ISSN 2788-5518

СЛАВА УКРАЇНІ!
ГЕРОЯМ СЛАВА!

***

GLORY TO UKRAINE!
GLORY TO HEROES!

ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

INFOCOMMUNICATION AND COMPUTER TECHNOLOGY

№ 1 (03), 2022

УНІВЕРСИТЕТ "УКРАЇНА"
КИЇВ 2022

УДК 621.396.969.1

ПОРІВНЯННЯ ПРОДУКТИВНОСТІ ЗАВАДОСТІЙКИХ КОДІВ НА ОСНОВІ ПРОГРАМНОГО HDL МОДЕЛЮВАННЯ ДЛЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

DOI 10.36994/2788-5518-2022-01-03-03

Пятін І.С., *к.т.н.,доц. Хмельницький політехнічний фаховий коледж Національного університету «Львівська політехніка», Хмельницький, Україна, ilkhmel@ukr.net*

Бойко Ю.М., *д.т.н., проф. Хмельницький національний університет, Хмельницький, Україна, boiko_julius@ ukr.net*

Анотація: *Канальне кодування є одним із фундаментальних методів, які дозволяють роботу в каналах зв'язку з гаусовим шумом. Досліджено енергетичний виграш систем зв'язку з турбо, низькою щільністю перевірок на парність (LDPC) та полярним кодуванням. Турбокодування виконується з використанням двох рекурсивних згорткових кодерів. Полярні коди базуються на явищі поляризації інформаційного каналу. Незважаючи на відносну простоту реалізації LDPC кодера, декодер має значну обчислювальну складність. У роботі розглянута HDL реалізація турбо, LDPC, полярного кодерів і декодерів для захищених інформаціний технологій.*

Ключові слова: *турбо код, LDPC код, полярний код, мова описання апаратури (HDL), енергетичний виграш кодування, інформаційні технології.*

COMPARISON THE PERFORMANCE OF ERROR-CONTROL CODE BASED ON SOFTWARE HDL MODELING FOR INFORMATION SECURITY TECHNOLOGIES

Ilya Pyatin, *Ph.D., Ass.Prof. Khmelnytskyi Polytechnic Professional College by Lviv Polytechnic National University, Khmelnytskyi, Ukraine, ilkhmel@ukr.net*

Juliy Boiko, *Dr.habil., Prof. Khmelnytskyi National University, Khmelnytskyi, Ukraine, boiko_julius@ ukr.net*

Abstract: *Channel coding is one of the fundamental methods that allows you to work in Gaussian noise communication channels. High-performance codes with low-complexity encoding and decoding are required for wireless systems. By introducing structured redundancy in the transmitter and using it in the receiver, a wide range of error detection and correction capabilities can be achieved. The energy gain of turbo communication systems, low density parity (LDPC) and polar coding has been studied. Turbocoding is performed using two recursive convolutional encoders. The input stream is transmitted to the first encoder, and the rearranged version is transmitted to the second. On the receiver side, two decoders are used, each of which decodes*

the streams of the corresponding encoder. Decoders iteratively exchange information to achieve the desired bit error probability. Despite the acceptable complexity and good performance of turbocodes, delayed decoding is a major drawback for their use in real-time applications. Polar codes are based on the phenomenon of channel polarization. Its essence is that by relatively simple transformations, the transmission channel can be split into virtually silent and almost completely noisy synthetic subchannels. After that, useful data can be transmitted by almost silent subchannels with a fairly high degree of reliability. Some known data (zeros) should be transmitted over almost completely noisy synthetic subchannels. Encoding is performed using a generator matrix derived from polarization transformation, and decoding can be performed by Successive Cancellation (SC). Despite the relative ease of implementation of such a codec, soft decoding of LDPC code has considerable computational complexity. The LDPC code decoding algorithm can be reduced to iteratively updating the vertices of the Tanner graph and obtaining the final metrics. The reliability values of the test nodes are calculated using the associated variable nodes, and the variables are calculated using the test nodes according to the Tanner graph. These operations are independent of each other and can be performed in parallel. One way to perform this procedure is the Iterative Belief Propagation (IBP) algorithm, known as the SumProduct algorithm. The paper considers HDL implementation of turbo, LDPC, polar encoders and decoders for information security technologies.

Key words: *turbo code, LDPC code, polar code, hardware description language (HDL), energy gain coding, information technology.*

Вступ

У системах мобільного зв’язку використовують бездротову передачу даних між призначеним для користувача обладнанням і базовими станціями. Прийняті дані відрізняються від переданих через помилки, викликаних шумом, завадами і завмираннями. Для виправлення цих помилок системи стільникового зв'язку використовують коди прямого виправлення помилок.

Полярні коди побудовані з використанням явища поляризації каналу. Окрім високої продуктивності, вони досягають пропускної здатності каналу на нескінченній довжині [1]. Кодування виконується з використанням матриці генератора, отриманої з поляризаційного перетворення, і декодування відбувається за алгоритмом послідовного виключення [1-5].

Іншим класом кодів, що наближаються до пропускної спроможності, є коди LDPC [6]. Незважаючи на складність реалізації, завдяки розвитку вбудованих мікропроцесорних пристроїв, вони широко використовуються у стандарті DVB-S2 супутникової передачі даних для цифрового телебачення, стандарті DVB-T2 для цифрового наземного телевізійного мовлення, тощо. LDPC коди є блоковими кодами з розрідженою матрицею перевірки на парність. Така розрідженість допускає декодування з низькою складністю з використанням ітеративного алгоритму поширення довіри, який також називають алгоритмом суми – добутку [7-9].

Турбокоди представляють клас кодів, які можуть працювати дуже близько до межі пропускної здатності. У загальному вигляді турбокодування виконується з використанням двох рекурсивних згорткових кодерів [2]. Вхідний потік передається першому кодеру, а сигнал з виходу перемежувача передається другому. На боці приймача використовуються два декодера,

кожен з яких декодує потоки відповідного кодера. Шляхом обміну ймовірнісною інформацією два декодера можуть ітеративно допомагати один одному.

У вказаних роботах [10-13] відсутнє дослідження HDL моделей вказаних кодерів і декодерів. Робота присвячена порівнянню енергетичного виграшу у інформаціних системах з турбо, LDPC і полярним кодуванням.

Turbo код

Турбокоди використовують для кодування даних користувача мобільного широкосмугового зв'язку (МВВ) в стільникових системах 3G UMTS і 4G LTE. Для дослідження продуктивності системи зв’язку з турбо кодуванням складена модель, приведена на рис. 1. Проведення досліджень складається з наступних кроків [2]:

1. Вхідні дані надходять на перетворювач фреймів вхідних даних у потік вибірок.
2. Кодування вибірок. Перетворення потоку вибірок у фрейми.
3. Модуляція закодованих даних, дія каналу зв’язку і демодуляція отриманого сигналу.
4. Перетворення паралельних даних у послідовний потік вибірок і декодування сигналу.
5. Перетворення потоку вибірок у фрейми. Визначення кількості бітових помилок

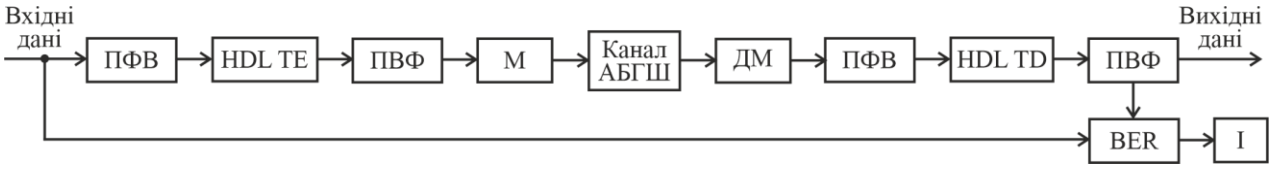

Рис. 1. Структурна схема моделі дослідження турбо кодера і декодера ПФВ – перетворити фрейми у вибірки; HDL TE – HDL алгоритм кодера турбокоду; ПВФ – перетворити вибірки у фрейми; М – модулятор; Канал АБГШ – канал зв’язку з адитивним білим гаусовим шумом; ДМ – демодулятор; HDL TD – HDL алгоритм декодера турбокоду; BER – підрахунок кількості бітових помилок; І – індикація отриманого результату

Турбо кодер

Турбокодер побудований на основі паралельного каскадного згорткового кода (PCCC). Він має два складових кодера і внутрішній перемежувач. Перший кодер працює з потоком вхідних даних, а другий кодер працює з даними на виході перемежувача. На виході кожного кодера до сигналу додаються кінцеві бити. Швидкість кодування - 1/3. Закодовані вихідні біти для кожного вхідного біта повертаються як вектор 3 на 1, [S P1 P2]. У цьому векторі S - це систематичний біт, а P1 і P2 - біти парності від двох кодерів.

Турбо кодер має шину, яка містить три керуючих сигнали. Ці сигнали вказують на достовірність кожної вибірки і межі фрейму. В кінці кожного блоку додаються 17 циклів затримки, які пов'язані з конвеєрними затримками в алгоритмі.

Вхідні порти для кодера і декодера:

- data - відліки вхідного сигналу,;
- ctrl - керуючі сигнали, що супроводжують потік відліків;
- blockSize - розмір блоку турбокоду.

Вихідні порти для кодера і декодера:

- data - потік відліків на виході кодера;
- ctrl - керуючі сигнали, що супроводжують потік відліків;
- додаткові порти кодера tail1 і tail2 необхідні для зазначення положення хвостових бітів.

Simulink модель кодера турбокоду приведена на рис. 2 [14].

