

УДК 681.5

doi:10.20998/2413-4295.2025.01.06

**АНАЛІЗ СПЕКТРАЛЬНИХ МЕТОДІВ ОБРОБКИ КОДОВИХ ПОСЛІДОВНОСТЕЙ В ЦИФРОВИХ КАНАЛАХ ЗВ'ЯЗКУ****В. А. КРИЛОВА\*, Р. О. КОТКО***Автоматика та управління в технічних системах, НТУ «ХПІ», м. Харків, УКРАЇНА**\*e-mail: vika\_hpi@outlook.com*

**АНОТАЦІЯ** Розглядаються класичний алгоритм Герцеля обчислення прямого та зворотнього дискретного перетворення Фур'є для елементів кінцевого поля  $GF(2^m)$ , а також його модифікація. Показано, що модифікований алгоритм знаходження позицій помилок в кодовій послідовності належить скоріше до класу швидких алгоритмів обчислення дискретного перетворення Фур'є, ніж до класу напівшвидких. Проведено аналіз існуючих методів декодування кодових послідовностей циклічних двійкових кодів, що дозволяють визначити та виправити помилки, які виникають у результаті дії зовнішніх завад. Представлено для оцінки ефективності роботи засоби обчислення поліному локаторів помилок в часовій та в спектральній області. Визначено основні переваги спектрального підходу, що дає можливість використання прямого перетворення Фур'є у кінцевих полях Галуа. Показано, що декодування БЧХ-кодів у спектральній області з використанням перетворення Фур'є для знаходження помилок та виправлення кодових слів значно пришвидшує декодування, особливо для довгих кодів. Розглянуто метод обчислення спектральних компонент з визначенням вектору синдрому за допомогою поліному залишку від ділення на мінімальний многочлен. Алгоритм дає можливість отримати значення многочлена в усіх точках кінцевого поля Галуа за меншу кількість операцій додавання та множення, за рахунок того що поліном залишку обчислюється один раз для кожного сполученого класу. Запропоновано алгоритм знаходження  $n-2t$  спектральних компонент вектора помилок через відомі  $t$  коефіцієнтів поліному локаторів помилок та відомі  $2t$  синдромних компонент, обчислених на першому етапі декодування. Підтверджено, що запропонований спектральний метод декодування БЧХ-кодів базується на використанні швидкого перетворення Фур'є у полях Галуа дозволяє прискорити обчислення синдромів та знаходження поліному локаторів помилок без ітерацій, а саме використовуючи перетворення Фур'є замість алгоритму Берлекемпа-Мессі.

**Ключові слова** канал зв'язку; спектр сигналу; перетворення Фур'є, параметри кодера; декодування завадостійких кодів, поля Галуа.

**ANALYSIS OF SPECTRAL METHODS FOR PROCESSING CODE SEQUENCES IN DIGITAL COMMUNICATION CHANNELS****V. KRYLOVA\*, R. KOTKO***Department of Automation and Control in Technical Systems, NTU "KhPI", Kharkiv, UKRAINE*

**ABSTRACT** The classical Herzel algorithm for calculating the forward and inverse discrete Fourier transform for elements of the finite field  $GF(2^m)$  is considered, as well as its modification. It is shown that the modified algorithm for finding error positions in a code sequence belongs to the class of fast algorithms for calculating the discrete Fourier transform rather than to the class of semi-fast ones. An analysis of existing methods for decoding code sequences of cyclic binary codes is carried out, which allow to identify and correct errors that arise as a result of the action of external interference. Means for calculating the polynomial of error locators in the time and spectral domains are presented to assess the efficiency of the work. The main advantages of the spectral approach are determined, which makes it possible to use the forward Fourier transform in finite Galois fields. It is shown that decoding BCH codes in the spectral domain using the Fourier transform for finding errors and correcting codewords significantly speeds up decoding, especially for long codes. A method for calculating spectral components with the definition of the syndrome vector using the polynomial of the remainder from division by the minimal polynomial is considered. The algorithm makes it possible to obtain the value of the polynomial at all points of the finite Galois field for a smaller number of addition and multiplication operations, due to the fact that the remainder polynomial is calculated once for each connected class. An algorithm for finding  $n-2t$  spectral components of the error vector through the known  $t$  coefficients of the polynomial of error locators and the known  $2t$  syndrome components calculated at the first stage of decoding is proposed. It is confirmed that the proposed spectral method for decoding BCH codes based on the use of the fast Fourier transform in Galois fields allows to speed up the calculation of syndromes and finding the polynomial of error locators without iterations, namely, using the Fourier transform instead of the Berlekamp-Massey algorithm.

**Keywords:** communication channel; signal spectrum; Fourier transform, encoder parameters; decoding of noise-resistant codes, Galois fields

**Вступ**

В сучасних телекомунікаційних мережах мережах супутниковий зв'язок відіграє важливу роль

у глобальних комунікаціях, особливо там, де немає можливості використовувати наземну інфраструктуру (океан, пустеля, гори). Він застосовується в телекомунікаціях, GPS, телебаченні, військових і

наукових місіях. В системах обробки та передачі даних головною вимогою до телекомунікаційних мереж є стабільний та надійний зв'язок з високою ступеню достовірності. Швидкість та якість передачі даних повинна відповідати потребам користувачів, а саме забезпечувати низький рівень затримок (latency), особливо для реального часу (онлайн-дзвінки, відеоконференції, VoIP). Головною вимогою до каналів зв'язку є стійкість до перешкод, в наслідок яких інформація що передається може бути спотворена [1]. В наслідок використання супутникового зв'язку в складних умовах (дощ, сніг, сонячна активність) питання захисту сигналу від перешкод є особливо актуальним.

В супутникових мережах використовується технологія Adaptive Coding and Modulation (ACM) – адаптивна кодомодуляція, яка динамічно змінює параметри модуляції та кодовий швидкість залежно від умов роботи каналу зв'язку. Основні етапи функціонування ACM технології [2].

1. Моніторинг якості каналу – система вимірює рівень сигналу, завади, затримки та інші параметри..

2. Вибір оптимальної модуляції – якщо канал чистий, використовується складніша модуляція для більшої швидкості (16-QAM, 64-QAM). Якщо є перешкоди, вибирається простіша модуляція (QPSK, BPSK).

3. Зміна кодування (FEC – Forward Error Correction) – якщо сигнал слабкий, збільшується рівень корекції помилок.

Адаптивна модуляція та кодування (ACM) – це одна з ключових технологій Starlink, яка допомагає підтримувати стабільний зв'язок, навіть при складних умовах. Завдяки ACM, Starlink може гнучко змінювати параметри передачі, забезпечуючи високу швидкість, низьку затримку та ефективність використання спектру [3,4]. Адаптивна модуляція та кодування дозволяє збільшити швидкість зв'язку та зменшити втрати даних у супутникових мережах. В ACM системах для виявлення та виправлення помилок використовують коди Ріда-Соломона (Reed-Solomon Codes) та БЧХ коди які разом з LDPC використовуються для виправлення перш за все пакетних помилок. Вони забезпечують захист від втрати пакетів, радіоперешкод і космічного випромінювання [5,6]. І хоча коди Ріда-Соломона (RS) є потужним методом виправлення помилок у GPS, вони мають певні обмеження та недоліки, які можуть впливати на продуктивність та ефективність системи. В наслідок того що RS-коди базуються на алгебраїчних операціях у полях Галуа вони є обчислювально складними. Декодування потребує матриць обернень та інших складних операцій. Це може бути вузьким місцем для енергоспоживання мобільних пристроїв та вбудованих GPS-чипів. Якщо сигнал ослаблений через погодні умови або багатопроменеve поширення, RS-коди можуть не виправити всі помилки, тому що високе

обчислювальне навантаження та складні алгоритми неефективні для слабких процесорів [7].

Так як при кодуванні та декодуванні БЧХ та RS-кодів використовується арифметика полів Галуа обчислювальні процедури потребують складних та надмірних алгебраїчних операцій, що значно ускладнюють процес передачі кодових послідовностей. Тому сучасні алгоритми БЧХ, RS-кодів потребують оптимізації з точки зору складності обчислювальних операцій.

### Мета роботи

Метою роботи є проведення аналізу засобів та алгоритмів захисту інформації від помилок в цифрових каналах зв'язку, порівняння спектральних та часових методів декодування кодових послідовностей циклічних кодів з елементами поля Галуа, опис прискореного алгоритму обчислення спектральних компонент сіндромного вектору та знаходження поліному локаторів помилок з фіксацією позицій помилок.

