УДК 512.563 : 517.987.3
DOI: 10.20535/SRIT.2308-8893.2020.1.12

# МЕТОД ТРИКУТНИКА ДЛЯ ПОБУДОВИ ПОЛІНОМА ЖЕГАЛКІНА: ЗВ'ЯЗОК З ТРИКУТНИКОМ ПАСКАЛЯ

**І.Я. СПЕКТОРСЬКИЙ, О.А. ГАЛГАНОВ**

**Анотація.** Поліном Жегалкіна — зручний спосіб зображення булевої функції у вигляді суми за операцією $\oplus$ (xor, або сума за модулем 2) скінченної кількості кон'юнкцій змінних — запропонований у 1927 р. радянським ученим І.І. Жегалкіним. Одним з алгоритмів побудови полінома Жегалкіна для заданої булевої функції є метод трикутника, запропонований у 1985–1987 рр. радянським математиком В.П. Супруном. Застосування методу трикутника збігається з почерговою побудовою рядків трикутника Паскаля з використанням відомого співвідношення $C_{n+1}^{k+1} = C_n^k + C_n^{k+1}$. Природно очікувати на зв'язок обчислення полінома Жегалкіна методом трикутника з розташуванням біноміальних коефіцієнтів у трикутнику Паскаля. Проаналізовано зв'язок методу трикутника з побудовою рядків трикутника Паскаля; запропоновано відносно просте доведення коректності методу трикутника шляхом зіставлення кожного кроку алгоритма з покроковою побудовою рядків біноміальних коефіцієнтів у трикутнику Паскаля.

**Ключові слова:** булева функція, поліном Жегалкіна, метод трикутника, трикутник Паскаля.

## ВСТУП

Поліном Жегалкіна — зручний спосіб зображення булевої функції у вигляді суми за операцією $\oplus$ (xor, або сума за модулем 2) скінченної кількості кон'юнкцій (логічного добутку) змінних — запропонований у 1927 р. радянським ученим І.І. Жегалкіним ([1]). Відомо (див., напр., [2, 3]), що кожну булеву функцію можна зобразити у вигляді полінома Жегалкіна єдиним способом (з точністю до переставлення доданків та множників у межах доданка).

Відомі різні алгоритми побудови полінома Жегалкіна для заданої булевої функції — метод еквівалентних перетворень (з побудованої диз'юнктивної або кон'юнктивної нормальної форми), метод невизначених коефіцієнтів, метод Паскаля (половинне ділення) тощо. Менш відомий зручний (хоча не найефективніший) метод трикутника, запропонований у 1985 р. радянським математиком В.П. Супруном для симетричних булевих функцій [4], а в 1987 р. — поширений на довільні булеві функції [5].

Застосування методу трикутника по суті збігається з побудовою кожного наступного рядка трикутника Паскаля почерговим додаванням двох сусідніх значень у попередньому рядку, тобто з використанням співвідношення $C_{n+1}^{k+1} = C_n^k + C_n^{k+1}$. Природно очікувати на зв'язок обчислення полінома Жегалкіна методом трикутника (і зрештою будь-яким іншим методом) з розташуванням біноміальних коефіцієнтів у трикутнику Паскаля. Проте ані опис

методу трикутника у працях [5, 6], ані доведення у [5] (як узагальнення аналогічного результату, доведеному для симетричних булевих функцій [4]) не розкривають зв'язок цього методу з біноміальними коефіцієнтами.

**Мета роботи**: надати відносно просте доведення методу трикутника з розкриттям тісного зв'язку між матрицею перетворення вектора значень булевої функції у вектор коефіцієнтів полінома Жегалкіна з розташуванням біноміальних коефіцієнтів у трикутнику Паскаля.

## ОПЕРАТОР ПЕРЕТВОРЕННЯ ВЕКТОРА ЗНАЧЕНЬ БУЛЕВОЇ ФУНКЦІЇ У ВЕКТОР КОЕФІЦІЄНТІВ ПОЛІНОМА ЖЕГАЛКІНА

Нехай $f$ — $n$-арна булева функція, тобто $f: B^n \to B$, де $B = \{0,1\}$; за потреби арність $n \geq 0$ вказують у позначенні функції $f$, використовуючи позначення $f^{(n)}$. У випадку $n = 0$ функцію $f^{(0)}$ вважають константою 0 або 1.

Булеву функцію $f(x_1, x_2, \ldots, x_n)$ зазвичай задають її вектором значень $w_f = (f_0, f_1, \ldots, f_{2^n-1})$, де $f_k$ $(0 \leq k \leq 2^n - 1)$ — значення $f$ на двійковому наборі $(x_1, x_2, \ldots, x_n) \in B^n$, що відповідає двійковому запису числа $k$, тобто $f_k = f(x_1, x_2, \ldots, x_n)$, якщо $k = \sum_{i=1}^{n} x_i 2^{n-i}$.

Поліномом Жегалкіна називають суму за операцією $\oplus$ (суму за модулем 2) скінченної кількості кон'юнктів (добутку змінних); кожна змінна входить у кожен кон'юнкт не більше одного разу; порожній кон'юнкт (що не містить жодної змінної) є константою 1; кон'юнкти, що містять ті самі змінні і відрізняються лише порядком їх запису, вважають однаковими; кожен кон'юнкт входить у поліном не більше одного разу. Очевидно, що поліном Жегалкіна є «традиційним» поліномом над полем $\langle \{0,1\}, \oplus, \cdot \rangle$, яке ізоморфне полю Галуа GF(2) (також використовують позначення $\mathbb{F}_2$) та кільцю класів лишків $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$, і яке у цьому контексті називають алгеброю Жегалкіна.

Поліном Жегалкіна можна подати у вигляді

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\substack{1 \leq j_1 < j_2 < \ldots < j_k \leq n \\ 0 \leq k \leq n}} a_m x_{j_1} x_{j_2} \cdots x_{j_k}, \qquad (1)$$

де $a_m \in \{0,1\}$ $(1 \leq j_1 < j_2 < \ldots < j_k \leq n, 1 \leq k \leq n)$, індекси $j_1, j_2, \ldots, j_k$ відповідають розрядам у двійковому записі номера $m$, тобто

$$m = \sum_{i=1}^{k} 2^{n-j_i} = \overbrace{0\ldots\underset{j_1}{1}0\ldots\underset{j_2}{1}0\ldots\ldots\underset{j_k}{1}0\ldots0}^{n}.$$

**Приклад 1.** Зведемо у таблицю номери коефіцієнтів $a_m$ у десятковій системі та двійковому коді для $n = 0, 1, 2, 3$ і запишемо відповідні кон'юнкти (див. таблицю).

