. Первое слагаемое получается равным нулю, а в сумме оказывается только одно слагаемое, соответствующее $wi = 0$: $\Pi_2(1, 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1, 1) = 1 \cdot 1 = 1$. Равенство доказано.

Пусть теперь длина слов больше 1. Пусть $wt = 1w_1$, $wn = 1w_2$, $\overline{w_1} < \overline{w_2}$. Получаем

$$\begin{aligned} \begin{bmatrix} 1 \\ 0 \end{bmatrix} (1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_2, wi + 1) &\equiv \\ \equiv \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) &\pmod{2}. \end{aligned}$$

К последнему выражению применяем лемму 8 и получаем требуемое.

Пусть $wt = 0w_1$, $wn = 1w_2$. Получаем

$$\begin{aligned} \begin{bmatrix} 1 \\ 0 \end{bmatrix} (1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_2, wi + 1) &= \\ = \Pi_2(1w_2, 100\dots 0) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_2, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(1w_2, 0(wi + 1)) + \\ + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(1w_2, 1(wi + 1)) &\equiv \Pi_1(w_2, 00\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} (\Pi_1(w_2, wi + 1) + \Pi_1(w_2, wi + 1)) \equiv \\ &\equiv 1 \pmod{2}. \end{aligned}$$

Утверждение доказано.

Пусть, наконец, $wt = 0w_1$, $wn = 0w_2$, $\overline{w_1} < \overline{w_2}$. Получаем

$$\begin{aligned} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} (0w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, wi + 1) = \\ & = 1 + \Pi_2(0w_2, 100\dots 0) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 0(wi + 1)) \cdot 0 + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 1 \equiv 1 + \Pi_1(w_2, 00\dots 0) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \equiv \\ & \equiv \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \pmod{2}. \end{aligned}$$

К последнему выражению применяем лемму 8 и получаем требуемое. ■

Лемма 10. Пусть $\overline{wn} \leq \overline{wt}$. Тогда

$$\sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_1(wn, wi + 1) \equiv 0 \pmod{2}.$$

Доказательство. Докажем это утверждение индукцией по длине слов wt и wn . Для слов длины 1 в сумме есть слагаемые лишь при $wt = 0$, а значит, и $wn = 0$. В этом случае единственное слагаемое равно $\Pi_1(0, 1) = 0$. База индукции доказана.

Докажем переход. Пусть утверждение доказано для слов длины не больше k , докажем его для слов длины $k + 1$.

Пусть $wt = 1w_1$, $wn = 1w_2$. Тогда $\overline{w_2} \leq \overline{w_1}$. Получаем

$$\sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_1(1w_2, wi + 1) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(1w_2, 1(wi + 1)) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1).$$

По предположению индукции это выражение сравнимо с 0 по модулю 2.

Пусть $wt = 1w_1$, $wn = 0w_2$. Получаем

$$\sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_1(0w_2, wi + 1) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(0w_2, 1(wi + 1)) = 0.$$

Утверждение доказано.

Пусть $wt = 0w_1$, $wn = 0w_2$. Тогда $\overline{w_2} \leq \overline{w_1}$. Получаем

$$\begin{aligned} & \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_1(0w_2, wi + 1) = \Pi_1(0w_2, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(0w_2, 0(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(0w_2, 1(wi + 1)) = 0 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} (\Pi_1(w_2, wi + 1) + \Pi_1(w_2, wi + 1) \cdot 0) = \\ & = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1). \end{aligned}$$

По предположению индукции это выражение сравнимо с 0 по модулю 2. Переход доказан. ■

Теорема 4. Пусть для некоторых непустых слов w_1 и w_2 выполнено $wt = 10w_1$, $wn = 11w_2$ и $\overline{w_2} > \overline{w_1}$; или $wt = 01w_1$, $wn = 10w_2$ и $\overline{w_2} \leq \overline{w_1}$. Тогда

$$1 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_2(wn, wi + 1) M_1^*(wn, wi + 1) \equiv 2 \pmod{4}.$$

Доказательство. Рассмотрим первый случай: $wt = 10w_1$, $wn = 11w_2$ и $\overline{w_2} > \overline{w_1}$. Поскольку wt начинается с 1, то и wi начинается с 1. Получаем

$$\begin{aligned} & 1 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preceq wi}} \Pi_2(wn, wi + 1) M_1^*(wn, wi + 1) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preceq wi}} \Pi_2(11w_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (11w_2, 1(wi + 1)) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preceq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 3 & 1 \end{bmatrix} (wi + 1) \cdot 1. \end{aligned}$$

Выделяем слагаемое $wi = 011\dots 1$, а остальные слагаемые разбиваем на две суммы:

$$\begin{aligned} & 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preceq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 3 & 1 \end{bmatrix} (wi + 1) = \\ & = 1 + \Pi_2(1w_2, 100\dots 0) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(1w_2, 0(wi + 1)) \cdot 3 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(1w_2, 1(wi + 1)) \cdot 1 = \\ & = 1 + \begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \cdot 3 \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} (w_2, wi + 1) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} (w_2, wi + 1) \equiv \\ & \equiv \begin{bmatrix} 2 \\ 0 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix} (w_2, wi + 1) \pmod{4}. \end{aligned}$$

Сокращая на 2, получаем, что утверждение теоремы преобразуется к виду

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1) \equiv 1 \pmod{2},$$

который в точности совпадает с леммой 9.

Рассмотрим теперь случай $wt = 01w_1$, $wn = 10w_2$ и $\overline{w_2} \leq \overline{w_1}$:

$$\begin{aligned} & 1 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preceq wi}} \Pi_2(wn, wi + 1) M_1^*(wn, wi + 1) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 01w_1 \preceq wi}} \Pi_2(10w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (10w_2, wi + 1) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 01w_1 \preceq wi}} \Pi_2(10w_2, wi + 1) \cdot 1 = 1 + \Pi_2(10w_2, 100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preceq wi}} \Pi_2(10w_2, 0(wi + 1)) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preceq wi}} \Pi_2(10w_2, 1(wi + 1)) = \\ & = 1 + 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preceq wi}} (\Pi_2(0w_2, wi + 1) \begin{bmatrix} 1 & 2 \end{bmatrix} (wi + 1) + \Pi_2(0w_2, wi + 1) \begin{bmatrix} 1 & 0 \end{bmatrix} (wi + 1)) = \\ & = 2 + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preceq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 2 & 2 \end{bmatrix} (wi + 1) = 2 + 2 \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preceq wi}} \Pi_2(0w_2, wi + 1). \end{aligned}$$

Сокращая на 2, получаем, что утверждение преобразуется к виду

$$\sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \equiv 0 \pmod{2}.$$

Продолжая преобразования, получаем

$$\sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \equiv \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \pmod{2}.$$

Утверждение теперь непосредственно следует из леммы 10. ■

Лемма 11. При $\overline{wt} - 2^{|wt|-1} < \overline{wn}$ выполнено

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} (wn) + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 1 \\ 0 \end{bmatrix} (wn) \equiv 1 \pmod{2}.$$

Доказательство. Если wn начинается с 1, то $\begin{bmatrix} 1 \\ 0 \end{bmatrix} (wn) = 0$, а значит, сумма равна нулю. Остается лишь $\begin{bmatrix} 0 \\ 1 \end{bmatrix} (wn) = 1$, что и требуется доказать.

Пусть теперь $wn = 0w_2$. Если $wt = 1w_1$, то получаем $\overline{w_1} < \overline{w_2}$, а выражение преобразуется к виду

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} (0w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \begin{bmatrix} 1 \\ 0 \end{bmatrix} (0w_2) \equiv 0 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \cdot 1 \pmod{2}.$$

Применяя лемму 8, получаем требуемое.

Если $wt = 0w_1$, то выражение преобразуется к виду

$$\begin{aligned} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} (0w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 1 \\ 0 \end{bmatrix} (0w_2) = \\ & = 0 + \Pi_2(0w_2, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 0(wi + 1)) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 1 \equiv \\ & \equiv \Pi_1(w_2, 00\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \equiv 1 \pmod{2}. \end{aligned}$$

Утверждение доказано. ■

Лемма 12. Обозначим 0^t последовательность нулей длины t . При $wt = 0^t 0w_1$, $wn = 0^t 1w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2}$, $t \geq 0$ имеет место

$$1 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (wn, wi + 1) \equiv 0 \pmod{4}.$$

Доказательство. Докажем утверждение индукцией по t . Пусть $t = 0$, откуда $wt = 0w_1$, $wn = 1w_2$. Преобразуем выражение:

$$\begin{aligned} & 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (1w_2, wi + 1) = \\ & = 1 + \Pi_2(1w_2, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(1w_2, 0(wi + 1)) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(1w_2, 1(wi + 1)) \cdot 1 = \end{aligned}$$

$$\begin{aligned}
&= 1 + \begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} (w_2, wi + 1) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 0 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 2 & 2 \\ 0 & 0 \end{bmatrix} (w_2, wi + 1).
\end{aligned}$$

Сокращая на 2 и прибавляя к обеим частям 1, преобразуем утверждение к виду

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 \\ 0 \end{bmatrix} (w_2) \equiv 1 \pmod{2},$$

который совпадает с леммой 11. База индукции доказана.

Пусть утверждение доказано для $t \leq k$, докажем его для $t = k + 1$. Тогда для слов wt и wn получаем представление $wt = 00^k 0w_1$, $n = 00^k 1w_2$. Преобразуем выражение:

$$\begin{aligned}
&1 + \sum_{\substack{wi \neq 11\dots 1, \\ 00^k 0w_1 \preceq wi}} \Pi_2(00^k 1w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (00^k 1w_2, wi + 1) = \\
&= 1 + \Pi_2(00^k 1w_2, 100\dots 0) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (00^k 1w_2, 100\dots 0) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ 0^k 0w_1 \preceq wi}} \Pi_2(00^k 1w_2, 0(wi + 1)) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^k 0w_1 \preceq wi}} \Pi_2(00^k 1w_2, 1(wi + 1)) \cdot 0 = \\
&= 1 + \Pi_2(00^k 1w_2, 100\dots 0) \cdot 0 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^k 0w_1 \preceq wi}} \Pi_2(0^k 1w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^t 1w_2, wi + 1).
\end{aligned}$$

Последнее выражение сравнимо с 2 по модулю 4 по предположению индукции. ■

Лемма 13. При $wt = 0^t 0w_1$, $wn = 0^t 1w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2}$, $t \geq 0$ выполнено

$$\begin{bmatrix} 1 \\ 3 \end{bmatrix} (wn) + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preceq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (wn, wi + 1) \equiv 2 \pmod{4}. \quad (4)$$

Доказательство. Пусть $t = 0$, откуда $wt = 0w_1$, $wn = 1w_2$. Преобразуем выражение:

$$\begin{aligned}
&\begin{bmatrix} 1 \\ 3 \end{bmatrix} (1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preceq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (1w_2, wi + 1) = \\
&= 3 + \Pi_2(1w_2, 100\dots 0) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(1w_2, 0(wi + 1)) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(1w_2, 1(wi + 1)) \cdot 1 = \\
&= 3 + \begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} (\Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} (w_2, wi + 1) + \\
&\quad + \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} (w_2, wi + 1)) \equiv \\
&\equiv \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preceq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 2 & 2 \\ 0 & 0 \end{bmatrix} (w_2, wi + 1) \pmod{4}.
\end{aligned}$$

Сокращая на 2, преобразуем утверждение к виду

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 \\ 0 \end{bmatrix} (w_2) \equiv 1 \pmod{2},$$

который совпадает с леммой 11.