### Виклад основного матеріалу

БЧХ коди задаються своїми параметрами:  $n$  – довжина кода,  $t$  – кількість помилок, які здатен виправити код, породжуючий поліном  $g(x)$ , що задається коренями  $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+2t-1}$  – елементи кінцевого поля  $GF(2^m)$  [1]

$$g(x) = \prod_{i=b}^{b+2t-1} (x + \alpha^i). \quad (1)$$

При отриманні інформаційної послідовності  $u(x) = u_{k-1}x^{k-1} + u_{k-2}x^{k-2} + \dots + u_1x^1 + u_0$  з коефіцієнтами, що належать полю  $GF(2^m)$   $\{u_i \in GF(2^m)\}$  кодовий RS пристрій виконує кодування за допомогою породжуючого поліному  $g(x)$  за наступним алгоритмом [2,8]

$$R(x) = u(x) \cdot x^r \bmod (g(x)). \quad (2)$$

Тоді закодована послідовність систематичного коду представляє коефіцієнти деякого полінома  $v(x)$ , обчислюваного як сума зрушеного на  $r$  позицій вліво інформаційного полінома та полінома залишку  $R(x)$  [3]

$$v(x) = u(x) \cdot x^r + R(x). \quad (3)$$

При передачі кодового слова по каналу зв'язку або при зберіганні даних на носії інформація може бути спотворена в силу дії шумів у каналі передачі даних або пошкодження носія даних. У такому випадку можна говорити, що на кодову послідовність буде накладено деяке спотворення  $e(x)$  і поліном  $v(x)$  в результаті матимемо поліном спотвореного кадру  $f(x) = v(x) + e(x)$ . При цьому можуть спотворюватися

будь-які коефіцієнти кодового полінома як інформаційні, так і надлишкові.

При декодуванні кодів Боуза-Чоудхурі-Хоквінгема (БЧХ-кодів) найскладнішим етапом з обчислювальної точки зору є розв'язання системи алгебраїчних рівнянь для знаходження позицій помилок. Цей етап включає [9]:

1. обчислення синдромів помилок та визначення синдрому поліному  $S(x)$ ,
2. розв'язання ключового рівняння та формування поліному локаторів помилок  $\sigma(x)$ ,
3. знаходження корнів поліному локаторів помилок (найскладніший етап)
4. обчислення значення та позиції помилок в кодовій послідовності.

Як відомо ці етапи можна виконати як за різними методами – в часовій (класичні алгоритми, наприклад, Берлекемпа-Мессі, Чорлецького) та і в спектральній області (з використанням перетворення Фур'є в полях Галуа – FFT) [10]. В табл. 1 надано порівняння за основним критеріями цих методів.

Таблиця 1 – Порівняння засобів декодування БЧХ кодів

| Критерій                                      | Часова область                                   | Спектральна область                                          |
|-----------------------------------------------|--------------------------------------------------|--------------------------------------------------------------|
| Обчислювальна складність                      | $O(t^2)$ , де $t$ – кількість помилок            | $O(n \log n)$ , де $n$ – довжина коду                        |
| Ефективність для коротких кодів ( $n < 100$ ) | Висока (швидкий алгоритм)                        | Малоефективна через накладні витрати FFT                     |
| Ефективність для довгих кодів ( $n > 255$ )   | Неоптимальна, складність $O(t^2)$ швидко зростає | Дуже ефективна, працює в $O(n \log n)$                       |
| Апаратна реалізація                           | Просте апаратне виконання                        | Потребує швидкого перетворення Фур'є                         |
| Гнучкість                                     | Добре працює навіть при малих $t$                | Ефективна тільки при великих $n$ і великій кількості помилок |
| Залежність від розміру поля $GF(2^m)$         | Складність зростає при великих $m$               | Добре підходить для великих полів                            |
| Застосування                                  | Класичні БЧХ-коди, компактні пристрої            | Довгі кодові слова, швидкісні канали                         |

Для коротких БЧХ кодів ((63,51), (127,99)) краще використовувати метод Берлекемпа-Мессі, оскільки FFT не дає вигоди для малих  $n$ . Для довгих БЧХ кодів ((255,223), (1023,973)) спектральний метод із FFT суттєво зменшує обчислювальні витрати (з  $O(t^2)$  до  $O(n \log n)$ ). Якщо потрібно швидке апаратне декодування, то методи спектральної області можуть

бути ефективнішими, якщо реалізоване FFT у  $GF(2^m)$ . Таким чином, більш перспективним є метод декодування БЧХ кодів на базі спектральних обчислень [11]. Отже для знаходження основних компонент спектру через дискретне перетворення Фур'є довжини  $n$  вектора  $f=(f_i)$ ,  $i \in [0, n-1]$  необхідно обчислити вектор  $F = (F_j)$  [12,13]

$$F_j = f(\alpha^j) = \sum_{i=0}^{n-1} f_i \alpha^{ij}, \quad j \in [0, n-1], \quad (4)$$

де  $\alpha$  – елемент поля  $GF(2^m)$ .