Кодування кон'юнктів у поліномі Жегалкіна для $n = 3$

| $m$ | | Кон'юнкт |
|---|---|---|
| десяткова система | двійковий код | |
| $n = 0$ : номер відсутній | | 1 |
| $n = 1$ | | |
| 0 | 0 | 1 |
| 1 | 1 | $x_1$ |
| $n = 2$ | | |
| 0 | 00 | 1 |
| 1 | 01 | $x_1$ |
| 2 | 10 | $x_2$ |
| 3 | 11 | $x_1x_2$ |

| $m$ | | Кон'юнкт |
|---|---|---|
| десяткова система | двійковий код | |
| $n = 3$ | | |
| 000 | 0 | 1 |
| 001 | 1 | $x_3$ |
| 010 | 2 | $x_2$ |
| 011 | 3 | $x_1x_2$ |
| 100 | 4 | $x_1$ |
| 101 | 5 | $x_1x_3$ |
| 110 | 6 | $x_1x_2$ |
| 111 | 7 | $x_1x_2x_3$ |

Для $n = 1, 2, 3$ співвідношення (1) набуває вигляду

$$f(x_1) = a_0 \oplus a_1x_1\,,\ f(x_1, x_2) = a_0 \oplus a_1x_2 \oplus a_2x_1 \oplus a_3x_1x_2\,;$$

$$f(x_1, x_2, x_3) = a_0 \oplus a_1x_3 \oplus a_2x_2 \oplus a_3x_2x_3 \oplus a_4x_1 \oplus a_5x_1x_3 \oplus a_6x_2x_3 \oplus a_7x_1x_2x_3\,;$$

у випадку $n = 0$ булева функція $f$ та відповідний поліном Жегалкіна $a$ є константою 0 або 1.

Очевидно, що поліном Жегалкіна над змінними $x_1, x_2, \ldots, x_n$ однозначно (з точністю до порядку доданків та множників у межах кожного доданка) визначено коефіцієнтами $a_m$ $(0 \le m \le 2^n - 1)$, які формують вектор $p_f$ коефіцієнтів полінома Жегалкіна.

Відомо [2, 3], що для кожної булевої функції існує єдиний (з точністю до порядку доданків та множників у межах кожного доданка) поліном Жегалкіна. Ураховуючи очевидну лінійну залежність між вектором значень $w_f$ та вектором коефіцієнтів полінома Жегалкіна $p_f$ булевої функції $f^{(n)}$, можемо розглядати співвідношення (тут і далі, якщо не вказано інше, операції додавання та множення, визначені за арифметикою поля $\mathbb{F}_2$)

$$A_n p_f = w_f\,, \tag{2}$$

де $A_n$ — матриця розмірності $2^n \times 2^n$ над полем $\mathbb{F}_2$ (двійкова матриця). Матриця $A_n$ у співвідношенні (2) визначає систему $2^n$ лінійних рівнянь, які (а отже і $A_n$) можна отримати підставленням у формулу (1) усіх можливих наборів значень змінних $x_1, x_2, \ldots, x_n$ у порядку зростання за номером $k = \sum_{i=1}^{n} x_i 2^{n-i}$.

**Приклад 2.** Для $n = 0,1,2,3$ співвідношення (2) набуває вигляду

$$(1)a = f;\ \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}a_0\\ a_1\end{pmatrix} = \begin{pmatrix}f(0)\\ f(1)\end{pmatrix};\ \begin{pmatrix}1 & 0 & 0 & 0\\ 1 & 1 & 0 & 0\\ 1 & 0 & 1 & 0\\ 1 & 1 & 1 & 1\end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ a_2\\ a_3\end{pmatrix} = \begin{pmatrix}f(0,0)\\ f(0,1)\\ f(1,0)\\ f(1,1)\end{pmatrix};$$

$$\begin{pmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0\\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0\\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6\\ a_7\end{pmatrix} = \begin{pmatrix}f(0,0,0)\\ f(0,0,1)\\ f(0,1,0)\\ f(0,1,1)\\ f(1,0,0)\\ f(1,0,1)\\ f(1,1,0)\\ f(1,1,1)\end{pmatrix}.$$

Зазначимо, що за обраної нумерації елементів у векторах $w_f$ та $p_f$ матриця $A_n$ для будь-якого $n \geq 0$ є нижньотрикутною. З огляду на існування та єдиність полінома Жегалкіна для кожної булевої функції рівняння (2) відносно $p_f$ за будь-якого фіксованого $w_f$ має єдиний розв'язок.

Множину $B^k$ для $k \geq 1$ розглядатимемо як лінійний простір над полем $\mathbb{F}_2$ з покоординатним застосуванням $\oplus$ як суми векторів; $A_n$ — матриця лінійного перетворення у $B^{2^n}$, визначеного за співвідношенням (2).

Матрицю $A_n$ можна побудувати рекурсивно за $n \geq 0$ (див., напр., [6]); для зручності наведемо відповідне твердження та його просте доведення.

**Лема 1.** Для послідовності матриць $A_n$ ($n \geq 0$) справджується рекурентне співвідношення:

- база рекурсії

$$A_0 = (1); \tag{3}$$

- крок рекурсії

$$A_{n+1} = \begin{matrix}\\ 2^n\{\\ 2^n\{\end{matrix}\begin{matrix}\overbrace{\phantom{00}}^{2^n} & \overbrace{\phantom{00}}^{2^n}\\ \end{matrix}\begin{pmatrix}A_n & 0\\ A_n & A_n\end{pmatrix}. \tag{4}$$

**Доведення.** Застосуємо принцип математичної індукції, якщо $n \geq 0$.

*База.* Для $n = 0$ отримуємо: $f^{(0)}(x) = a_0$, $p_f = w_f = (a_0)$, звідки $A_0 = (1)$ як матриця тотожного перетворення у $B^1 = B$. Отже, співвідношення (3) справджується.

