

# АЛГОРИТМИ КОДУВАННЯ ТА ДЕКОДУВАННЯ КОДІВ З НИЗЬКОЮ ЩІЛЬНІСТЮ ПЕРЕВІРОК НА ПАРНІСТЬ

Вінницький національний технічний університет

## Анотація

У даній роботі формалізовано математичний апарат кодів з низькою щільністю перевірок на парність. Наведено алгоритми кодування та ітеративного декодування.

**Ключові слова:** завадостійке кодування, блокові коди, LDPC-код, перевірна матриця, кодер, декодер, алгоритм Sum-Product.

## Abstract

In this paper the mathematical apparatus of the low-density parity-check codes has been formalized. The algorithms of coding and iterative decoding have been presented.

**Keywords:** error-correcting coding, block codes, LDPC-code, parity-check matrix, encoder, decoder, Sum-Product algorithm.

## Вступ

Коди з низькою щільністю перевірок на парність (*low-density-parity-check codes – LDPC codes*) є завадостійкими кодами, які вперше запропоновані у дисертаційній роботі Галлагера у 1962 році [1]. Але через технічні та обчислювальні обмеження їх потенціал залишився невідкритим. У 1993 році затишся у теорії завадостійкого кодування порушила поява турбо-кодів, які були розроблені Берру, Глав'є та Цітімаджімою. Впродовж наступних років проводились дослідження турбо-кодових конструкцій. У 1996 році МакКей та Ніл представили новий клас блокових кодів, які мали багато спільного з турбо-кодами [2-4]. Після детального дослідження стало зрозуміло, що ці коди є повторним відкриттям LDPC-кодів. У процесі покращення характеристик LDPC-кодів група дослідників, таких як Лабі, Міценмахер, Шокроллахі, Спілман, Річардсон та Урбанке, створила нові нерегулярні LDPC-коди [5]. Перевагою LDPC-коду є мала щільність значущих елементів перевіркової матриці та існування ефективного методу декодування з лінійною складністю від довжини кодового слова. Одним із основних недоліків LDPC-кодів, який виникає через специфічну структуру перевіркової матриці, є квадратична залежність складності кодування від довжини коду, хоча існують підходи, що дозволяють при ретельному проектуванні знизити складність кодування до лінійної. Крім того, апаратна реалізація часто буває складна: не дозволяє простої зміни кодової швидкості, довжини блоку, оскільки при цьому необхідно формувати нову перевірку матрицю [6].

**Мета** роботи полягає у формалізації та аналізі алгоритмів кодування та декодування кодів з низькою щільністю перевірок на парність.

## Результати дослідження

Розглянемо алгоритм кодування LDPC-коду:

*Крок 1.* Нехай маємо певну інформаційну послідовність  $u = (u_1, \dots, u_k)^T$  та розріджену перевірку матрицю  $H$  розміром  $m$  (кількість перевірок символів) на  $n$  (довжина кодового слова). Потрібно зробити  $H$  квазінижньотрикутною матрицею  $H_t$  [6, 7], використовуючи лише перестановки стовпчиків та рядків, для того, щоб залишити матрицю розрідженою. Для цього матриця  $H$  розкладається на 6 підматриць  $(A, B, C, D, E, T)$ , причому матриця  $T$  повинна бути нижньотрикутною матрицею, а кількість рядків матриць  $C, D$  та  $E$  формує "проміжок"  $g$  (gap), причому чим він менший, тим менша обчислювальна складність кодування (рис. 1).

$$H_t = \begin{bmatrix} A_{(m-g) \times (n-m)} & B_{(m-g) \times g} & T_{(m-g) \times (m-g)} \\ C_{g \times (n-m)} & D_{g \times g} & E_{g \times (m-g)} \end{bmatrix}. \quad (1)$$

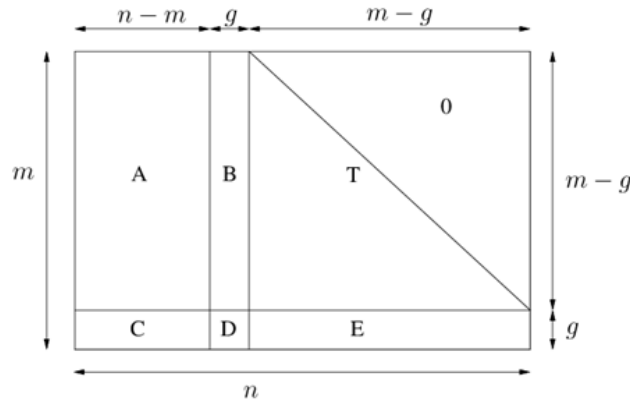


Рисунок 1 – Структура перевірконої матриці  $H_t$

Крок 2. Для того, щоб отримати кодову комбінацію необхідно занулити матрицю  $E$ . Для цього необхідно виконати наступні дії