Для малих значень  $n$  як ми бачимо з табл. 1 FFT є мало ефективним, адже не дають суттєвого вибору, оскільки їхні переваги проявляються лише при великих  $n$ , але при цьому процес декодування потребує складних обчислень з операціями додавання та множення  $n^2$  і при великих значеннях  $n$  воно стає не ефективним з точки зору швидкості та якості. Таким чином, в системах з довгими кодами швидкість обчислення може бути збільшена, якщо використовувати швидкі алгоритми перетворення Фур'є. Одним з таких представників є алгоритм Герцеля, що використовує мінімальні многочлени  $\phi_i(x)$  поля  $GF(2^m)$  [14,15].

Елементи з розширеного поля  $GF(2^m)$   $\alpha^i, \alpha^{2i}, \alpha^{4i}, \dots, \alpha^t$ , які є корінням одного і того ж самого многочлена над  $GF(2)$  є сполученими. Ступені сполучених елементів поля утворюють циклотомічні суміжні класи [16]

$$C_i = \{i, 2i, 2^2i, 2^3i, \dots, 2^k i\},$$

де  $i$  – ступень елемента розширеного поля  $GF(2^m)$ .

Двійковий поліном найменшого ступеня, для якого елемент  $\alpha^i$  з розширеного кінцевого поля  $GF(2^m)$  є коренем є мінімальним многочленом  $\phi_i(x)$ . При цьому ступінь мінімального многочлена дорівнює числу елементів відповідного циклотомічного класу. Тоді многочлен  $\phi_i(x)$  за допомогою його коренів може бути представлений [17].

$$\phi_s(x) = \prod_{i \in C_s} (x + \alpha^i). \quad (5)$$

Отже, компоненти спектру  $F_j$  можуть бути знайдені за два етапи:

1. Обчислити залишки від ділення поліному  $f(x)$  на мінімальний многочлен кожного циклотомічного класу [18]

$$r(x) = f(x) \bmod \phi_i(x), \quad (6)$$

де  $\deg r(x) < \deg \phi_i(x)$ ,  $r_k(x) = \sum_{j=0}^{m_k-1} r_{j,k} x^j$ ,  $k = 0, 1, \dots, l$ ,  $l$  – кількість сполучених класів.

Таким чином, для  $l$  циклотомічних класів ми отримаємо поліноми виду

$$\begin{aligned} r_0(x) &= r_{0,0} + r_{1,1}x^1 + \dots + r_{m_0-1,1}x^{m_0-1} \\ r_1(x) &= r_{0,1} + r_{1,1}x^1 + \dots + r_{m_1-1,1}x^{m_1-1} \\ r_2(x) &= r_{0,2} + r_{1,2}x^1 + \dots + r_{m_2-1,1}x^{m_2-1} \end{aligned}$$

$$r_{l-1}(x) = r_{0,l-1} + r_{1,l-1}x^1 + \dots + r_{m_{l-1}-1,l-1}x^{m_{l-1}-1}$$

2. Обчислити значення поліному залишку  $r_k(x)$  в усіх значеннях елементів кінцевого поля  $GF(2^m)$

$$F_i = r_k(\alpha^i) = \sum_{j=0}^{m_k-1} r_{j,k} \alpha^{ij}, \quad i \in [0, n-1]. \quad (7)$$

де  $\alpha^i$  – корінь мінімального многочлена  $\varphi_i(x)$ .

Знаходження синдромних компонентів  $S_j$  в спектральній області за представленим алгоритмом дає можливість далі обчислити вектор помилок на частотах  $j = 1, 2, \dots, 2t$

$$S_j = E_j, \quad j = 1, 2, \dots, 2t. \quad (8)$$

Якщо перші  $2t$  спектральних компонент вектору помилок визначені через синдромні коефіцієнти  $E_0 = S_1, E_1 = S_2, \dots, E_{2t-1} = S_{2t}$ , то інші  $n-2t$  невідомих компонент вектору  $E$  можна знайти за допомогою коефіцієнтів  $\Delta_1, \Delta_2, \dots, \Delta_t$  за формулою

