

УДК 681.391

DOI: 10.31891/2219-9365-2020-66-2-5

ПЯТИН І. С., МІШАН В. В., РЕЗНИЧУК Р. В.
Хмельницький національний університет

МЕТОДИ ГЕНЕРАЦІЇ ПЕРЕВІРОЧНИХ МАТРИЦЬ LDPC КОДУ

LDPC коди - це лінійні блокові коди, де перевірочні біти додаються в кінець інформаційного повідомлення. Стаття присвячена проблемі побудови перевірочних матриць коду з низькою щільністю перевірок на парність для заданих характеристик швидкості і довжини коду. Розглянуто метод генерації перевірочних матриць на основі випадкової перестановочної підматриці (квазіциклічне регулярне кодування), і структурований метод генерації матриці на основі евклідово-геометричного коду з можливістю видалення рядків і розподілу стовпців. Виконано моделювання кодів.

Ключові слова: коди LDPC, перевірочна матриця, квазіциклічний LDPC код.

PYATIN I., MISHAN V., REZNICHUCK R.
Khmelnitskyi National University

METHODS OF GENERATION OF LDPC CODE VERIFICATION MATRIXES

LDPC codes are linear block codes, where check bits are added to the end of the information message. The coding procedure is the multiplication of the information message vector of length K by the generating matrix G . The generating matrix is associated with the parity check matrix. The parity check matrix has $(N-K)$ rows and N columns, where N corresponds to the required length of the codeword, K corresponds to the length of the message. The article is devoted to the problem of construction of code verification matrices with low density of parity checks for given characteristics of code speed and length. A method for generating test matrices based on a random permutation submatrix, known as quasicyclic regular coding, and a structured method for generating a matrix based on a Euclidean geometric code with the ability to delete rows and distribute columns are considered. An important characteristic of the LDPC code matrix is the absence of cycles of a certain size. Under the cycle of length 4 means the formation in the test matrix of a rectangle in the corners of which are units. The absence of a cycle of length 4 can also be determined by the scalar product of the columns (or rows) of the matrix. If each pairwise scalar product of all columns (or rows) of the matrix is not more than 1, this indicates the absence of a cycle of length 4. Cycles of greater length (6, 8, 10, etc.) can be determined by constructing a graph in the test matrix, vertices of which there are units, and the edges are all possible connections of vertices parallel to the sides of the matrix (ie vertical or horizontal lines). The minimum cycle in this graph will be the minimum cycle in the LDPC code check matrix. Code simulation performed.

Keywords: LDPC codes, verification matrix, QC-LDPC code, permutation matrix.

Вступ. Проблема побудови, адаптації та модифікації відомих кодів є актуальним завданням в області телекомунікацій. Висока продуктивність і коригувальна здатність, що отримується при ітеративному декодуванні турбокодів, стимулювали активні дослідження щодо застосування даного методу до декодування інших видів кодів. Зокрема, виявилось, що можливо отримати на порядок кращі характеристики при використанні кодів низької щільності (low density parity check – LDPC). Коди LDPC сьогодні все ширше застосовуються на практиці: їх використовують стандарти DVB-T2, DVB-S2, DVB-C2, WiFi, WiMax, IEEE 802.15.3. Також передбачено передавання даних користувача транспортного каналу за допомогою кодів LDPC у системах зв'язку 5G. Коди LDPC пропонують кращу спектральну ефективність ніж турбо-коди, і підтримують високу пропускну здатність [1].

Одним із завдань, пов'язаних з побудовою кодів низької щільності, є генерація перевірочних матриць із заданими властивостями. LDPC код задається перевірочною матрицею H , що має властивість розрідженої, тобто її рядки і стовпці містять малу кількість ненульових елементів в порівнянні з розмірністю матриці. Перевірочна H і генераторна G матриці повинні задовольняти наступній умові:

$$GH^T = 0.$$

Кодування послідовності (m_1, m_2, \dots, m_k) полягає в отриманні кодової послідовності (c_1, c_2, \dots, c_n) :

$$C = (m_1, m_2, \dots, m_k)G = (c_1, c_2, \dots, c_n)$$

за умови, що:

