

## ДОСЛІДЖЕННЯ ІНДЕКСУ РОЗГАЛУЖЕННЯ МАТРИЧНИХ ПЕРЕТВОРЕНЬ НАД КІЛЬЦЯМИ ЛИШКІВ

О. В. Курінний<sup>1, а</sup>

<sup>1</sup>Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»,  
Фізико-технічний інститут

### Анотація

У даній роботі досліджено питання існування MDS-матриць над кільцями лишків за модулем, який є парним числом. Даний результат демонструє границі застосування  $(0, 1)$ -матриць над конкретним типом алгебраїчних структур. Також були сформульовані твердження, які є достатніми умовами побудови  $(0, 1)$ -матриць з високим індексом розгалуження, що дозволяють економити ресурси при побудові матриць такого типу, та на їх основі був побудований алгоритм пошуку  $(0, 1)$ -матриці з заданим індексом розгалуження.

*Ключові слова:* індекс розгалуження, матриці над кільцями лишків,  $(0, 1)$ -матриці, MDS-матриці

### Вступ

При конструюванні SP-мереж дуже важливим є побудова якісного лінійного перетворення, оскільки лінійне перетворення забезпечує властивість поширення. У роботі Йона Демена [1] була сформульована характеристика, яка відповідає за якість лінійного перетворення, – індекс розгалуження. У сучасних SP-мережах використовуються складні лінійні перетворення, які, як правило, побудовані або над скінченними полями, або над кільцями лишків. Особливим випадком є  $(0, 1)$ -матриці, які є ефективними в реалізації, оскільки дозволяють дуже швидко виконувати необхідні операції. Тому питання побудови  $(0, 1)$ -матриць з високим індексом розгалуження потребує дослідження. Іншим підходом до побудови лінійного перетворення є використання матриць над кільцями лишків. Як правило, такі матриці будуються за модулем  $2^m$ , а для таких матриць були отримані оцінки індексу розгалуження [4]. Але для кільців лишків за іншим модулем навіть не з'ясоване питання існування MDS-матриць, тому в даній роботі були також розглянуті кільця лишків за парним модулем.

### 1. Індекс розгалуження та його оцінки для матриць над кільцями лишків

Індекс розгалуження є мірою властивості поширення лінійного перетворення. Як правило, лінійне перетворення реалізується множенням на деяку матрицю, тому визначимо індекс розгалуження матриці.

**Визначення.** Індексом розгалуження матриці  $A$  розміру  $m \times m$  є величина  $BN(A)$ , яка визначається наступним чином ( $x$  – вектор розміру  $m \times 1$ ):

$$BN(A) = \min_{x \neq 0} \{wt(x) + wt(Ax)\}$$

Матриця є невиродженою, якщо для неї існує обернена матриця. Для індексу розгалуження невироджених матриць виконується наступна нерівність:

$$1 \leq BN(A) \leq m + 1$$

В даному випадку  $m$  – розмір матриці  $A$ .

Цілком зрозуміло, що найбільший інтерес складають матриці з максимальним індексом розгалуження, оскільки володіють найкращим поширенням.

**Визначення.** Матриця  $A$  розміру  $m \times m$  називається MDS-матрицею, якщо  $BN(A) = m + 1$ .

Для визначення чи є матриця MDS-матрицею відомий наступний критерій [3].

**Твердження.** Матриця є MDS-матрицею тоді і тільки тоді, коли всі її підматриці є невиродженими.

Досить ефективним рішенням є використання матриць над кільцями лишків, оскільки вони є обчислювально ефективними. Було показано [2], що серед  $(0, 1)$ -матриць не існує MDS-матриць, а також отримана верхня оцінка для індексу розгалуження  $(0, 1)$ -матриць.

**Твердження.** Для  $(0, 1)$ -матриці  $A$  розміру  $m \times m$  виконується нерівність:

$$BN(A) \leq \frac{2m + 4}{3}$$

Аналогічна оцінка була отримана для матриць над кільцем лишків  $\mathbb{Z}_{2^n}$ .

Матриці над кільцями лишків можна зустріти у таких криптосистемах як Midori [6], SAFER+ [7], ARIA [5].

При доведенні оцінок індексу розгалуження будемо користуватись формулою включень-виключень для XOR'у.

**Твердження.** Нехай  $a_1, \dots, a_n$  – бінарні вектори однакового розміру. Тоді виконується наступна рів-

<sup>а</sup>ol.kurinnoy@gmail.com

ність:

$$wt(a_1 \oplus \dots \oplus a_n) = \sum_{i=1}^n wt(a_i) - 2 \sum_{1 \leq i < j \leq n} wt(a_i \& a_j) + \dots + (-2)^{n-1} wt(a_1 \& \dots \& a_n)$$

Якщо відкинути у формулі включень-виключень усі доданки, починаючи з другого, то отримаємо оцінку для ваги XOR'у векторів:

$$wt\left(\bigoplus_{i=1}^n a_i\right) \leq \sum_{i=1}^n wt(a_i)$$

Введемо наступне позначення: нехай для деякого вектору  $x$  число  $nz(x)$  – це кількість нульових координат цього вектору. Очевидно, що для вектору  $x$  розміру  $n$  виконується  $nz(x) = n - wt(x)$ . Інколи ця функція називається антивагою вектору  $x$ .

Нескладно переконатись в тому, що для операції XOR виконується наступна властивість:  $a \oplus b = \bar{a} \oplus \bar{b}$ , де  $a, b$  – деякі бінарні вектори, а  $\bar{a}, \bar{b}$  – вектори, отримані з  $a$  і  $b$  інвертуванням нулей та одиниць. Виходячи з цієї властивості, нескладно отримати ще одну оцінку для ваги XOR'у сукупності векторів:

$$wt\left(\bigoplus_{i=1}^{2n} a_i\right) = wt\left(\bigoplus_{i=1}^{2n} \bar{a}_i\right) \leq \sum_{i=1}^{2n} wt(\bar{a}_i) = \sum_{i=1}^{2n} nz(a_i)$$

Якщо  $n = 1$ , то отримуємо наступну нерівність:

$$wt(a_1 \oplus a_2) \leq nz(a_1) + nz(a_2)$$

Частковий випадок для двох бінарних векторів дуже часто використовується на практиці, тому був виділений окремо.

## 2. MDS-матриці над кільцем $\mathbb{Z}_{2^n}$

Будемо позначати  $\mathbb{Z}_{2^n}$  – кільце за модулем  $2^n$ . Виявляється, що для матриць над такою структурою виконується наступне твердження.

**Твердження.** Над кільцем лишків  $\mathbb{Z}_{2^n}$  не існує MDS-матриць.

**Доведення.** Позначимо  $M_m(\mathbb{Z}_{2^n})$  – множина матриць розміру  $m \times m$  над кільцем лишків  $\mathbb{Z}_{2^n}$ . Розглянемо довільну матрицю  $A \in M_m(\mathbb{Z}_{2^n})$ . Припустимо, що вона має максимально можливий індекс розгалуження, тобто  $m+1$ . Також припустимо, що у матриці  $A$  є хоча б один парний елемент, тобто для деяких індексів  $i$  та  $k$  виконується:  $a_{ik} = 2l$ , де  $l \in \mathbb{Z}_{2^{n-1}}$ . Побудуємо вектор  $x$  наступного виду:

$$x_j = \begin{cases} 2^{n-1}, & j = k, \\ 0, & \text{інакше.} \end{cases}$$

Очевидно, що  $wt(x) = 1$ . В такому разі  $wt(Ax)$  має дорівнювати  $m$ , оскільки інакше матриця  $A$  не буде мати індекс розгалуження  $m+1$ , тобто не буде MDS-матрицею. Позначимо для зручності  $Ax = y = (y_1, \dots, y_m)$  і подивимось чому дорівнює компонента цього вектору  $y_i$ . Перемноживши матрицю на вектор отримуємо:

$$y_i = \sum_{j=1}^m a_{ij} \cdot x_j = a_{ik} \cdot x_k = 2l \cdot 2^{n-1} = 2^n \cdot l = 0 \pmod{2^n}$$

