https://doi.org/10.31649/1997-9266-2025-181-4-90-94

УДК 519.725 + 004.312.26

Ю. Ю. Іванов[1]
Т. В. Малоштан[1]
Є. О. Звуздецький[1]

МОДИФІКОВАНИЙ АЛГОРИТМ ДЕКОДУВАННЯ БЛОКОВИХ КОДІВ ТУРБО-ДОБУТКІВ

[1]Вінницький національний технічний університет

Забезпечення надійного передавання даних є невід'ємною вимогою до сучасних комунікаційних систем. Для виконання цієї вимоги можна використати завадостійкий код турбо-добуток, здатний ефективно працювати з невеликими інформаційними блоками на високих кодових швидкостях, але вимагаючи значних обчислювальних витрат на етапі декодування даних, що може значно навантажувати систему зв'язку, особливо в режимі реального часу та за умов обмежених ресурсів. Варто зазначити, що алгоритми декодування кодів турбо-добутків складно ефективно реалізувати на практиці. Найпоширенішим є алгоритм декодування Піндайя–Чейза, який застосовує перебір тестових кодових слів, що ставить завдання глобальної дискретної оптимізації з експоненціальною складністю. Важливо балансувати між надійністю коригування помилок і ефективним використанням обчислювальних ресурсів. Тому у статті запропоновано субоптимальну модифікацію цього алгоритму декодування, яка основана на евристичній процедурі генерації списку ймовірних кодових слів.

Ефективність роботи модифікації показана у експериментах із застосуванням комп'ютерного імітаційного моделювання системи передавання цифрових даних, враховуючи випадкові інформаційні пакети та мультимедійні дані. У ході експериментів проаналізовано частоти виникнення бітових та символьних помилок залежно від відношення сигнал/шум у каналі зв'язку. Визначено, що модифікований алгоритм незначно переважає свій оригінальний варіант за енергетичним виграшем, і, враховуючи евристичну природу перебору кодових слів, має складність меншу або, в наймалоймовірнішому випадку, таку ж, як у базового алгоритму. Стаття може бути корисною для проєктувальників комунікаційних систем, оскільки надає можливість аналізувати та синтезувати декодери кодів турбо-добутків для застосування у різних практичних задачах.

Ключові слова: *передавання даних, завадостійкий код, блоковий код турбо-добуток, евристика, декодування, експерименти.*

Вступ

Одним з найперспективніших та вагомих досягнень у теорії завадостійкого кодування за останні роки є турбо-коди, які розвиваються за двома напрямками — згорткові турбо-коди [1], [2] і блокові коди турбо-добутки (БКТД) [3], [4]. У наукових роботах [3]—[8] показано, що клас БКТД ефективно працює з невеликими кодовими блоками на дуже високих кодових швидкостях, має велику кодову відстань, переважаючи низку інших завадостійких кодів в умовах середнього рівня шуму у каналі зв'язку, також у них практично відсутній «поріг насичення» [4]. Але такі коди мають більшу за згорткові турбо-коди складність декодування [9]. На практиці їх застосовують у роботі супутникових модемів, бездротових мереж, твердотільних та жорстких дисків тощо [5].

Під час роботи з цим кодом постає актуальна задача його ефективного декодування, а відповідно і реалізації цієї ресурсомісткої процедури. Загалом існують «жорсткі» (Редді–Робінсона, інверсії біта) та «м'які» (спискові: Піндайя–Чейза, Хартмана–Назарова, Фанга–Баттайла; на графах М. Таннера — сума добутків, мінімум суми; на принципах Дж. Вольфа — максимум апостеріорної імовірності та його логарифмічна форма, алгоритм Вітербі з м'яким виходом) декодери БКТД [4], [5]. Теоретична основа, математичний апарат та їхня структура наведені у працях [3], [6]—[8], [10]. Але низку розглянутих теоретичних алгоритмів дуже складно реалізувати на практиці для БКТД, враховуючи особливості обробки даних та досягнення ними необхідних показників завадостійкості. Нині вчені акцентують увагу на ефективному алгоритмі ітеративного декодування Піндайя–Чейза

[3]—[8], який зручний для практичної реалізації, але у ході перебору тестових кодових слів постає задача глобальної дискретної оптимізації з експоненціальною складністю [4], [6].