Пусть теперь $t > 0$. Тогда, уменьшая t на единицу, получаем $wt = 00^t 0 w_1$, $n = 00^t 1 w_2$. Преобразуем левую часть (4):

$$\begin{aligned} & \begin{bmatrix} 1 \\ 3 \end{bmatrix} (00^t 1 w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 00^t 0 w_1 \preccurlyeq wi}} \Pi_2(00^t 1 w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (00^t 1 w_2, wi + 1) = \\ & = 1 + \Pi_2(00^t 1 w_2, 100\dots 0) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (00^t 1 w_2, 100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0 w_1 \preccurlyeq wi}} \Pi_2(00^t 1 w_2, 0(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (00^t 1 w_2, 0(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0 w_1 \preccurlyeq wi}} \Pi_2(00^t 1 w_2, 1(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (00^t 1 w_2, 1(wi + 1)) = \\ & = 1 + \begin{bmatrix} 3 \\ 1 \end{bmatrix} (0^t 1 w_2) \cdot 2 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0 w_1 \preccurlyeq wi}} \Pi_2(0^t 1 w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^t 1 w_2, wi + 1) \cdot 3 + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0 w_1 \preccurlyeq wi}} \Pi_2(0^t 1 w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^t 1 w_2, wi + 1) \cdot 2 \equiv \\ & \equiv 1 + 2 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0 w_1 \preccurlyeq wi}} \Pi_2(0^t 1 w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^t 1 w_2, wi + 1). \end{aligned}$$

В результате утверждение преобразуется к виду

$$1 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0 w_1 \preccurlyeq wi}} \Pi_2(0^t 1 w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^t 1 w_2, wi + 1) \equiv 0 \pmod{4},$$

который совпадает с леммой 12. ■

Лемма 14. Пусть $\overline{wt} - 2^{|wm|-1} < \overline{wn} \leq \overline{wt}$. Тогда

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} (wn) + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (wn, wi + 1) \equiv 1 \pmod{2}.$$

Доказательство. Пусть $wt = 1w_1$, $wn = 1w_2$, тогда $\overline{w_2} \leq \overline{w_1}$. Преобразуем выражение:

$$\begin{aligned} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} (1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_2, wi + 1) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(1w_2, 1(wi + 1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_2, 1(wi + 1)) \equiv 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \cdot 1. \end{aligned}$$

Сумма равна 0 по модулю 2 в силу леммы 10, а значит, все выражение сравнимо с 1 по модулю 2, что и требовалось доказать.

Пусть $wm = 1w_1$, $wn = 0w_2$, тогда $\overline{w_1} < \overline{w_2}$. Преобразуем выражение:

$$\begin{aligned} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} (0w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, wi + 1) = \\ & = 0 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, 1(wi + 1)) \equiv \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \cdot 1. \end{aligned}$$

По лемме 8 это выражение сравнимо с 1 по модулю 2, что и требовалось доказать.

Пусть $wm = 0w_1$, $wn = 0w_2$, тогда $\overline{w_2} \leq \overline{w_1}$. Преобразуем выражение:

$$\begin{aligned} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} (0w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, wi + 1) = \\ & = 0 + \Pi_2(0w_2, 100\dots 0) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, 100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 0(wi + 1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, 0(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_2, 1(wi + 1)) \equiv \\ & \equiv 0 + \Pi_1(w_2, 00\dots 0) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \cdot 0 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \cdot 1 = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1). \end{aligned}$$

Рассуждая так же, как и в первом случае, получаем требуемое. ■

Теорема 5. Пусть для некоторых непустых слов w_1 и w_2 выполнено $wm = 010^t 0w_1$, $wn = 100^t 1w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2}$, $t \geq 0$; или $wm = 01w_1$, $wn = 11w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \leq \overline{w_1}$. Тогда

$$1 + \sum_{\substack{wi \neq 11\dots 1, \\ wm \preccurlyeq wi}} \Pi_3(wn, wi + 1) M_2^*(wn, wi + 1) \equiv 4 \pmod{8}.$$

Доказательство. Рассмотрим первый случай:

$$\begin{aligned} & 1 + \sum_{\substack{wi \neq 11\dots 1, \\ wm \preccurlyeq wi}} \Pi_3(wn, wi + 1) M_2^*(wn, wi + 1) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 010^t 0w_1 \preccurlyeq wi}} \Pi_3(100^t 1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (100^t 1w_2, wi + 1) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 010^t 0w_1 \preccurlyeq wi}} \Pi_3(100^t 1w_2, wi + 1) [1 \ 2 \ 1 \ 0] (wi + 1) = 1 + \Pi_3(100^t 1w_2, 100\dots 0) \cdot 1 + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(100^t 1w_2, 0(wi + 1)) [1 \ 2] (wi + 1) + \end{aligned}$$

$$\begin{aligned}
& + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(100^t 1w_2, 1(wi + 1)) [1 \ 0] (wi + 1) = 1 + \begin{bmatrix} 1 \\ 5 \end{bmatrix} (0^t 1w_2) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, wi + 1) \begin{bmatrix} 1 & 4 & 3 & 2 \\ 1 & 5 & 5 & 5 \\ 1 & 6 & 5 & 4 \\ 1 & 7 & 7 & 1 \end{bmatrix} (00^t 1w_2, wi + 1) [1 \ 2] (wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 3 & 6 \\ 5 & 1 & 1 & 1 \\ 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 \end{bmatrix} (00^t 1w_2, wi + 1) [1 \ 0] (wi + 1) \equiv \\
& \equiv \begin{bmatrix} 2 \\ 6 \end{bmatrix} (0^t 1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, wi + 1) \begin{bmatrix} 1 & 4 & 6 & 4 \\ 1 & 5 & 2 & 2 \\ 1 & 6 & 2 & 0 \\ 1 & 7 & 6 & 2 \end{bmatrix} (00^t 1w_2, wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 1 & 7 & 0 & 0 \end{bmatrix} (00^t 1w_2, wi + 1) \equiv \\
& \equiv \begin{bmatrix} 2 \\ 6 \end{bmatrix} (0^t 1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, wi + 1) \begin{bmatrix} 2 & 4 & 6 & 4 \\ 6 & 6 & 2 & 2 \\ 6 & 0 & 2 & 0 \\ 0 & 0 & 6 & 2 \end{bmatrix} (00^t 1w_2, wi + 1) \pmod{8}.
\end{aligned}$$

Сокращая на 2, получаем, что утверждение леммы сводится к виду

$$\begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^t 1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, wi + 1) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 3 & 0 & 1 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix} (00^t 1w_2, wi + 1) \equiv 2 \pmod{4}.$$

Преобразуем дальше:

$$\begin{aligned}
& \begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^t 1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 10^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, wi + 1) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 3 & 0 & 1 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix} (00^t 1w_2, wi + 1) = \\
& = \begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^t 1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0w_1 \preccurlyeq wi}} \Pi_3(00^t 1w_2, 1(wi + 1)) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 3 & 0 & 1 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix} (00^t 1w_2, 1(wi + 1)) \equiv \\
& \equiv \begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^t 1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0^t 0w_1 \preccurlyeq wi}} \Pi_2(0^t 1w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^t 1w_2, wi + 1).
\end{aligned}$$

Последнее выражение сравнимо с 2 по модулю 4 по лемме 13.

Рассмотрим второй случай:

$$1 + \sum_{\substack{wi \neq 11\dots 1, \\ wm \preccurlyeq wi}} \Pi_3(wm, wi + 1) M_2^*(wm, wi + 1) =$$

$$\begin{aligned}
&= 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 01w_1 \preccurlyeq wi}} \Pi_3(11w_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (11w_2, wi + 1) = \\
&= 1 + \Pi_3(11w_2, 100\dots 0) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (11w_2, 100\dots 0) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(11w_2, 0(wi + 1)) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (11w_2, 0(wi + 1)) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(11w_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (11w_2, 1(wi + 1)) = 1 + \begin{bmatrix} 5 \\ 1 \end{bmatrix} (w_2) \cdot 3 + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 4 & 3 & 2 \\ 1 & 5 & 5 & 5 \\ 1 & 6 & 5 & 4 \\ 1 & 7 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} (1w_2, wi + 1) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 3 & 6 \\ 5 & 1 & 1 & 1 \\ 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} (1w_2, wi + 1) \equiv \\
&\equiv \begin{bmatrix} 0 \\ 4 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 4 & 6 & 4 \\ 1 & 5 & 2 & 2 \\ 1 & 6 & 7 & 4 \\ 1 & 7 & 5 & 3 \end{bmatrix} (1w_2, wi + 1) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 7 & 6 & 1 & 0 \\ 3 & 5 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \equiv \\
&\equiv \begin{bmatrix} 0 \\ 4 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 2 & 4 & 6 & 4 \\ 6 & 6 & 2 & 2 \\ 0 & 4 & 0 & 4 \\ 4 & 4 & 4 & 4 \end{bmatrix} (1w_2, wi + 1) \pmod{8}.
\end{aligned}$$

Сокращая на 2, получаем, что утверждение леммы сводится к виду

$$\begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix} (1w_2, wi + 1) \equiv 2 \pmod{4}.$$

Преобразуем дальше:

$$\begin{aligned}
& \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix} (1w_2, wi + 1) = \\
& = \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(1w_2, 1(wi + 1)) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix} (1w_2, 1(wi + 1)) \equiv \\
& \equiv \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix} (w_2, wi + 1).
\end{aligned}$$

Сокращая на 2, получаем, что утверждение леммы сводится к виду

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1) \equiv 1 \pmod{2}.$$

Это выражение в точности совпадает с леммой 14. ■

Лемма 15. Пусть для непустых слов $\overline{wn} \leq \overline{wm}$. Тогда

$$\sum_{\substack{wi \neq 11\dots 1, \\ wm \preccurlyeq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (wn, wi + 1) \equiv 0 \pmod{4}.$$

Здесь $*$ обозначает произвольное фиксированное число.

Доказательство. Докажем утверждение индукцией по длине слов wm и wn . Если wm и wn имеют длину 1, то в сумме есть слагаемые только при $wm = 0$, а значит, и $wn = 0$. В этом случае единственное слагаемое равно

$$\Pi_2(0, 1) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (0, 1) = 1 \cdot 0 = 0.$$

База индукции доказана. Докажем переход. Пусть утверждение доказано для длин wm и wn не больше k . Докажем его для $|wm| = |wn| = k + 1$.