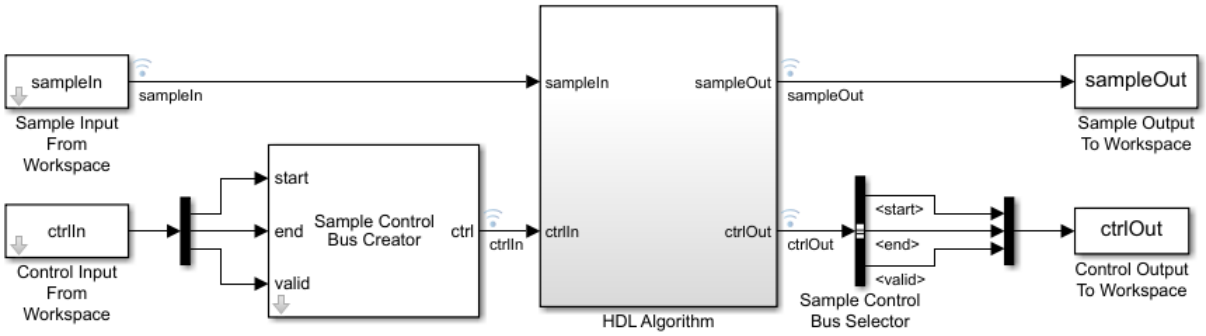

Рис. 2. Simulink модель кодера турбокоду

Для апаратної реалізації збереження індексів перемеження недоцільно. Для підтримки 188 розмірів блоку LTE буде потрібно 4 Мб пам'яті.

Передаточна функція складеного коду з 8 станами для PCCC задається виразом:

$$G(D) = \left[1, \frac{1 + D + D^3}{1 + D^2 + D^3}\right] \tag{1}$$

Вихідні біти перемежувача визначаються виразом:

$$c'_i = c_{\Pi(i)}, \; i = 0, 1, \ldots, (K-1), \tag{2}$$

де K – кількість вхідних бітів. Відношення між вихідним індексом i і вхідним індексом $\Pi(i)$ визначається виразом:

$$\Pi(i) = \left(f_1 \cdot i + f_2 \cdot i^2 \right) \bmod K, \tag{3}$$

де параметри f_1 і f_2 залежать від розміру блоку *K*.

Розрахунок показників спрощується на основі наступних рівнянь:

$$\pi(i+1) = \begin{cases} \pi(i) + g(i), & \pi(i) + g(i) < K \\ \pi(i) + g(i) - K, & \textit{інакше} \end{cases}, \quad \pi(0) = 0, \tag{4}$$

$$g(i+1) = \begin{cases} g(i) + 2f_2, & g(i) + 2f_2 < K \\ g(i) + 2f_2 - K, & \textit{інакше} \end{cases}, \quad g(0) = f_1 + f_2. \tag{5}$$

Отже, блок зберігає f_1 і f_2 в пам'яті і використовує ці дві константи і чотири суматора для обчислення індексів перемеження. Структурна схема кодера турбо коду приведена на рис. 3.

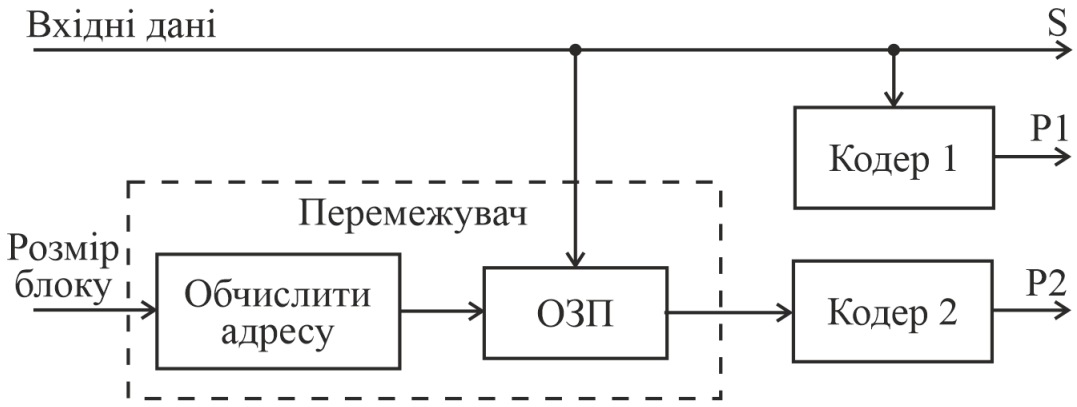

Рис. 3. Структурна схема кодера турбо коду

Блок використовує два постійних коефіцієнта для отримання адрес читання. Алгоритм зберігає 188 пар коефіцієнтів в ПЗУ (5 Кб). Потім блок зчитує співпадаючи пари під час виконання, щоб отримати перемежені адреси у пам'яті.

Турбо декодер

Turbo Decoder виконує послідовні ітерації між двома декодерами. Швидкість кодування - 1/3. Блок приймає закодовані біти як вектор [S P1 P2], де S - систематичний біт, а P1 і P2 - біти парності від двох кодерів.

Кожна вхідна вибірка представляє собою вектор трьох м'яких рішень з фіксованою точкою. Шини управління входом і виходом розширені для відображення сигналів управління. start і end показують межі кадру, а valid кваліфікує вибірки даних.

Simulink модель декодера турбокоду приведена на рис. 4.

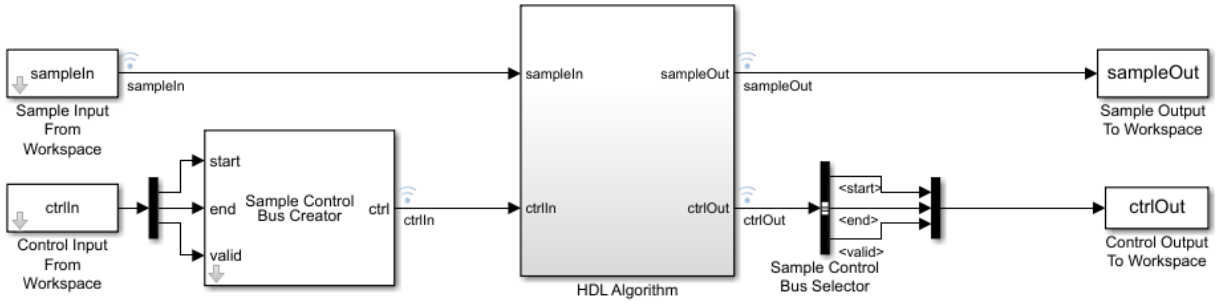

Рис. 4. Simulink модель декодера турбокоду

Блок реалізує алгоритм ітеративного декодування. На рис. 5 показаний концептуальний алгоритм для одної ітерації. Декодер виконує одну половину ітерації і перемежує результати. Потім вихідні дані прямують назад на вхід для наступної напів-ітерації. Перемежувач обчислює індекси перемежения за розміром блоку.

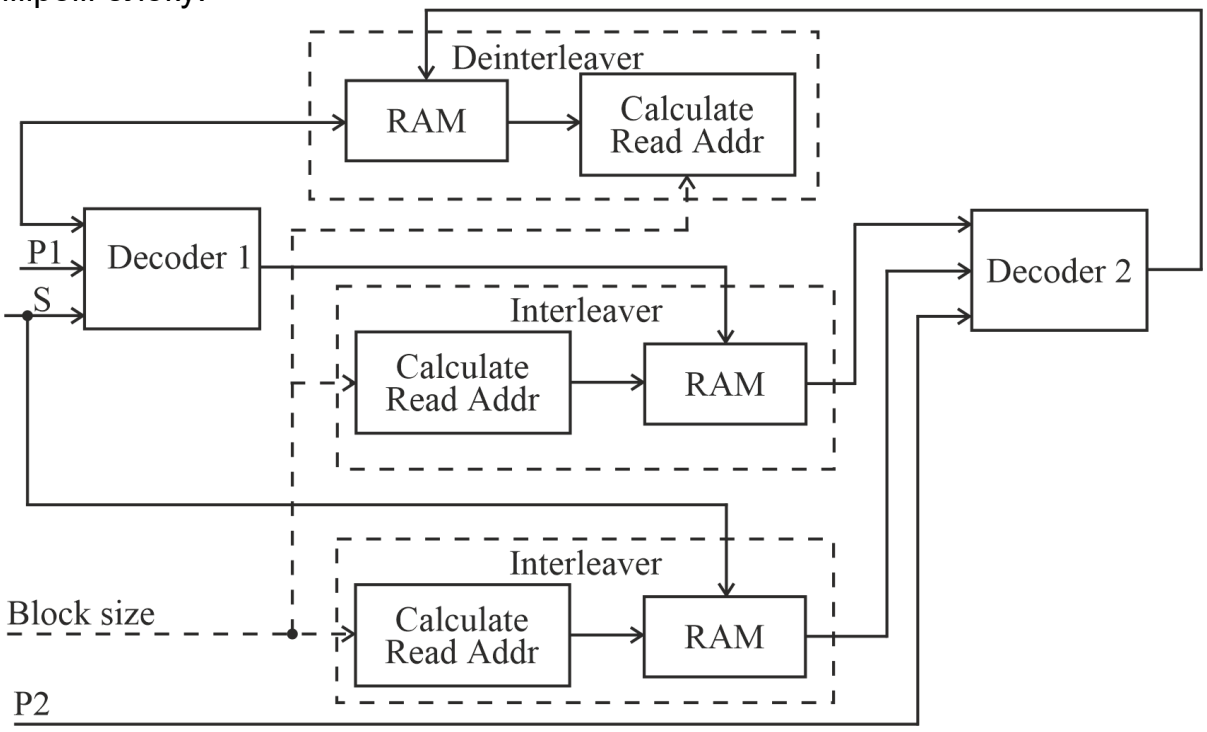

Рис. 5. Структурна схема декодера турбо коду

Непарні напів-ітерації обчислюють відношення правдоподібності на основі не перемежених бітів (P1, S і результати зворотного перемеження P2). Парні напів-ітерації обчислюють відношення правдоподібності з перемеженням бітів (P2 і перемеженням результатів декодування P1 і S).