Тому актуальною є науково-прикладна задача, суть якої полягає в тому, що необхідно модифікувати алгоритм декодування Піндайя–Чейза, досягнувши компромісу між обчислювальною складністю та ефективністю декодування даних.

Метою роботи є розробка евристичної модифікації цього алгоритму декодування БКТД, особливістю якої є скорочення списку кодових слів, що дозволяє зменшити експоненціальну складність задачі декодування без втрати ефективності передавання даних у системі зв'язку.

Результати теоретичного дослідження

Кодова структура БКТД вимагає використання ідентичних блокових кодів. Вихідні дані записуються в бінарний масив $C = (c_{11}, \ldots, c_{1n}, \ldots, c_{n1}, \ldots, c_{nn})$, який часто має квадратну форму розміром $n \times n$, але у загальному випадку можна сформувати прямокутник і, навіть, багатовимірну структуру (гіперкод) [11]. Кодування виконується за рядками та стовпчиками з використанням блокових кодів (Хеммінга, Боуза–Чоудхурі–Хоквінгема або БЧХ, Ріда–Соломона). Відповідно ітеративна процедура декодування в цьому випадку є двоетапною — горизонтальне та вертикальне декодування до виконання критерію зупинки [12].

У алгоритмі декодування Піндайя–Чейза для початку обмінного процесу необхідно у отриманій зашумленій послідовності даних $R = (r_1, r_2, \ldots, r_n)$ вибрати t позицій, які містять найменш надійні за абсолютним значенням символи r_j, та сформувати множину $P = (p_1, p_2, \ldots, p_q)$. Далі потрібно знайти всі можливі 2^t векторів помилок для відповідних до символів з множини P бітів [5], [13]. Зрозуміло, що зі збільшенням значення t кількість обчислень у декодері різко зростає. Тому замість цих дій у процедурі Д. Чейза [13] запропоновано евристичний підхід.

У модифікації враховується, що ймовірність p_j появи бінарного символу c_j для m-го конкурентного кодового слова в гаусівському каналі з дисперсією шуму σ^2 залежить від надійності r_j. Ймовірність того, що прийнятий бінарний символ y_i після жорсткого квантування буде інтерпретований як 1, якщо істинний біт $c_{ij} = 1$, записують у такому вигляді [10], [11]:

$$p_j = p\left(r_j \mid c_{ij} = 1\right) = \frac{1}{1 + \exp\left(-\dfrac{2 \cdot r_j}{\sigma^2}\right)}. \tag{1}$$

Тоді для кожного символу із множини R можна задати евристичну формулу:

$$p_{new\_j} = \begin{cases} 0, p_j \le 0{,}5 - \varepsilon, \\ 1, p_j \ge 0{,}5 + \varepsilon, \\ \dfrac{1}{1 + \exp\left(-\gamma \cdot r_j\right)}, \text{ інакше}, \end{cases} \tag{2}$$

де $\varepsilon \in (0; 0{,}5)$ — порогове значення, зменшення якого запобігає інвертуванню найменш надійних бітів, тоді як збільшення захищає тільки найнадійніші біти; $\gamma > 0$ — позитивна константа.

Далі потрібно згенерувати τ тестових векторів кодових слів (незалежно від того, є вони унікальними або ні, але повторювані шаблони варто видалити після завершення процедури) за таким імовірнісним виразом:

$$y_j = \begin{cases} 0, rand_j \ge p_{new\_j}, \\ 1, \text{інакше}, \end{cases} \tag{3}$$

де $rand_j$ — незалежне дійсне випадкове число, рівномірно розподілене на інтервалі [0; 1].