$$E_k = -\sum_{j=1}^t \Delta_j E_{k-j}, \quad k = 2t, \dots, n-1. \quad (9)$$

Таким чином, можна визначити всі значення вектора в частотній області  $E_i = \{E_0, E_1, \dots, E_{n-1}\}$ . Далі для знаходження поліному помилок  $e(x)$  в часовій області необхідно обчислити вектор помилок  $e_i = \{e_0, e_1, \dots, e_{n-1}\}$  як зворотне перетворення Фур'є за формулою

$$e_j = \frac{1}{n} \sum_{i=0}^{n-1} E_i \alpha^{-ij}. \quad (10)$$

Тоді процедура декодування завершується правильно, якщо фактичне число помилок не перевищує виправну здатність коду.

Алгоритм декодування БЧХ кодів в частотній області із застосуванням дискретного перетворення Фур'є та формули Герцеля.

1. Формування кодового слова з помилками для процесу декодування.
2. Обчислення та знаходження  $2t$  компонент синдрому алгоритмом Герцеля.
3. Обчислення ключового рівняння та знаходження  $t$  коефіцієнтів поліному локаторів помилок  $\Delta_1, \Delta_2, \dots, \Delta_t$  методом Берлекемпа-Мессі.
4. Знаходження інших  $n-2t$  компонент синдрому через рекурентну схему та отримання вектору помилок в частотній області  $E_i = \{E_0, E_1, \dots, E_{n-1}\}$ .
5. Виконання зворотнього перетворення Фур'є для компонент вектору помилок та отримання значень коефіцієнтів многочлена помилок в часовій області.

Алгоритм дає можливість отримати значення многочлена в усіх точках кінцевого поля Галуа за меншу кількість операцій додавання та множення.

### Обговорення результатів

Розглянемо кінцеве поле  $GF(2^3)$  з примітивним поліномом  $p(x) = x^3 + x + 1$ , що має три циклотомічних класів з відповідними сполученими елементами та мінімальними многочленами (табл.2). Припустимо що кодовий вектор має ступінь 6  $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$  для коду з параметрами  $(7, 4, 3)$ .

Таблиця 2 – Мінімальні поліноми поля  $GF(2^3)$

| Циклотомічні класи $C_s$ | Сполучені елементи.            | Мінімальний многочлен          |
|--------------------------|--------------------------------|--------------------------------|
| $C_0 = \{0\}$            | 1                              | $\varphi_0(x) = x + 1$         |
| $C_1 = \{1, 2, 4\}$      | $\alpha, \alpha^2, \alpha^4$   | $\varphi_1(x) = x^3 + x + 1$   |
| $C_3 = \{3, 6, 5\}$      | $\alpha^3, \alpha^6, \alpha^5$ | $\varphi_2(x) = x^3 + x^2 + 1$ |

Обчислимо синдромні компоненти в частотній області через поліноми залишків  $r_0(x), r_1(x), r_2(x)$  ступінь яких складає  $\deg r_0(x) = 0, \deg r_1(x) = 2, \deg r_2(x) = 2$ . скориставшись схемою ділення поліномів з залишком.

На рис. 1 представлено за допомогою регістрів зсуву схема ділення многочлена  $f(x)$ , коефіцієнти якого є  $\{f_0, f_1, f_2, f_3, f_4, f_5, f_6\}$  на мінімальний многочлен  $\varphi_1(x) = x^3 + x + 1$ .

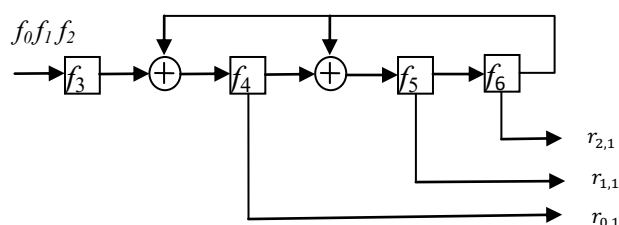


Рис. 1 – Схема ділення поліному  $f(x)$  на мінімальний многочлен  $\varphi_1(x)$

Після проходження всіх двійкових коефіцієнтів  $\{f_0, f_1, f_2, f_3, f_4, f_5, f_6\}$  полінома  $f(x)$  через регістр зсуву на виходах отримаємо алгоритм для формування відповідних коефіцієнтів поліному  $r_1(x)$  (рис. 2).