Пусть $wm = 1w_1$, $wn = 1w_2$, $\overline{w_2} \leq \overline{w_1}$. Преобразуем выражение:

$$\begin{aligned}
& \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (1w_2, wi + 1) = \\
& = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(1w_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (1w_2, 1(wi + 1)) = \\
& = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} (w_2, wi + 1) \cdot 1 \equiv 0 \pmod{4}.
\end{aligned}$$

Здесь последнее сравнение следует из предположения индукции.

Пусть $wt = 1w_1$, $wn = 0w_2$. Получаем

$$\begin{aligned} & \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (0w_2, wi + 1) = \\ = & \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (0w_2, 1(wi + 1)) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 0 = 0. \end{aligned}$$

Пусть $wt = 0w_1$, $wn = 0w_2$, $\overline{w_2} \leq \overline{w_1}$. Имеем

$$\begin{aligned} & \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (0w_2, wi + 1) = \Pi_2(0w_2, 100\dots 0) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (0w_2, 100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 0(wi + 1)) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (0w_2, 0(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} (0w_2, 1(wi + 1)) = \\ = & \Pi_2(0w_2, 100\dots 0) \cdot 0 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 0(wi + 1)) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 0 = \\ = & \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1) \equiv 0 \pmod{4}, \end{aligned}$$

где последнее сравнение следует из предположения индукции. Переход доказан. ■

Лемма 16. Пусть для непустых слов $\overline{wm} - 2^{|wm|-1} < \overline{wn} \leq \overline{wm}$. Тогда

$$\begin{bmatrix} 0 \\ 2 \end{bmatrix} (wn) + \sum_{\substack{wi \neq 11\dots 1, \\ wm \preccurlyeq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (wn, wi + 1) \equiv 2 \pmod{4}.$$

Доказательство. Пусть $wt = 1w_1$, $wn = 1w_2$. Тогда $\overline{w_2} \leq \overline{w_1}$. Преобразуем выражение:

$$\begin{aligned} & \begin{bmatrix} 0 \\ 2 \end{bmatrix} (1w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(1w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (1w_2, wi + 1) = \\ = & 2 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(1w_2, 1(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (1w_2, 1(wi + 1)) = \\ = & 2 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} (w_2, wi + 1) \cdot 1. \end{aligned}$$

Применяя лемму 15, получаем требуемое.

Пусть $wt = 1w_1$, $wn = 0w_2$. Тогда $\overline{w_2} > \overline{w_1}$. Имеем

$$\begin{aligned} & \begin{bmatrix} 0 \\ 2 \end{bmatrix} (0w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0w_2, wi + 1) = \\ = & 0 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0w_2, 1(wi + 1)) = \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 2. \end{aligned}$$

Сокращая на 2, получаем, что утверждение преобразуется к виду

$$\sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \equiv 1 \pmod{2},$$

но
$$\sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \equiv \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \pmod{2}.$$

Утверждение теперь следует из леммы 8.

Пусть $wt = 0w_1$, $wn = 0w_2$. Тогда $\overline{w_2} \leq \overline{w_1}$. Преобразуем выражение:

$$\begin{aligned} & \begin{bmatrix} 0 \\ 2 \end{bmatrix} (0w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_2(0w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0w_2, wi + 1) = \\ & = 0 + \Pi_2(0w_2, 100\dots 0) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0w_2, 100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 0(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0w_2, 0(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0w_2, 1(wi + 1)) = \begin{bmatrix} 3 \\ 1 \end{bmatrix} (w_2) \cdot 2 + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1) \cdot 3 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 2. \end{aligned}$$

Заметим, что вторая сумма равна 0 по модулю 4 по лемме 15. Сокращая оставшиеся члены на 2, получаем

$$\begin{bmatrix} 3 \\ 1 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \equiv 1 \pmod{2},$$

но
$$\begin{bmatrix} 3 \\ 1 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \equiv 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_1(w_2, wi + 1) \pmod{2}.$$

По лемме 10 получаем требуемое. ■

Лемма 17. Пусть $\overline{wn} > \overline{wt}$. Тогда

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} (wn) + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_2(wn, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (wn, wi + 1) \equiv 1 \pmod{2}.$$

Доказательство. Если длина wn и wt равна 1, то $wt = 0$, $wn = 1$. В этом случае в сумме одно слагаемое, соответствующее $wi = 0$:

$$\Pi_2(1, 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1, 1) = 1 \cdot 1 = 1.$$

Пусть теперь $|wn| = |wt| > 1$. Рассмотрим случай $wn = 1w_1$, $wt = 1w_2$, откуда $\overline{w_1} > \overline{w_2}$. Имеем

$$\begin{aligned} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} (1w_1) + \sum_{\substack{wi \neq 11\dots 1, \\ 1w_2 \preccurlyeq wi}} \Pi_2(1w_1, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_1, wi + 1) = \\ & = \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_2(1w_1, 1(wi + 1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_1, 1(wi + 1)) \equiv \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_1(w_1, wi + 1) \cdot 1. \end{aligned}$$

Применяя лемму 8, получаем требуемое.

Пусть $wn = 1w_1$, $wt = 0w_2$. Имеем

$$\begin{aligned}
 & \begin{bmatrix} 1 \\ 0 \end{bmatrix} (1w_1) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_2 \preccurlyeq wi}} \Pi_2(1w_1, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (1w_1, wi + 1) = \\
 & = \sum_{\substack{wi \neq 11\dots 1, \\ 0w_2 \preccurlyeq wi}} \Pi_2(1w_1, wi + 1) [1 \ 1] (wi + 1) = \sum_{\substack{wi \neq 11\dots 1, \\ 0w_2 \preccurlyeq wi}} \Pi_2(1w_1, wi + 1) = \\
 & = \Pi_2(1w_1, 100\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_2(1w_1, 0(wi + 1)) + \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_2(1w_1, 1(wi + 1)) \equiv \\
 & \equiv \Pi_1(w_1, 00\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_1(w_1, wi + 1) + \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_1(w_1, wi + 1) \equiv 1 \pmod{2}.
 \end{aligned}$$

Пусть $wn = 0w_1$, $wt = 0w_2$, откуда $\overline{w_1} > \overline{w_2}$. Имеем

$$\begin{aligned}
 & \begin{bmatrix} 1 \\ 0 \end{bmatrix} (0w_1) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_2 \preccurlyeq wi}} \Pi_2(0w_1, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (0w_1, wi + 1) = \\
 & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_2 \preccurlyeq wi}} \Pi_2(0w_1, wi + 1) [0 \ 1] (wi + 1) = \\
 & = 1 + \Pi_2(0w_1, 100\dots 0) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_2(0w_1, 1(wi + 1)) \cdot 1 \equiv \\
 & \equiv 1 + \Pi_1(w_1, 00\dots 0) + \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_1(w_1, wi + 1) \equiv \sum_{\substack{wi \neq 11\dots 1, \\ w_2 \preccurlyeq wi}} \Pi_1(w_1, wi + 1).
 \end{aligned}$$

Применяя лемму 8, получаем требуемое. ■

Лемма 18. Пусть для $t \geq 0$ выполнено $wt = 0^t 01w_1$, $wn = 0^t 10w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \leq \overline{w_1}$, $|w_2| = |w_1| > 0$; или $wt = 0^t 100w_1$, $wn = 0^t 111w_2$, $\overline{w_2} > \overline{w_1}$. Тогда

$$7 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_3(wn, wi + 1) M_3^*(wn, wi + 1) \equiv 4 \pmod{8}.$$

Доказательство. Докажем утверждение индукцией по t . Пусть $t = 0$ и $wt = 01w_1$, $wn = 10w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \leq \overline{w_1}$. Имеем

$$\begin{aligned}
 & 7 + \sum_{\substack{wi \neq 11\dots 1, \\ 01w_1 \preccurlyeq wi}} \Pi_3(10w_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (10w_2, wi + 1) = 7 + \\
 & + \sum_{\substack{wi \neq 11\dots 1, \\ 01w_1 \preccurlyeq wi}} \Pi_3(10w_2, wi + 1) [1 \ 2 \ 1 \ 0] (wi + 1) = 7 + \Pi_3(10w_2, 100\dots 0) [1 \ 2 \ 1 \ 0] (100\dots 0) + \\
 & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 01(wi + 1)) [1 \ 2 \ 1 \ 0] (01(wi + 1)) + \\
 & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 11(wi + 1)) [1 \ 2 \ 1 \ 0] (11(wi + 1)) = \\
 & = 7 + \begin{bmatrix} 1 \\ 5 \end{bmatrix} (w_2) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 01(wi + 1)) \cdot 2 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 11(wi + 1)) \cdot 0 \equiv \\
 & \equiv \begin{bmatrix} 0 \\ 4 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 2 \pmod{8}.
 \end{aligned}$$

Последний переход от Π_3 к Π_2 возможен благодаря тому, что все слагаемые в сумме умножены на 2. Сокращая на 2, сводим утверждение леммы к следующему:

$$\begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \equiv 2 \pmod{4}.$$

Преобразуя левую часть, получим

$$\begin{aligned} & \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) = \\ & = \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1) \equiv 2 \pmod{4}, \end{aligned}$$

где последнее сравнение следует из леммы 16.

Пусть $t = 0$ и $wm = 100w_1$, $wn = 111w_2$, $\overline{w_2} > \overline{w_1}$. Имеем

$$\begin{aligned} & 7 + \sum_{\substack{wi \neq 11\dots 1, \\ 100w_1 \preccurlyeq wi}} \Pi_3(111w_2, wi + 1) M_3^*(111w_2, wi + 1) = \\ & = 7 + \sum_{\substack{wi \neq 11\dots 1, \\ 00w_1 \preccurlyeq wi}} \Pi_3(111w_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (111w_2, 1(wi + 1)) = \\ & = 7 + \sum_{\substack{wi \neq 11\dots 1, \\ 00w_1 \preccurlyeq wi}} \Pi_3(11w_2, wi + 1) \begin{bmatrix} 1 & 0 & 3 & 6 \\ 5 & 1 & 1 & 1 \\ 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 \end{bmatrix} (11w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} (11w_2, wi + 1) = \\ & = 7 + \sum_{\substack{wi \neq 11\dots 1, \\ 00w_1 \preccurlyeq wi}} \Pi_3(11w_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 7 & 6 & 1 & 0 \\ 3 & 5 & 7 & 1 \end{bmatrix} (11w_2, wi + 1) = \\ & = 7 + \Pi_3(11w_2, 100\dots 0) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 7 & 6 & 1 & 0 \\ 3 & 5 & 7 & 1 \end{bmatrix} (11w_2, 100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(11w_2, 0(wi + 1)) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 7 & 6 & 1 & 0 \\ 3 & 5 & 7 & 1 \end{bmatrix} (11w_2, 0(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(11w_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 7 & 6 & 1 & 0 \\ 3 & 5 & 7 & 1 \end{bmatrix} (11w_2, 1(wi + 1)) = 7 + \begin{bmatrix} 5 \\ 1 \end{bmatrix} (w_2) \cdot 7 + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 4 & 3 & 2 \\ 1 & 5 & 5 & 5 \\ 1 & 6 & 5 & 4 \\ 1 & 7 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \begin{bmatrix} 7 & 6 \\ 3 & 5 \end{bmatrix} (1w_2, wi + 1) + \end{aligned}$$

$$\begin{aligned}
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 3 & 6 \\ 5 & 1 & 1 & 1 \\ 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 7 & 1 \end{bmatrix} (1w_2, wi + 1) \equiv \\
& \equiv \begin{bmatrix} 2 \\ 6 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 7 & 4 & 2 & 4 \\ 7 & 3 & 6 & 6 \\ 3 & 2 & 1 & 4 \\ 3 & 5 & 3 & 5 \end{bmatrix} (1w_2, wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 1 & 0 & 0 \\ 3 & 6 & 1 & 0 \\ 7 & 1 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \equiv \\
& \equiv \begin{bmatrix} 2 \\ 6 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 0 & 4 & 2 & 4 \\ 4 & 4 & 6 & 6 \\ 6 & 0 & 2 & 4 \\ 2 & 6 & 2 & 6 \end{bmatrix} (1w_2, wi + 1) \pmod{8}.
\end{aligned}$$