$$H(c_1, c_2, \dots, c_n)^T = 0.$$

Перевірочна матриця LDPC-коду. Використовуються два принципи побудови перевірочних матриць. Перший заснований на генерації початкової перевірочної матриці за допомогою псевдовипадкового генератора. Коди, отримані таким методом, називають випадковими (random-like codes). Основні недоліки випадкових кодів – необхідність застосування алгоритмів видалення коротких циклів і нестабільні робочі характеристики коду. Другий базується на використанні спеціальних структурованих методів, заснованих на групах, кінцевих полях, тощо. Краще виправлення помилок забезпечують випадкові

LDPC-коди. Структуровані методи дозволяють використовувати оптимізацію процедур зберігання, кодування і декодування, а також отримувати коди з більш передбачуваними і стійкими характеристиками.

Галлагером була запропонована наступна структура перевірконої матриці H з параметрами (n, λ, ρ) , де n – кількість стовпців матриці, яка має λ одиниць в кожному стовпці і ρ одиниць в кожному рядку (інші нулі). Приклад матриці для (20, 3, 4) LDPC-коду представлений виразом:

[illegible]

Як видно, структурно вона складається з трьох підматриць, в кожній з яких міститься тільки одна одиниця в стовпці: в H_1 кожний i -й рядок містить одиниці в стовпці від $(i-1)k+1$ до ik ; H_2 і H_3 отримані шляхом випадкової перестановки стовпців матриці H_1 . Всі рядки і стовпці матриці H мають однакові ваги, що робить код регулярним.

Оскільки використовувалася випадкова перестановка і немає чітко визначеного правила, то в подальшому необхідно проведення комп'ютерного пошуку для вибору з потенційної множини кодів з найкращими характеристиками. Більш універсальним є структурований метод побудови коду на основі евклідово-геометричних кодів $EG(m, 2^k)$ [2]. Даний метод дозволяє наблизитися до границі Шеннона при BER (Bit Error Rate), що дорівнює 10^{-4} .

Евклідово-геометричні коди будуються як система кодів $EG(m, p^s)$. Код має наступні характеристики: довжина кодового слова – $n = 2^{2s} - 1$; довжина інформаційного повідомлення – $k = 2^{2s} - 3^s$; кількість надлишкових біт – $n - k = 3^s - 1$; мінімальна відстань – $d_{\min} = 2^s + 1$. Оскільки число одиниць в перевіірчій матриці евклідово-геометричного коду мало в порівнянні з розміром матриці, то такий код можна розглядати як LDPC-код. Перевіірча матриця H_{EG} будується наступним чином: рядки перевіірчої матриці відповідають лініям евклідової геометрії, стовпці – ненульовим точкам в $EG(m, p^s)$. Елементи матриці H_{EG} визначаються з векторів геометрії Евкліда:

$$H_{EG}(i, j) = \begin{cases} 1, & \text{якщо точка на прямій } i, \\ 0, & \text{в іншому випадку.} \end{cases}$$

Якщо ввести позначення $q = p^s$, то матриця H_{EG} має $n = q^m$ стовпців і $r = q^{m-1}(q^m - 1)/(q - 1)$ рядків. Кожен стовпець матриці містить $\lambda = q^{m-1}(q^m - 1)/(q - 1)$ одиниць, кожен рядок містить $\rho = p^s$ одиниць. Наприклад, евклідово-геометричний код $EG(2, 2^2)$ буде мати перевіірочну матрицю, що відповідає структурі регулярного коду LDPC (15, 4, 4). Нерегулярні LDPC-коди (ваги стовпців і рядків описуються за допомогою функцій $\lambda(i)$ і $\rho(i)$, які задають частку стовпців і рядків з вагою i) мають кращі характеристики, ніж регулярні.

Розглянемо метод побудови LDPC-кодів, в основі якого лежить властивість – будь-який циклічний зсув кодового слова є також кодове слово. Такий блоковий код називається квазіциклічним (QC-LDPC) [3].