Зрозуміло, що за рахунок евристики з виразів (1)—(3) значно прискорюється перебір кодових слів у процедурі Д. Чейза, тобто складність запропонованого алгоритму буде не більшою (меншою або, в наймалоймовірнішому випадку, такою ж) за складність базового алгоритму Піндайя–Чейза [9]. Якщо $\tau \to \infty$, то будуть згенеровані всі можливі кодові слова, тобто така евристика теоретично дозволяє асимптотично наблизитись до алгоритму максимальної правдоподібності.

Подальші кроки не відрізняються від класичного варіанту. Тепер потрібно декодувати отримані

кодові слова за допомогою жорсткого декодера та отримати множину конкурентних кодових слів $Z = (z_1, z_2, \ldots, z_l)$. Для декодованих послідовностей розраховується м'яка лінійна метрика [5], [14]:

$$M_m = \sum_{j=1}^{n} r_j \left(1 - 2y_{ij}\right). \tag{4}$$

Розв'язком є найімовірніше кодове слово $z_{\min}$, тобто:

$$M = \min\left\{M_m, m = \overline{1,l}\right\}. \tag{5}$$

Для кожного біта d_j в отриманій послідовності $z_{\min}$ розраховується надійність символу за формулою Р. Піндайя [3], [7]

$$\lambda_j = \begin{cases} \frac{1}{4}\left(\min\left\{M_j, y_{ij} \neq y_{\min,j}\right\} - M_{\min}\right)\left(2y_{\min,j} - 1\right), \; y_{ij} = y_{\min,j}, \\ \beta\left(2y_{\min,j} - 1\right), \text{ інакше}, \end{cases} \tag{6}$$

де $\beta = \left[0,2;\ 0,4;\ 0,6;\ 0,8;\ 1,0;\ 1,0;\ 1,0;\ 1,0;\ldots\right]$ — заданий числовий масив [3], [7].

Застосувавши елементарний декодер за знаком, можна знайти інформаційну послідовність:

$$c'_j = \begin{cases} 1, \; \lambda_j > 0, \\ 0, \text{ інакше}. \end{cases} \tag{7}$$

Значення зовнішньої інформації E з декодера для кожного біта d_j розраховується за виразом

$$E_j = \lambda_j - r_j. \tag{8}$$

Перехід до $(I + 1)$-ї ітерації (оновлення інформації) відбувається з використанням рівняння

$$r_j^{(I+1)} = r_j^{(I)} + \alpha^{(I+1)} \cdot E_j^{(I)}, \tag{9}$$

де $\alpha = [0,0;\ 0,2;\ 0,3;\ 0,5;\ 0,7;\ 0,9;\ 1,0;\ 1,0;\ldots]$ — масив множників для зменшення впливу зовнішньої інформації з декодера [3], [7].

Алгоритм повторюється для всіх рядків, далі потрібно виконати декодування стовпців, використавши множину значень надійності $\Omega = (\lambda_{11}, \ldots, \lambda_{1n}, \ldots, \lambda_{n1}, \ldots, \lambda_{nn})$, отриману після декодування рядків. Такий алгоритм застосовується для всієї кодової структури впродовж N ітерацій декодування. Закінчення процесу відбувається із застосуванням заданого критерію зупинки (кількість ітерацій, стабілізація обчислень, час роботи).