*Припущення.* Нехай $m \geq 0$, і для $n = m$ твердження леми справджується.

*Крок.* Доведемо твердження леми для $n = m+1$. Увівши $m$-арні функції $f_{x_1}(x_2,\ldots,x_m,x_{m+1}) = f(1,x_2,\ldots,x_m,x_{m+1})$ та $f_{\bar{x}_1}(x_2,\ldots,x_m,x_{m+1}) = f(0,x_2,\ldots,x_m,x_{m+1})$, отримаємо:

$$f(x_1,x_2,\ldots,x_m,x_{m+1}) = \bar{x}_1 f_{\bar{x}_1}(x_2,\ldots,x_m,x_{m+1}) \oplus x_1 f_{x_1}(x_2,\ldots,x_m,x_{m+1}) =$$

$$= (x_1 \oplus 1) f_{\bar{x}_1}(x_2,\ldots,x_m,x_{m+1}) \oplus x_1 f_{x_1}(x_2,\ldots,x_m,x_{m+1}) =$$

$$= f_{\bar{x}_1}(x_2,\ldots,x_m,x_{m+1}) \oplus x_1 (f_{\bar{x}_1}(x_2,\ldots,x_m,x_{m+1}) \oplus f_{x_1}(x_2,\ldots,x_m,x_{m+1})). \quad (5)$$

Визначення функцій $f_{x_1}$ і $f_{\bar{x}_1}$ та розклад (5) дозволяють записати вектор коефіцієнтів $p_f$ та вектор значень $w_f$ і через $p_{f_{\bar{x}_1}}$ і $p_{f_{x_1}}$ та через $w_{f_{\bar{x}_1}}$ і $w_{f_{x_1}}$ відповідно (тут і далі операція $\oplus$ на векторах застосовується покоординатно):

$$w_f = \begin{matrix} 2^m \{ \\ 2^m \{ \end{matrix} \begin{pmatrix} w_{f_{\bar{x}_1}} \\ w_{f_{x_1}} \end{pmatrix}; \; p_f = \begin{matrix} 2^m \{ \\ 2^m \{ \end{matrix} \begin{pmatrix} p_{f_{\bar{x}_1}} \\ p_{f_{\bar{x}_1}} \oplus p_{f_{x_1}} \end{pmatrix},$$

звідки

$$\begin{pmatrix} A_m & 0 \\ A_m & A_m \end{pmatrix} p_f = \begin{pmatrix} A_m & 0 \\ A_m & A_m \end{pmatrix} \begin{pmatrix} p_{f_{\bar{x}_1}} \\ p_{f_{\bar{x}_1}} \oplus p_{f_{x_1}} \end{pmatrix} = \begin{pmatrix} A_m p_{f_{\bar{x}_1}} \\ A_m p_{f_{\bar{x}_1}} \oplus A_m (p_{f_{\bar{x}_1}} \oplus p_{f_{x_1}}) \end{pmatrix} =$$

$$= \begin{pmatrix} A_m p_{f_{\bar{x}_1}} \\ A_m p_{f_{x_1}} \end{pmatrix} = \begin{pmatrix} w_{f_{\bar{x}_1}} \\ w_{f_{x_1}} \end{pmatrix} = w_f .$$

Отже, $\begin{pmatrix} A_m & 0 \\ A_m & A_m \end{pmatrix} p_f = w_f$ для довільної булевої функції $f^{(m)}$. Оскільки матрицю лінійного у $B^n$ перетворенні $p_f \mapsto w_f$ у співвідношенні (2) визначено однозначно, отримуємо твердження кроку рекурсії (4): $A_{m+1} = \begin{pmatrix} A_m & 0 \\ A_m & A_m \end{pmatrix}$.

**Наслідок.** Перетворення $p_f \mapsto w_f$ інволютивне, тобто $A_n{}^2 = I_{2^n}$ (або $A_n = A_n{}^{-1}$) для кожного $n \geq 0$.

**Доведення.** Достатньо довести рівність $A_n{}^2 = I_{2^n}$ для довільного $n \geq 0$, застосовуючи принцип математичної індукції.

*База.* Для $n = 0$ з урахуванням співвідношення (3) отримуємо: $A_0{}^2 = (1)^2 = (1) = I_1$.

*Припущення.* Нехай $m \geq 0$, і для $n = m$ твердження $A_n^2 = I_{2^n}$ справджується.

*Крок.* Доведемо твердження $A_n{}^2 = I_{2^n}$ для $n = m+1$. З урахуванням співвідношення (4) маємо:

$$A_n{}^2 = A_{m+1}{}^2 = \begin{pmatrix} A_m & 0 \\ A_m & A_m \end{pmatrix}^2 = \begin{pmatrix} A_m{}^2 & 0 \\ A_m \oplus A_m & A_m{}^2 \end{pmatrix} = \begin{pmatrix} I_{2^m} & 0 \\ 0 & I_{2^m} \end{pmatrix} = I_{2^{m+1}} = I_{2^n}.$$

**Приклад 3.** Обчислимо $A_n$ для $0 \le n \le 3$ за рекурентними співвідношеннями (3) і (4):

$$A_0 = (1);\ A_1 = \begin{pmatrix} A_0 & 0 \\ A_0 & A_0 \end{pmatrix} = \left(\begin{array}{c|c} 1 & 0 \\ \hline 1 & 1 \end{array}\right);\ A_2 = \begin{pmatrix} A_1 & 0 \\ A_1 & A_1 \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{array}\right);$$

$$A_3 = \begin{pmatrix} A_2 & 0 \\ A_2 & A_2 \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

**Зауваження 1.** Існування та єдиність розв'язку рівняння (2) і трикутність матриці $A_n$ для довільного $n \ge 0$ дозволяє знаходити коефіцієнти полінома Жегалкіна добре відомим методом невизначених коефіцієнтів, розв'язуючи рівняння (2) послідовним обчисленням координат вектора $p_f$ без безпосереднього обчислення $A_n$ (детальніше див., напр., [6]).

**Зауваження 2.** Твердження леми 1 фактично обґрунтовує коректність відомого методу Паскаля — рекурсивне обчислення вектора коефіцієнтів полінома Жегалкіна за вектором значень булевої функції послідовним діленням вектора значень навпіл (детальніше див., напр., [6]).

**Зауваження 3.** Завдяки співвідношенню $A_n = A_n^{-1}$, яке забезпечує наслідок з леми 1, рівняння (2) допускає обертання: $A_n w_f = p_f$, що дозволяє (за наявності матриці $A_n$) безпосередньо обчислювати вектор коефіцієнтів полінома Жегалкіна $p_f$ за заданим вектором значень $w_f$.

## МЕТОД ТРИКУТНИКА: МАТРИЦЯ ОПЕРАТОРА ПЕРЕТВОРЕННЯ

Метод трикутника побудови полінома Жегалкіна для булевої функції $f : B^n \to B$, який запропонував радянський вчений В.П. Супрун [4–6], полягає у побудові векторів $v^0, v^1, \ldots, v^{2^n-1} \in B^{2^n}$ за рекурентними співвідношеннями

$$v^0 = w_f,\ v_i^{k+1} = \begin{cases} v_i^k, & \text{якщо } 0 \le i \le k; \\ v_{i-1}^k \oplus v_i^k, & \text{якщо } k+1 \le i \le 2^n \end{cases} \tag{6}$$

для $0 \le k \le 2^n - 2$. Доведено [5] і для випадку симетричних булевих функцій [4], що координати $v_0^k$ $(0 \le k \le 2^n - 1)$ утворюють вектор коефіцієнтів полінома Жегалкіна, тобто

$$p_f = \left( v_0^0, v_1^1, \ldots, v_{2^n-1}^{2^n-1} \right).$$

Зі співвідношення (6) очевидно, що $v_k^k = v_k^{k+1} = \cdots = v_k^{2^n-1}$ $(0 \le k \le 2^n - 1)$, а отже,

$$p_f = \left( v_0^0, v_1^1, \ldots, v_{2^n-1}^{2^n-1} \right) = \left( v_0^{2^n-1}, v_1^{2^n-1}, \ldots, v_{2^n-1}^{2^n-1} \right) = v^{2^n-1},$$

тобто застосуванням рекурентного співвідношення (6) дістаємо $p_f = v^{2^n-1}$ за $2^n - 2$ кроків.

**Приклад 4.** Для булевої функції $f^{(2)}$ з вектором значень $w_f = (1101)$ маємо:

$$v^0 = w_f = (1101);$$

$$v^1 = (1, 1 \oplus 1, 1 \oplus 0, 0 \oplus 1) = (1011);$$

$$v^2 = (1, 0, 0 \oplus 1, 1 \oplus 1) = (1010);$$

$$v^3 = (1, 0, 1, 1 \oplus 0) = (1011).$$

Таким чином, $p_f = v^3 = (1011)$, тобто поліном Жегалкіна функції $f$ містить кон'юнкти з номерами 0, 2 і 3, що відповідає двійковим кодам 00 10 та 11. Отже, отримуємо такий поліном Жегалкіна:

$$f(x_1, x_2) = 1 \oplus x_1 \oplus x_1 x_2.$$

**Приклад 5.** Для булевої функції $f^{(3)}$ з вектором значень $w_f = (11111101)$ отримуємо:

$$v^0 = w_f = (11111101);$$

$$v^1 = (1, 1 \oplus 1, 1 \oplus 1, 1 \oplus 1, 1 \oplus 1, 1 \oplus 1, 1 \oplus 0, 0 \oplus 1) = (10000011);$$

$$v^2 = (1, 0, 0 \oplus 0, 0 \oplus 0, 0 \oplus 0, 0 \oplus 0, 0 \oplus 1, 1 \oplus 1) = (10000010);$$

$$v^3 = (1, 0, 0, 0 \oplus 0, 0 \oplus 0, 0 \oplus 0, 0 \oplus 1, 1 \oplus 0) = (10000011);$$

$$v^4 = (1, 0, 0, 0, 0 \oplus 0, 0 \oplus 0, 0 \oplus 1, 1 \oplus 1) = (10000010);$$

$$v^5 = (1, 0, 0,0, 0, 0 \oplus 0, 0 \oplus 1, 1 \oplus 0) = (10000011);$$

$$v^6 = (1, 0, 0,0, 0, 0, 0 \oplus 1, 1 \oplus 1) = (10000010);$$

$$v^7 = (1, 0, 0,0, 0, 0, 1, 1 \oplus 0) = (10000011).$$

Таким чином, $p_f = v^7 = (10000011)$, тобто поліном Жегалкіна функції $f$ містить кон'юнкти з номерами 0, 6 та 7, що відповідає двійковим кодам 000, 110 та 111. Отже, маємо такий поліном Жегалкіна:

$$f(x_1, x_2, x_3) = 1 \oplus x_1 x_2 \oplus x_1 x_2 x_3 .$$

Зазначимо, що за побудовою (співвідношення (6)) у кожному з векторів $v^k \in B^{2^n}$ $(1 \le k \le 2^n - 1)$ перші $k$ координат збігаються з відповідними координатами вектора $v^{k-1}$, що дозволяє визначати вектори $v^k$ $(0 \le k \le 2^n - 1)$ як вектори меншої розмірності ($v^k \in B^{2^n - k}, 0 \le k \le 2^n - 1$), і саме так зазвичай діють під час опису методу [4–6]. Однак у цій роботі для подальшого розгляду доцільно не зменшувати розмірність векторів $v^k$ $(0 \le k \le 2^n - 1)$ на кожному кроці рекурсії, доповнюючи перші *k* координат відповідними координатами вектора $v^{k-1}$, отриманого на попередньому кроці.

Запишемо рекурентне співвідношення (6) у векторно-матричному вигляді над полем $\mathbb{F}_2$:

$$v^0 = w_f ,\ v^{k+1} = T_{n,k+1} v^k ,$$

де $T_{n,k} = \left(\begin{array}{ccccc|ccccc} & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & I_k & & & & \vdots & & \vdots & & \vdots \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ & & \vdots & & & & & \ddots & \vdots & & \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{array}\right)$, $1 \le k \le 2^n - 1$,

звідки для перетворення $w_f \mapsto p_f$ дістаємо $p_f = T_{n,2^n-1} T_{n,2^n-2} \cdots T_{n,1} w_f$ за арифметикою $\mathbb{F}_2$.

Уведемо до розгляду матриці

$$T_n = T_{n,2^n-1} T_{n,2^n-2} \cdots T_{n,1} \text{ за арифметикою поля } \mathbb{F}_2 ;$$

$$T_n^{\mathbb{Z}} = T_{n,2^n-1} T_{n,2^n-2} \cdots T_{n,1} \text{ за арифметикою кільця } \mathbb{Z} .$$

Очевидно, що $T_n = T_n^{\mathbb{Z}} \bmod 2$, де $\bmod 2$ застосовується до кожного елемента матриці $T_n^{\mathbb{Z}}$.

**Приклад 6.** Для $n = 2$ отримуємо:

$$T_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

за арифметикою $\mathbb{F}_2$;

$$T_2^{\mathbb{Z}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix}$$

за арифметикою $\mathbb{Z}$.

Легко пересвідчитися, що $T_2 = T_2^{\mathbb{Z}} \bmod 2$. Наведемо проміжний етап обчислення для $T_2^{\mathbb{Z}}$:

$$T_{2,2}^{\mathbb{Z}}\, T_{2,1}^{\mathbb{Z}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

**Приклад 7.** Для $n = 3$ отримуємо:

$$T_3^{\mathbb{Z}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 4 & 6 & 4 & 1 & 0 & 0 & 0 \\ 1 & 5 & 10 & 10 & 5 & 1 & 0 & 0 \\ 1 & 6 & 15 & 20 & 15 & 6 & 1 & 0 \\ 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \end{pmatrix}$$

за арифметикою $\mathbb{Z}$;

$$T_3 = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&1&1&0&0&0\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \times \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&1&1&0&0&0&0\\ 0&0&0&1&1&0&0&0\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&1&1&0&0&0&0&0\\ 0&0&1&1&0&0&0&0\\ 0&0&0&1&1&0&0&0\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} \times$$

$$\times \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 0&1&1&0&0&0&0&0\\ 0&0&1&1&0&0&0&0\\ 0&0&0&1&1&0&0&0\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 1&0&1&0&0&0&0&0\\ 1&1&1&1&0&0&0&0\\ 1&0&0&0&1&0&0&0\\ 1&1&0&0&1&1&0&0\\ 1&0&1&0&1&0&1&0\\ 1&1&1&1&1&1&1&1 \end{pmatrix}$$

за арифметикою $\mathbb{Z}$;

Легко пересвідчитися, що $T_3 = T_3^{\mathbb{Z}} \bmod 2$. Наведемо проміжні етапи обчислення для $T_3^{\mathbb{Z}}$:

$$T_{2,2}^{\mathbb{Z}} T_{2,1}^{\mathbb{Z}} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 1&2&1&0&0&0&0&0\\ 0&1&2&1&0&0&0&0\\ 0&0&1&2&1&0&0&0\\ 0&0&0&1&2&1&0&0\\ 0&0&0&0&1&2&1&0\\ 0&0&0&0&0&1&2&1 \end{pmatrix}; \quad T_{3,3}^{\mathbb{Z}} T_{3,2}^{\mathbb{Z}} T_{3,1}^{\mathbb{Z}} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 1&2&1&0&0&0&0&0\\ 1&3&3&1&0&0&0&0\\ 0&1&3&3&1&0&0&0\\ 0&0&1&3&3&1&0&0\\ 0&0&0&1&3&3&1&0\\ 0&0&0&0&1&3&3&1 \end{pmatrix};$$

$$T_{3,4}^{\mathbb{Z}} T_{3,3}^{\mathbb{Z}} T_{3,2}^{\mathbb{Z}} T_{3,1}^{\mathbb{Z}} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0\\ 1&2&1&0&0&0&0&0\\ 1&3&3&1&0&0&0&0\\ 1&4&6&4&1&0&0&0\\ 0&1&4&6&4&1&0&0\\ 0&0&1&4&6&4&1&0\\ 0&0&0&1&4&6&4&1 \end{pmatrix};$$

$$T_{3,5}^{\mathbb{Z}}T_{3,4}^{\mathbb{Z}}T_{3,3}^{\mathbb{Z}}T_{3,2}^{\mathbb{Z}}T_{3,1}^{\mathbb{Z}}=\begin{pmatrix}1&0&0&0&0&0&0&0\\1&1&0&0&0&0&0&0\\1&2&1&0&0&0&0&0\\1&3&3&1&0&0&0&0\\1&4&6&4&1&0&0&0\\1&5&10&10&5&1&0&0\\0&1&5&10&10&5&1&0\\0&0&1&5&10&10&5&1\end{pmatrix};$$

$$T_{3,6}^{\mathbb{Z}}T_{3,5}^{\mathbb{Z}}T_{3,4}^{\mathbb{Z}}T_{3,3}^{\mathbb{Z}}T_{3,2}^{\mathbb{Z}}T_{3,1}^{\mathbb{Z}}=\begin{pmatrix}1&0&0&0&0&0&0&0\\1&1&0&0&0&0&0&0\\1&2&1&0&0&0&0&0\\1&3&3&1&0&0&0&0\\1&4&6&4&1&0&0&0\\1&5&10&10&5&1&0&0\\1&6&15&20&15&6&1&0\\0&1&6&15&20&15&6&1\end{pmatrix}.$$

**Теорема 1.** Матриця $T_n^{\mathbb{Z}}$ $(n\geq 0)$ містить трикутник Паскаля під головною діагоналлю:

$$T_n^{\mathbb{Z}}=\begin{pmatrix}C_0^0&0&0&\cdots&0\\C_1^0&C_1^1&0&\cdots&0\\&&\vdots&&\\C_{2^n-1}^0&C_{2^n-1}^1&C_{2^n-1}^2&\cdots&C_{2^n-1}^{2^n-1}\end{pmatrix}. \qquad (7)$$