Таким чином, якщо хоча б один елемент матриці  $A$  парний, то завжди можна підібрати такий вектор одиничної ваги  $x$ , що вектор  $Ax$  буде мати вагу, меншу за  $m$ , тобто матриця  $A$  не буде MDS-матрицею. Тому у всіх наступних міркуваннях вважаємо, що всі елементи матриці  $A$  є непарними числами.

Тепер розглянемо будь-яку підматрицю  $A'$  розміру  $2 \times 2$  матриці  $A$ . Нехай ця підматриця має вид:

$$A' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Як було показано раніше, ця матриця повинна складатись виключно з непарних елементів. Обчислимо її визначник:  $\det(A') = ad - bc$ . Зрозуміло, що різниця двох непарних чисел є числом парним, тому  $\gcd(\det(A'), 2) > 1$ . Таким чином, матриця  $A'$  є виродженою, тому, за критерієм MDS-матриць, матриця  $A$  не є MDS-матрицею, отже над кільцем лишків  $\mathbb{Z}_{2^n}$  не існує MDS-матриць.

## 3. Необхідні умови побудови $(0, 1)$ -матриць з високим індексом розгалуження

Розглянемо ряд обмежень, які дозволяють будувати матриці з високим індексом розгалуження. Позначимо  $M_n(\{0, 1\})$  – множина  $(0, 1)$ -матриць розміру  $m \times m$ .

**Твердження 1.** Якщо у матриці  $A \in M_n(\{0, 1\})$  деякий стовпець має вагу не більшу за  $\frac{n}{2}$ , то така матриця має індекс розгалуження  $BN(A) \leq \frac{n}{2} + 1$ .

**Доведення.** Нехай для деякого стовпця  $a_i$  матриці  $A$ , де  $i = \bar{1}, n$ , виконується  $wt(a_i) \leq \frac{n}{2}$ . Тоді підберемо такий вектор  $x$ , що  $wt(x) = 1$  та  $x_i = 1$ , а всі інші координати цього вектору покладемо рівними нулю. Тоді  $wt(Ax)$  буде не перевищувати  $\frac{n}{2}$ , і, відповідно,  $wt(x) + wt(Ax) \leq \frac{n}{2} + 1$ .

**Наслідок.** Доведене твердження ілюструє той факт, що при підборі матриці потрібно, щоб усі стовпці мали вагу, більшу за  $\frac{n}{2}$ . Інакше індекс розгалуження цієї матриці впаде до  $\frac{n}{2}$ , що є поганою оцінкою для індексу розгалуження.

**Твердження 2.** Якщо у матриці  $A \in M_n(\{0, 1\})$  два стовпця мають вагу не меншу за  $\frac{3n}{4}$ , то така матриця має індекс розгалуження  $BN(A) \leq \frac{n}{2} + 2$ .

**Доведення.** Нехай деякі два стовпця  $a_i$  та  $a_j$  матриці  $A$ , де  $i, j = \bar{1}, n$ , мають вагу, яка не менша за  $\frac{3n}{4}$ . Побудуємо такий вектор  $x$ , що  $wt(x) = 2$  та  $x_i = x_j = 1$ , а всі інші координати цього вектору дорівнюють нулю. Будемо шукати вагу вектору  $Ax$  і скористаємось введеним раніше позначенням  $nz(x)$  – кількість нульових елементів вектору  $x$ . Тоді виконується наступна нерівність:  $wt(Ax) = wt(a_i \oplus a_j) \leq nz(a_i) + nz(a_j) = \frac{n}{2}$ . Тоді  $wt(x) + wt(Ax) \leq \frac{n}{2} + 2$ .