Експериментальне дослідження

Для тестування ефективності модифікації застосовано імітаційне моделювання системи передавання даних [15]. Параметри експериментів: генератор псевдовипадкових послідовностей символів; код турбо-добуток $(n, k)^2$ із квадратною кодовою структурою розміром $n \times n$ (n кодових та k інформаційних символів); 2-компонентні БЧХ-кодери з параметрами (127, 106), (127, 64), декодер Берлекемпа–Мессі; базовий і модифікований алгоритми Піндайя–Чейза; кількість ітерацій декодування $N = 10$; двійкова фазова маніпуляція; канал з адитивним білим гаусівським шумом; показник сигнал/шум $E_b/N_0 = \{4{,}0;\ 4{,}5;\ 5{,}0\}$ дБ; критерії закінчення — час (до 3 годин на крок) і кількість пошкоджених кадрів (не менше $q = 15$). Визначено, що хороші результати можна отримати, задавши для модифікованого алгоритму параметри $\varepsilon = 0{,}435$, $\gamma = 5{,}875$, $\tau = 1000$. Оцінками ефективності вибрано частоту виникнення помилок у пакетах даних (FER) і кількість декодувань за алгоритмом Берлекемпа—Мессі (Δ_{av}) [5], [11]. Для модифікованого алгоритму значення Δ_{av} залежить від середньої кількості тестових шаблонів τ, а для базового алгоритму — найменш надійних символів t. Результати подані у табл. 1.

Таблиця 1

Статистика процесу передавання даних

–	Базовий алгоритм		Модифікація	
E_b/N_0	FER	Δ_{av}	FER	Δ_{av}
4,0	$8{,}431 \cdot 10^{-4}$	512	$6{,}856 \cdot 10^{-4}$	434
4,5	$1{,}862 \cdot 10^{-4}$	256	$1{,}016 \cdot 10^{-4}$	232
5,0	$2{,}865 \cdot 10^{-5}$	128	$2{,}432 \cdot 10^{-5}$	105
$(127, 64)^2$				
4,0	$8{,}041 \cdot 10^{-4}$	1024	$5{,}123 \cdot 10^{-4}$	957
4,5	$1{,}011 \cdot 10^{-5}$	1024	$1{,}754 \cdot 10^{-6}$	832
5,0	$3{,}162 \cdot 10^{-6}$	1024	$1{,}132 \cdot 10^{-6}$	762

Таким чином, модифікація переважає базовий алгоритм, маючи менші складність декодування

та кількість пошкоджених пакетів даних, що пов'язано з аналізом більшого різноманіття тестових кодових слів. Результати моделювання показують, що зі збільшенням значення E_b/N_0 зменшується кількість декодувань за алгоритмом Берлекемпа–Мессі, а зі зменшенням значення t кількості декодувань Δ_{av} поступово зрівнюються, найгіршого випадку $\Delta_{av} = 2^t$ не отримано.

Далі протестуємо роботу модифікованого турбо-декодера на мультимедійних даних. Модель експерименту практично повторює попередню, але задано кольорове зображення "barcelona.jpg" (768 кадрів, 2048 бітів у пакеті), БЧХ-код з параметрами (127, 64) та фіксований показник сигнал/шум E_b/N_0 = 5,0 *дБ*. Результати показано на рис. 2 (у верхньому лівому куті вказано кількість ітерацій декодування N), а криві частот бітових (BER) та символьних помилок (SER) показані на рис. 3.