**Доведення.** Математичною індукцією за $k\geq 1$ $(k\leq 2^n-1)$ доведемо рівність

$$T_{n,k}^{\mathbb{Z}}T_{n,k-1}^{\mathbb{Z}}\cdots T_{n,1}^{\mathbb{Z}}=\begin{pmatrix}C_0^0&0&\cdots&0&0&0&0&\cdots&0&0\\C_1^0&C_1^1&0&\cdots&0&0&0&\cdots&0&0\\&&\ddots&&&&&\vdots&&\\C_k^0&C_k^1&\cdots&C_k^k&0&0&0&\cdots&0&0\\0&C_k^0&C_k^1&\cdots&C_k^k&0&0&\cdots&0&0\\0&0&C_k^0&C_k^1&\cdots&C_k^k&0&0&0&0\\0&0&0&\ddots&&&\ddots&\vdots&&\\0&0&\cdots&0&C_k^0&C_k^1&\cdots&C_k^k&0&0\\0&0&0&\cdots&0&C_k^0&C_k^1&\cdots&C_k^k&0\\0&0&0&0&\cdots&0&C_k^0&C_k^1&\cdots&C_k^k\end{pmatrix}. \qquad (8)$$

*База*. У випадку $k=1$ співвідношення (8) є тривіальним:

$$T_{n,1}^{\mathbb{Z}} = \left(\begin{array}{ccccc|cccccc} & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & I_1 & & & & \vdots & & \vdots & & \vdots \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ & & \vdots & & & & & \ddots & \vdots & & \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{array}\right) = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ & \ddots & & \ddots & & \\ 0 & \cdots & 0 & 1 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}.$$

*Припущення.* Нехай $1 \le m \le 2^n - 2$, і для $k = m$ співвідношення (8) справджується.

*Крок.* Доведемо рівність (8) для $k = m+1$. Використовуючи відому тотожність $C_m^{i+1} + C_m^i = C_{m+1}^{i+1}$, а також очевидні рівності $C_m^0 + 0 = C_{m+1}^0$ та $0 + C_m^m = C_{m+1}^{m+1}$, отримуємо:

$$T_{n,m+1}^{\mathbb{Z}} T_{n,m}^{\mathbb{Z}} \cdots T_{n,1}^{\mathbb{Z}} = \left(\begin{array}{ccccc|cccccc} & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & I_{m+1} & & & & \vdots & & \vdots & & \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ & & \vdots & & & & & \ddots & \vdots & & \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{array}\right) \times$$

$$\times v \left(\begin{array}{ccccc|cc|cccc} C_0^0 & 0 & \cdots & 0 & 0 & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ C_1^0 & C_1^1 & 0 & \cdots & 0 & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & \ddots & & & & & & & & \vdots & & \\ C_{m-1}^0 & C_{m-1}^1 & \cdots & C_{m-1}^{m-1} & 0 & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ C_m^0 & C_m^1 & \cdots & C_m^{m-1} & C_m^m & & & 0 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & C_m^0 & C_m^1 & \cdots & C_m^{m-1} & C_m^m & & 0 & 0 & \cdots & 0 & 0 & \\ 0 & 0 & C_m^0 & \cdots & C_m^{m-2} & C_m^{m-1} & C_m^m & 0 & \cdots & 0 & 0 & & \\ & & & \ddots & & & & & \ddots & & & & \\ 0 & 0 & 0 & 0 & 0 & C_m^0 & C_m^1 & \cdots & C_m^m & 0 & 0 & & \\ 0 & 0 & 0 & 0 & 0 & 0 & C_m^0 & C_m^1 & \cdots & C_m^m & 0 & & \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & C_m^0 & C_m^1 & \cdots & C_m^m & & \end{array}\right) =$$

$$= \left(\begin{array}{ccccc|c|ccccccc}
C_0^0 & 0 & \cdots & 0 & 0 & 0 & & 0 & 0 & 0 & \cdots & 0 & 0 \\
C_1^0 & C_1^1 & 0 & \cdots & 0 & 0 & & 0 & 0 & 0 & \cdots & 0 & 0 \\
 & & \ddots & & & \vdots & & & & & & & \\
C_{m-1}^0 & C_{m-1}^1 & \cdots & C_{m-1}^{m-1} & 0 & 0 & & 0 & 0 & 0 & \cdots & 0 & 0 \\
C_m^0 & C_m^1 & \cdots & C_m^{m-1} & C_m^m & 0 & & 0 & 0 & 0 & \cdots & 0 & 0 \\
\hline
C_{m+1}^0 & C_{m+1}^1 & \cdots & C_{m+1}^{m-1} & C_{m+1}^m & C_{m+1}^m & & 0 & 0 & 0 & \cdots & 0 & 0 \\
\hline
0 & C_{m+1}^0 & \cdots & C_{m+1}^1 & C_{m+1}^{m-1} & C_{m+1}^m & C_{m+1}^{m+1} & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & C_{m+1}^0 & \cdots & C_{m+1}^{m-2} & C_{m+1}^{m-1} & C_{m+1}^m & C_{m+1}^{m+1} & 0 & \cdots & 0 & 0 \\
 & & & \ddots & & & & & \ddots & & & \\
0 & 0 & 0 & 0 & \cdots & 0 & C_{m+1}^0 & C_{m+1}^1 & \cdots & C_{m+1}^{m+1} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & C_{m+1}^0 & C_{m+1}^1 & \cdots & C_{m+1}^{m+1} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & C_{m+1}^0 & C_{m+1}^1 & \cdots & C_{m+1}^{m+1}
\end{array}\right).$$

Отже, співвідношення (8) справджується для $k = m+1$. Таким чином, згідно з принципом математичної індукції, рівність (8) справджується для кожного $1 \le k \le 2^n - 1$. Шукану рівність (7) тепер дістаємо зі співвідношення (8), якщо $k = 2^n - 1$. □

Твердження теореми 1, а також «проміжну» рівність (8), продемонстровано у прикладах 6 та 7.

## КОРЕКТНІСТЬ МЕТОДУ ТРИКУТНИКА

### Деякі властивості парності біноміальних коефіцієнтів

Парність біноміальних коефіцієнтів зручно досліджувати, використовуючи техніку кільця поліномів $\mathbb{F}_2[x]$ над полем $\mathbb{F}_2$. Нагадаємо (див. [7]), що кільце поліномів $K[x]$ над комутативним кільцем $K$ з одиницею визначають як сукупність нескінченних послідовностей елементів із $K$, у кожній з яких усі члени, починаючи з деякого, дорівнюють 0 (нулю кільця $K$). Операції додавання та множення кільця $K$ природним чином поширюють на $K[x]$, трактуючи елементи послідовностей як коефіцієнти полінома. Елементи кільця $K[x]$ для зручності зображують поліномами зі змінною $x$ (змінну $x$ уведено винятково для зручності позначень).

