

ДЕЯКІ АСПЕКТИ ЗАВАДОСТІЙКОГО КОДУВАННЯ ТА ДЕКОДУВАННЯ LDPC-КОДІВ

Вінницький національний технічний університет

Анотація

У даній роботі проаналізовано певні особливості LDPC-кодів та представлено загальні методи, які допомагають розв'язати задачу їхнього кодування та декодування в системах передавання даних різного функціонального призначення.

Ключові слова: завадостійке кодування, ітеративне декодування, LDPC-код, обмінні ймовірнісні методи, синдром коду.

Abstract

In this paper some features of the LDPC codes are analyzed and general methods, that help to solve the problem of encoding and decoding this code in data transmission systems of various functional purposes, are presented.

Keywords: error-correcting coding, iterative decoding, LDPC-code, message passing methods, code syndrome.

Вступ

У 1948 р. американський інженер К. Шеннон опублікував фундаментальну роботу [1], в якій запропонував метод об'єктивного вимірювання кількості інформації, а також сформулював математичні принципи передавання даних. Для підвищення вірогідності переданих даних він запропонував застосовувати *завадостійке кодування* (error-correcting coding), подальший розвиток якого пов'язаний з роботами багатьох науковців. З моменту створення основ передавання даних розроблено велику кількість завадостійких кодів, і до теперішнього часу дослідження в цьому напрямі інтенсивно розвиваються. В сучасних цифрових системах зв'язку використовується завадостійке кодування, яке дозволяє, на відміну від криптографічного шифрування й ущільнення даних, ефективно боротися з помилками в каналі, забезпечуючи надійність і вірогідність переданих даних (кращі показники коефіцієнта бітових помилок), а також енергетичний вигаш [2-5].

Одним із найбільш поширених та ефективних методів декодування є LDPC-код (Low-Density Parity-Check code – код з малою щільністю перевірок на парність) або код R. G. Gallager [6]. Даний код представляє собою особливий випадок лінійного блокового коду з перевіркою парності. Перевагою LDPC-коду є мала щільність значущих елементів перевіркової матриці та існування ефективного методу декодування з лінійною складністю від довжини кодового слова. Один з основних недоліків LDPC-кодів, який виникає через специфічну структуру перевіркової матриці, є квадратична залежність складності кодування від довжини коду, хоча існують підходи, які 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 перевірочну матрицю коду [4, 6]. Але дані коди є надзвичайно ефективними [7].

Мета роботи полягає в аналізі структури LDPC-коду та огляді методів, які допомагають розв'язати екстремальну задачу їхнього декодування в системах передавання даних.

Результати дослідження

Описати структуру LDPC-коду можна декількома способами: *перевірочною матрицею, біграфом* M. Tanner, *спеціальними способами*. Зазвичай LDPC-коди описуються за допомогою перевіркової матриці, яка містить переважно більшість нулів та малу кількість одиниць. Для формування перевіркової матриці використовують два методи: генерація початкової матриці з

використанням псевдовипадкового генератора (випадкові коди); застосування методів, які засновані на групах і кінцевих полях (структуровані коди) [4, 8-10].

Алгоритм кодування [9]. Введемо вектор $u = [u_1, u_2, \dots, u_k]$, який містить біти переданого повідомлення. Тоді кодове слово c , яке буде відповідати бінарному повідомленню u , можна знайти за допомогою виразу

$$c = u \cdot G, \quad (1)$$

де $G = [I_k, A^T]$ – породжуюча матриця коду розмірності $k \cdot n$; I – одинична матриця розмірності k ; A – матриця розмірності $(n-k) \cdot k$; T – операція транспонування матриці.

Перевірочну матрицю коду H можна записати у такій формі

$$H = [A, I_{n-k}], \quad (2)$$

де I – одинична матриця розмірності $(n-k)$.

Простір рядків G ортогональний H , тобто виконується умова ортогональності

$$G \cdot H^T = 0. \quad (3)$$

Декодування LDPC-кодів зводиться до розв'язання задачі глобальної оптимізації, а саме задачі цілочисельного програмування, та полягає у пошуку максимального значення цільової функції, яка характеризується нелінійністю, багатоекстремальністю та високою розмірністю простору пошуку. Методи декодування LDPC-кодів можна інтерпретувати як реалізацію техніки, відомої як *обмінні ймовірнісні методи* (message passing methods), які ґрунтуються на ітеративному декодуванні повідомлення до того моменту, коли буде отриманий необхідний результат, або процес завершиться за певним критерієм зупинки [11, 12]. Прикладом є *метод оцінювання символів з розповсюдженням довіри* (belief propagation), який розроблений J. Pearl у 1982 р. для роботи з імовірнісними моделями на графах. Модифікований метод для оптимального м'якого посимвольного декодування LDPC-кодів має назву *Sum-Product*, а його субоптимальна модифікація – *Min-Sum*. Вони використовують алгебру логарифма відношення функцій правдоподібності, в якій операції виконуються над кінцевим полем $GF(2)$. Для оптимального декодування послідовності символів застосовують також *методу D. Chase* в евклідовому просторі. У деяких випадках можна застосувати жорстке посимвольне декодування, наприклад *метод інверсії бінарного символу* (bit-flipping) [4, 9].