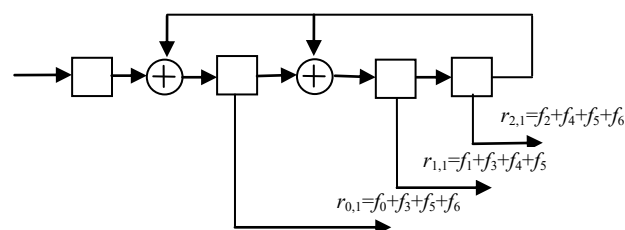


Рис. 2 – Формування коефіцієнтів полінома  $r_1(x)$

Використовуючи запропонований метод знаходження залишків від ділення через схему регістру зсуву, знайдемо алгоритм формування коефіцієнтів полінома  $r_2(x)$  як залишок від ділення многочлена  $f(x)$  на мінімальний поліном  $\varphi_2(x) = x^3 + x^2 + 1$  (рис. 3).

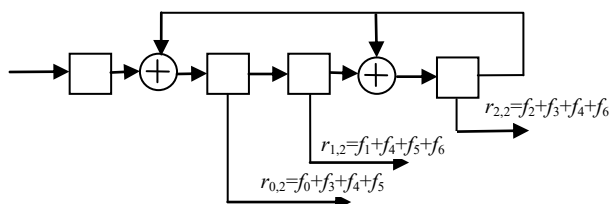


Рис. 3 – Формування коефіцієнтів полінома  $r_2(x)$

Таким чином, спектральні компоненти спектру для елементів сполученого класу  $\alpha$ ,  $\alpha^2$ ,  $\alpha^4$  в загальному вигляді можна знайти через добуток матриці коефіцієнтів кодового поліному та вектора  $f(x)$ .

$$\begin{pmatrix} F_1 \\ F_2 \\ F_3 \end{pmatrix} = \begin{bmatrix} 1 & \alpha^1 & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \\ 1 & \alpha^4 & \alpha^2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \end{bmatrix}$$

Після отримання синдромних компонент в спектральній області  $S_j = F_j$  за формулою (8), (9) можна обчислити спектральні компоненти вектору помилок для подальшого знаходження позицій помилок в часовій області. Таким чином, запропонований алгоритм дає складність порядку  $\frac{1}{2}n \log n$  операцій множення та порядку  $n^2$  операцій додавання над елементами поля  $GF(2^m)$ .

### Висновки

Для знаходження спектральних компонент в усіх точках кінцевого поля Галуа необхідно знайти залишок від ділення на мінімальний многочлен поля для кожного циклотомічного класу та обчислити значення отриманого залишку в точці  $\alpha^i$ . Оскільки всі елементи поля Галуа діляться на сполучені класи, кожен з яких має свій мінімальний многочлен і відповідно загальний залишок від ділення, тому достатньо обчислити один раз цей залишок для всього класу сполучених елементів. Якщо вхідний вектор належить кінцевому полю  $GF(2)$  то його перетворення Фур'є може бути обчислено без множення в полі  $GF(2^m)$ , так як розрахунок спектральних компонентів зводиться до множення елементів з поля  $GF(2)$  на елементи з  $GF(2^m)$ . Таким чином, для двійкового кода синдром обчислюється без множення в полі  $GF(2^m)$  не більш ніж з  $n \log n$  додавання в  $GF(2)$  та не більш ніж з  $\log n$  додавання в  $GF(2^m)$ .