Сокращая на 2, сводим утверждение к виду

$$\begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 0 & 2 & 1 & 2 \\ 2 & 2 & 3 & 3 \\ 3 & 0 & 1 & 2 \\ 1 & 3 & 1 & 3 \end{bmatrix} (1w_2, wi + 1) \equiv 2 \pmod{4}.$$

Продолжая вычисления, получаем

$$\begin{aligned}
& \begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 0 & 2 & 1 & 2 \\ 2 & 2 & 3 & 3 \\ 3 & 0 & 1 & 2 \\ 1 & 3 & 1 & 3 \end{bmatrix} (1w_2, wi + 1) = \\
& = \begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + \Pi_3(1w_2, 100\dots 0) \begin{bmatrix} 0 & 2 & 1 & 2 \\ 2 & 2 & 3 & 3 \\ 3 & 0 & 1 & 2 \\ 1 & 3 & 1 & 3 \end{bmatrix} (1w_2, 100\dots 0) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(1w_2, 0(wi + 1)) \begin{bmatrix} 0 & 2 & 1 & 2 \\ 2 & 2 & 3 & 3 \\ 3 & 0 & 1 & 2 \\ 1 & 3 & 1 & 3 \end{bmatrix} (1w_2, 0(wi + 1)) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(1w_2, 1(wi + 1)) \begin{bmatrix} 0 & 2 & 1 & 2 \\ 2 & 2 & 3 & 3 \\ 3 & 0 & 1 & 2 \\ 1 & 3 & 1 & 3 \end{bmatrix} (1w_2, 1(wi + 1)) \equiv \\
& \equiv \begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + \Pi_2(w_2, 00\dots 0) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 3 & 0 \\ 1 & 3 \end{bmatrix} (w_2, wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} (w_2, wi + 1) \equiv
\end{aligned}$$

$$\begin{aligned}
&\equiv \begin{bmatrix} 1 \\ 3 \end{bmatrix} (w_2) + 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix} (w_2, wi + 1) \equiv \\
&\equiv \begin{bmatrix} 2 \\ 0 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix} (w_2, wi + 1) \pmod{4}.
\end{aligned}$$

Сократив на 2, сводим утверждение к виду

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1) \equiv 1 \pmod{2},$$

который совпадает с леммой 17. База индукции доказана.

Пусть утверждение доказано для $t \leq k$, докажем его для $t = k + 1 > 0$. Заметим, что $w_1 = 0v_1$, $w_2 = 0v_2$, где v_1 и v_2 удовлетворяют условиям леммы. Имеем

$$\begin{aligned}
&7 + \sum_{\substack{wi \neq 11\dots 1, \\ 0v_1 \preccurlyeq wi}} \Pi_3(0v_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (0v_2, wi + 1) = \\
&= 7 + \Pi_3(0v_2, 100\dots 0) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (0v_2, 100\dots 0) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(0v_2, 0(wi + 1)) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (0v_2, 0(wi + 1)) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(0v_2, 1(wi + 1)) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (0v_2, 1(wi + 1)) = 7 + \Pi_3(0v_2, 100\dots 0) \cdot 0 + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 1 & 0 & 7 & 6 \\ 1 & 1 & 1 & 5 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (v_2, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (v_2, wi + 1) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(0v_2, 1(wi + 1)) \cdot 0 = \\
&= 7 + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (v_2, wi + 1) \equiv 4 \pmod{8}.
\end{aligned}$$

Последнее сравнение следует из предположения индукции. Переход доказан. ■

Лемма 19. Пусть для $t \geq 0$ выполнено $wt = 0^t 01w_1$, $wn = 0^t 10w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \leq \overline{w_1}$; или $wt = 0^t 100w_1$, $wn = 0^t 111w_2$, $\overline{w_2} > \overline{w_1}$. Тогда

$$\begin{bmatrix} 1 \\ 5 \\ 7 \\ 3 \end{bmatrix} (wn) + \sum_{\substack{wi \neq 11\dots 1, \\ wt \preccurlyeq wi}} \Pi_3(wn, wi + 1) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (wn, wi + 1) \equiv 4 \pmod{8}.$$

Доказательство. Пусть $t = 0$ и $wt = 01w_1$, $wn = 10w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \leq \overline{w_1}$. Имеем

$$\begin{aligned} & \begin{bmatrix} 1 \\ 5 \\ 7 \\ 3 \end{bmatrix} (10w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 01w_1 \preccurlyeq wi}} \Pi_3(10w_2, wi + 1) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (10w_2, wi + 1) = 7 + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ 01w_1 \preccurlyeq wi}} \Pi_3(10w_2, wi + 1) [1 \ 6 \ 1 \ 4] (wi + 1) = 7 + \Pi_3(10w_2, 100\dots 0) [1 \ 6 \ 1 \ 4] (100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 01(wi + 1)) [1 \ 6 \ 1 \ 4] (01(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 11(wi + 1)) [1 \ 6 \ 1 \ 4] (11(wi + 1)) = \\ & = 7 + \begin{bmatrix} 1 \\ 5 \end{bmatrix} (w_2) \cdot 1 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 01(wi + 1)) \cdot 6 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_3(10w_2, 11(wi + 1)) \cdot 4 \equiv \\ & \equiv \begin{bmatrix} 0 \\ 4 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 6 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \cdot 4 = \\ & = \begin{bmatrix} 0 \\ 4 \end{bmatrix} (w_2) + 2 \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \pmod{8}. \end{aligned}$$

Переход от Π_3 к Π_2 выполнен благодаря тому, что все слагаемые в суммах домножены на чётные числа 6 и 4. Сокращая на 2, сводим утверждение к следующему:

$$\begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) \equiv 2 \pmod{4}.$$

Преобразуя левую часть, получим

$$\begin{aligned} & \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) = \\ & = \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1) \equiv 2 \pmod{4}, \end{aligned}$$

где последнее сравнение следует из леммы 16.

Пусть $t = 0$ и $wt = 100w_1$, $wn = 111w_2$, $\overline{w_2} > \overline{w_1}$. Имеем

$$\begin{aligned}
& \begin{bmatrix} 1 \\ 5 \\ 7 \\ 3 \end{bmatrix} (111w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 100w_1 \preccurlyeq wi}} \Pi_3(111w_2, wi + 1) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (111w_2, wi + 1) = \\
& = 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 00w_1 \preccurlyeq wi}} \Pi_3(111w_2, 1(wi + 1)) \begin{bmatrix} 5 & 7 & 7 & 5 \end{bmatrix} (1(wi + 1)) = \\
& = 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 00w_1 \preccurlyeq wi}} \Pi_3(11w_2, wi + 1) \begin{bmatrix} 1 & 0 & 3 & 6 \\ 5 & 1 & 1 & 1 \\ 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 \end{bmatrix} (11w_2, wi + 1) \begin{bmatrix} 7 & 5 \end{bmatrix} (wi + 1) \equiv \\
& \equiv 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 00w_1 \preccurlyeq wi}} \Pi_3(11w_2, wi + 1) \begin{bmatrix} 7 & 0 & 7 & 6 \\ 3 & 7 & 5 & 5 \\ 3 & 6 & 5 & 0 \\ 7 & 1 & 3 & 5 \end{bmatrix} (11w_2, wi + 1) = \\
& = 3 + \Pi_3(11w_2, 100\dots 0) \begin{bmatrix} 7 & 0 & 7 & 6 \\ 3 & 7 & 5 & 5 \\ 3 & 6 & 5 & 0 \\ 7 & 1 & 3 & 5 \end{bmatrix} (11w_2, 100\dots 0) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(11w_2, 0(wi + 1)) \begin{bmatrix} 7 & 0 & 7 & 6 \\ 3 & 7 & 5 & 5 \\ 3 & 6 & 5 & 0 \\ 7 & 1 & 3 & 5 \end{bmatrix} (11w_2, 0(wi + 1)) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(11w_2, 1(wi + 1)) \begin{bmatrix} 7 & 0 & 7 & 6 \\ 3 & 7 & 5 & 5 \\ 3 & 6 & 5 & 0 \\ 7 & 1 & 3 & 5 \end{bmatrix} (11w_2, 1(wi + 1)) = 3 + \begin{bmatrix} 5 \\ 1 \end{bmatrix} (w_2) \cdot 3 + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 4 & 3 & 2 \\ 1 & 5 & 5 & 5 \\ 1 & 6 & 5 & 4 \\ 1 & 7 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \begin{bmatrix} 3 & 6 \\ 7 & 1 \end{bmatrix} (1w_2, wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 1 & 0 & 3 & 6 \\ 5 & 1 & 1 & 1 \\ 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) \begin{bmatrix} 5 & 0 \\ 3 & 5 \end{bmatrix} (1w_2, wi + 1) \equiv \\
& \equiv \begin{bmatrix} 2 \\ 6 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 3 & 4 & 2 & 4 \\ 3 & 7 & 6 & 6 \\ 7 & 2 & 5 & 4 \\ 7 & 1 & 7 & 1 \end{bmatrix} (1w_2, wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 5 & 0 & 0 & 0 \\ 1 & 5 & 0 & 0 \\ 7 & 6 & 5 & 0 \\ 3 & 5 & 3 & 5 \end{bmatrix} (1w_2, wi + 1) \equiv \\
& \equiv \begin{bmatrix} 2 \\ 6 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0w_1 \preccurlyeq wi}} \Pi_3(1w_2, wi + 1) \begin{bmatrix} 0 & 4 & 2 & 4 \\ 4 & 4 & 6 & 6 \\ 6 & 0 & 2 & 4 \\ 2 & 6 & 2 & 6 \end{bmatrix} \pmod{8}.
\end{aligned}$$

Это выражение уже получалось в лемме 18, где доказывалось, что оно сравнимо с 4 по модулю 8, как и требуется.