Перевірочна матриця коду являє собою поєднання $H = [H_1, H_2, \dots, H_p]$ циклічних матриць:

$$H_{QC} = \begin{bmatrix} P_{a1,1} & P_{a1,2} & \dots & P_{a1,c-1} & P_{a1,c} \\ P_{a2,1} & P_{a2,2} & \dots & P_{a2,c-1} & P_{a2,c} \\ \dots & \dots & \dots & \dots & \dots \\ P_{am,1} & P_{am,2} & \dots & P_{am,c-1} & P_{am,c} \end{bmatrix},$$

де $a_{j,k}$ являє собою циклічний зсув стовпців матриці на i розрядів. Таким чином, P_j – перестановочна матриця розміром $L \times L$, яка утворюється в результаті циклічного зсуву стовпців на i позицій. У реальних системах L вибирається досить великим, наприклад, $L = 101$. Вибір одиничної матриці в якості P_0 не є обов'язковим, наприклад, для $L = 5P_0$, одинична матриця може бути наступною:

$$P_0 = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ 1 & & & & 1 \\ & 1 & & 1 & \\ & & 1 & & 1 \end{bmatrix}$$

Генерація перевірконої матриці. У загальному випадку циклічна матриця описується асоційованим поліномом:

$$p_i(x) = \sum_{j=0}^{L-1} (P_i)_{oj} x^j$$

Перший спосіб генерації перевірконої матриці квазіциклічного LDPC-коду заснований на випадковому розподілі перестановочних матриць із заданим розподілом $p(x)$ і $\lambda(x)$ (залежно від їх вибору можуть бути побудовані регулярні і нерегулярні коди). Якщо $L = 47$, $m = 6$, $j = 12$, то загальний розмір матриці QC-LDPC коду H буде $L_m \times L_j$ або 250×450 . Приклад структури перевірконої матриці показаний на рис. 1.

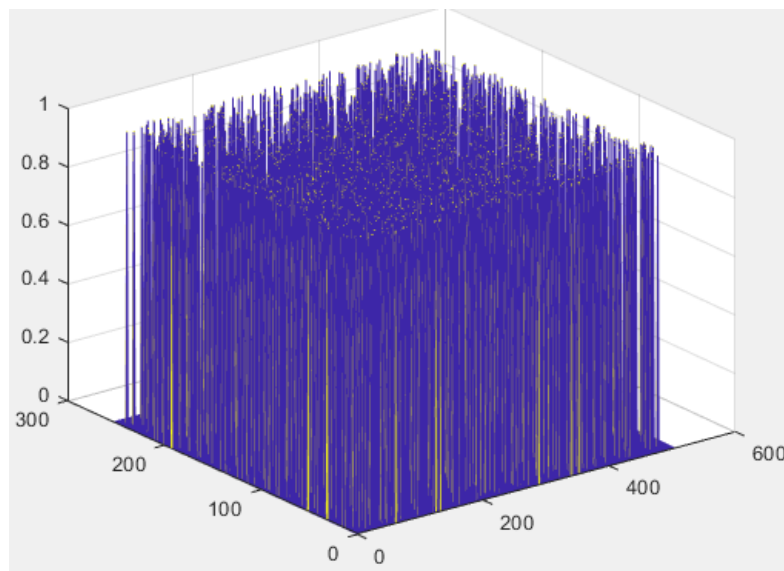


Рис. 1. Приклад будови перевірконої матриці QC-LDPC коду

Другий спосіб отримання перевірконої матриці заснований на виборі двох чисел a і b , що належать ненульовим елементам поля Галуа $GF(L)$, де L – просте число. Тоді заповнення матриці H розміром $L_m \times L_j$ – розстановка перестановочних матриць.

Отримуємо регулярний квазіциклічний LDPC-код з $\lambda = m - 1$, $\sigma = j - 1$ і швидкістю $r \geq 1 - (m/j)$. Для даної матриці довжина найкоротшого циклу буде 8 (що значно більше, ніж у LDPC-кодів, побудованих на

основі евклідово-геометричних кодів). Велика величина довжини циклу дозволяє ефективно використовувати декодування з поширенням довіри.