### Список літератури

1. Blahut Richard E. *Algebraic Codes for Data Transmission*. Cambridge: Cambridge University Press, 2003. 482 p.
2. Lin S., Costello D. J. *Error control coding: fundamentals and applications*. Prentice-Hall Inc.: Printed in the United States of America, 2004. 624 p.
3. Bardet M., Dragoi V., Otmani A., and Tillich J.-P. Algebraic Properties of Polar Codes from a New Polynomial Formalism. *Proceedings of IEEE International Symposium on Information Theory*. Barcelona, Spain, 2016. P. 230-234. doi: 10.1109/ISIT.2016.7541295.
4. Blahut R. E. *Algebraic Codes on Lines, Planes, and Curves: An Engineering Approach*. United Kingdom: Cambridge University Press, 2008. doi: 10.1017/CBO9780511543401.
5. Wu Y. New List Decoding Algorithms for Reed-Solomon and BCH Codes. *IEEE Transactions on Information Theory*. 2007. Vol. 54, Issue 8. P. 2806-2810. doi: 10.48550/arXiv.cs/0703105.
6. Wu Y. Fast Chase Decoding Algorithms and Architectures for Reed-Solomon Codes. *IEEE Transactions on Information Theory*. 2012. Vol. 58, Issue 1. P. 109-129. doi: 10.1109/TIT.2011.2165524.
7. Trifonov P. Efficient interpolation in the Guruswami-Sudan algorithm. *IEEE Transactions on Information Theory*. 2010. Vol. 56, Issue 9. P. 4341-4349. doi: 10.1109/TIT.2010.2053901.
8. Fedorenko S. V., Trifonov P. V. Finding roots of polynomials over finite fields. *IEEE Transactions on Communications*. 2002. Vol. 50, Issue 11. P. 1709-1711.
9. Fedorenko S. V., Trifonov P. V., Costa E. Improved hybrid algorithm for finding roots of error-locator polynomials. *European Transactions on Telecommunications*. 2003. Vol. 14, Issue 5. pp. 411-416.
10. Costa E., Fedorenko S., Trifonov P. Efficient algorithm for computing syndrome polynomial in Reed-Solomon decoder. *Proceedings of 5th International ITG Conference on Source and Channel Coding (SCC)*. 2004. Vol. 181. P. 179-183.
11. Freyman V. I. Research of the reed-solomon codes characteristic for realization within control systems devices. *Radio Electronics, Computer Science, Control*. 2019. Vol. 3. P. 143-151.
12. Fedorenko S. V. A spectral algorithm for decoding systematic BCH codes. *IEEE Access*. 2022. Vol. 10. P. 110639-110645. doi: 10.1109/ACCESS.2022.3215005.
13. Liang Z., Zhang W. Efficient Berlekamp-Massey Algorithm and Architecture for Reed-Solomon Decoder. *Journal of Signal Processing Systems*. 2017. Vol. 86, Issue 1. P. 51-65. doi: 10.1007/s11265-015-1094-1.
14. Almuzakkia M. Z., Oharac K. Computing general error locator polynomial of 3-error-correcting BCH codes via syndrome varieties using minimal polynomial. *ISCS Selected Papers*. 2015. P. 80-85.
15. Krylova V. A., Tverytnykova E. E., Vasylenkov O. G., Kolisnyk T. P. Modified algorithm for searching the roots of the error locators polynomial while decoding BCH codes. *Radio Electronics, Computer Science, Control*. 2020. Issue 3. P. 150-157. doi: 10.15588/1607-3274-2020-3-14.
16. Krylova V., Miroshnyk M., Korytchinko T., Demihev O. Practical methods for de Bruijn sequences generation using non-linear feedback shift registers. *14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine, 2018. P. 1157-1161. doi: 10.1109/TCSET.2018.8336400.
17. Gan C., Li C., Qian H. et al. On Bose distance of a class of

BCH codes with two types of designed distances. *Des. Codes Cryptogr.* 2024. Vol. 92. P. 2031–2053. doi:10.1007/s10623-024-01378-x.

18. Pang B., Zhu S., Yang T. et al. BCH codes with larger dimensional hull. *Des. Codes Cryptogr.* 2023. Vol. 91. P. 3933–3951. doi:10.1007/s10623-023-01281-x.