Рис. 2. Результати передачі зображення

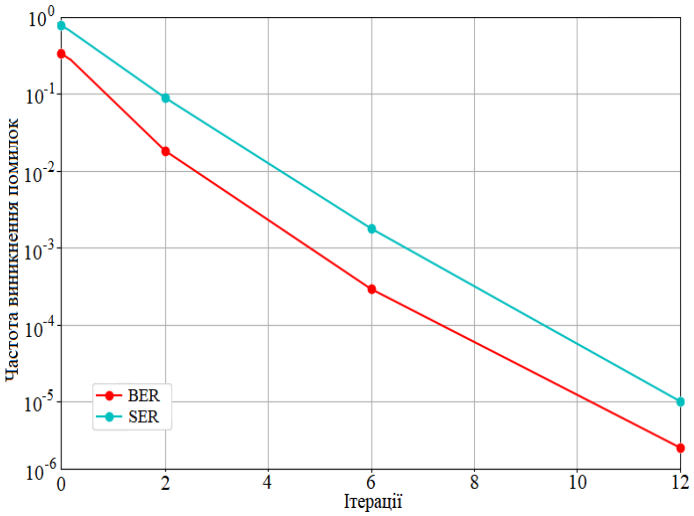

Рис. 3. Залежність частот виникнення помилок від кількості ітерацій декодування

Таким чином, зі збільшенням кількості ітерацій декодування підвищується якість зображення (зменшується кількість помилок у бітах та символах), а це свідчить про те, що модифікація дозволяє досягти хорошої коригувальної здатності за заданих умов.

Висновки

У роботі запропоновано евристичну модифікацію алгоритму декодування Піндайя–Чейза для БКТД, яка спрощує відбір конкурентних кодових слів у ході роботи турбо-декодера. Після проведеного моделювання визначено, що удосконалений алгоритм дещо переважає базовий варіант за енергетичною ефективністю та має меншу обчислювальну складність. З недоліків модифікації варто зазначити евристичну природу перебору тестових кодових слів, що створює задачу метаоптимізації параметрів алгоритму. Результати роботи можуть бути корисними у ході розробки турбо-декодерів, враховуючи вимоги, які висуваються до системи передавання даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes," *Proceedings of ICC*, pp. 1064-1070, 1993. https://doi.org/10.1109/ICC.1993.397441 .

[2] F. L. Morgos, A.-M. Cuc, and C. Grava, "Performance Analysis of Turbo Codes, LDPC Codes, and Polar Codes over an AWGN Channel in the Presence of Inter Symbol Interference," *Sensors*, 19 p., 2023. https://doi.org/10.3390/s23041942 .

[3] R. M. Pyndiah, "Near-Optimum Decoding of Product Codes: Block Turbo Codes," *IEEE Transactions on Communications*, pp. 1003-1010, 1998. https://doi.org/10.1109/26.705396 .

[4] A. Dweik, H. Mukhtar, and A. Shami, "Turbo Product Codes: Applications, Challenges, and Future Directions," *IEEE Communications Surveys & Tutorials*, pp. 3052-3068, 2016. https://doi.org/10.1109/COMST.2016.2587863 .

[5] C. Douillard, et al, *Codes and Turbo Codes*, 2010, 424 p.

[6] K. Suman, "Optimization of Heuristic Algorithms for Improving BER of Adaptive Turbo Codes," *International Journal of Advanced Research in Engineering and Technology*, pp. 414-421, 2019. https://doi.org/10.34218/IJARET.10.2.2019.040 .

[7] A. Al-Dweik, S. Le Goff, and B. Sharif, "A Hybrid Decoder for Block Turbo Codes," *IEEE Transactions on Communications*, pp. 1229-1232, 2009. https://doi.org/10.1109/TCOMM.2009.05.070107.

[8] J. H. Kishore, B. Yamuna, and K. Balasubramanian, "Design of a Fast Chase Algorithm based High Speed Turbo Product Code Decoder," *Proceedings of the International Conference on Advances in Computing and Communications*, pp. 1-5, 2022. https://doi.org/10.1109/ICACC-202152719.2021.9708201 .

[9] Ю. Ю. Іванов, Б. О. Боднаренко, Є. О. Звуздецький, і Ю. С. Здітовецький, «Оцінювання складності декодування згорткових турбо-кодів та блокових кодів турбо-добутків,” *Вісник Вінницького політехнічного інституту*, № 1, с. 51-55, 2024. https://doi.org/10.31649/1997-9266-2024-172-1-51-55 .

[10] C. Leroux, S. Hemati, Sh. Mannor, and W. J. Gross, “Stochastic Chase Decoding of Reed-Solomon Codes,” *IEEE Communications Letters*, pp. 863-865, 2010. https://doi.org/10.1109/LCOMM.2010.09.100594 .