Блок декодера використовує алгоритм BCJR для знаходження відношення правдоподібності конкретного біта [2].

$$L(u_k) \triangleq \log\left(\frac{p(u_k=+1|\,y)}{p(u_k=-1|\,y)}\right) = \log\left(\frac{\sum\limits_{s^+} p(s_{k-1}=s', s_k=s, y)\,/\,p(y)}{\sum\limits_{s^-} p(s_{k-1}=s', s_k=s, y)\,/\,p(y)}\right) \quad (6)$$

Імовірності можуть бути представлені у вигляді поточного і майбутнього станів. Визначимо спільну імовірність $P(s', s, y)$. Ця імовірність обчислюється як добуток трьох імовірностей:

$$P(s', s, y) = \alpha_{k-1}(s') \cdot \gamma_k(s', s) \cdot \beta_k(s)\,, \quad (7)$$

Вони визначаються виразами:

$$\alpha_{k-1}(s') = P(s' \mid y_{<k}) \quad (8)$$

$$\gamma_k(s', s) = P(y_k, s \mid s') \quad (9)$$

$$\beta_k(s) = P(y_{>k} \mid s) \quad (10)$$

У момент часу k імовірності α, γ та β пов’язані з минулою, поточною та майбутньою послідовностями відповідно.

LDPC код

Коди з низькою щільністю перевірок на парність (LDPC) використовують для кодування даних користувача розширеного мобільного широкосмугового зв’язку (eMBB) у 5G New Radio.

На рис. 6 приведена структурна схема дослідження системи зв’язку з LDPC кодуванням [8].

Спочатку відбувається генерація вхідних даних для кодера. Обирається послідовність вхідних значень для номера базового графа (bgn) і коефіцієнта розширення (LiftingSize), а також будуються вхідні вектори значень bgn і LiftingSize.

Далі відбувається LDPC кодування, модуляція закодованого сигналу, проходження через канал з АБГШ і демодуляція. Для декодування отриманого сигналу створюються вектори bgn і LiftingSize і перетворюються фрейми даних у вхідні вектори логарифмічних відношень правдоподібності (LLR) з керуючими сигналами.

Код LDPC можна описати за допомогою породжуючої матриці G, розміром $k \times n$, де k - довжина інформаційної послідовності, n - довжина кодового слова. Тоді отримання кодового вектора C буде здійснюватись за виразом: $C = m \cdot G$, де m - інформаційна послідовність.

Породжуюча матриця визначається виразом: $G=[I,P]$, де I - одинична матриця $k\times k$,

Р – парна частина. LDPC код буде описуватись виразом: $H=\left[P^T,I\right]$, причому

$$C\cdot H^T=0. \tag{11}$$

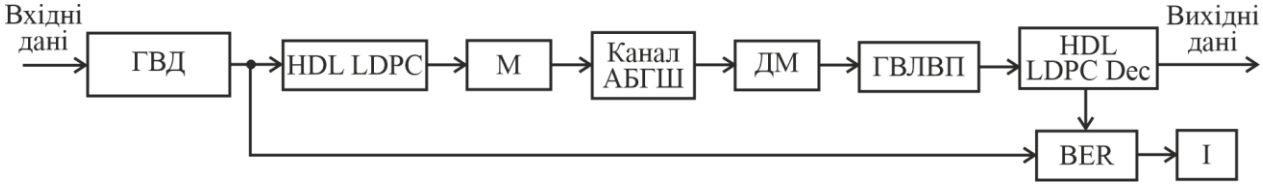

Рис. 6. Структурна схема моделі дослідження кодера і декодера LDPC(ГВД – генерація векторів вхідних даних; HDL LDPC – HDL алгоритм LDPC кодера; М – модулятор; Канал АБГШ – канал зв’язку з адитивним білим гаусовим шумом; ДМ – демодулятор; ГВЛВП – генерація вхідних логарифмічних відношень правдоподібності; HDL LDPC Dec – HDL алгоритм декодера LDPC коду; BER – підрахунок кількості бітових помилок; І – індикація отриманого результату

Елементами такої матриці є коефіцієнти перевірочних рівнянь, за допомогою яких обчислюються перевірочні символи.

Породжуюча матриця пов’язана з матрицею перевірки на парність (parity check matrix).

Матриця перевірки на парність має $(N-K)$ рядків і N стовпців, де N відповідає довжині кодового слова, а K – довжині повідомлення. Матриця перевірки на парність задана виразом:

$$H=\left[P^T\ I\right] \tag{12}$$

Розглянемо матрицю перевірки на парність і відповідний граф Танера (рис. 7), де N =10, K =6:

$$H=\begin{bmatrix}1&1&0&1&0&0&1&0&0&0\\0&1&1&0&1&0&0&1&0&0\\1&0&0&0&1&1&0&0&1&0\\0&0&1&1&0&1&0&0&0&1\end{bmatrix}$$

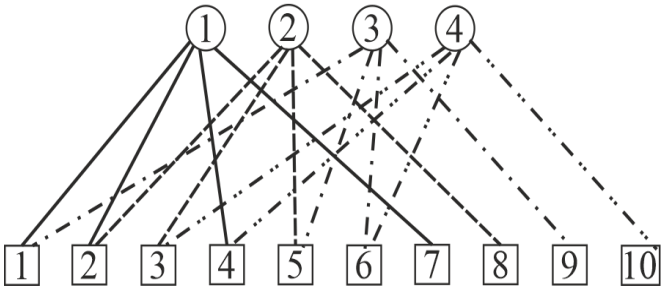

Рис. 7. Граф Танера LDPC коду для *N* = 10, *K* = 6

Існує два види вузлів: вузли змінних (variable nodes), кількість яких відповідають числу стовпців N, та вузли перевірки (check nodes), що відповідають числу рядків ($N-K$). Вузли пов'язані між собою, і зв'язок визначається положенням одиниць матриці *H*.

Кодер LDPC

Розглянемо блок HDL реалізації кодера з низькою щільністю перевіркок на парність (LDPC). Блок приймає біти даних, шину ctrl, номер базового графу і коефіцієнт розширення. Блок виводить закодовані біти, шину ctrl, коефіцієнт розширення.

Вхідні порти для кодера і декодера:

- data - біти вхідних даних;
- ctrl - керуючі сигнали, що супроводжують потік вибірок;
- bgn - номер базового графу;
- liftingSize - вхідний коефіцієнт розширення

Вихідні порти для кодера і декодера:

- data - закодовані біти даних на виході;
- ctrl - керуючі сигнали, що супроводжують потік вибірок;
- liftingSize - вихідний коефіцієнт розширення;
- nextFrame - готовий до нових вхідних даних.

Якщо значення порту bgn дорівнює 0, блок встановлює *n* = 22. Коли значення bgn = 1, блок встановлює *n* = 10. Коли коефіцієнт розширення менше 64, значення bgn дорівнює 0.

Для значення LiftingSize, рівного 2, блок приймає перші два біта вхідних даних в кожному тактовому циклі і ігнорує решту 62 елемента в цьому тактовому циклі. Загальна кількість тактів, необхідних блоку для прийому бітів вхідних даних, дорівнює 22.

Коли значення LiftingSize більше 64, а значення bgn дорівнює 0:для значення LiftingSize, рівного 104, блок приймає 104 біта даних за два тактових цикли: перші 64 біта даних в першому тактовом циклі і 40 бітів даних у другому тактовом циклі. Блок ігнорує решту 24 елемента в другому тактовом циклі. Необхідно 44 такти для приймання вхідних даних.

Simulink модель кодера LDPC приведена на рис. 8.

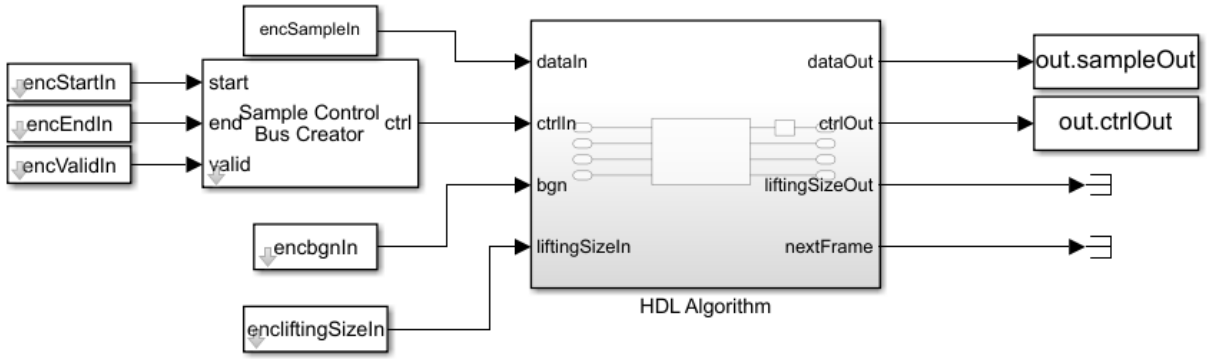

Рис. 8. Simulink модель кодера LDPC

На рис. 9 показана структурна схема блоку NR LDPC Encoder.

Архітектура складається з блоків Controller, Check Matrix LUT, Shifter, Memory, Negative Position Selector і XOR Unit. Блок контролера управляє потоком даних в блок пам'яті і з нього і надає керуючі сигнали для управління функціональністю всіх цих блоків. Блок LUT матриці перевірки складається з значень матриці перевірки на парність стандарту 5G [1]. На основі значень порту bgn і LiftingSize блок LUT матриці перевірки надає вхідні дані для блоку Shifter. Блок Systematic Parity Generator генерує біти парності для перших чотирьох рядків матриці і використовує ці біти для обчислення інших рядків матриці.