#### References (transliterated)

1. Blahut Richard E. *Algebraic Codes for Data Transmission*. Cambridge. Cambridge University Press, 2003. 482 p.
2. Lin S., Costello D. J. *Error control coding: fundamentals and applications*. Prentice-Hall Inc. Printed in the United States of America, 2004. 624 p.
3. Bardet M., Dragoi V., Otmani A., and Tillich J.-P. Algebraic Properties of Polar Codes from a New Polynomial Formalism. *Proceedings of IEEE International Symposium on Information Theory*. Barcelona, Spain, 2016, pp. 230–234, doi: 10.1109/ISIT.2016.7541295.
4. Blahut R. E. *Algebraic Codes on Lines, Planes, and Curves: An Engineering Approach*. United Kingdom. Cambridge University Press, 2008. doi: 10.1017/CBO9780511543401.
5. Wu Y. New List Decoding Algorithms for Reed-Solomon and BCH Codes. *IEEE Transactions on Information Theory*, 2007, vol. 54, Issue 8, pp. 2806–2810, doi: 10.48550/arXiv.cs/0703105.
6. Wu Y. Fast Chase Decoding Algorithms and Architectures for Reed-Solomon Codes. *IEEE Transactions on Information Theory*, 2012, vol. 58, Issue 1, pp. 109–129, doi: 10.1109/TIT.2011.2165524.
7. Trifonov P. Efficient interpolation in the Guruswami-Sudan algorithm. *IEEE Transactions on Information Theory*, 2010, vol. 56, Issue 9, pp. 4341–4349, doi: 10.1109/TIT.2010.2053901.
8. Fedorenko S. V., Trifonov P. V. Finding roots of polynomials over finite fields. *IEEE Transactions on Communications*, 2002, vol. 50, Issue 11, pp. 1709–1711.
9. Fedorenko S. V., Trifonov P.V., Costa E. Improved hybrid algorithm for finding roots of error-locator polynomials. *European Transactions on Telecommunications*, 2003, vol. 14, Issue 5, pp. 411–416.
10. Costa E., Fedorenko S., Trifonov P. Efficient algorithm for computing syndrome polynomial in Reed-Solomon decoder. *Proceedings of 5th International ITG Conference on Source and Channel Coding (SCC)*, 2004, vol. 181, pp. 179–183.
11. Freyman V. I. Research of the reed-solomon codes characteristic for realization within control systems devices, *Radio Electronics, Computer Science, Control*, 2019, vol. 3, pp. 143–151.
12. Fedorenko S. V. A spectral algorithm for decoding systematic BCH codes. *IEEE Access*, 2022, vol. 10, pp. 110639–110645, doi: 10.1109/ACCESS.2022.3215005.
13. Liang Z., Zhang W. Efficient Berlekamp-Massey Algorithm and Architecture for Reed-Solomon Decoder. *Journal of Signal Processing Systems*, 2017, vol. 86, Issue 1, pp. 51–65, doi: 10.1007/s11265-015-1094-1.
14. Almuzakkia M. Z., Oharac K. Computing general error locator polynomial of 3-error-correcting BCH codes via syndrome varieties using minimal polynomial. *ISCS Selected Papers*, 2015, pp. 80–85.
15. Krylova V. A., Tverytnykova E. E., Vasylenkov O. G., Kolisnyk T. P. Modified algorithm for searching the roots of the error locators polynomial while decoding BCH codes. *Radio Electronics, Computer Science, Control*, 2020, Issue 3, pp. 150–157, doi: 10.15588/1607-3274-2020-3-14.
16. Krylova V., Miroshnyk M., Korytchinko T., Demihev O. Practical methods for de Bruijn sequences generation using non-linear feedback shift registers. *14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine, 2018, pp. 1157–1161, doi: 10.1109/TCSET.2018.8336400.
17. Gan C., Li C., Qian H. et al. On Bose distance of a class of BCH codes with two types of designed distances. *Des. Codes Cryptogr.*, 2024, vol. 92, pp. 2031–2053, doi:10.1007/s10623-024-01378-x.
18. Pang B., Zhu S., Yang T. et al. BCH codes with larger dimensional hull. *Des. Codes Cryptogr.*, 2023, vol. 91, pp. 3933–3951, doi:10.1007/s10623-023-01281-x.

#### Відомості про авторів (About authors)

**Крилова Вікторія Анатоліївна** – кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри Автоматика та управління в технічних системах; м. Харків, Україна; ORCID: <https://orcid.org/0000-0002-4540-8670>; e-mail: vika\_hpi@outlook.com.

**Viktoriia Krylova** – candidate of technical sciences, associate professor “Department of Automation and Control in Technical Systems”, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv; e-mail: vika\_hpi@outlook.com.

**Котко Роман Олегович** – аспірант кафедри «Автоматика та управління в технічних системах», Національний технічний університет «Харківський політехнічний інститут», м. Харків; e-mail: roman.kotko@cit.khpi.edu.ua.

**Roman Kotko** – PhD student of the Department “Department of Automation and Control in Technical Systems”, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv; e-mail: roman.kotko@cit.khpi.edu.ua..

*Будь ласка, посилайтесь на цю статтю наступним чином:*

Крилова В. А., Котко Р. О. Аналіз спектральних методів обробки кодових послідовностей в цифрових каналах зв'язу. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях.* – Харків: НТУ «ХПІ». 2025. № 1 (23). С. 48–53. doi:10.20998/2413-4295.2025.01.06.

*Please cite this article as:*

Krylova V., Kotko R. Analysis of spectral methods for processing code sequences in digital communication channels. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology.* – Kharkiv: NTU "KhPI", 2025, no. 1(23), pp. 48–53, doi:10.20998/2413-4295.2025.01.06.

*Надійшла (received) 10.01.2025*

*Прийнята (accepted) 19.03.2025*