**Наслідок.** Доведений факт демонструє, що всі стовпці, можливо за винятком одного, повинні мати вагу, меншу за  $\frac{3n}{4}$ . Таким чином, як дуже мала вага стовпця, так і дуже велика, погано впливають на індекс розгалуження.

Насправді, твердження 1 та 2 можна узагальнити, оскільки формула для оцінки ваги вектору  $Ax$  буде працювати у випадку більшої кількості векторів.

**Твердження 3.** Якщо у матриці  $A \in M_n(\{0, 1\})$  деякі  $k$  стовпців, де  $k$  – парне число, мають вагу не меншу за  $\frac{2k-1}{2k} \cdot n$ , то така матриця має індекс розгалуження  $BN(A) \leq \frac{n}{2} + k$ .

**Доведення.** Нехай деякі  $k$  стовпців, де  $k$  – парне число,  $a_{i_1}, \dots, a_{i_k}, i_1, \dots, i_k = \overline{1, n}$  матриці  $A$  мають вагу, яка не менша за  $\frac{2k-1}{2k} \cdot n$ . Побудуємо такий вектор  $x$ , що  $wt(x) = k$  та  $x_{i_1} = \dots = x_{i_k} = 1$ , а всі інші координати цього вектору покладемо рівними нулю. Тоді для ваги вектору  $Ax$  виконується нерівність:

$$wt(Ax) \leq \sum_{l=1}^k nz(a_{i_l}) \leq k \cdot \frac{1}{2k} \cdot n = \frac{n}{2}$$

Тоді очевидно, що  $wt(x) + wt(Ax) \leq \frac{n}{2} + k$ .

**Зауваження.** Доведена нерівність є інформативною лише в тому разі, коли  $k$  значно менше ніж  $\frac{n}{2}$ . Якщо  $k = \frac{n}{2} + 1$ , то отримуємо теоретичну оцінку, яка не надає корисної інформації.

При підстановці у доведене твердження  $k = 4$ , маємо, що при побудові матриці потрібно обирати вагу стовпців таким чином, щоб усі, за виключенням можливо трьох, мали вагу, яка не перевищує  $\frac{7n}{8}$ . Здається, що це твердження є слабшим попереднього, але є сенс його розглядати, оскільки твердження включають лише необхідні умови побудови матриць з високим індексом розгалуження.

На основі вищенаведених тверджень можна сформулювати алгоритм побудови матриць з високим індексом розгалуження. Перевага такого алгоритму над звичайним випадковим пошуком полягає в тому, що він є більш економним по відношенню до використаних ресурсів. Слід зауважити, що на вхід цього алгоритму подається число  $b$  – індекс розгалуження, який бажаємо отримати, тобто алгоритм має повернути першу знайдену матрицю з індексом розгалуження, який перевищує задане на початку  $b$ . Очевидно, що  $b \leq \frac{2n+4}{3}$ , де  $n$  – розмір шуканої матриці, але з огляду на те, що у багатьох випадках, частина з яких наведена у твердженнях, індекс розгалуження падає нижче  $\frac{n}{2}$ , то можлива ситуація, що алгоритм не знайде потрібної матриці. Оскільки поки не відома нижня оцінка індексу розгалуження  $(0, 1)$ -матриць, то невідомо якого індексу розгалуження можна гарантовано досягти. Тому встановимо деяке порогове значення  $N$ , яке буде обмежувати обсяг перебору.

**Алгоритм.** Побудова матриці заданого розміру з заданим індексом розгалуження.

*Вхід.* Числа  $n$  та  $b$  такі, що  $1 \leq b \leq \frac{2n+4}{3}$ , а також число  $N$ .

*Вихід.*  $(0, 1)$ -матриця розміру  $n \times n$  з індексом розгалуження  $b$  або символ « $\emptyset$ » (у тому випадку, коли не вдалось знайти жодну матрицю з потрібним індексом розгалуження).