Декодування кодів LDPC. Алгоритм декодування LDPC кодів базується на логарифмічному відношенні правдоподібності (log-likelihood ratio – LLR), що визначається виразом:

$$LLR(x|y) = \ln \left[\frac{p(y|x=0)}{p(y|x=1)} \right]$$

Припустимо, $x = [x_1, x_2, \dots, x_n]$ позначає кодове слово, яке модулюється при використанні двійкової фазової модуляції, і модульовані значення x передаються по каналу з адитивним білим гаусовим шумом (АБГШ). Припустимо $y = [y_1, y_2, \dots, y_n]$ позначає вхідну послідовність прийнятих сигналів (символів). Демодулятор приймає вхідну послідовність сигналів і обчислює відповідні LLR значення для: $j = 1, 2, \dots, n$.

$$\lambda_j = LLR(y_j|x_j) = \ln \left[\frac{p(y_j|x_j=0)}{p(y_j|x_j=1)} \right].$$

При двійковій біполярній передачі по каналу LLR значення обчислюються за допомогою виразу:

$$\lambda_j = \frac{2}{\sigma^2} \cdot y_j,$$

де σ^2 – дисперсія шуму у каналі зв'язку.

На рис. 2 показана залежність ймовірності помилки на біт (BER) від відношення сигнал/шум (E_b/N_0) для системи зв'язку з LDPC-кодом та модуляцією.

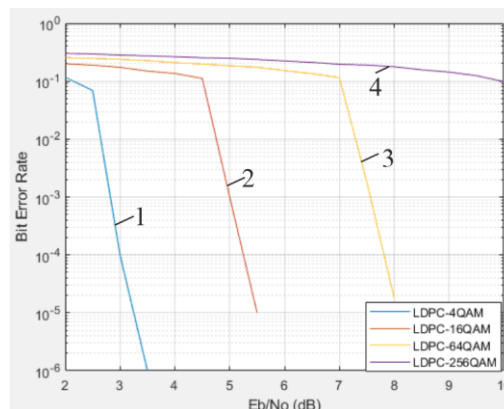


Рис. 2. Залежність ймовірності помилки на біт (BER) від відношення сигнал/шум (E_b/N_0) для системи зв'язку з LDPC кодом та модуляцією (1 – QPSK; 2 – 16QAM; 3 – 64-QAM; 4 – 256QAM)

З аналізу отриманої залежності можна зробити висновок, що найбільшу енергетичну ефективність забезпечує використання LDPC коду з модуляцією QPSK. Модуляція QPSK на 2 дБ ефективніше модуляції 16QAM і на 5 дБ ефективніше модуляції 64QAM.

Висновки. За результатами синтезу коди з перевірочними квазіциклічними матрицями низької щільності, отриманими на основі випадкових перестановок, мають вищу продуктивність, ніж коди з матрицями на основі структурованих евклідово-геометричних кодів при однаковій швидкості коду (0,5), при однаковій кількості перевірочних і інформаційних розрядів (283, 564). Однак коригувальна здатність кодів на основі квазіциклічних матриць нестабільна і змінюється в діапазоні від 10^{-3} до 10^{-5} (SNR = 6 дБ).

Література

1. H. Li, B. Bai, X. Mu, J. Zhang and H. Xu, "Algebra-Assisted Construction of Quasi-Cyclic LDPC Codes for 5G New Radio," in IEEE Access, vol. 6, pp. 50229-50244, 2018, doi: 10.1109/ACCESS.2018.2868963.
2. S. K. Chilappagari, D. V. Nguyen, B. Vasic and M. W. Marcellin, "Girth of the Tanner graph and error correction capability of LDPC codes," 2008 46th Annual Allerton Conference on Communication, Control, and Computing, Urbana-Champaign, IL, 2008, pp. 1238-1245, doi: 10.1109/ALLERTON.2008.4797702.
3. Yige Wang, J. S. Yedidia and S. C. Draper, "Construction of high-girth QC-LDPC codes," 2008 5th International Symposium on Turbo Codes and Related Topics, Lausanne, 2008, pp. 180-185, doi: 10.1109/TURBOCODING.2008.4658694.

Надійшла / Paper received: 12.09.2020

Надрукована / Paper Printed : 02.12.2020