Пусть теперь $t = k + 1 > 0$. Обозначим $wt = 0v_1$, $wn = 0v_2$, где v_1 и v_2 удовлетворяют условиям леммы. Имеем

$$\begin{aligned}
& \begin{bmatrix} 1 \\ 5 \\ 7 \\ 3 \end{bmatrix} (0v_2) + \sum_{\substack{wi \neq 11\dots 1, \\ 0v_1 \preccurlyeq wi}} \Pi_3(0v_2, wi + 1) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (0v_2, wi + 1) = \\
& = \begin{bmatrix} 1 \\ 5 \end{bmatrix} (v_2) + \Pi_3(0v_2, 100\dots 0) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (0v_2, 100\dots 0) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(0v_2, 0(wi + 1)) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (0v_2, 0(wi + 1)) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(0v_2, 1(wi + 1)) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (0v_2, 1(wi + 1)) = \begin{bmatrix} 1 \\ 5 \end{bmatrix} (v_2) + \\
& + \begin{bmatrix} 1 \\ 5 \\ 5 \\ 1 \end{bmatrix} (v_2) \begin{bmatrix} 6 \\ 2 \end{bmatrix} (v_2) + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 1 & 0 & 7 & 6 \\ 1 & 1 & 1 & 5 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (v_2, wi + 1) \begin{bmatrix} 3 & 4 \\ 7 & 7 \end{bmatrix} (v_2, wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 1 & 4 & 7 & 2 \\ 5 & 5 & 5 & 1 \\ 5 & 6 & 5 & 4 \\ 1 & 3 & 3 & 1 \end{bmatrix} (v_2, wi + 1) \begin{bmatrix} 6 & 4 \\ 2 & 2 \end{bmatrix} (v_2, wi + 1) \equiv \\
& \equiv \begin{bmatrix} 1 \\ 5 \end{bmatrix} (v_2) + \begin{bmatrix} 6 \\ 2 \end{bmatrix} (v_2) + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 3 & 0 & 4 & 0 \\ 3 & 3 & 4 & 4 \\ 7 & 6 & 7 & 0 \\ 7 & 5 & 5 & 7 \end{bmatrix} (v_2, wi + 1) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 6 & 0 & 4 & 0 \\ 6 & 6 & 4 & 4 \\ 2 & 4 & 2 & 0 \\ 2 & 6 & 6 & 2 \end{bmatrix} (v_2, wi + 1) \equiv \\
& \equiv 7 + \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{bmatrix} (v_2, wi + 1) \pmod{8}.
\end{aligned}$$

Применяя лемму 18, получаем требуемое. ■

Теорема 6. Пусть для некоторых непустых слов w_1 и w_2 выполнено $wt = 011w_1$, $wn = 110w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \leq \overline{w_1}$; или $wt = 010^t01w_1$, $wn = 100^t10w_2$, $\overline{w_1} - 2^{|w_1|-1} <$

$< \overline{w_2} \leq \overline{w_1}$, $t \geq 0$; или $wt = 010^t 100w_1$, $wn = 100^t 111w_2$, $\overline{w_2} > \overline{w_1}$, $t \geq 0$. Тогда

$$1 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \leq wi}} \Pi_4(wn, wi + 1) M_3^*(wn, wi + 1) \equiv 8 \pmod{16}. \quad (5)$$

Доказательство. Вычисления показывают, что

$$M_4 = \begin{bmatrix} 1 & 0 & 15 & 6 & 1 & 12 & 15 & 10 & 1 & 8 & 15 & 15 & 1 & 4 & 15 & 2 \\ 1 & 1 & 1 & 5 & 5 & 13 & 13 & 9 & 9 & 9 & 9 & 13 & 13 & 5 & 5 & 1 \\ 1 & 2 & 1 & 0 & 5 & 14 & 13 & 4 & 9 & 10 & 9 & 8 & 13 & 6 & 5 & 12 \\ 1 & 3 & 3 & 1 & 1 & 3 & 3 & 1 & 1 & 3 & 3 & 1 & 1 & 3 & 3 & 1 \\ 1 & 4 & 3 & 2 & 1 & 0 & 3 & 6 & 1 & 12 & 3 & 10 & 1 & 8 & 3 & 14 \\ 1 & 5 & 5 & 5 & 5 & 1 & 1 & 9 & 9 & 13 & 13 & 13 & 13 & 9 & 9 & 1 \\ 1 & 6 & 5 & 12 & 5 & 2 & 1 & 0 & 9 & 14 & 13 & 4 & 13 & 10 & 9 & 8 \\ 1 & 7 & 7 & 1 & 1 & 7 & 7 & 1 & 1 & 7 & 7 & 1 & 1 & 7 & 7 & 1 \\ 1 & 8 & 7 & 14 & 1 & 4 & 7 & 2 & 1 & 0 & 7 & 6 & 1 & 12 & 7 & 10 \\ 1 & 9 & 9 & 5 & 5 & 5 & 5 & 9 & 9 & 1 & 1 & 13 & 13 & 13 & 13 & 1 \\ 1 & 10 & 9 & 8 & 5 & 6 & 5 & 12 & 9 & 2 & 1 & 0 & 13 & 14 & 13 & 4 \\ 1 & 11 & 11 & 1 & 1 & 11 & 11 & 1 & 1 & 11 & 11 & 1 & 1 & 11 & 11 & 1 \\ 1 & 12 & 11 & 10 & 1 & 8 & 11 & 14 & 1 & 4 & 11 & 2 & 1 & 0 & 11 & 6 \\ 1 & 13 & 13 & 5 & 5 & 9 & 9 & 9 & 9 & 5 & 5 & 13 & 13 & 1 & 1 & 1 \\ 1 & 14 & 13 & 4 & 5 & 10 & 9 & 8 & 9 & 6 & 5 & 12 & 13 & 2 & 1 & 0 \\ 1 & 15 & 15 & 1 & 1 & 15 & 15 & 1 & 1 & 15 & 15 & 1 & 1 & 15 & 15 & 1 \end{bmatrix},$$

$$M_3^* \equiv \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 4 & 6 & 4 & 1 & 0 & 0 & 0 \\ 1 & 5 & 10 & 10 & 5 & 1 & 0 & 0 \\ 1 & 6 & 15 & 4 & 15 & 6 & 1 & 0 \\ 1 & 7 & 5 & 3 & 3 & 5 & 7 & 1 \end{bmatrix} \pmod{16}.$$

Рассмотрим первый случай: $wt = 011w_1$, $wn = 110w_2$, $\overline{w_1} - 2^{|w_1|-1} < \overline{w_2} \leq \overline{w_1}$. Преобразуем левую часть (5):

$$\begin{aligned} & 1 + \sum_{\substack{wi \neq 11\dots 1, \\ wt \leq wi}} \Pi_4(wn, wi + 1) M_3^*(wn, wi + 1) = \\ & = 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 011w_1 \leq wi}} \Pi_4(110w_2, wi + 1) M_3^*(110w_2, wi + 1) \equiv \\ & \equiv 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 011w_1 \leq wi}} \Pi_4(110w_2, wi + 1) [1 \ 6 \ 15 \ 4 \ 15 \ 6 \ 1 \ 0] (wi + 1) = \\ & = 1 + \Pi_4(110w_2, 100\dots 0) [1 \ 6 \ 15 \ 4 \ 15 \ 6 \ 1 \ 0] (100\dots 0) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \leq wi}} \Pi_4(110w_2, 011(wi + 1)) [1 \ 6 \ 15 \ 4 \ 15 \ 6 \ 1 \ 0] (011(wi + 1)) + \\ & + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \leq wi}} \Pi_4(110w_2, 111(wi + 1)) [1 \ 6 \ 15 \ 4 \ 15 \ 6 \ 1 \ 0] (111(wi + 1)) = 1 + \left[\frac{1}{9} \right] (w_2) \cdot 15 + \end{aligned}$$

$$\begin{aligned}
& + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_4(110w_2, 011(wi + 1)) \cdot 4 + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_4(110w_2, 111(wi + 1)) \cdot 0 \equiv \\
& \equiv \begin{bmatrix} 0 \\ 8 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_4(110w_2, 011(wi + 1)) \cdot 4 \pmod{16}.
\end{aligned}$$

Сокращая на 4, получаем, что утверждение теоремы сводится к виду

$$\begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_4(110w_2, 011(wi + 1)) \equiv 2 \pmod{4}.$$

Исбавляясь от Π_4 , получаем

$$\begin{aligned}
& \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_4(110w_2, 011(wi + 1)) \equiv \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(0w_2, 1(wi + 1)) = \begin{bmatrix} 0 \\ 2 \end{bmatrix} (w_2) + \sum_{\substack{wi \neq 11\dots 1, \\ w_1 \preccurlyeq wi}} \Pi_2(w_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (w_2, wi + 1).
\end{aligned}$$

Применяя лемму 16, получаем требуемое.

Рассмотрим второй и третий случаи: $wm = 01v_1$, $wn = 10v_2$, где v_1 и v_2 удовлетворяют условию леммы 19. Имеем

$$\begin{aligned}
1 + \sum_{\substack{wi \neq 11\dots 1, \\ wm \preccurlyeq wi}} \Pi_4(wn, wi + 1) M_3^*(wn, wi + 1) &= 1 + \sum_{\substack{wi \neq 11\dots 1, \\ 01v_1 \preccurlyeq wi}} \Pi_4(10v_2, wi + 1) M_3^*(10v_2, wi + 1) = \\
&= 1 + \Pi_4(10v_2, 100\dots 0) M_3^*(10v_2, 100\dots 0) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_4(10v_2, 01(wi + 1)) M_3^*(10v_2, 01(wi + 1)) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_4(10v_2, 11(wi + 1)) M_3^*(10v_2, 11(wi + 1)) = 1 + \begin{bmatrix} 1 \\ 9 \\ 9 \\ 1 \end{bmatrix} (v_2) \begin{bmatrix} 1 \\ 5 \end{bmatrix} (v_2) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_4(0v_2, 1(wi + 1)) M_4(10v_2, 01(wi + 1)) \begin{bmatrix} 6 & 4 \\ 10 & 10 \end{bmatrix} (v_2, wi + 1) + \\
&+ \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_4(0v_2, 1(i + 1)) M_4(10v_2, 11(wi + 1)) \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (v_2, wi + 1) \equiv 1 + \begin{bmatrix} 1 \\ 9 \\ 13 \\ 5 \end{bmatrix} (v_2) + \\
&+ 2 \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 1 & 4 & 7 & 2 \\ 5 & 5 & 5 & 9 \\ 5 & 6 & 5 & 12 \\ 1 & 11 & 11 & 1 \end{bmatrix} (v_2, wi + 1) \begin{bmatrix} 3 & 2 \\ 5 & 5 \end{bmatrix} (v_2, wi + 1) \equiv \\
&\equiv 2 \begin{bmatrix} 1 \\ 5 \\ 7 \\ 3 \end{bmatrix} (v_2) + 2 \sum_{\substack{wi \neq 11\dots 1, \\ v_1 \preccurlyeq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (v_2, wi + 1) \pmod{16}.
\end{aligned}$$

Сокращая на 2, получаем, что нужно доказать

$$\begin{bmatrix} 1 \\ 5 \\ 7 \\ 3 \end{bmatrix} (v_2) + \sum_{\substack{wi \neq 11 \dots 1, \\ v_1 \leq wi}} \Pi_3(v_2, wi + 1) \begin{bmatrix} 3 & 4 & 6 & 4 \\ 7 & 7 & 2 & 2 \\ 1 & 6 & 1 & 4 \\ 5 & 7 & 7 & 5 \end{bmatrix} (v_2, wi + 1) \equiv 4 \pmod{8}.$$

Используя лемму 19, получаем требуемое. ■

5. Оценки сумм биномиальных коэффициентов

Приступим теперь к оценке области возможных значений m и n . В работе [6] доказана

Теорема 7. При $n \geq 12$ выполнение (3) влечет

$$\frac{n}{2} + \frac{1}{2} \log_2 n + \frac{1}{2} \log_2 \left(\frac{\pi}{2} e^{8/9} \right) - 1 > m \geq \frac{n-1}{2}.$$

Далее будем предполагать, что экстремальная функция с параметрами n и m существует, а значит, при $n \geq 12$ можно использовать неравенство, указанное в теореме. Вычисления показывают, что $\frac{1}{2} \log_2 \left(\frac{\pi}{2} e^{8/9} \right) = 0,9669 \dots < 1$, поэтому будем использовать более удобную оценку $\frac{n}{2} + \frac{1}{2} \log_2 n > m$.

Пусть $n \geq 32$. Заметим, что $2n - 2m - 2 > 2n - n - \log_2 n - 2 = n - \log_2 n - 2 \geq 32 - 5 - 2 = 25$, поскольку $(n+1) - \log_2(n+1) = n - \log_2 \frac{n+1}{2} > n - \log_2 n$ при $n > 1$. Отсюда следует, что левая часть в формуле (3) делится на 2^{25} , а значит, все значения $m = \overline{wm}$ и $n = \overline{wn} \geq 32$ из условий теорем 4, 5 и 6 не подходят.

Лемма 20. Если $n \geq 32$, то двоичная запись n не начинается с 11.

Доказательство. Предположим противное, тогда n имеет вид $n = \overline{11w_2} = 2^{s+1} + 2^s + \overline{w_2}$, $|w_2| = s \geq 4$. Из теоремы 4 следует, что $m \notin I_1 = [2^{s+1}; 2^{s+1} + \overline{w_2}]$; из теоремы 5 — $m \notin I_2 = [2^s + \overline{w_2}; \min(2^s + 2^{s-1} + \overline{w_2}, 2^{s+1})]$; ввиду теоремы 6 для $\overline{w_2} < 2^{s-1}$ выполнено $m \notin I_3 = [2^s + 2^{s-1} + \overline{w_2}; \min(2^s + 2^{s-1} + 2^{s-2} + \overline{w_2}, 2^{s+1})]$. Заметим, что $m \geq \frac{n-1}{2} = 2^s + 2^{s-1} + \frac{\overline{w_2}-1}{2} \geq 2^s + 2^{s-1} + \frac{\overline{w_2}-1 + (\overline{w_2}-2^s+1)}{2} = 2^s + 2^{s-1} + \overline{w_2} - 2^{s-1} = 2^s + \overline{w_2}$. Поскольку $m \notin I_2$, то $m \geq \min(2^s + 2^{s-1} + \overline{w_2}, 2^{s+1})$. Если $\overline{w_2} \geq 2^{s-1}$, то $m \geq 2^{s+1}$, а поскольку $m \notin I_1$, то $m \geq 2^{s+1} + \overline{w_2}$. Если же $\overline{w_2} < 2^{s-1}$, то $m \geq 2^s + 2^{s-1} + \overline{w_2}$, а поскольку $m \notin I_3$ для таких $\overline{w_2}$, то $m \geq \min(2^s + 2^{s-1} + 2^{s-2} + \overline{w_2}, 2^{s+1})$. Если $\overline{w_2} < 2^{s-2}$, то $m \geq 2^s + 2^{s-1} + 2^{s-2} + \overline{w_2}$, а если $2^{s-2} \leq \overline{w_2} < 2^{s-1}$, то $m \geq 2^{s+1}$, откуда из $m \notin I_1$ следует $m \geq 2^{s+1} + \overline{w_2}$. Получаем, что во всех случаях выполнено по крайней мере $m \geq 2^s + 2^{s-1} + 2^{s-2} + \overline{w_2}$. Отсюда $m - \frac{n}{2} \geq 2^s + 2^{s-1} + 2^{s-2} + \overline{w_2} - 2^s - 2^{s-1} - \frac{\overline{w_2}}{2} = 2^{s-2} + \frac{\overline{w_2}}{2} \geq 2^{s-2}$. Но $m < \frac{n}{2} + \frac{1}{2} \log_2 n$, значит, $\frac{1}{2} \log_2 n > 2^{s-2}$. С другой стороны, $\frac{1}{2} \log_2 n < \frac{1}{2} \log_2 2^{s+2} = \frac{s+2}{2}$. Легко видеть, что функция $f(s) = 2^{s-1} - s - 2$, $s \in \mathbb{Z}$, не убывает при $s \geq 1$, а $f(4) = 8 - 4 - 2 = 2 > 0$. Поскольку у нас $s \geq 4$, то $\frac{s+2}{2} < \frac{2^{s-1}}{2} = 2^{s-2}$. Получили противоречие. ■

Для удобства далее будем считать, что $2^{p-1} \leq n < 2^p$ ($p \geq 6$).

Лемма 21. Пусть $n = \overline{10^k 1 w_2} = 2^{s+k+1} + 2^s + \overline{w_2}$, $|w_2| = s \geq 3$, $k \geq 1$. Тогда $m \geq \frac{n}{2} + 2^{s-3}$.

Доказательство. В предположениях леммы $p = s + k + 2$. Из теоремы 4 известно, что $m \notin I_1 = [2^{p-2} + 2^s + \overline{w_2}; 2^{p-1}]$; по теореме 5 имеет место $m \notin I_2 = [2^{p-2}; \min(2^{p-2} + 2^{s-1} + \overline{w_2}, 2^{p-2} + 2^s)]$; по теореме 6 для $\overline{w_2} < 2^{s-1}$ выполнено $m \notin I_3 = [2^{p-2} + 2^{s-1} + \overline{w_2}; \min(2^{p-2} + 2^{s-1} + 2^{s-2} + \overline{w_2}, 2^{p-2} + 2^s)]$, а для $\overline{w_2} \geq 2^{s-1} + 2^{s-2}$ — $m \notin I_4 = [2^{p-2} + 2^s; 2^{p-2} + 2^{s-2} + \overline{w_2}]$. Замечаем, что $m \geq \frac{n-1}{2} = 2^{p-2} + 2^{s-1} + \frac{\overline{w_2}-1}{2} \geq 2^{p-2} + 2^{s-1} + \frac{\overline{w_2}-1 + (\overline{w_2}-2^s+1)}{2} = 2^{p-2} + 2^{s-1} + \overline{w_2} - 2^{s-1} = 2^{p-2} + \overline{w_2}$. Поскольку $m \notin I_2$, то $m \geq \min(2^{p-2} + 2^{s-1} + \overline{w_2}, 2^{p-2} + 2^s)$. Рассмотрим несколько случаев. Если $\overline{w_2} \geq 3 \cdot 2^{s-2}$, то $m \geq 2^{p-2} + 2^s$, а поскольку $m \notin I_4$, то $m \geq 2^{p-2} + 2^{s-2} + \overline{w_2} \geq 2^{p-2} + 2^{s-2} + 3 \cdot 2^{s-3} + \frac{\overline{w_2}}{2} = \frac{n}{2} + 2^{s-3}$. Если $3 \cdot 2^{s-2} > \overline{w_2} \geq 2^{s-1}$, то $m \geq 2^{p-2} + 2^s \geq 2^{p-2} + 2^s - 3 \cdot 2^{s-3} + \frac{\overline{w_2}}{2} = \frac{n}{2} + 2^{s-3}$. Если $2^{s-1} > \overline{w_2} \geq 2^{s-2}$, то $m \geq 2^{p-2} + 2^{s-1} + \overline{w_2} \geq 2^{p-2} + 2^{s-1} + 2^{s-3} + \frac{\overline{w_2}}{2} = \frac{n}{2} + 2^{s-3}$. Если $2^{s-2} > \overline{w_2}$, то $m \geq 2^{p-2} + 2^{s-1} + \overline{w_2}$, а поскольку $m \notin I_3$, то $m \geq \min(2^{p-2} + 2^{s-1} + 2^{s-2} + \overline{w_2}, 2^{p-2} + 2^s) = 2^{p-2} + 2^{s-1} + 2^{s-2} + \overline{w_2} \geq 2^{p-2} + 2^{s-1} + 2^{s-2} + \frac{\overline{w_2}}{2} = \frac{n}{2} + 2^{s-2}$. Получаем, что во всех случаях $m \geq \frac{n}{2} + 2^{s-3}$. ■

Лемма 22. Выполнены неравенства

$$2^{p-1} \leq n < 2^{p-1} + 8p, \quad 2^{p-2} \leq m < 2^{p-2} + \frac{9}{2}p, \quad m < 2^{p-1}.$$

Доказательство. По лемме 20, двоичная запись n не может начинаться с 11. Если n не имеет вида $\overline{10^k 1 w_2}$, $|w_2| = s \geq 3$, то $n \leq 2^{p-1} + 7 < 2^{p-1} + 8p$. В противном случае применим лемму 21. Получим, что $m \geq \frac{n}{2} + 2^{s-3}$. Но $m < \frac{n}{2} + \frac{1}{2} \log_2 n < \frac{n}{2} + \frac{p}{2}$. Значит, $2^{s-3} < \frac{p}{2}$. Получаем, что $2^{p-1} \leq n = 2^{p-1} + 2^s + |w_2| < 2^{p-1} + 2^{s+1} < 2^{p-1} + 8p$. Первое неравенство доказано. Второе неравенство легко следует из первого: $2^{p-2} \leq \frac{n}{2} \leq m < \frac{n}{2} + \frac{1}{2} \log_2 n < 2^{p-2} + \frac{9}{2}p$. Учитывая, что двоичная запись n не может начинаться с 11, получаем, что при $p \geq 6$ выполнено $m < \frac{n}{2} + \frac{1}{2} \log_2 n < 2^{p-2} + 2^{p-3} + \frac{p}{2} < 2^{p-2} + 2^{p-3} + 2^{p-3} = 2^{p-1}$. ■