$$H^* = \begin{bmatrix} I_{(m-g) \times (m-g)} & 0 \\ -E_{g \times (m-g)} T_{(m-g) \times (m-g)}^{-1} & I_{g \times g} \end{bmatrix} \cdot H_t = \begin{bmatrix} A_{(m-g) \times (n-m)} & B_{(m-g) \times g} & T_{(m-g) \times (m-g)} \\ C^*_{g \times (n-m)} & D^*_{g \times g} & 0 \end{bmatrix}, \quad (2)$$

де

$$C^*_{g \times (n-m)} = -E_{g \times (m-g)} \cdot T_{(m-g) \times (m-g)}^{-1} \cdot A_{(m-g) \times (n-m)} + C_{g \times (n-m)}, \quad (3)$$

$$D^*_{g \times g} = -E_{g \times (m-g)} \cdot T_{(m-g) \times (m-g)}^{-1} \cdot B_{(m-g) \times g} + D_{g \times g}. \quad (4)$$

Крок 3. Кодова комбінація  $c = (c_1, \dots, c_n)$  складається з трьох частин  $[u, p_1, p_2]$ , які представляють  $k$  інформаційних бітів,  $g$  та  $m-g$  бітів парності відповідно. Для розрахунку перевірочних бітів можна застосувати формули

$$p_1 = -D^*_{g \times g}^{-1} \cdot C^*_{g \times (n-m)} \cdot u, \quad (5)$$

$$p_2 = -T_{(m-g) \times (m-g)}^{-1} \cdot (A_{(m-g) \times (n-m)} \cdot u + B_{(m-g) \times g} \cdot p_1). \quad (6)$$

Крок 4. Для перевірки правильності отриманої кодової комбінації необхідно перевірити синдром коду

$$s = c \cdot H^{*T} = [u^T, p_1^T, p_2^T] \cdot H^{*T} = 0. \quad (7)$$

Методи декодування LDPC-кодів можна інтерпретувати як реалізацію техніки, відомої під назвою “обмінні ймовірнісні алгоритми” (*message passing algorithms – MPA*), які ґрунтуються на ітеративному декодуванні повідомлення до того моменту, коли буде отриманий необхідний результат, або процес завершиться за певним критерієм зупинки.

Розглянемо алгоритм декодування *Sum-Product*, який використовує критерій максимуму апостеріорної імовірності символу (*maximum a posteriori probability – MAP*) [6]:

Крок 1. Нехай сформоване кодове слово  $c$  передане після бінарної фазової модуляції через канал з адитивним білим гаусівським шумом. Тоді апіорні логарифмічні відношення функцій правдоподібності можна визначити за формулою

$$r_i = 4Ry_i \frac{E_b}{N_0}, \quad (8)$$

де  $r$  – повідомлення на виході з каналу;  $R$  – швидкість коду;  $y$  – повідомлення на виході модулятора;  $E_b$  – енергія сигналу на бінарний символ;  $N_0$  – енергетична спектральна щільність шуму.

Крок 2. За перевірконою матрицею будується біграф Таннера (рис. 2).

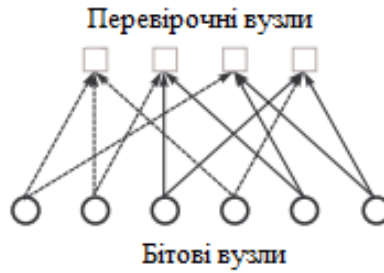


Рисунок 2 – Приклад біграфу Таннера

*Крок 3.* Виконуємо ініціалізацію значень для кожного значущого елементу (всіх одиниць) розрідженої перевірконої матриці коду, тобто

$$M_{j,i} = r_i, \quad (9)$$

де  $j$  та  $i$  – перевірочний та бітовий вузли, які з'єднано на графі Таннера.

*Крок 4.* Обчислюємо значення зовнішньої інформації з декодера за ”правилом тангенса”, тобто

$$E_{j,i} = \ln \left( \frac{1 + \prod_{v \in B_j, v \neq i} \tanh(M_{j,v}/2)}{1 - \prod_{v \in B_j, v \neq i} \tanh(M_{j,v}/2)} \right) = 2 \tanh^{-1} \left( \prod_{v \in B_j, v \neq i} \tanh(M_{j,v}/2) \right), \quad (10)$$

де  $B_j$  – множина входів до  $j$ -ого перевірконого рівняння.