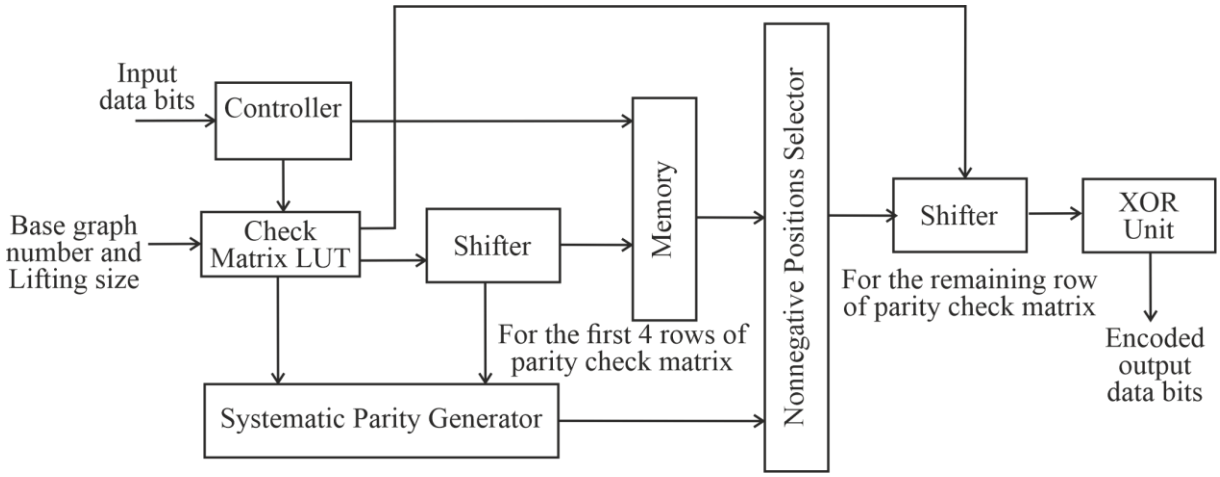

Рис. 9. Архітектура кодера LDPC

Блок селектора не від’ємної позиції вибирає невід'ємні позиції матриці перевірки на парність. Блок XOR Unit виконує операцію по модулю, завершуючи операцію кодування. Затримка варіюється в залежності від значень bgn і LiftingSize. Якщо значення портів bgn і LiftingSize встановлені на 0 і 384 відповідно, затримка блоку становить 1911 тактів. Якщо значення

портів bgn і LiftingSize встановлені на 1 і 48, затримка блоку складає 233 такти.

LDPC декодер

Декодування вхідних даних з низькою щільністю перевірок на парність (LDPC) виконується за методом багаторівневого поширення довіри алгоритмом апроксимації мінімальної суми.

Додатковий вхідний порт для декодера: iter - кількість ітерацій.

Simulink модель декодера LDPC представлена на рис. 10.

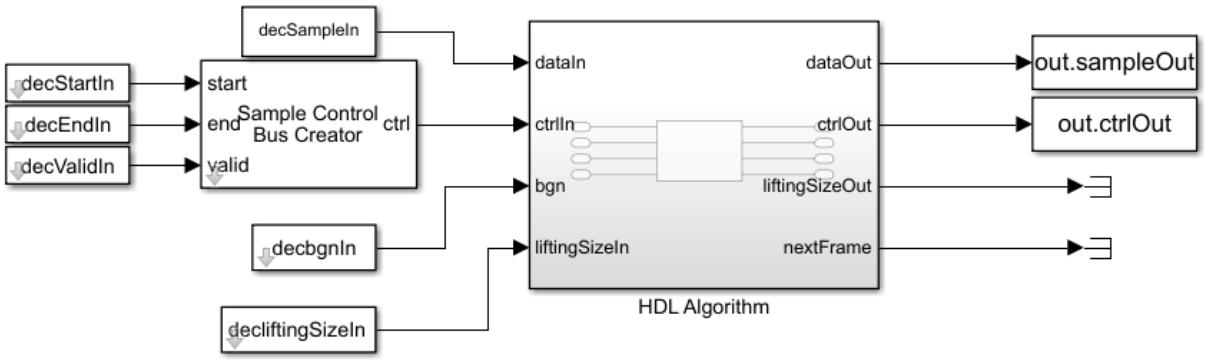

Рис. 10. Simulink модель декодера LDPC

Враховуючи слово, яке передається: $c=\{c_0,c_1,\ldots,c_{n-1}\}$ і слово, яке приймається: $v=\{v_0,v_1,\ldots,v_{n-1}\}$, необхідно визначити логарифмічне відношення правоподібності (LLR) прийнятого символа. LLR визначається виразом:

$$L(v_i)=\log\left(\frac{\Pr(v_i=0\,|\,y_i)}{\Pr(v_i=1\,|\,y_i)}\right) \tag{13}$$

Для сигналу з двопозиційною модуляцією і каналу з АБГШ, LLR прийнятого сигналу визначається виразом:

$$L(v_i)={}^{2y_i}\!\!\diagup\!\!_{\sigma^2}\ . \tag{14}$$

де y_i - прийнятий символ; σ^2 - напруга шуму. Ці повідомлення передаються на перевірочний вузол, де оперують не логарифмічними відношеннями правдоподібності, а ймовірностями символів.

Алгоритм декодування LDPC передбачає ітеративне пересилання повідомлень від вузлів змінних до вузлів перевірки (V2C) і від вузлів перевірки до вузлів змінних (C2V). Початковою точкою алгоритму декодування є матриця логарифмічних відношень правдоподібності (LLR), яка повторює структуру матриці *H*.

$$\underset{M\times N}{M} = \left(\underset{N\times 1}{r} \cdot \underset{1\times M}{I} \right)^T \odot \underset{M\times N}{H}, \tag{15}$$

де I одинична матриця, $\odot$ - добуток Адамара (по-елементний добуток).

Далі алгоритм потребує обробки повідомлення (V2C) в області імовірностей. Для переходу від LLR до імовірностей скористаємось співвідношенням:

$$\mathrm{tgh}\left(\frac{1}{2} \ln\left(\frac{1-p}{p} \right) \right) = 1 - 2p \tag{16}$$

Для передачі інформацій від вузла змінних до вузла перевірки (V2C), виконується добуток ненульових імовірностей в кожному рядку:

$$E_{j,i} = \log\left(\frac{1+\prod_{i'\in B_j, i'\neq i} \tanh\left(M_{j,i'} / 2 \right)}{1-\prod_{i'\in B_j, i'\neq i} \tanh\left(M_{j,i'} / 2 \right)} \right) = \log\left(\frac{1+\prod_{i'\in B_j, i'\neq i} M'_{j,i'}}{1-\prod_{i'\in B_j, i'\neq i} M'_{j,i'}} \right), \tag{17}$$

де j - номер рядка, i - номер стовпця, B_j - множина ненульових елементів у j-му рядку

На цьому етапі потрібно:

- вибрати елемент в матриці M, переведений в область імовірностей;
- якщо його позиція відповідає позиції ненульового елемента матриці H, визначити добуток всіх ненульових імовірностей у рядку даного елемента;
- виключити даний елемент з операції знаходження добутку;
- повторити всі попередні кроки для кожного елемента матриці.

Виключення поточного вузла з розгляду можна провести видаленням його значення з результатів після підрахунків.

Для перевірки критерію зупинення декодування необхідно оновити апріорні ймовірності – зробити їх апостеріорними:

$$l_i = r_i + \sum_{j\in A_i} E_{j,i} \tag{18}$$

де A_i - множина елементів, що відповідають ненульовим елементам матриці перевірки на парність у i -му стовпці.

Закодуємо біти оберненим кодом «без повернення до нуля»:

$$z_i = \begin{cases} 0, & l_i \geq 0 \\ 1, & l_i < 0 \end{cases}. \tag{19}$$

Для того, щоб вважати процедуру декодування успішною, потрібно, щоб на всіх перевірочних вузлах при визначенні добутку матриці перевірки на парність з апостеріорними значеннями бітів, сформувалися нулі:

$$s = H \cdot z_i = 0. \tag{20}$$

Ця матриця визначає матрицю перевірки на парність.

На рис. 11 показана архітектура блоку NR LDPC Decoder. Блок Functional Processing Unit обчислює повідомлення змінного вузла (ЗВ) і повідомлення перевірочного вузла (ПВ) на основі методу багаторівневого поширення довіри за допомогою алгоритму апроксимації мінімальної суми. ЗВ і ПВ ітераційно обмінюються повідомленнями і імовірностями вірності символів, що надходять з каналу зв’язку.

Затримка варіюється в залежності від значень bgn, LiftingSize і iter.

Для значення порту bgn = 0, *t* має значення +1046, а *n* = 66. Для значення порту bgn, = *1*, *t* = 772, а *n* дорівнює 50.

Polar codes

Полярні коди використовуються для кодування каналів управління низхідною (DCI), висхідною (UCI) лінії звязку і широкомовного каналу (BCH) у інформаційних технологіях 5G New Radio. Явище поляризації каналу складається у створенні множини синтетичних бітових каналів. Ці канали поляризуються, тобто передають один біт інформації з різною надійністю. Для достатньо великої множини синтетичних каналів, їх взаємна інформація або близька до нуля (шумові канали), або близька до одиниці (безшумні канали). Полярний код поділяє канал передачі на надійні і не надійні бітові канали. Полярні коди нескінченної довжини можуть досягти пропускної здатності двійкового симетричного каналу без пам'яті [12], [14].