Лемма 23. Пусть $m = \overline{10^k w_1}$, $|w_1| = t$, $k \geq 0$, z — число нулей в слове w_1 , $p \geq 9$. Тогда

$$1 + \sum_{\substack{i, \\ \binom{i}{m} \equiv 1 \pmod{2}}} \binom{n}{i+1} > 2^{n-t-2+z}.$$

Доказательство. Заметим, что

$$1 + \sum_{\substack{i, \\ \binom{i}{m} \equiv 1 \pmod{2}}} \binom{n}{i+1} = 1 + \sum_{j=0}^{2^z-1} \sum_{i=0}^{2^k-1} \binom{n}{m_j + i2^t + 1},$$

где m_j обозначает число, полученное из m заменой нулевых битов в слове w_1 на биты двоичной записи числа j . При этом биты числа j не могут сдвинуться влево больше,

чем на число единиц в w_1 , т. е. на $t - z$ позиций. Отсюда получаем, что $m_j \leq m + 2^{t-z}j$, а значит, с учётом $m_j \geq m \geq n/2$ можем записать

$$\begin{aligned} 1 + \sum_{j=0}^{2^z-1} \sum_{i=0}^{2^k-1} \binom{n}{m_j + i2^t + 1} &> \sum_{j=0}^{2^z-1} \sum_{i=0}^{2^k-1} \binom{n}{m + j2^{t-z} + i2^t + 1} \geq \\ &\geq 2^{z-t} \sum_{j=0}^{2^t-1} \sum_{i=0}^{2^k-1} \binom{n}{m + j + i2^t + 1} = 2^{z-t} \sum_{i=0}^{2^{p-2}-1} \binom{n}{m + i + 1} = \\ &= 2^{z-t-1} \underbrace{\left(\sum_{i=0}^{2^{p-2}-1} \binom{n}{m + i + 1} + \sum_{i=0}^{2^{p-2}-1} \binom{n}{n - m - i - 1} \right)}_A. \end{aligned}$$

Обозначим последнее выражение в скобках через A . Тогда A совпадает с $\sum_{i=0}^n \binom{n}{i} = 2^n$, за исключением нескольких недостающих крайних и средних слагаемых. Крайних слагаемых по $n - m - 2^{p-2} \leq n - \left\lfloor \frac{n-1}{2} \right\rfloor - 2^{p-2} = \left\lfloor \frac{n+1}{2} \right\rfloor - 2^{p-2} \leq 2^{p-2} + 4p - 2^{p-2} = 4p$ с каждой из сторон. Каждое из них не превосходит $\binom{n}{4p} < \left(\frac{ne}{4p} \right)^{4p} < 2^{4p^2}/p^{4p}$. Получаем, что сумма крайних слагаемых не больше $8p2^{4p^2}/p^{4p}$. Количество средних слагаемых равно $2m + 1 - n \leq n + \lfloor \log_2 n \rfloor + 1 - n = p$. Каждое из них, как известно, не превосходит $2^n / \sqrt{\pi n/2}$, а значит, их сумма не больше $2^n p 2^{-p/2} \sqrt{2/\pi}$. Таким образом, для того, чтобы получить $A > 2^{n-1}$, достаточно потребовать $8p2^{4p^2}/p^{4p} < 2^n(1/2 - p2^{-p/2}\sqrt{2/\pi})$. Заметим, что при $p = 9$ выполнено $p2^{-p/2} = 9 \cdot 2^{-9/2} = \frac{9}{16\sqrt{2}} < \frac{9}{16 \cdot 7/5} = \frac{45}{112} < \frac{45}{105} = \frac{3}{7}$. При дальнейшем увеличении p это выражение уменьшается, поскольку $(p+1)/p = 1 + 1/p \leq 1 + 1/9 \leq \sqrt{2}$. Поэтому достаточно доказать неравенство $8p2^{4p^2}/p^{4p} < 2^{2^{p-1}}(1/2 - 3\sqrt{2/\pi}/7)$. Заметим, что $1/2 - 3\sqrt{2/\pi}/7 > 1/2 - 3\sqrt{2/3}/7 > 1/2 - 3\sqrt{49/64}/7 = 1/2 - 3/8 = 1/8$, поэтому достаточно доказать неравенство $8p2^{4p^2}/p^{4p} < 2^{2^{p-1}}/8$. Используя $p \geq 9$, оцениваем левую часть как $8p2^{4p^2}/p^{4p} = 2^{4p^2+3}/p^{4p-1} < 2^{4p^2+3}/2^{12p-3} = 2^{4p^2-12p+6}$. Неравенство сводится к $4p^2 - 12p + 6 < 2^{p-1} - 3$, или $(2p-3)^2 < 2^{p-1}$, откуда $2p-3 < 2^{(p-1)/2}$. При $p = 9$ неравенство верно, поскольку $2p-3 = 15 < 16 = 2^{(p-1)/2}$. А для $p > 9$ оно выполнено, поскольку левая часть растёт медленнее правой: $(2p-1)/(2p-3) = 1 + 2/(2p-3) \leq 1 + 2/15 < \sqrt{2}$. Таким образом, $2^{z-t-1}A > 2^{z-t-1} \cdot 2^{n-1} = 2^{n-t-2+z}$. ■

Лемма 24. Пусть $p \geq 9$. Тогда

$$2^{p-1} \leq n < 2^{p-1} + 16, \quad 2^{p-2} \leq m < 2^{p-2} + 8.$$

Доказательство. Предположим, что $n \geq 2^{p-1} + 16$. Тогда $n = \overline{10^k 1 w_2} = 2^{p-1} + 2^s + \overline{w_2}$, $|w_2| = s \geq 4$, $k \geq 1$. Используя лемму 21, получаем $m \geq n/2 + 2^{s-3}$, откуда $2m - 2^{s-2} \geq n$. Используя же лемму 23, получаем неравенство $2^{2n-2m-2} = 1 + \sum_{i, \binom{i}{m} \equiv 1 \pmod{2}} \binom{n}{i+1} > 2^{n-t-2+z}$, откуда $n \geq 2m - t + z + 1$. Из $2m - 2^{s-2} \geq n \geq 2m - t + z + 1$ следует $2^{s-2} + 1 \leq t - z$. Заметим, что $t - z$ равно количеству единиц в двоичной записи числа m , не считая самой старшей. Значит, выполнено неравенство

$m \geq 2^{p-2} + 2^{t-z} - 1$. Получаем $n + t - z - 1 \geq 2m \geq 2^{p-1} + 2^{t-z+1} - 2$. Оценивая n , получим $2^{p-1} + 2^{t-z+1} - 2 \leq 2^{p-1} + 2^{s+1} - 1 + t - z - 1$, откуда $2^{t-z+1} - (t - z) \leq 2^{s+1}$. Поскольку $s \geq 4$, отсюда следует, что $t - z \leq s$. В таком случае $2^{s-2} + 1 \leq t - z \leq s$, но это неравенство ложно для всех $s \geq 4$. Получили противоречие, значит, $n < 2^{p-1} + 16$.

Предположим теперь, что $m \geq 2^{p-2} + 8$. Из леммы 23, как доказано выше, следует неравенство $n \geq 2m - (t - z) + 1$. При $m = 2^{p-2} + 8$ получаем $2m - (t - z) + 1 = 2^{p-1} + 16 - 1 + 1 = 2^{p-1} + 16$. Заметим, что при увеличении числа m на единицу количество единиц в его двоичной записи может возрасти максимум на 1, а $2m$ при этом увеличивается на 2. Значит, $2m - (t - z) + 1 \geq 2^{p-1} + 16$ для всех $m \geq 2^{p-2} + 8$, что противоречит доказанному неравенству $n < 2^{p-1} + 16$. Следовательно, предположение не верно, и $m < 2^{p-2} + 8$. ■

Лемма 25. Пусть $p \geq 9$, $m = \overline{10^k w_1}$, $|w_1| = t \leq 3$, z — число нулей в слове w_1 . Тогда выполнено

$$1 + \sum_{i, \binom{i}{m} \equiv 1 \pmod{2}} \binom{n}{i+1} < 2^{n-t+z}.$$

Доказательство. Имеем

$$\begin{aligned} 1 + \sum_{i, \binom{i}{m} \equiv 1 \pmod{2}} \binom{n}{i+1} &\leq 1 + 2^z \sum_{i=0}^{2^{p-t-2}-1} \binom{n}{m+1+i2^t} \leq \\ &\leq 1 + 2^z 2^{-t} \left((2^t - 1) \binom{n}{m+1} + \sum_{i=m+1}^n \binom{n}{i} \right) < 2^{z-t} \left(2^t \binom{n}{\lfloor n/2 \rfloor} + 2^{n-1} \right). \end{aligned}$$

В последнем неравенстве использована оценка $2^{z-t} \binom{n}{\lfloor n/2 \rfloor} \geq 2^{-3} \binom{n}{\lfloor n/2 \rfloor} > 1$. Заметим, что из $p \geq 9$ следует неравенство $\binom{n}{\lfloor n/2 \rfloor} \leq \frac{2^n}{\sqrt{\pi n/2}} \leq \frac{2^n}{\sqrt{n}} \leq \frac{2^n}{2^4} \leq 2^{n-t-1}$. Значит, $2^{z-t} \left(2^t \binom{n}{\lfloor n/2 \rfloor} + 2^{n-1} \right) \leq 2^{z-t} (2^t \cdot 2^{n-t-1} + 2^{n-1}) = 2^{z-t} \cdot 2^n = 2^{n-t+z}$, что и требовалось доказать. ■

Лемма 26. Пусть $p \geq 9$. Тогда $m = \overline{10^k w_1}$, $|w_1| = t \leq 3$ и $n = 2m - t + z + 1$, где z — число нулей в слове w_1 .

Доказательство. Представимость числа m в указанном виде следует из леммы 24. Применяя леммы 25 и 23, получаем, что выражение

$$2^{2n-2m-2} = 1 + \sum_{i, \binom{i}{m} \equiv 1 \pmod{2}} \binom{n}{i+1}$$

заклучено между $2^{n-t+z-2}$ и 2^{n-t+z} . Значит, $2n - 2m - 2 = n - t + z - 1$, откуда получаем утверждение леммы. ■

Таким образом, при $p \geq 9$ для пары (m, n) остаются следующие возможности: $(2^{p-2}, 2^{p-1} + 1)$, $(2^{p-2} + 1, 2^{p-1} + 2)$, $(2^{p-2} + 2, 2^{p-1} + 4)$, $(2^{p-2} + 3, 2^{p-1} + 5)$, $(2^{p-2} + 4, 2^{p-1} + 8)$, $(2^{p-2} + 5, 2^{p-1} + 9)$, $(2^{p-2} + 6, 2^{p-1} + 11)$, $(2^{p-2} + 7, 2^{p-1} + 12)$. Первые две пары удовлетворяют равенству по лемме 7. Из оставшихся пар достаточно проверить

лишь половину, поскольку для чётных m выполнено

$$\begin{aligned}
 1 + \sum_{i, \binom{i}{m} \equiv 1 \pmod{2}} \binom{n}{i+1} &= 1 + \sum_{2|i, \binom{i}{m} \equiv 1 \pmod{2}} \left(\binom{n}{i+1} + \binom{n}{i+2} \right) = \\
 &= 1 + \sum_{i, \binom{i+1}{m+1} \equiv 1 \pmod{2}} \left(\binom{n}{i+1} + \binom{n}{i+2} \right) = 1 + \sum_{i, \binom{i}{m+1} \equiv 1 \pmod{2}} \left(\binom{n}{i} + \binom{n}{i+1} \right) = \\
 &= 1 + \sum_{i, \binom{i}{m+1} \equiv 1 \pmod{2}} \binom{n+1}{i+1}.
 \end{aligned}$$

Из пар с нечётным $m = (2^{p-2} + 3, 2^{p-1} + 5)$, $(2^{p-2} + 5, 2^{p-1} + 9)$ и $(2^{p-2} + 7, 2^{p-1} + 12)$ — первые два случая невозможны по теореме 6. Рассмотрим третий случай.