Дану формулу можна апроксимувати та записати у такому вигляді

$$E_{j,i} = \left( \prod_{v \in B_j, v \neq i} \text{sign}(M_{j,v}) \right) \cdot \left( \min_{v \in B_j, v \neq i} |M_{j,v}| \right). \quad (11)$$

*Крок 5.* Загальне логарифмічне відношення функцій правдоподібності для  $i$ -ого біта буде сумою апіорних значень і значень логарифмічного відношення правдоподібності з кожного приєднаного перевірконого вузла, тобто

$$L_i = r_i + \sum_{j \in A_i} E_{j,i}, \quad (12)$$

де  $A_i$  – множина значень перевірконих вузлів, які входять до  $i$ -ого бітового вузла.

*Крок 6.* Отримуємо жорстке рішення

$$z_i = \begin{cases} 1, & L_i \leq 0; \\ 0, & L_i > 0. \end{cases} \quad (13)$$

*Крок 7.* Перевіряємо декодовану послідовність за допомогою умови (7). Якщо дана умова не виконується, то відбувається перехід до кроку 3 із використанням формули

$$M_{j,i} = r_i + \sum_{j \in A_i, j \neq j} E_{j,i}. \quad (14)$$

*Крок 8.* Процес декодування можна зупинити через певну кількість ітерацій  $I$ . Це означає, що завади із каналу зв'язку сильно вплинули на передану послідовність, і вона не може бути відновлена ідеально.

### Висновки

У роботі формалізовано та проаналізовано математичний апарат, який застосовується для кодування та декодування кодів з низькою щільністю перевірок на парність. Представлено алгоритми, які можна реалізувати у програмному забезпеченні.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Gallager R.G. Low-Density Parity-Check Codes / R.G. Gallager // IRE Transaction of Information Theory. – 1962. – 90 p.
2. Иванов Ю.Ю. О некоторых аспектах итеративной стратегии декодирования турбо-кодов: ретроспектива и ”турбо”-принцип: матер. IV международной научно-практической конференции “Информационные технологии и компьютерная инженерия” / Ю.Ю. Иванов, А.Я. Кулик. – Винница: ВНТУ, 2014. – С. 157-160.
3. Особливості оцінювання параметрів процесу передавання даних із використанням турбо-кодів / Р.Н. Квстний, Ю.Ю. Иванов, С.Г. Кривогубченко, О.В. Стукач // Метрологія та прилади. – К: ВКФ «Фавор ЛТД», 2017. – № 3 (65). – С. 25-32.
4. A Novel Suboptimal Piecewise-Linear-log-MAP Algorithm for Turbo Decoding / Yu.Yu. Ivanov, A.N. Romanyuk, A.Ia. Kulyk, O.V. Stukach // Proceedings on XI IEEE International Siberian Conference on Control and Communications. – Omsk, 2015. – DOI: 10.1109/SIBCON.2015.7147195. – P. 1-8.
5. Richardson T.J. Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes / T. J. Richardson M.A. Shokrollahi, R.L. Urbanke // IEEE Transactions on Information Theory. – 2001. – P. 619-637.
6. Johnson S.J. Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes / S.J. Johnson. – New York: Cambridge University Press, 2009. – 356 p.
7. Qi H. Low-Complexity Encoding of LDPC Codes: An New Algorithm and its Performance [Web Resource] / H. Qi, N. Goertz. – 6 p. – Access mode: [http://www.hamilton.ie/hanghang\\_qi/publications/encoding\\_07.pdf](http://www.hamilton.ie/hanghang_qi/publications/encoding_07.pdf).

**Кравчук Сергій Миколайович** — студент групи 2СІ-16б, факультет комп’ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця, e-mail: serhiikravhuk@gmail.com

**Іванов Юрій Юрійович** — канд. техн. наук, старший викладач кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: Yura881990@i.ua.

**Кривогубченко Сергій Григорович** — канд. техн. наук, доцент кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: Yura881990@i.ua.

**Kravchuk Serhii M.** — student, Faculty of Computer Control Systems and Automatics, Vinnytsia National Technical University, Vinnytsia, e-mail: serhiikravhuk@gmail.com

**Ivanov Yurii Yu.** — Cand. Sc. (Eng), Senior Lecturer, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: Yura881990@i.ua.

**Krivogubchenko Sergiy G.** — Cand. Sc. (Eng), Docent, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: Yura881990@i.ua.