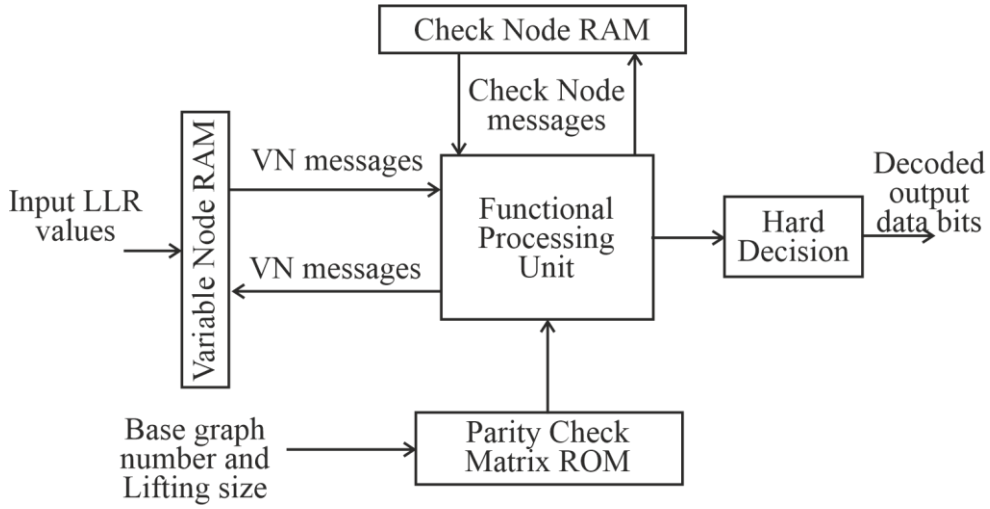

Рис. 11. Архітектура декодера LDPC

Для двійкових каналів зв’язку з адитивним білим гаусовим шумом (AWGN) і дисперсією шуму σ^2 імовірність переходу між виходом (y) і входом (x), може бути записана виразом:

$$W(y \mid x) = \begin{cases} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y-x_0)^2}{2\sigma^2}}, & x = 0 \\ \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(y+x_0)^2}{2\sigma^2}}, & x = 1 \end{cases}, \tag{21}$$

де x_0 - середнє значення переданого сигналу x. Припускаючи, що біти модулюються з використанням двійкової фазової маніпуляції (BPSK), логарифмічне відношення правдоподібності (LLR) кожного прийнятого символу визначається виразом:

$$l(y) = \ln \frac{W(y \mid 0)}{W(y \mid 1)} = \frac{2yx_0}{\sigma^2} \tag{22}$$

Полярний код визначається матрицею перетворення $T_{Nm} = T_2^{\otimes n}$, де $N_m = 2^n$ - довжина материнського коду, n - ціле число, $n = \log_2 N_m$, $\otimes n$ -n-кратний добуток Кронекера ядра:

$$T_2 = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \tag{23}$$

і замороженої множини $F \subseteq \{1,\ldots,N_m\}$ розміром $N_m - K_m$, K_m - кількість інформаційних біт материнського коду. Заморожена множина проектується таким чином, щоб імовірність помилки при SC-декодуванні була мінімізована, тобто позиції $N_m - K_m$ з найменшою бітовою надійністю утворюють заморожену множину F.

Інформаційне слово $u \in F_2^{Km}$ кодується в кодове слово $x \in F_2^{Km}$ шляхом визначення вектора $v \in F_2^{Km}$ такого, що $v_I = u$ - вектор інформаційної множини та $v_F = 0$, де v_I та v_F - підвектори v, що визначаються інформаційною множиною (I) та замороженою множиною (F) відповідно, та шляхом обчислення кодового слова $x = v \cdot T_{Nm}$. Для деяких конструкцій інформаційне слово містить перевірку циклічним надлишковим кодом (CRC).

Структурна схема моделі проведення експерименту приведена на рис. 12.

Для генерації вхідних даних кодера задаємо серію вхідних значень для K і E, генеруємо випадкові фрейми вхідних даних і додаємо кодове слово CRC. Використовується режим висхідної лінії зв'язку, тому кожне повідомлення має 11 бітів CRC. Перетворюємо кадри повідомлення в потоки логічних вибірок і керуючих сигналів, які вказують межі кадру. У моделі імпортуються змінні робочої області encSampleIn, encCtrlIn, encKfi, encEfi, sampleTime і simTime. Кількість холостих циклів між кадрами вибирається емпірично, щоб узгодити затримку полярного кодера для зазначених значень K і E. При виконанні моделі змінні вхідного сигналу імпортуються з робочої області і повертається потік вихідних відліків з полярним кодуванням.

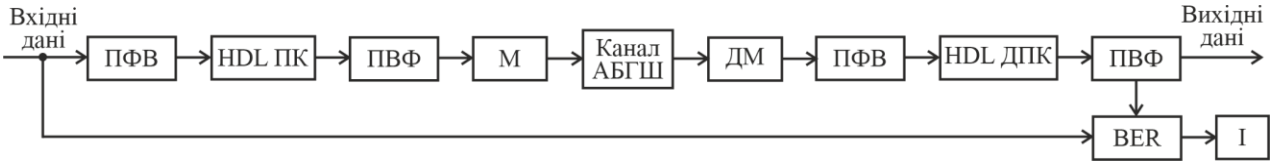

Рис. 12. Структурна схема моделі дослідження полярного кодера і декодера: ПФВ – перетворити фрейми у вибірки; HDL ПК – HDL алгоритм полярного кодера; ПВФ – перетворити вибірки у фрейми; М – модулятор; Канал АБГШ – канал зв’язку з адитивним білим гаусовим шумом; ДМ – демодулятор; HDL ДПК – HDL алгоритм декодера полярного коду; BER – підрахунок кількості бітових помилок; I – індикація отриманого результату

Для декодування даних запускається окрема модель з відповідним HDL алгоритмом. Закодовані дані є джерелом для генерації вхідних логарифмічних відношень правдоподібності (LLR) для полярного декодера. Використовуються системні об'єкти каналу, модулятора і демодулятора для додавання шуму до сигнала [1, 5]. Далі перетворюються фрейми у відліки.

Кодер полярного коду

Процедура кодування визначається виразом: $x_1^N = u_1^N G_N$, де x_1^N - кодове слово; u_1^N - вектор, що включає інформаційні символи ($u_1 \notin F$, $1 \le i \le N$) і заморожені біти ($u_1 \in F$, $1 \le i \le N$); G_N - породжуюча матриця, що задається виразом: $G_N = B_N T_2^{\otimes n}$, де B_N - матриця перестановки.

Затримка виконання операції полярного кодування залежить від параметрів коду.

Вхідні порти для кодера і декодера:

- data – вхідні біти даних, задані як скаляр;
- ctrl - керуючі сигнали, що супроводжують потік відліків, заданий як шина samplecontrol bus.
- K - довжина інформаційного блоку в бітах;
- E - узгоджена за швидкістю довжина коду на виході в бітах.

Вихідні порти для кодера і декодера:

- data - біти даних;
- ctrl - керуючі сигнали, що супроводжують потік відліків;
- nextFrame - готовий до нових даних на вході.

Simulink модель кодера полярного коду приведена на рис. 13.

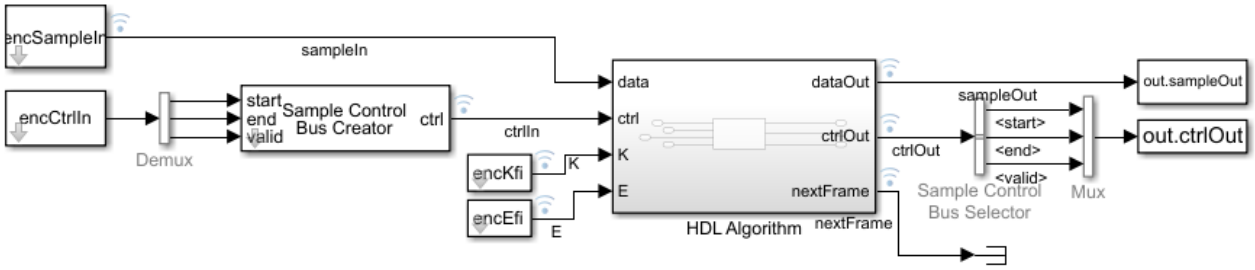

Рис. 13. Simulink модель кодера полярного коду

HDL алгоритм кодера полярного коду

Потоки даних та управління від MAC-рівня кодуються та декодуються для надання транспортних послуг. Схема канального кодування є комбінацією виявлення помилок, виправлення помилок, узгодження швидкостей, перемежування та відображення транспортного каналу або керуючої інформації у напрямку від фізичних каналів.

Блок зберігає всі повідомлення в буфері, а потім перемежує і відображає інформаційні біти на основі шаблону, зазначеного в стандарті для значень K і E. Перемеження включається для низхідної лінії зв’язку. На рис. 14 приведена архітектура полярного кодера.