[11] J. Justesen, and T. Hoholdt, *A Course in Error-Correcting Codes*, 2017, 226 p.

[12] Yu. Yu. Ivanov, and Ye. O. Zvuzdetskii, “Features of Decoding Block Turbo-Product Codes,” *Міжнародна науково-технічна конференція MiningMetalTech*, 2023, с. 238-240.

[13] D. Chase, “Class of Algorithms for Decoding Block Codes with Channel Measurement Information,” *IEEE Transactions on Information Theory*, pp. 170-182, 1972. https://doi.org/10.1109/TIT.1972.1054746 .

[14] Ye. O. Zvuzdetskyi, and Yu. Yu. Ivanov, “List Decoding of Block Turbo-Products-Codes,” *Proceedings of the 8th International Scientific and Practical Conference “Scientific research in the modern world*,” 2023, pp. 199-201.

[15] Yu. Yu. Ivanov, and V. V. Kovtun, “Crypto Coding System Based on the Turbo Codes with Secret Keys,” *ICT Express*, South Korea, 2024, pp. 330-335. https://doi.org/10.1016/j.icte.2023.08.007 .

Рекомендована кафедрою автоматизації та інтелектуальних інформаційних технологій ВНТУ

Стаття надійшла до редакції 29.05.2025

Іванов Юрій Юрійович — канд. техн. наук, доцент, доцент кафедри автоматизації та інтелектуальних інформаційних технологій, e-mail: Yura881990@i.ua ;

Малоштан Тимофій Вікторович — аспірант кафедри автоматизації та інтелектуальних інформаційних технологій, e-mail: tim.maloshtan@gmail.com ;

Звуздецький Єгор Олегович — аспірант кафедри автоматизації та інтелектуальних інформаційних технологій, e-mail: egorzvuzdetskyi@gmail.com .

Вінницький національний технічний університет, Вінниця

Yu. Yu. Ivanov[1]
T. V. Maloshtan[1]
Ye. O. Zvuzdetskyi[1]

Modified Algorithm for Decoding Block Turbo-Product Codes

[1]Vinnytsia National Technical University

Ensuring reliable data transmission is an essential requirement for modern communication systems. To implement it, an error-correcting turbo-product code can be used, which can work effectively with small information blocks at high code rates, but requires significant computational costs at the data decoding stage, which can significantly load the communication system, especially in real-time mode and under conditions of limited resources. It should be noted that turbo-product code decoding algorithms are difficult to implement effectively*. The most common is the Pyndiah–Chase decoding algorithm, which uses a brute force of test codewords, which poses a global discrete optimization task with exponential complexity. It is important to balance the reliability of error correction and the efficient use of computational resources. Therefore, in this article developed a suboptimal modification of this decoding algorithm, which is based on a heuristic procedure for generating a list of probable codewords.*

The effectiveness of the modification is shown in experiments using computer simulation of a digital data transmission system, taking into account random information packets and multimedia data. During the experiments, the bit and symbol error rates were analyzed depending on the signal-to-noise ratio in the communication channel. It is determined that the modified algorithm is slightly outperforms its original version in terms of energy gain, and, taking into account the heuristic nature of codeword brute force, has a complexity lower or, in the most unlikely case, the same as that of the basic algorithm. The article can be useful for communication system designers, since it provides an opportunity to analyze and synthesize turbo-product code decoders for use in different practical tasks.

Keywords: data transmission, error-correcting code, block turbo-product code, heuristics, decoding, experiments.

Ivanov Yurii Yu. — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Automation and Intellectual Information Technologies, e-mail: Yura881990@i.ua ;

Maloshtan Tymofii V. — Post-Graduate Student of the Chair of Automation and Intellectual Information Technologies, e-mail: tim.maloshtan@gmail.com ;

Zvuzdetskyi Yehor O. — Post-Graduate Student of the Chair of Automation and Intellectual Information Technologies, e-mail: egorzvuzdetskyi@gmail.com