- 1) Ініціалізуємо змінну  $count$ , покладаючи її значення рівне нулю:  $count := 0$ .
- 2) Якщо  $count > N$ , то подаємо на вихід символ « $\emptyset$ », інакше виконуємо наступні дії. Генеруємо випадковим та незалежним чином  $n - 1$   $(0, 1)$ -векторів  $a_1, \dots, a_{n-1}$  таких, що  $\frac{n}{2} \leq wt(a_i) \leq \frac{3n}{4}$ ,  $i = \overline{1, n-1}$ . Генеруємо ще один  $(0, 1)$ -вектор  $a_n$

випадковим і незалежним по відношенню до усіх раніше згенерованих векторів чином, такий, що  $\frac{n}{2} \leq wt(a_n) \leq n + 1$ .

- 3) Шукаємо усі можливі попарні XOR'и між згенерованими  $n$  векторами. Якщо хоча б для однієї пари векторів  $(a_i, a_j)$  виконується  $wt(a_i \oplus a_j) < b - 2$ , то збільшуємо  $count := count + 1$  і повертаємось до пункту 2). Проводимо такий ж пошук для усіх трійок, четвірок і т.д., включаючи значення  $n$ . Таким чином, якщо поточний крок дорівнює  $t$ , тобто розглядаємо усі вибірки без повторення розміру  $t$ , то умова переривання алгоритму буде:  $wt(a_{i_1} \oplus \dots \oplus a_{i_t}) < b - t$ .
- 4) Якщо пункт 3) був виконаний успішно, то матриця з потрібним індексом розгалуження або навіть більше потрібного, була знайдена. Подаємо цю  $(0, 1)$ -матрицю на вихід.

Слід відзначити, що можна використовувати такий самий алгоритм для послідовного перебору і пошуку потрібної  $(0, 1)$ -матриці.

## Висновки

В даній роботі було досліджено питання існування MDS-матриць над кільцем лишків  $\mathbb{Z}_{2^n}$ . Таким чином розширено клас алгебраїчних структур, для яких це питання з'ясовано. Також були сформульовані достатні твердження для побудови матриць з високим індексом розгалуження. Вони були застосовані для побудови алгоритму, який дозволяє значно швидше виконувати пошук  $(0, 1)$ -матриць з заданим індексом розгалуження.

## Перелік використаних джерел

1. J. Daemen, V. Rijmen. The Wide Trail Design Strategy. — 2001. — С. 17 с. — Режим доступу: [http://jda.noekeon.org/JDA\\_VRI\\_Wide\\_2001.pdf](http://jda.noekeon.org/JDA_VRI_Wide_2001.pdf).
2. J. Chloy, K. Khoo. New Applications of Differential Bounds of the SDS Structure. — 2008. — С. 17 с. — Режим доступу: <https://eprint.iacr.org/2008/395.pdf>.
3. T. Kranz, G. Leander, K. Stoffelen, F. Wiemer. Shorter Linear Straight-Line Programs for MDS Matrices. — 2017. — С. 24 с. — Режим доступу: <https://eprint.iacr.org/2017/1151.pdf>.
4. Яковлев С.В., Дідан В.В. Криптографічні властивості перетворень, лінійних відносно додавання за модулем  $2^n$  — Київ, 2016.
5. D. Kwon, J. Kim, S. Park and others. New Block Cipher: ARIA. — 2004. — С. 14 с. — Режим доступу: <http://www.math.snu.ac.kr/~jinhong/04Aria.pdf>.
6. S. Banik, A. Bogdanov, T. Isobe and others. Midori: A Block Cipher for Low Energy — 2015. — С. 29 с. — Режим доступу: <https://eprint.iacr.org/2015/1142.pdf>.
7. Massey J., Khachatrian G., Kuregian M. Nomination of SAFER+ as Candidate Algorithm for the Advanced Encryption Standard (AES). — NIST AES Proposal, 1998.