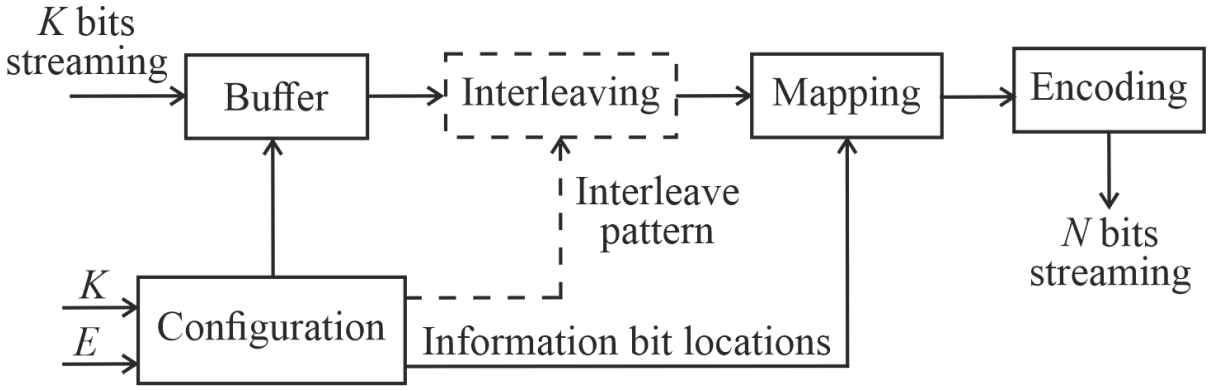

Рис. 14. Архітектура полярного кодера

Етап конфігурації використовується при зміні вхідних значень K і E. Блок обчислює нову довжину повідомлення N і розташування інформаційних бітів, потім передає їх в буфер і на етап відображення. Шаблони відображення обчислюються в міру необхідності, а не зберігаються в обладнанні. На етапі конфігурації також обчислюється шаблон перемеження, коли встановлюється для параметра Link direction значення Downlink.

Точна затримка залежить від значень K і E. Затримка більше для кадрів, в яких значення K і E змінюються, і блок повинен обчислити нову конфігурацію. Затримка змінюється в залежності від значень K і E. Для першого кадру з заданими значеннями K і E блок повинен визначити довжину повідомлення та відображення інформаційних бітів для цих значень. Коли вхідні значення K і E рівні 132 і 256, відповідно, блок має затримку в 535 циклів. Для подальших кадрів з такими ж значеннями K і E блок буде готовий раніше, оскільки йому не потрібно повторно обчислювати конфігурацію. Ця затримка становить 389 циклів. Коли значення K і E змінюються на 54 і 124 відповідно, блок повинен обчислити нову конфігурацію, і маємо затримку 443 цикли.

Декодер полярного коду

Блок використовує схеми кодування низхідної або висхідної лінії зв'язку. Полярні коди використовуються для кодування каналів керуванням низхідною (DCI) і висхідною (UCI) ліній зв’язку, а також радіомовного каналу (BCH) у інформаціних технологіях 5G.

Додатковий вихідний порт декодера: err - результат CRC.

Відсутність перерахунку бітів CRC зменшує час очікування обладнання та ресурси. Simulink модель декодера полярного коду зображена на рис. 15.

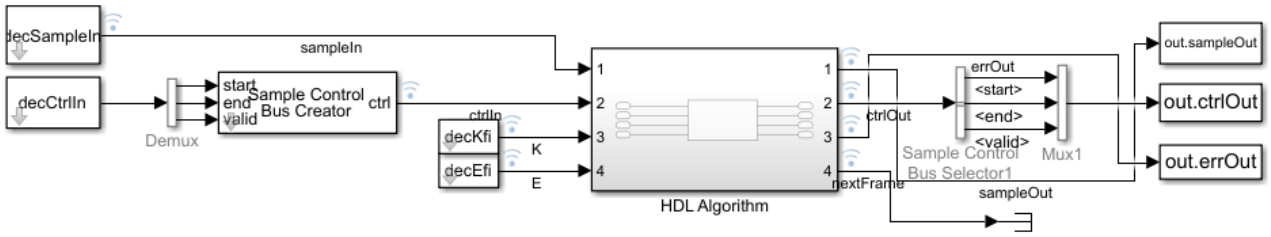

Рис. 15. Simulink модель декодера полярного коду

Блок NR Polar Decoder реалізує списковий декодер послідовного виключення за допомогою CRC. Декодер перебирає всі LLR в дереві, щоб прийняти рішення для біта, а потім використовує це рішення для декодування наступного біта. Крок деперемеження включається для низхідної лінії зв’язку. На рис. 16 показана архітектура полярного декодера.

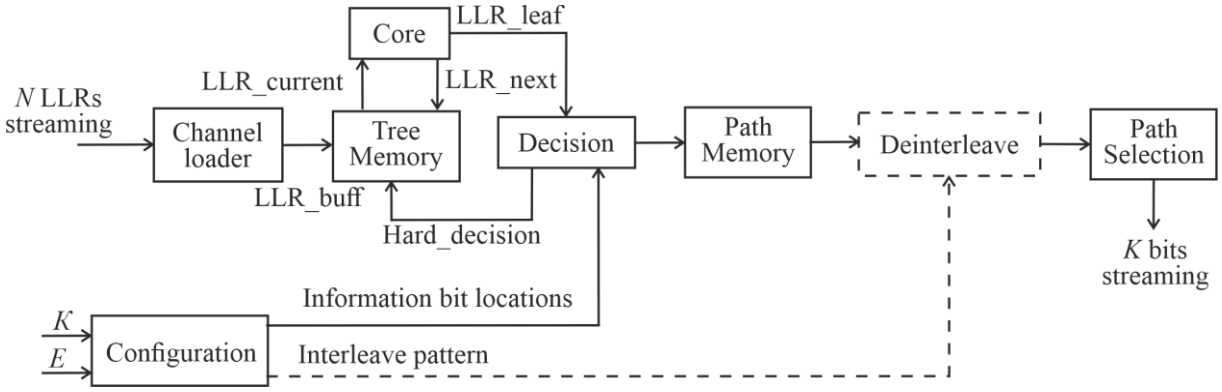

Рис. 16. Архітектура полярного декодера

Етап конфігурації використовується при зміні значень вхідного порту K і E. Блок обчислює розташування інформаційних бітів і передає їх на етап прийняття рішення. Щоб зменшити обчислення для кожного декодування, деревоподібна пам'ять зберігає ймовірність того, що кожен вузол буде одиницею або нулем. Кожна ітерація оновлюється, якщо змінилися LLR.

Етап прийняття рішення перевіряє значення LLR на відповідність очікуваним місцям розташування інформаційних бітів і заморожених бітів і повертає жорстке рішення в деревоподібну пам'ять. Якщо очікується, що біт буде заморожений, етап прийняття рішення повертає жорстке рішення, яке дорівнює нулю, і оновлює ймовірності пов'язаних шляхів. Пам'ять шляхів реконструює два найбільш ймовірні шляхи з результатів жорсткого рішення і передає їх та результати на наступний етап. На етапі вибору шляху обчислюється CRC для обох шляхів, а потім обирається шлях, який проходить через CRC. Якщо обидва CRC зазнають невдачі, блок повертає шлях з більш високою оцінкою [14].

Для поліпшення характеристик полярних кодів, об'єднують полярні коди з контролем циклічного надлишкового коду (CRC). Декодер виконує декодування за списковим алгоритмом послідовного виключення (SC-List), а потім обчислює CRC для кожного з вижившихшляхів.

Для більшості отриманих кадрів декодер SC-List з L=2 може успішно декодувати інформаційні біти, і дуже мало кадрів, яким потрібен великий L для успішного декодування. Тому, щоб зменшити складність декодування, використовують адаптивний декодер SC-List для полярних кодів з CRC. Адаптивний декодер SC-List спочатку використовує дуже маленьке L, а потім ітеративно збільшує L (якщо немає шляху виживання, що проходить через CRC), поки L не досягне заздалегідь відомого числа Lmax.

Списковий декодер послідовного виключення має алгоритм:

1. Ініціалізуйте L = 1 для декодера SC-списку.

2. Виконайте декодування SC-List, а потім обчисліть CRC на кожному шляху виживання.

3. Якщо є один або декілька шляхів, що проходять через CRC, виведіть шлях з найбільшою ймовірністю, і вийдіть з декодування; в іншому випадку перейдіть до 4;

4. Оновлення L до 2L. Якщо L ≤ Lmax, перейдіть до 2; в іншому випадку виведіть шлях з найбільшою ймовірністю і вийдіть з декодування;

Затримка декодера полярного коду для N=128, Uplink Latency=1179 циклів.

Затримка більше для фремів, в яких значення вхідного порту K і E змінюються, і блок повинен обчислити нову конфігурацію.

Експериментальні дослідження HDL моделей кодерів і декодерів

Згенерований HDL направляється на оціночну плату Xilinx Zynq-7000 ZC706.

В таблиці1 наведено порівняння ресурсів оціночної плати для побудови кодерів і декодерів.

LUT (Look-Up Table) - це невелика асинхронна SRAM, яка використовується для реалізації комбінаційної логіки, а тригер (Flip-Flop) - це однобітова комірка пам'яті, яка використовується для зберігання стану. LUT зазвичай доступні тільки для читання, і їх вміст можна змінити тільки під час конфігурації FPGA. Але в FPGA Xilinx зазвичай можна записати половину LUT, тому їх можна використовувати для реалізації багатьох невеликих RAM (так звана «розподілена RAM»). На тригер можна писати, і це їх головне призначення. До значенням тригера можна отримати доступ безпосередньо, і його можна направити в будь-яке місце, в той час як для читання вмісту LUT потрібна адреса, тому є можливість отримати доступ тільки до одного збереженого біту за раз. Через це LUT можуть зберігати більше, ніж тригери. LUT не мають стану і використовуються для реалізації комбінаторної логіки.

Таблиця 1.
Ресурси оціночної плати для кодерів і декодерів

Ресурси	Полярний кодер	Полярний декодер	LDPC кодер	LDPC декодер	Турбо кодер	Турбо декодер
Slice LUTs	637	3048	7951	69335	253	4771
Slice Registers	934	2562	8504	75296	-	-
Block RAM (16K)	2,5	4,5	3,5	147,5	0,5	7
Flip-Flops	-	-	-	-	222	4691
LUTRAM	-	-	-	-	2	212
F, МГЦ	450	250	430	293	312,5	306,6

Логічний блок (рис. 17) складається з декількох логічних комірок (ALM, LE, Slice, тощо).