У кільці поліномів $K[x]$ справджується низка алгебричних властивостей, відомих для класичних поліномів кільця $\mathbb{R}[x]$; зокрема, у кільці $K[x]$ справджується біноміальна формула. Детальніше про кільце поліномів див., напр. [7].

**Лема 2.** Число $C_{2^n}^k$ є парним для всіх $n \ge 0$, $1 \le k \le 2^n - 1$.

**Доведення.** Твердження леми доводитимемо математичною індукцією за $n \ge 0$.

*База.* Для $n = 0$ твердження леми тривіальне завдяки відсутності цілих $1 \le k \le 2^0 - 1$.

*Припущення.* Нехай твердження леми справджується для $n = n_0$, тобто $C_{2^{n_0}}^{k}$ є парним для всіх $1 \le k \le 2^{n_0} - 1$.

*Крок.* Нехай $n = n_0 + 1$. Для полінома $(1 \oplus x)^{2^{n_0+1}}$ за біноміальною формулою отримуємо розклад

$$(1 \oplus x)^{2^{n_0+1}} =$$

$$= C_{2^{n_0+1}}^{0} \oplus C_{2^{n_0+1}}^{1} x \oplus C_{2^{n_0+1}}^{2} x^2 \oplus \cdots \oplus C_{2^{n_0+1}}^{2^{n_0+1}-1} x^{2^{n_0+1}-1} \oplus C_{2^{n_0+1}}^{2^{n_0+1}} x^{2^{n_0+1}}, \quad (9)$$

а з урахуванням припущення індукції за арифметикою $\mathbb{F}_2$:

$$(1 \oplus x)^{2^{n_0+1}} = \left((1 \oplus x)^{2^{n_0}}\right)^2 = \left(1 \oplus x^{2^{n_0}}\right)^2 = 1 \oplus 2x^{2^{n_0}} \oplus x^{2^{n_0+1}} = 1 \oplus x^{2^{n_0+1}}. \quad (10)$$

Порівнюючи коефіцієнти поліномів у розкладах (9) та (10) за арифметикою $\mathbb{F}_2$ (зокрема, ототожнюючи цілі числа за еквівалентністю $\bmod 2$), отримуємо твердження кроку індукції:

$$C_{2^{n_0+1}}^{k} \equiv \begin{cases} 1, \text{ якщо } k = 0 \text{ або } k = 2^{n_0+1}; \\ 0, \text{ якщо } 1 \le k \le 2^{n_0+1}. \end{cases} \pmod 2.$$

Таким чином, згідно з принципом математичної індукції, твердження леми справджується для кожного $n \ge 0$, тобто число $C_{2^n}^{k}$ є парним для всіх $n \ge 0$, $1 \le k \le 2^n - 1$.

Надалі для зручності позначень покладемо

$$C_i^j = 0 \text{ для } j > i, \quad (11)$$

вважаючи біноміальні коефіцієнти $C_i^j$ визначеними для всіх невід'ємних $i, j \in \mathbb{Z}$. Легко пересвідчитись, що тотожність $C_i^j + C_i^{j+1} = C_{i+1}^{j+1}$ для $j \ge i$ також справджується:

$$j > i: \; C_i^j + C_i^{j+1} = C_{i+1}^{j+1} = 0;$$

$$j = i: \; C_i^i + C_i^{i+1} = C_{i+1}^{i+1} = 1.$$

**Лема 3.** Числа $C_m^k$, $C_{m+2^n}^{k}$, $C_{m+2^n}^{k+2^n}$ мають однакову парність для всіх $0 \le m \le 2^n - 1$, $0 \le k \le 2^n - 1$, $n \ge 0$.

**Доведення.** Для полінома $(1 \oplus x)^{2^n + m}$ $(0 \le m \le 2^n - 1)$ за арифметикою $\mathbb{F}_2$ з урахуванням леми **2** отримуємо:

$$(1 \oplus x)^{2^n+m} = (1 \oplus x)^{2^n} (1 \oplus x)^m = (1 \oplus x^{2^n})(C_m^0 \oplus C_m^1 x \oplus \cdots \oplus C_m^m x^m) =$$

$$= C_m^0 \oplus C_m^1 x \oplus \cdots \oplus C_m^m x^m \oplus C_m^0 x^{2^n} \oplus C_m^1 x^{2^n+1} \oplus \cdots \oplus C_m^m x^{2^n+m}. \quad (12)$$

Порівнюючи коефіцієнти у розкладі (12) з відповідними коефіцієнтами у розкладі за біноміальною формулою, дістаємо шукане твердження леми:

$$C_m^k \equiv C_{m+2^n}^k \equiv C_{m+2^n}^{k+2^n} \pmod 2$$

для $0 \le m \le 2^n - 1$, $0 \le k \le 2^n - 1$, $n \ge 0$.

**Приклад 8.** Продемонструємо результат леми 3 для $n = 2$, $0 \le m \le 3$, $0 \le k \le 3$:

$$\begin{array}{cccc} 1 & 0 & 0 & 0 \\ {\scriptstyle 1,1} & {\scriptstyle 4,0} & {\scriptstyle 6,0} & {\scriptstyle 4,0} \\ 1 & 1 & 0 & 0 \\ {\scriptstyle 1,5} & {\scriptstyle 5,1} & {\scriptstyle 10,0} & {\scriptstyle 10,0} \\ 1 & 2 & 1 & 0 \\ {\scriptstyle 1,15} & {\scriptstyle 6,6} & {\scriptstyle 15,1} & {\scriptstyle 20,0} \\ 1 & 3 & 3 & 1 \\ {\scriptstyle 1,35} & {\scriptstyle 7,21} & {\scriptstyle 21,7} & {\scriptstyle 35,1} \end{array}$$

$$\begin{array}{cccccccc} 1 & 4 & 6 & 4 & 1 & 0 & 0 & 0 \\ 1 & 5 & 10 & 10 & 5 & 1 & 0 & 0 \\ 1 & 6 & 15 & 20 & 15 & 6 & 1 & 0 \\ 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \end{array}.$$

У наведеному фрагменті трикутника Паскаля з урахуванням рівності (11) біля кожного елемента $C_m^k$ для $0 \le m \le 3$, $0 \le k \le 3$ (лівий верхній кут) наведено елементи $C_{m+4}^k$, $C_{m+4}^{k+4}$. Легко пересвідчитися, що для кожних $0 \le m \le 3$, $0 \le k \le 3$ елементи $C_m^k$, $C_{m+4}^k$, $C_{m+4}^{k+4}$ дійсно мають однакову парність.