Лемма 27. Для любого $k \geq 0$ выполнено

$$3 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^k + 1111 \leq wi}} \Pi_2(0^k 1100, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^k 1100, wi + 1) \equiv 2 \pmod{4}.$$

Доказательство. Докажем утверждение по индукции. База: $k = 0$.

$$\begin{aligned}
 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 0111 \leq wi}} \Pi_2(1100, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (1100, wi + 1) &= \\
 = 3 + \Pi_2(1100, 1000) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (1100, 1000) &= 3 + 3 \cdot 1 \equiv 2 \pmod{4}.
 \end{aligned}$$

Докажем переход. Пусть утверждение верно для $k = t$, докажем его для $k = t + 1$. Поскольку $k > 0$, то в сумме отличны от нуля лишь слагаемые, у которых $wi + 1$ начинаются с 0:

$$\begin{aligned}
 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{t+1} 111 \leq wi}} \Pi_2(0^{t+1} 1100, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^{t+1} 1100, wi + 1) &= \\
 = 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{t+1} 111 \leq wi}} \Pi_2(0^{t+1} 1100, 0(wi + 1)) \cdot 1 &= \\
 = 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{t+1} 111 \leq wi}} \Pi_2(0^t 1100, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^t 1100, wi + 1).
 \end{aligned}$$

Последнее выражение сравнимо с 2 по модулю 4 по предположению индукции. Переход доказан. ■

Теорема 8. Пусть $wm = 010^k 111$, $wn = 10^k 1100$. Тогда

$$1 + \sum_{\substack{wi \neq 11\dots 1, \\ wm \leq wi}} \Pi_3(wn, wi + 1) M_2^*(wn, wi + 1) \equiv 4 \pmod{8}.$$

Доказательство. Преобразуем выражение:

$$\begin{aligned}
& 1 + \sum_{\substack{wi \neq 11\dots 1, \\ wm \preccurlyeq wi}} \Pi_3(wm, wi + 1) M_2^*(wm, wi + 1) = 1 + \Pi_3(10^k 1100, 100\dots 0) M_2^*(10^k 1100, 100\dots 0) + \\
& \quad + \sum_{\substack{wi \neq 11\dots 1, \\ 10^k 111 \preccurlyeq wi}} \Pi_3(10^k 1100, 0(wi + 1)) M_2^*(10^k 1100, 0(wi + 1)) + \\
& \quad + \sum_{\substack{wi \neq 11\dots 1, \\ 10^k 111 \preccurlyeq wi}} \Pi_3(10^k 1100, 1(wi + 1)) M_2^*(10^k 1100, 1(wi + 1)) = 1 + \begin{bmatrix} 1 \\ 5 \\ 5 \\ 1 \end{bmatrix} (0^k 1100) \begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^k 1100) + \\
& \quad + \sum_{\substack{wi \neq 11\dots 1, \\ 10^k 111 \preccurlyeq wi}} \Pi_3(0^k 1100, wi + 1) \begin{bmatrix} 1 & 4 & 3 & 2 \\ 1 & 5 & 5 & 5 \\ 1 & 6 & 5 & 4 \\ 1 & 7 & 7 & 1 \end{bmatrix} (0^k 1100, wi + 1) \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} (0^k 1100, wi + 1) + \\
& \quad + \sum_{\substack{wi \neq 11\dots 1, \\ 10^k 111 \preccurlyeq wi}} \Pi_3(0^k 1100, wi + 1) \begin{bmatrix} 1 & 0 & 3 & 6 \\ 5 & 1 & 1 & 1 \\ 5 & 2 & 1 & 0 \\ 1 & 7 & 7 & 1 \end{bmatrix} (0^k 1100, wi + 1) \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} (0^k 1100, wi + 1) \equiv \\
& \equiv \begin{bmatrix} 2 \\ 6 \\ 0 \\ 4 \end{bmatrix} (0^k 1100) + \sum_{\substack{wi \neq 11\dots 1, \\ 10^k 111 \preccurlyeq wi}} \Pi_3(0^k 1100, wi + 1) \begin{bmatrix} 2 & 4 & 6 & 4 \\ 6 & 6 & 2 & 2 \\ 0 & 4 & 0 & 4 \\ 4 & 4 & 4 & 4 \end{bmatrix} (0^k 1100, wi + 1) \pmod{8}.
\end{aligned}$$

Сократив на 2, получим, что нужно доказать

$$\begin{bmatrix} 1 \\ 3 \\ 0 \\ 2 \end{bmatrix} (0^k 1100) + \sum_{\substack{wi \neq 11\dots 1, \\ 10^k 111 \preccurlyeq wi}} \Pi_3(0^k 1100, wi + 1) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix} (0^k 1100, wi + 1) \equiv 2 \pmod{4}.$$

В случае $k = 0$ в сумме нет слагаемых, а значит, левая часть равна $\begin{bmatrix} 1 \\ 3 \\ 0 \\ 2 \end{bmatrix} (1100) = 2$,

что и требуется. Пусть $k > 0$. Продолжаем вычисления:

$$\begin{aligned}
& \begin{bmatrix} 1 \\ 3 \\ 0 \\ 2 \end{bmatrix} (0^k 1100) + \sum_{\substack{wi \neq 11\dots 1, \\ 10^k 111 \preccurlyeq wi}} \Pi_3(0^k 1100, wi + 1) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix} (0^k 1100, wi + 1) = \\
& = \begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^{k-1} 1100) + \sum_{\substack{wi \neq 11\dots 1, \\ 0^k 111 \preccurlyeq wi}} \Pi_3(0^k 1100, 1(wi + 1)) \begin{bmatrix} 1 & 2 & 3 & 2 \\ 3 & 3 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{bmatrix} (0^k 1100, 1(wi + 1)) \equiv \\
& \equiv \begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^{k-1} 1100) + \sum_{\substack{wi \neq 11\dots 1, \\ 0^k 111 \preccurlyeq wi}} \Pi_2(0^{k-1} 1100, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^{k-1} 1100, wi + 1) \pmod{4}.
\end{aligned}$$

В случае $k = 1$ в сумме одно слагаемое, значит, выражение равно $\begin{bmatrix} 1 \\ 3 \end{bmatrix} (1100) + \Pi_2(1100, 1000) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (1100, 1000) = 3 + 3 \cdot 1 \equiv 2 \pmod{4}$, что и требуется. Пусть $k \geq 2$. Продолжаем вычисления:

$$\begin{aligned}
& \begin{bmatrix} 1 \\ 3 \end{bmatrix} (0^{k-1}1100) + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{k-1}111 \leq wi}} \Pi_2(0^{k-1}1100, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^{k-1}1100, wi + 1) = \\
& = 1 + \Pi_2(0^{k-1}1100, 100\dots 0) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^{k-1}1100, 100\dots 0) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{k-1}111 \leq wi}} \Pi_2(0^{k-1}1100, 0(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^{k-1}1100, 0(wi + 1)) + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{k-1}111 \leq wi}} \Pi_2(0^{k-1}1100, 1(wi + 1)) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^{k-1}1100, 1(wi + 1)) = \\
& = 1 + \begin{bmatrix} 3 \\ 1 \end{bmatrix} (0^{k-2}1100) \cdot 2 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{k-1}111 \leq wi}} \Pi_2(0^{k-2}1100, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^{k-2}1100, wi + 1) \cdot 3 + \\
& + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{k-1}111 \leq wi}} \Pi_2(0^{k-2}1100, wi + 1) \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} (0^{k-2}1100, wi + 1) \cdot 2 \equiv \\
& \equiv 3 + \sum_{\substack{wi \neq 11\dots 1, \\ 0^{k-1}111 \leq wi}} \Pi_2(0^{k-2}1100, wi + 1) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} (0^{k-2}1100, wi + 1) \pmod{4}.
\end{aligned}$$

Остаётся воспользоваться леммой 27. ■

Таким образом, случай $m = 2^{p-2} + 7$, $n = 2^{p-1} + 12$ невозможен. Поэтому при $p \geq 9$ единственными подходящими парами являются пары $m = 2^{p-2}$, $n = 2^{p-1} + 1$ и $m = 2^{p-2} + 1$, $n = 2^{p-1} + 2$. Отсюда получаем основной результат.

Теорема 9. Если $n \geq 512$, $0 < m < n - 1$ и пара n, m не принадлежит сериям $m = 2^s$, $n = 2^{s+1} + 1$ и $m = 2^s + 1$, $n = 2^{s+1} + 2$ при $s \geq 0$, то для корреляционно-иммунной порядка m булевой функции f от n переменных выполнено неравенство

$$\text{nl}(f) \leq 2^{n-1} - 2^{m+1}.$$

Проверка равенства (1) для $n < 512$, $n - 2 \geq m \geq (n - 1)/2$ на компьютере позволяет убрать ограничение $n \geq 512$ из предыдущей теоремы.

ЛИТЕРАТУРА

1. *Sarkar P. and Maitra S.* Nonlinearity bounds and constructions of resilient boolean functions // LNCS. 2000. V. 1880. P. 515–532.
2. *Tarannikov Yu.* On resilient Boolean functions with maximal possible nonlinearity // LNCS. 2000. V. 1977. P. 19–30.
3. *Zheng Y. and Zhang X. M.* Improved upper bound on the nonlinearity of high order correlation immune functions // LNCS. 2001. V. 2012. P. 264–274.
4. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 91–148.

5. *Халлявин А. В.* Построение 4 корреляционно-иммунных булевых функций от 9 переменных с нелинейностью 240 // Материалы X Междунар. семинара «Дискретная математика и её приложения». Москва, МГУ, 1–6 февраля 2010 г. М.: Изд-во механико-математического факультета МГУ, 2010. С. 534.
6. *Ботев А. А.* О соотношениях между корреляционной иммунностью, нелинейностью и весом для неуравновешенных булевых функций // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 149–162.
7. *Guo-Zhen X. and Massey J. A.* Spectral characterization of correlation-immune combining functions // IEEE Trans. Information Theory. 1988. V. 34. No. 3. P. 569–571.