Типова комірка складається з LUT з 4 входами, повного суматора (FA) і тригера D-типу, як показано на рисунку. LUT на цьому малюнку розділені на дві LUT з трьома входами. У нормальному режимі вони об'єднуються в LUT з чотирма входами через лівий мультиплексор. В арифметичному режимі їх виходи подаються на Full adder (FA). Вибір режиму програмується в середньому мультиплексорі. Вихід може бути або синхронним, або асинхронним, в залежності від програмування мультиплексора справа, як показано на рисунку. На практиці, вся або частини FA поміщаються в LUT як функції для економії місця.

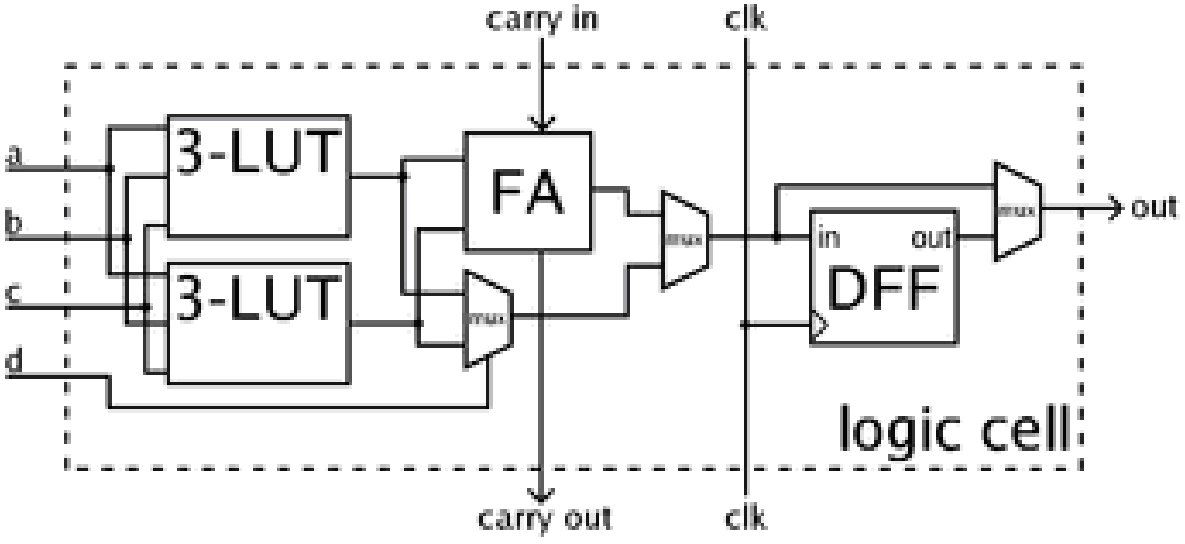

Рис. 17. Структура логічного блоку програмованої логіки

Логічні блоки зазвичай містять декілька Slices. ALM і зрізи зазвичай містять 2 або 4 структури з деякими загальними сигналами.

В останні роки виробники почали переходити на 6-вхідні LUT в своїх високопродуктивних компонентах, заявляючи про підвищення продуктивності.

Проведені дослідження моделей систем зв’язку з розглянутими кодами (рис. 18 – рис. 22):

- для декодерів вибираємо 8 ітерацій для турбо, 16 ітерацій для LDPC та розмір списку 8 для полярних кодів;

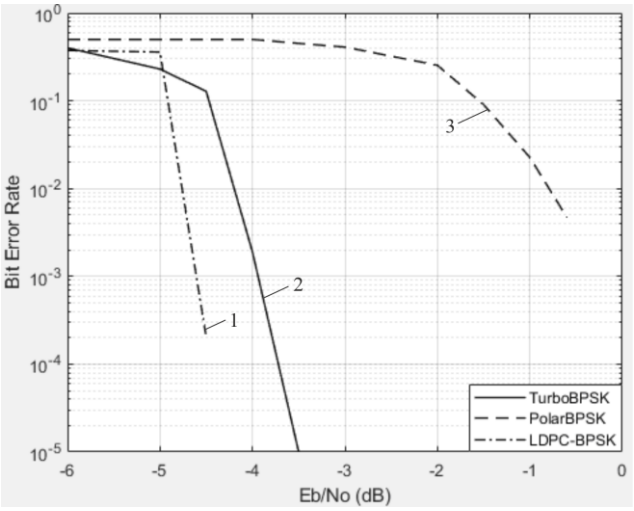

Рис. 18. Залежність кількості бітових помилок від відношення сигнал-шум для системи зв’язку з модуляцією BPSK і кодуванням: 1 – LDPC; 2 – турбо;
3 – полярним

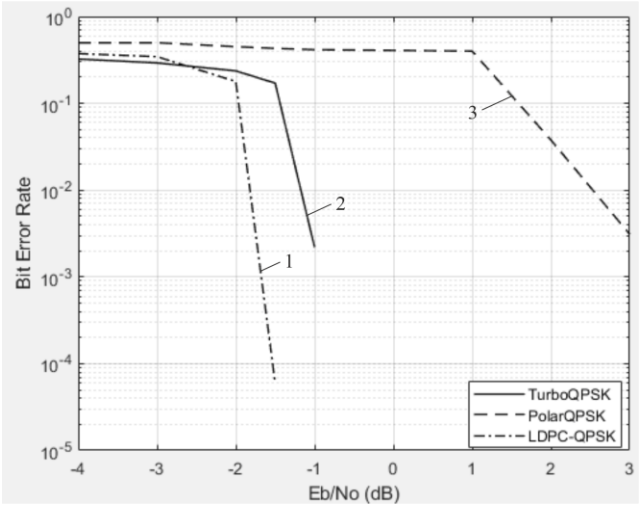

Рис. 19. Залежність кількості бітових помилок від відношення сигнал-шум для системи зв’язку з модуляцією QPSK і кодуванням: 1 – LDPC; 2 – турбо;
3 – полярним

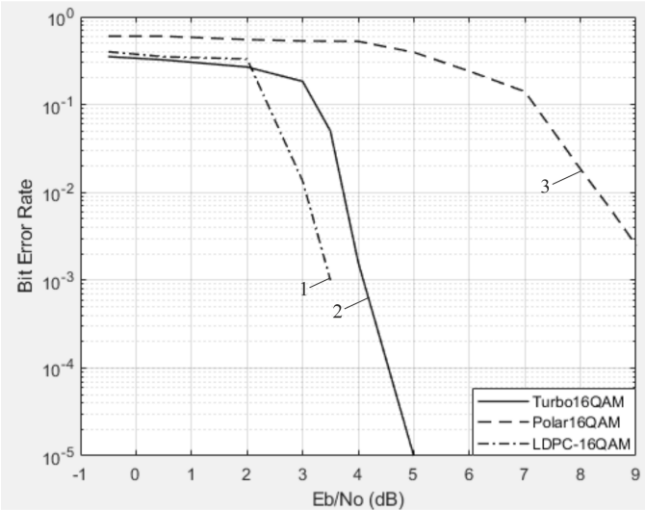

Рис. 20. Залежність кількості бітових помилок від відношення сигнал-шум для системи зв’язку з модуляцією 16-QAM і кодуванням: 1 – LDPC; 2 – турбо;
3 – полярним

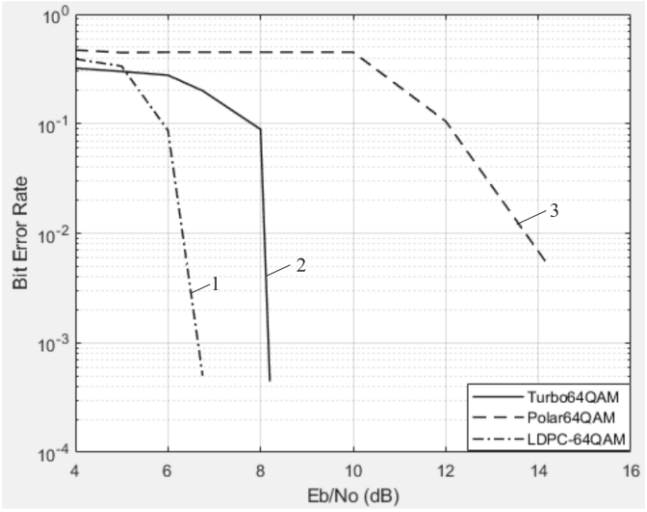

Рис. 21. Залежність кількості бітових помилок від відношення сигнал-шум для системи зв’язку з модуляцією 64-QAM і кодуванням: 1 – LDPC; 2 – турбо; 3 – полярним

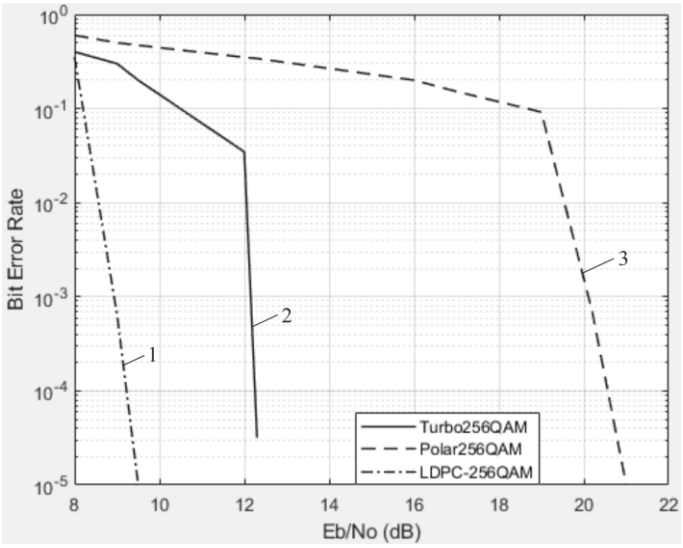

Рис. 22. Залежність кількості бітових помилок від відношення сигнал-шум для системи зв’язку з модуляцією 256-QAM і кодуванням: 1 – LDPC; 2 – турбо; 3 – полярним

- полярний код: довжина інформаційного блоку K= 132 біт; узгоджена за швидкістю довжина коду на виході E = 256 біт; кодова швидкість R = 0,5;
- LDPC код: коефіцієнт розширення liftingSize = 144; базовий граф bgn = 1; довжина блоку frameLen = 1440 біт;
- турбо код: кодова швидкість R = 1/3; довжина блоку 6144 біт.

Висновки

Проведені дослідження HDL реалізацій кодерів і декодерів полярного, LDPC і турбо кодів.

Проведені дослідження енергетичної ефективності для систем зв’язку з наступними параметрами: турбо кодер – кодова швидкість R = 1/3; довжина блоку 6144 біт, турбо декодер має 8 ітерацій; LDPC кодер – коефіцієнт розширення liftingSize = 144; базовий граф bgn = 1; довжина блоку frameLen = 1440 біт, LDPC декодер має 16 ітерацій; полярний кодер – довжина інформаційного блоку K= 132 біт; узгоджена за швидкістю довжина коду на виході E = 256 біт; кодова швидкість R = 0,5, полярний декодер має розмір списку 8.

За ресурсами FPGA, потрібними для реалізації, найменш вимогливі турбо кодер і полярний кодер. При цьому полярний код з короткою довжиною має найменший енергетичний виграш кодування (ЕВК). Турбо код з довжиною блоку 6144 біт ефективніше полярного коду з довжиною блоку 132 біт на 3,5 дБ для модуляції BPSK і на 8 дБ для модуляції 256-QAM. LDPC декодер вимагає в 20 разів більше ресурсів FPGA ніж полярний декодер і в 15 разів більше ніж турбо декодер і має найкращий ЕВК, що збільшується при великій позиційності модуляції.

Література

1. Пятін І.С., Бойко Ю.М. Методика полярного кодування в 5G мобільних засобах телекомунікацій з багатопозиційною модуляцією. *Вимірювальна та обчислювальна техніка в технологічних процесах*, 2020. №1. С.67-76.

2. Бойко Ю. М., Дружинін В. А., Толюпа С. В. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія. Київ : Логос, 2018. 227 с.

3. Bioglio V., Condo C., Land I. Design of Polar Codes in 5G New Radio. *IEEE Communications Surveys & Tutorials*, 2020. P. 1.

4. Kaykac Egilmez Z. B., Xiang L., Maunder R. G., Hanzo L. The Development Operation and Performance of the 5G Polar Codes. *IEEE Communications Surveys & Tutorials*, 2020. Vol. 22, No. 1, P. 96-122.

5. Пятін І. С. Бойко Ю.М. Дослідження енергетичної ефективності канального кодування даних користувача кодами LDPC для систем зв'язку 5G. *Вісник Хмельницького національного університету. Технічні науки*, 2020. №3. С. 174-185.

6. Tahir B., Schwarz S., Rupp M. *BER comparison between Convolutional, Turbo, LDPC, and Polar codes*: 2017 24th International Conference on Telecommunications (ICT), Limassol 3-5 May 2017, Limassol, 2017. P. 1-7.

7. Boiko J., Pyatin I., Eromenko O., Stepanov M. Method of the adaptive decoding of self-orthogonal codes in telecommunication. *Indonesian Journal of Electrical Engineering and Computer Science*, 2020. Vol 19, No. 3. P. 1287-1296.

8. Berkman L., Turovsky O., Kyrpach L., Varfolomeeva O., Dmytrenko V., Pokotylo O. Analyzing the code structures of multidimensional signals for a continuous information transmission channel. *Eastern-European Journal of Enterprise Technologies*, 2021. vol. 5., No. 9. P. 70-82.

9. Пятін І. С., Бойко Ю. М. *Адаптивне управління формою сигнально-кодової конструкції у телекомунікаційному каналі з полярними кодами*: збірник тез та доповідей XV Міжнар. конф., Контроль і управління в складних системах (КУСС-2020), м. Вінниця, 8-10 жовтня 2020 р. Вінниця, ВНТУ, 2020. С. 82-84.

10. Berkman L., Tkachenko O., Turovsky O., Fokin V., Strelnikov V. Designing a system to synchronize the input signal in a telecommunication network under the condition for reducing a transitional component of the phase error. *Eastern-European Journal of Enterprise Technologies*, 2021. Vol. 1, No. 9(109). P.66-76.

11. Boiko J., Pyatin I., Eromenko O. *Simulation of the Transport Channel with Polar Codes for the 5G Mobile Communication*: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T'2020), Kharkiv 6-9 October 2020, Kharkiv, 2020. P. 182-186.

12. Бойко Ю.М., Пятін І.С. Моделі систем завадостійкого кодування у телекомунікаціях. *Вісник Хмельницького національного університету*, 2020. №4. С. 174-183.

13. Boiko J., Pyatin I., Chornyi R., Davydova T. *Design and Performance Evaluation of Channel Coding Schemes for Information Technologies*: 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv 15-17 Dec. 2021, Kyiv, 2021. P. 195-200.

14. Семенко А.І., Кушнір М. Я., Бокла Н. І. Синтез широкосмугової телекомункацйної системи з підвищеною конфіденційністю передачі інформації шляхом використання псевдовипадкових послідовностей на основі хаосу. *Вісник університету «Україна». Серія: інформатика, обчислювальна техніка та кібернетика*, 2020. №1(24). С .65-75.

References

1. Piatin I.S., Boiko J.M. Polar coding technique in 5G mobile telecommunications with multi-position modulation. *Measuring and computing devices in technological processes*, 2020. №1. S.67-76.

2. Boiko J. M. Druzhynin V. A., Toliupa S. V. Teoretychni aspekty pidvyshchennia zavadostiikosti y efektyvnosti obrobky syhnaliv v radiotekhnichnykh prystroiakh ta zasobakh telekomunikatsiinykh system za naiavnosti zavad : monohrafiia. Kyiv : Lohos, 2018. 227 s.

3. Bioglio V., Condo C., Land I. Design of Polar Codes in 5G New Radio. *IEEE Communications Surveys & Tutorials*, 2020. P. 1.

4. Kaykac Egilmez Z. B., Xiang L., Maunder R. G., Hanzo L. The Development Operation and Performance of the 5G Polar Codes. *IEEE Communications Surveys & Tutorials*, 2020. Vol. 22, No. 1, P. 96-122.

5. Piatin I. S., Boiko J. M. Investigation of energy efficiency of channel coding of user data by LDPC codes for 5G communication systems. *Herald of Khmelnytskyi National University. Tekhnichni nauky*, 2020. №3. S. 174-185.

6. Tahir B., Schwarz S., Rupp M. *BER comparison between Convolutional, Turbo, LDPC, and Polar codes*: 2017 24th International Conference on Telecommunications (ICT), Limassol 3-5 May 2017, Limassol, 2017. P. 1-7.

7. Boiko J., Pyatin I., Eromenko O., Stepanov M. Method of the adaptive decoding of self-orthogonal codes in telecommunication. *Indonesian Journal of Electrical Engineering and Computer Science*, 2020. Vol 19, No. 3. P. 1287-1296.

8. Berkman L., Turovsky O., Kyrpach L., Varfolomeeva O., Dmytrenko V., Pokotylo O. Analyzing the code structures of multidimensional signals for a continuous information transmission channel. *Eastern-European Journal of Enterprise Technologies*, 2021. vol. 5., No. 9. P. 70-82.

9. Piatin I. S., Boiko J. M. *Adaptyvne upravlinnia formoiu syhnalno-kodovoi konstruktsii u telekomunikatsiinomu kanali z poliarnymy kodamy*: zbirnyk tez ta dopovidei XV Mizhnar. konf., Kontrol i upravlinnia v skladnykh systemakh (KUSS-2020), m. Vinnytsia, 8-10 zhovtnia 2020 r. Vinnytsia, VNTU, 2020. S. 82-84.

10. Berkman L., Tkachenko O., Turovsky O., Fokin V., Strelnikov V. Designing a system to synchronize the input signal in a telecommunication network under the condition for reducing a transitional component of the phase error. *Eastern-European Journal of Enterprise Technologies*, 2021. Vol. 1, No. 9(109). P.66-76.

11. Boiko J., Pyatin I., Eromenko O. *Simulation of the Transport Channel with Polar Codes for the 5G Mobile Communication*: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T'2020), Kharkiv 6-9 October 2020, Kharkiv, 2020. P. 182-186.

12. Boiko J. M., Piatin I.S. Models of noiseless coding systems in telecommunications. *Herald of Khmelnytskyi National University. Technical sciences*, 2020. №4. S. 174-183.

13. Boiko J., Pyatin I., Chornyi R., Davydova T. *Design and Performance Evaluation of Channel Coding Schemes for Information Technologies*: 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv 15-17 Dec. 2021, Kyiv, 2021. P. 195-200.

14. Semenko A.I., Kushnir M. Y., Bokla N.I. Syntez shyrokosmuhovoi telekomunkatsinoi systemy z pidvyshchenoiu konfidentsiinistiu peredachi informatsii shliakhom vykorystannia psevdovypadkovykh poslidovnostei na osnovi khaosu. *Visnyk universytetu «Ukraina». Seriia: informatyka, obchysliuvalna tekhnika ta kibernetyka*, 2020. №1(24). S .65-75.