**Зауваження 4.** Розглядаючи розклад поліномів над полем $\mathbb{F}_p$, можна досліджувати подільність біноміальних коефіцієнтів на довільне просте $p$; *н*априклад, нескладно довести:

- $C_{p^n}^k \equiv 0 \pmod p$ для $1 \le k \le p^n - 1$, $n \ge 0$;
- $C_{p^n-1}^k \equiv 0 \pmod p$ для $0 \le k \le p^n$, $n \ge 0$.

Детальніше про властивості біноміальних коефіцієнтів за $\bmod p$ для простого $p$ див., напр., [8].

## Доведення коректності методу трикутника

**Теорема 2.** Матриця $T_n$, що визначає метод трикутника для булевої функції $f^{(n)}$, визначає перетворення $w_f \mapsto p_f$, тобто $T_n w_f = p_f$ за арифметикою поля $\mathbb{F}_2$.

**Доведення.** З урахуванням леми 1 для доведення рівності $T_n = A_n$ достатньо довести математичною індукцією рекурентні співвідношення (3) і (4) для $T_n$ ($n \ge 0$).

*База.* Для $n = 0$ отримуємо: $T_0 = A_0 = (1)$, тобто співвідношення (3) для $T_0 = A_0$ справджується.

*Припущення.* Нехай твердження теореми справджується для $n = n_0$, тобто $T_{n_0} = A_{n_0}$.

*Крок.* Нехай $n = n_0 + 1$. За теоремою 1 для $0 \le i, j \le 2^{n_0+1} - 1$ та з урахуванням рівності (11) маємо:

$$(T_{n_0+1})_{i,j} = \begin{cases} C_i^j \bmod 2, & \text{якщо } j \le i; \\ 0, & \text{якщо } j > i, \end{cases} = C_i^j \bmod 2;$$

де mod — бінарна операція взяття остачі від ділення; зокрема, для $a \in \mathbb{Z}$

$$a \bmod 2 = \begin{cases} 0, & \text{якщо } a \text{ парне;} \\ 1, & \text{якщо } a \text{ непарне.} \end{cases}$$

Далі з теореми 1 негайно випливає рівність $(T_{n_0+1})_{i,j} = (T_{n_0})_{i,j} = C_i^j \bmod 2$ для $0 \le i, j \le 2^{n_0} - 1$. Звідси за лемою 3 отримуємо:

$$(T_{n_0})_{i,j} = (T_{n_0+1})_{i,j} = (T_{n_0+1})_{i+2^{n_0},j} = (T_{n_0+1})_{i+2^{n_0},j+2^{n_0}} = C_i^j \bmod 2$$

для $0 \le i, j \le 2^{n_0} - 1$. Таким чином, три блоки $(T_{n_0+1})_{\substack{0 \le i \le 2^{n_0}-1 \\ 0 \le j \le 2^{n_0}-1}}$, $(T_{n_0+1})_{\substack{0 \le i \le 2^{n_0}-1 \\ 2^{n_0} \le j \le 2^{n_0+1}-1}}$, $(T_{n_0+1})_{\substack{2^{n_0} \le i \le 2^{n_0+1}-1 \\ 2^{n_0} \le j \le 2^{n_0+1}-1}}$ збігаються між собою та з матрицею $T_{n_0}$. Отже, з урахуванням кроку індукції та леми 1

$$T_{n_0+1} = \begin{pmatrix} T_{n_0} & 0 \\ T_{n_0} & T_{n_0} \end{pmatrix} = \begin{pmatrix} A_{n_0} & 0 \\ A_{n_0} & A_{n_0} \end{pmatrix} = A_{n_0+1},$$

що доводить твердження кроку індукції. Згідно з принципом математичної індукції співвідношення рекурсії (4) для $T_n$ справджується для всіх $n \ge 0$, що завершує доведення теореми. □

## ВИСНОВКИ

1. Метод трикутника побудови полінома Жегалкіна, запропонований у працях [4, 5], тісно пов'язаний з трикутником Паскаля: рядки трикутника Паскаля з точністю до еквівалентності за mod 2 формують не тільки матрицю методу $T_n$, а і проміжні матриці $T_{n,k}$ $(1 \le k \le 2^n - 1)$, які відповідають окремим крокам алгоритма.

2. Зв'язок з трикутником Паскаля дозволяє обґрунтувати коректність методу трикутника, зіставляючи рекурентну побудову матриць $T_n$ $(n \ge 0)$ та покрокову побудову рядків трикутника Паскаля (див. доведення теореми 1).

**ЛІТЕРАТУРА**

1. *Жегалкин И.И.* О технике вычислений предложений в символической логике / И.И. Жегалкин // Математический сборник. — 1927. — С. 9–28.
2. *Марченков С.С.* Замкнутые классы булевых функций / С.С. Марченков. — М.: Физматлит, 2000. — 128 с.
3. *Яблонский С.В.* Введение в дискретную математику / С.В. Яблонский. — М.: Наука. — 1986. — 272 с.
4. *Супрун В.П.* Полиномиальное разложение симметрических булевых функций / В.П. Супрун // Изв. АН СССР. Техническая кибернетика. — 1985. — № 4. — С. 123–127.
5. *Супрун В.П.* Табличный метод полиномиального разложения булевых функций / В.П. Супрун // Кибернетика. — 1987. — № 1. — С. 116–117.
6. *Супрун В.П.* Основы теории булевых функций / В.П. Супрун. — М.: Ленанд, 2017. — 208 с.
7. *Завало С.Т.* Курс алгебри / С.Т. Завало. — К.: Вища шк., 1985. — 503 с.
8. *Granville A.* Arithmetic Properties of Binomial Coefficients I: Binomial coefficients modulo prime powers / A. Granville // Canadian Mathematical Society Conference Proceedings. — 1997. — N 20. — P. 253–275.

*Надійшла 10.01.2020*