Алгоритм декодування [9]. Нехай кодове слово c було відправлене в канал із шумами, а в процесі передавання один або більше біт були інвертовані. Кожне кодове слово для LDPC-коду повинно формувати нульовий *синдром S* за наступною формулою

$$S = H \cdot c^T = 0, \quad (4)$$

$$S = H \cdot y^T = 0, \quad (5)$$

де y – отримане повідомлення після проходження каналу з шумами.

Синдром вказує на те, які перевіірочні вирази не задовольняють отримане кодове слово. Відповідно помилки можуть бути виявлені, якщо для кодового слова не виконується умова (5).

Приклад. Припустимо, що кодове слово $c = [1 \ 0 \ 1 \ 1 \ 1 \ 0]$ передається через канал із шумами, перевіірочна матриця коду H відома. В результаті був отриманий зашумлений бінарний вектор $y = [1 \ 0 \ 1 \ 0 \ 1 \ 0]$. Підстановка даних у вираз (5) дає можливість виконати наступні дії

$$S = H \cdot y^T = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \cdot (1 \ 0 \ 1 \ 0 \ 1 \ 0)^T = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Результат не дорівнює нулю, тому вектор y не є кодовим словом. З цього можна зробити висновок, що сталася бітова помилка під час передавання даних.

Висновки

У даній роботі проаналізовано структурні особливості LDPC-коду та представлено загальні методи, які допомагають розв'язати задачу їхнього кодування та декодування. Завдяки високій ефективності LDPC-коди знайшли своє місце в системах цифрового зв'язку різного функціонального призначення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Shannon C.E. A Mathematical Theory of Communication / C.E. Shannon // Reprinted from The Bell System Technical Journal. – 1948. – V. 27. – P. 379-423, 623-656.
2. Иванов Ю.Ю. Вступ до Computer Science. Дискретна математика цікава та не дуже: лекції, алгоритми та задачі / Ю.Ю. Иванов. – 2018. – 89 с. – Режим доступу: https://iq.vntu.edu.ua/method/read_url.php?tbl_num=2&url=/fdb/1166/Discrete_Math_by_IVANOV.djvu.
3. 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, 28-30 мая, 2014 г. – С. 157-160.
4. Івчук Н.В. Особливості завадостійкого кодування коду з низькою щільністю перевірок на парність у цифрових системах зв'язку: матер. IV міжнародної наукової конференції «Вимірювання, контроль та діагностика в технічних системах» / Н.В. Івчук, Ю.Ю. Иванов. – Вінниця: ПП «ТД Едельвейс і К», 31 жовтня – 2 листопада, 2017 р. – С. 251.
5. Иванов Ю.Ю. Експериментальне дослідження завадостійкості турбо-кодів: числові оцінки та імітаційне моделювання нового субоптимального алгоритму PL-log-MAP / Ю. Ю. Иванов // Вісник Вінницького політехнічного інституту. – Вінниця: ВНТУ, 2016. – № 5. – С. 76-84.
6. Gallager R.G. Low-density Parity Check-Codes / R.G. Gallager // IRE Transaction Info.Theory, IT- 8, 21-28, January. – 1962. – 90 p.
7. On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit / Chung S.-Y., G. D. Forney, T. J. Richardson, R. Urbanke // IEEE Communications Letters. – 2001. – P. 58-60.
8. Зубарев Ю.Б. Помехоустойчивое кодирование в цифровых системах передачи данных / Ю.Б. Зубарев, Г.В. Овечкин. – Р: РГРТУ, 2008. – 16 с.
9. 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.
10. Hanzo L. Turbo Coding, Turbo Equalisation and Space-Time Coding for Transmission over Wireless Channels / L. Hanzo, T.H. Liew, B.L. Yeap. – Southampton: Department of Electronics and Computer Science of UK, 2002. – 746 p.
11. Morelos-Zaragoza R. The Art of Error Correction Coding / R. Morelos-Zaragoza. – Chippenham: John Wiley & Sons, 2006. – P. 143-168.
12. Codes and Turbo Codes: edited by C. Berrou / C. Douillard, M. Jezequel, G. Battail and others. – Paris: Springer, 2010. – 424 p.

Кисляченко Максим Миколайович — студент групи I-156, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, м. Вінниця.

Іванов Юрій Юрійович — канд. техн. наук, асистент кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця, e-mail: Yura881990@i.ua.

Науковий керівник: **Іванов Юрій Юрійович** — канд. техн. наук, асистент кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця.

Kislyachenko Maxim M. — student, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia.

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

Supervisor: **Ivanov Yurii Yu.** — Cand. Sc. (Eng), Assistant Professor, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia.