DOI 10.31891/2307-5732-2025-347-22
УДК 004.4

КРИЛОВА ВІКТОРІЯ
Національний технічний університет «Харківський політехнічний інститут»
https://orcid.org/0000-0002-4540-8670
e-mail: viktoriia.krylova@khpi.edu.ua
ВОЙТЮК ОЛЕГ
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0003-2254-8977
e-mail: bubmain25@gmail.com
ДМИТРО ПЛЕЧИСТИЙ
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0002-4803-159X
e-mail: kkn_pdd@ztu.edu.ua

ДЕКОДУВАННЯ ЗАВАДОСТІЙКИХ ЦИКЛІЧНИХ КОДІВ В СПЕКТРАЛЬНІЙ ОБЛАСТІ

Оцінка здатності коду фіксувати помилки та виправляти їх здійснюється не тільки за характеристиками швидкості та мінімальної кодової відстані, але і за здатністю побудови для нього швидкісних методів декодування з низькою обчислювальною складністю за рахунок зниження кількості арифметичних операцій. Існує багато способів декодування лінійного блокового БЧХ коду. Вибір того чи іншого методу декодування коду залежить не тільки від параметрів (довжина, мінімальна відстань), але і від того яка частина алгоритму реалізована апаратно, а яка програмно, та від необхідної швидкості і навіть вартості наявних блоків схеми. Тому розробка нових швидких алгоритмів декодування блокових БЧХ кодів, що дозволяють збільшите надійність передачі інформації є актуальною задачею. В роботі проведено аналіз існуючих методів декодування лінійних БЧХ кодів, наведена оцінка обчислювальної складності як частотних так і часових алгоритмів. Розглянуто спосіб вирішення ключового рівняння (одного з етапів декодування) та обчислення поліному помилок в спектральній області. Запропоновано алгоритм знаходження n–2t спектральних компонент вектора помилок через відомі t коефіцієнтів поліному локаторів помилок та відомі 2t сіндромних компонент, обчислених на першому етапі декодування. В основу метода покладено алгоритми, які основані на спектральних перетвореннях Фур`є, що дозволяє отримати прискорену процедуру декодування БЧХ кодів в спектральній області. В роботі наведено схема реалізації дискретного перетворення Фур`є для отримання значень вектора помилок, та подальшого знаходження позицій помилок через зворотне перетворення Фур`є.

Ключові слова: Спектральні методи, перетворення Фур`є, БЧХ коди, декодування завадостійких кодів, поля Галуа.

KRYLOVA VIKTORIIA
National Technical University «Kharkiv Polytechnic Institute»
VOITIUK OLEG
Zhytomyr Polytechnic State University
PLECHYSTYY DMYTRO
Zhytomyr Polytechnic State University

DECODING OF NOISE-RESISTANT CYCLIC CODES IN THE SPECTRAL DOMAIN

The ability of a code to detect errors and correct them is assessed not only by the characteristics of speed and minimum code distance but also by the inherent ability to build high-speed decoding methods for it with low computational complexity by reducing the number of arithmetic operations. There are many effective ways to decode a linear block BFR code. The choice of a particular code decoding method depends not only on the parameters (length, minimum distance), but also on which part of the algorithm is implemented in hardware and which in software, and on the required speed and even the cost of the available circuit blocks. In particular, optimizing the implementation of such algorithms in hardware requires careful consideration of processing power, energy consumption, and memory allocation as these factors directly influence the feasibility of deploying these methods in real-world applications. Therefore, the development of new fast algorithms for decoding block FFT codes that increase the reliability of information transmission is an urgent task. The paper analyzes the existing methods for decoding linear FFT codes and estimates the computational complexity of both frequency and time algorithms. These analyses are critical as they form the foundation for identifying opportunities to enhance performance and reduce delays, particularly in systems requiring high throughput and low latency. A method for solving the key equation (one of the decoding stages) and efficiently calculating the error polynomial in the spectral domain is considered. An algorithm is proposed for finding the n-2t spectral components of the error vector using the known t coefficients of the error locator polynomial and the known 2t syndrome components calculated at the first stage of decoding.

Keywords: Spectral methods, Fourier transform, FFT codes, decoding of noise-resistant codes, Galois fields.

Постановка проблеми у загальному вигляді та її зв’язок із важливими науковими чи практичними завданнями

Розвиток мікроелектроніки, створив можливість для реалізації складних високопродуктивних обчислювальних систем. Причому зі зростанням їх продуктивності зростають вимоги до швидкості та якості зв'язку між ними. Для ефективного функціонування подібних систем необхідно використовувати завадостійкі коди, які дозволяють підтримувати високу надійність передачі інформації. Цифрові канали зв’язку с завадами потребують ефективних методів кодування та декодування, що дозволяють фіксувати та виправляти помилки в кодовій послідовності. Використання циклічних кодів Боуза-Чоудхурі-

Хоквінгема (БЧХ) в системах зв'язку дозволяє значно спрости реалізацію операції кодування, але складність універсальних алгоритмів декодування БЧХ кодів в більшості випадків виявляється занадто високою для практичного використання. Як відомо БЧХ коди відносяться до класу циклічних, тому для них можуть застосовуватися алгоритми та методи кодування/декодування циклічних кодів. Проте сучасні ітераційні алгоритми з розв'язком системи лінійних рівнянь та використанням алгебраїчних операцій над елементами розширених кінцевих полів Галуа більш ефективні. Найвідомішими методами декодування циклічних БЧХ кодів є алгоритм Пітерсона-Гренстейна-Цирлера (ПГЦ), алгоритм Берлекемпа-Мессі (АБМ), алгоритм Евкліда (АЕ) [1].

Складність розв'язування системи лінійних рівнянь для метода ПГЦ зростає пропорційно кубу мінімальної кодової відстані d_{min}, у зв'язку з тим що процедура обчислення оберненої матриці є досить ресурсоємною, тому використання на практиці цього алгоритму обмежується низьким значенням d_{min}. Зрозуміло, що кількість помилок, які можуть бути виправлені за допомогою цього метода не перевищує $\lfloor t - 1/2 \rfloor$. Якщо справжня мінімальна відстань перевищує t, то є принципово можливим виправлення більшого числа помилок. Кількість операцій, які виконуються під час знаходження оберненої матриці для алгоритму ПГЦ у випадку реалізації методом Гаусса складає $O(\omega^3)$, що робить його найбільш трудомістким етапом декодування. З точки зору обчислювальної складності алгоритм декодування БЧХ кодів методом АБМ є більш складним, так як він містить більшу кількість арифметичних та логічних операцій, та при великих значеннях d_{min} процес знаходження позицій помилок зазвичай проводиться за меншу кількість ітерацій [2]. Але реалізація алгебраїчних операцій над натуральними числами складніше і під час таких операцій може втрачатися обчислювальна точність.

При умові використання вище вказаних методів декодування, найбільш трудомістким і складним етапами алгебраїчного декодування лінійних блокових БЧХ кодів є обчислення компонент сіндромного вектору та процедура пошуку коренів полінома локаторів помилок для визначення позицій виправлених кодових символів. У відповідності до теореми Абеля [2], корені поліномів ступінь яких більше чотирьох в загальному випадку не можуть бути виражені через суми, добутки, частки та корені їх коефіцієнтів. Тому для пошуку коренів полінома локаторів помилок з елементами полів Галуа використовують алгоритмічні методи.

Аналіз досліджень та публікацій

Циклічні БЧХ коди мають особливу структуру, яка дозволяє використовувати алгебраїчні методи та алгоритми для декодування. Найбільш складним виявилось виправлення помилок аж до істинної мінімальної довжини при збільшення конструктивної довжини. Для багатьох кодів ця задача вирішена, але досі є невирішеною проблемою обчислення коефіцієнтів поліному локаторів помилок для виявлення позицій помилок.

Коди БЧХ представляють клас кодів, які задаються через корені породжуючого многочлена ступеня $n-k$.

$$g(x) = g_r x^r + g_{r-1} x^{r-1} + \ ... + \ g_o, \tag{1}$$

де $r = \deg[g(x)] = n-k$ – кількість перевірочних символів.

Тоді двійковий БЧХ код довжини n, що виправляє t-кратні помилки – це циклічний блоковий код над полем GF(2), коренями породжуючого полінома якого є α^b, α^{b+1}, … α^{b+2t-1}, де α – елемент розширеного кінцевого поля GF(2^m), b – ціле число. Елементи α^b, α^{b+1}, … α^{b+2t-1} називають нулями БЧХ коду [3].

Одним із головних етапів декодування БЧХ кодів є вирішення ключового рівняння з визначенням поліному локаторів помилок та знаходження коренів цього поліному. Одним із розповсюджених та часто використовуваних на практиці методів обчислення коренів многочлена локаторів помилок є метод Ченя, який може бути реалізована двома способами [2]. Класичний алгоритм Ченя складається з прямої підстановки усіх елементів поля до поліному локаторів помилок, обчислення в розширених полях Галуа і порівняння результату отриманих значень з нулем. Тобто використовується масив W, ініціалізований коефіцієнтами многочлена локаторів помилок $W_i = f_i$ і на кожному кроку j значення многочлена обчислюється

$$f(x_i) = \sum_{i=0}^{t} W_i, \tag{2}$$

після чого елементи масиву оновлюються $W_i = W_i \alpha^i$ [4,5]. Не менш ефективним з точки зору мінімальної кількості обчислювальних операцій вважається використання схеми Горнера з прямою підстановкою змінної [6]

$$f(x) = f_0 + x(f_1 + x(f_2 + \cdots + f_t)). \tag{3}$$

Кількість операцій множення та додавання у цьому разі не змінюється, проте необхідно виконати додаткові операції звернення до комірок пам'яті. Однак для многочленів з великим ступеням ця процедура стає доволі складною при обчисленнях в полях Галуа, адже виконання алгебраїчної операції піднесення до степені є досить складним для практичної реалізації.

Для пошуку коренів полінома локаторів помилок, який має вигляд афіного многочлена, використовується модифікований алгоритм найменшого афінного кратного. В якості прийому зниження складності обчислювальних процедур є повторне використання на кожній ітерації результатів раніше виконаних обчислень. Для лінєаризованих та афіних многочленів для цього може бути використано властивість [7]

$$l(a+b) = l(a) + l(b), \ \ a, b \ \in GF(2^m), \tag{4}$$

де $l(x) = \sum_i l_i x^{2^i}$, $l_i \in GF(2^m)$ – лінєаризований многочлен.

Якщо кожному елементу поля Галуа може бути відповідно поставлений двійковий вектор, то елементи поля можуть бути впорядковані наприклад кодом Грея і тоді на кожному кроці виконується рівно одне додавання. Модифікований алгоритм найменшого афінного кратного може бути реалізовано і на випадок довільних поліномів, якщо їх розбити на набір афіних [8].

Також існує табличний метод пошуку коренів поліному локаторів помилок, який полягає у зведенні довільного багаточлена до канонічної форми з невеликою кількістю параметрів та використання їх як ключ для пошуку за заздалегідь підготовленою таблиці коренів багато членів [9]. Основним недоліком цього є наявність порівняно великих таблиць коренів з нерегулярною структурою, що утруднює пошук.

Використання дискретного перетворення Фур'є (ДПФ) для методів декодування БЧХ кодів розглядаються в роботах деяких авторів. Наприклад метод Рейдера для знаходження коренів поліному з алгоритмом швидкого перетворення Фур'є (ШПФ) побудований на основі швидкого алгоритму обчислення циклічної згортки [10]. Алгоритм Герцеля для кінцевих полів використовує мінімальні многочлени $\varphi_i(x)$ елементів поля для знаходження залишків від поділу [11]

$$\mathrm{f(x)} = \mathrm{v_i(x)}\varphi_\mathrm{i}(\mathrm{x}) + \mathrm{r_i(x)}, \tag{5}$$

де $f(\alpha^j) = r_i(\alpha^j)$ для всіх α^j: $\varphi_i(\alpha^j) = 0$. Обчислення значення багаточлена $r_i(x)$, вимагає набагато менших обчислювальних витрат, ніж аналогічна операція над багаточленом $f(x)$. Обчислення власне багаточленів $r_i(x)$,вимагає тільки операцій над простим підполем GF(q), які, як правило, суттєво простіше операцій на GF(q^m).

Наявність обмежень на довжину n призводить до того, що побудова ефективного алгоритму ШПФ для довжин, що практично використовуються, стає завданням з погано формалізованими методами розв'язання. При реалізації алгоритмів декодування БЧХ кодів потрібне обчислення неповного ДПФ чи ШПФ багаточлена малого ступеня. Більшість з описаних швидких алгоритмів виявляються абсолютно неефективними при такій постановці завдання.

Формулювання цілей статті

Метою роботи є представлення прискореного алгоритму декодування БЧХ кодів, основні етапи якого (обчислення вектора синдрому, визначення спектральних компонент поліному локаторів помилок, обчислення вектора та позицій помилок) реалізовані в частотній області.

Виклад основного матеріалу

Більше простий, а в деяких випадках більш ефективний, алгоритм декодування кодів БЧХ можна отримати скориставшись спектральними методами [12]. Для опису алгоритмів кодування та декодування циклічних БЧХ кодів в частотній області с використанням перетворення Фур'є зазначимо основні параметри та компоненти коду.

Розглянемо двійковий вектор $f = \{f_0, f_1, \dots, f_{n-1}\}$ довжини n=2^m–1 компоненти якого належать кінцевому полю $GF(2)$ і який можна представити у вигляді многочлена $f(x) = \sum_{i=0}^{n-1} f_i x^i$. Тоді дискретне перетворення Фур'є для вектора $f = (f_i), i \in [0, n-1]$ над полем $GF(2^m)$ є вектор $F = (F_j), j \in [0, n-1]$

$$\mathrm{F_j} = \mathrm{f(\alpha^j)} = \textstyle\sum_{\mathrm{i=0}}^{\mathrm{n\text{-}1}} \mathrm{f_i}\alpha^{\mathrm{ij}}, \quad \mathrm{j} \in [0, \mathrm{n\text{-}1}], \tag{6}$$

де α – елемент поля $GF(2^m)$.

Відповідне зворотне дискретне перетворення Фур'є (ЗПФ) для вектора $F = \{F_0, F_1, \dots, F_{n-1}\}$ довжини n=2^m–1 компоненти якого належать кінцевому полю $GF(2^m)$ і який можна представити у вигляді многочлена $F(x) = \sum_{i=0}^{n-1} F_i x^i$ записується наступним чином

$$f_j = F(\alpha^j) = \frac{1}{n}\sum_{i=0}^{n-1} F_i \alpha^{-ij}, \quad j \in [0, n-1]. \tag{7}$$

Зазначимо також важливу властивість про згортку ДПФ [1]. Якщо є ДПФ довжина якого складає n і $e_i = f_i \cdot g_i, 0 \le i \le n$. Тоді

$$\mathrm{E_j} = \frac{1}{\mathrm{n}}\textstyle\sum_{\mathrm{k=0}}^{\mathrm{n\text{-}1}} \mathrm{F_{j\text{-}k \bmod n}} \mathrm{G_k}, 0 \le \mathrm{j} \le \mathrm{n}. \tag{8}$$

Інформаційна послідовність $a(x)$ довжини k визначається поліномом

$$\mathrm{a(x)} = \mathrm{a_{k\text{-}1}x^{k\text{-}1}} + \mathrm{a_{k\text{-}2}x^{k\text{-}2}} + \ \dots + \mathrm{a_0}. \tag{9}$$

Необхідно закодувати $a(x)$ блоковим БЧХ кодом з параметрами: n – довжина кода, t – кількість помилок, які здатен виправити код, породжуючий поліном $g(x)$, що задається коренями α^b, α^{b+1}, …, α^{b+2t-1} – елементи кінцевого поля $GF(2^m)$.

Для спрощення розрахунків приймемо значення коефіцієнта b=1. Тоді нулями БЧХ коду є елементи кінцевого полю $GF(2^m)$ – α, α^2, …, α^{2t}.

Кодова послідовність, декодування якої необхідно виконати дорівнює

$$v(x) = a(x)g(x) + e(x), \tag{10}$$

де $e(x)$ – вектора помилок.

Класичний алгоритм декодування в часовій області складається з декількох етапів – обчислення синдромів, вирішення ключового рівняння та обчислення поліному локаторів помилок, пошук коренів поліному локаторів помилок для визначення позицій помилок та формування вектора $e(x)$.

Розглянемо можливість отримання за допомогою ЗПФ вектора помилок $e_i = \{e_0, e_1, \dots, e_{n-1}\}$ в часовій області через спектральні компоненти $E_i = \{E_0, E_1, \dots, E_{n-1}\}$

$$e_j = \frac{1}{n}\sum_{i=0}^{n-1} E_i \alpha^{-ij}, \quad j \in [0, n-1]. \tag{11}$$

Якщо обчислити ДПФ порядку n для вектора v_i та знайти спектр, отримуємо

$$V_i = v(\alpha^i) = A_i G_i + E_i, 0 \le i \le n. \tag{12}$$

Оскільки $g(\alpha^i)=0$ в нулях кода α, α^2, …, α^{2t}, тоді спектральні компоненти добутку мають нульові значення $A_i G_i = 0$ на інтервалі $j = 1, 2, \ldots, 2t$, а значить на вказаних перевірочних частотах спектральні компоненти кодового слова V_i залежать виключно від векторі помилок E_i

$$V_j = v(\alpha^i) = E_j, \ 1 \le j \le 2t. \tag{13}$$

Для декодера, працюючого в спектральній області, компоненти сіндромного вектора $S = \{S_1, S_2, \ldots, S_{2t}\}$ знаходяться через ДПФ прийнятого кодового слова v_i

$$S_j = \sum_{i=0}^{n-1} v_i \alpha^{ij}, \ j = 1, \ldots, 2t. \tag{14}$$

Очевидно, що на частотах $j = 1, 2, \ldots, 2t$ значення сіндромних компонент дорівнюють компонентам спектру конфігурації помилок

$$S_j = E_j, \ j = 1, 2, \ldots, 2t. \tag{15}$$

Як відомо головною задачею декодування БЧХ кодів є рішення ключового рівняння з відомими сіндромними компонентами, а саме знаходження кількості помилок τ ($\tau<t$) в кодовій послідовності $v(x)$ та визначення поліному локаторів помилок

$$\Delta(X) = 1 + \Delta_1 X + \Delta_2 X^2 + \cdots + \Delta_\tau X^\tau, \tag{16}$$

де $\Delta_1, \ \Delta_2, \ldots, \Delta_\tau$ – коефіцієнти поліному локаторів помилок, які належать полю $GF(2^m)$.

При реалізації декодера за допомогою спектральних методів для вирішення цієї задачі використовується рекурентний алгоритм Бєрлєкемпа-Мессі, основою якого є структура звичайного регістру зсуву з лінійним зворотнім зв'язком. Знайдений поліном локаторів помилок з відповідними локаторами α^{i_k} в полі $GF(2^m)$ дорівнює

$$\Delta(x) = \prod_{k=1}^{\tau}(1 - x\alpha^{i_k}), k = 1, \ldots \tau \ . \tag{17}$$

Для вектора $\Delta(x)$ ЗПФ обчислюється як значення поліному в точках α^{-i}: $\delta_i = \Delta(\alpha^{-i})$. Якщо i – це позиція помилки та $e_i \ne 0$, тоді $\Delta(\alpha^{-i}) = 0$. Таким чином в часовій області поліном $\delta_i = 0$ і справедлива рівність $e_i \delta_i = 0, 0 \le i \le n$. Використовуючи правила згортки [1] тоді отримуємо

$$\sum_{j=0}^{\tau} \Delta_j E_{i-j} = 0, 0 \le i < n. \tag{18}$$

Якщо перший коефіцієнт поліному $\Delta_0 = 1$, та $deg\Delta(x) = \tau$ отримуємо вираз

$$1 \cdot E_i + \sum_{j=1}^{\tau} \Delta_j E_{i-j} = 0, 0 \le i < n. \tag{19}$$

Тоді

$$E_i = -\sum_{j=1}^{\tau} \Delta_j E_{i-j}, 0 \le i < n. \tag{20}$$

Враховуючи вираз (15) отримуємо рівняння яке зв'язує відомих ($2t$ компонент вектора синдрому S і τ коефіцієнтів поліному локаторів помилок Δ) та $n–2t$ невідомих спектральних компонент S

$$S_i = -\sum_{j=1}^{\tau} \Delta_j S_{i-j}, 2t + 1 \le i \le n. \tag{21}$$

Якщо перші $2t$ спектральних компонент вектору помилок визначені через сіндромні коефіцієнти $E_0 = S_1, \ E_1 = S_2, \ldots, E_{2t-1} = S_{2t}$, то інші $n–2t$ невідомих компонент вектору E можна знайти за допомогою коефіцієнтів Δ_1, Δ_2, …, Δ_τ за формулою

$$E_k = -\sum_{j=1}^{\tau} \Delta_j E_{k-j}, k = 2t, \ldots, n-1. \tag{22}$$

Обчислення за виразом () може бути виконано за допомогою регістру зсуву з лінійним зворотнім зв'язком, при цьому вагові множники у відводах співпадають з компонентами вектора Δ, а початкові значення стану регістру задаються сіндромними компонентами $E_0 = S_1, \ E_1 = S_2, \ldots, E_{2\tau-1} = S_{2\tau}$.

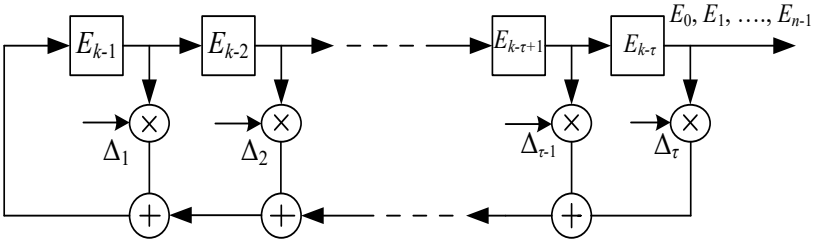

Рис. 1. Регістр здвигу з лінійним зворотнім зв'язком

Таким чином можна визначити всі значення вектора в частотній області $E_i = \{E_0, E_1, \ldots, E_{n-1}\}$. Далі для знаходження поліному помилок $e(x)$ в часовій області необхідно обчислити вектор помилок $e_i = \{e_0, e_1, \ldots, e_{n-1}\}$ як ЗПФ за формулою (7). Тоді процедура декодування завершується правильно, якщо фактичне число помилок не перевищує виправну здатність коду.

Покроковий алгоритм декодування БЧХ кодів в частотній області із застосуванням дискретного перетворення Фур'є та алгоритму знаходження поліному локаторів помилок методом Бєрлєкемпа-Мессі.

1. Отримання кодового слова з помилками $v(x)$.

2. Знаходження $2t$ компонент синдрому через ДПФ (6).

3. Обчислення ключового рівняння та знаходження τ коефіцієнтів поліному локаторів помилок $\Delta_1, \Delta_2, \dots, \Delta_\tau$ методом Бєрлєкемпа-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. Обчислення ЗПФ для компонент вектору помилок та отримання значень коефіцієнтів многочлена помилок в часовій області (7).

Приклад. Інформаційна послідовність $u(x) = x^4+x^2+x$ закодована систематичним БЧХ кодом (15, 5, 7), який здатен виправляти помилки кратні 3. При передачі була прийнята послідовність $v(x)=x^{14} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$. Вектор помилки $e(x) = 1+x^6+x^{12}$. Декодувати прийняту кодову послідовність, виправити помилки.

1. Обчислимо компоненти синдрому помилок $S_j = f(\alpha^j)$, $j = 1, \dots 2t$, де α^j – нулі кода, які дорівнюють $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$.

$S_1= \alpha$, $S_2= \alpha^2$, $S_3= \alpha^8$, $S_4= \alpha^4$, $S_5= 1$, $S_6= \alpha$.

2. Вирішимо ключове рівняння та знайдемо многочлен локаторів помилок. Для вирішення ключового рівняння, що пов'язує компоненти синдрому S_1, S_2, S_3, S_4, S_5, S_6 та коефіцієнти многочлена локаторів помилок $\Delta_1, \Delta_2, \dots, \Delta_\tau$ застосувавши алгоритм Бєрлєкемпа-Мессі. Коефіцієнти $\Delta_1 = \alpha, \Delta_2 = \alpha^7, \Delta_3 = \alpha^3$ та шуканий поліном локаторів помилок.

3. Якщо перші 6 компонент вектору помилок в часовій області дорівнює $E_0 = S_1 = \alpha, E_1 = S_2 = \alpha^2, E_2 = S_3 = \alpha^8, E_3 = S_4 = \alpha^4, E_4 = S_5 = 1, E_5 = S_6 = \alpha$. Тоді наступні $E_6, E_7, \dots, E_{14}$ знайдемо застосувавши рекурентну формулу для відомих синдромних компонент S_1, S_2, S_3, S_4, S_5, S_6 та коефіцієнтів поліному локаторів помилок $\Delta_1 = \alpha, \Delta_2 = \alpha^7, \Delta_3 = \alpha^3$.

$$S_i = -\sum_{j=1}^{3} \Delta_j S_{i-j}, i = 7, \dots, 15.$$

$$S_7 = \Delta_1 \cdot S_6 + \Delta_2 \cdot S_5 + \Delta_3 \cdot S_4 = \alpha \cdot \alpha + \alpha^7 \cdot 1 + \alpha^3 \cdot \alpha^4 = \alpha^2;$$
$$S_8 = \Delta_1 \cdot S_7 + \Delta_2 \cdot S_6 + \Delta_3 \cdot S_5 = \alpha \cdot \alpha^2 + \alpha^7 \cdot \alpha + \alpha^3 \cdot 1 = \alpha^8;$$
$$S_9 = \Delta_1 \cdot S_8 + \Delta_2 \cdot S_7 + \Delta_3 \cdot S_6 = \alpha \cdot \alpha^8 + \alpha^7 \cdot \alpha^2 + \alpha^3 \cdot \alpha = \alpha^4;$$
$$S_{10} = \Delta_1 \cdot S_9 + \Delta_2 \cdot S_8 + \Delta_3 \cdot S_7 = \alpha \cdot \alpha^4 + \alpha^7 \cdot \alpha^8 + \alpha^3 \cdot \alpha^2 = 1;$$
$$S_{11} = \Delta_1 \cdot S_{10} + \Delta_2 \cdot S_9 + \Delta_3 \cdot S_8 = \alpha \cdot 1 + \alpha^7 \cdot \alpha^4 + \alpha^3 \cdot \alpha^8 = \alpha;$$
$$S_{12} = \Delta_1 \cdot S_{11} + \Delta_2 \cdot S_{10} + \Delta_3 \cdot S_9 = \alpha \cdot \alpha + \alpha^7 \cdot 1 + \alpha^3 \cdot \alpha^4 = \alpha^2;$$
$$S_{13} = \Delta_1 \cdot S_{12} + \Delta_2 \cdot S_{10} + \Delta_3 \cdot S_9 = \alpha \cdot \alpha^2 + \alpha^7 \cdot \alpha + \alpha^3 \cdot 1 = \alpha^8;$$
$$S_{14} = \Delta_1 \cdot S_{13} + \Delta_2 \cdot S_{12} + \Delta_3 \cdot S_{11} = \alpha \cdot \alpha^8 + \alpha^7 \cdot \alpha^2 + \alpha^3 \cdot \alpha = \alpha^4;$$
$$S_{15} = \Delta_1 \cdot S_{14} + \Delta_2 \cdot S_{13} + \Delta_3 \cdot S_{12} = \alpha \cdot \alpha^4 + \alpha^7 \cdot \alpha^8 + \alpha^3 \cdot \alpha^2 = 1;$$

Таким чином, знайдені усі значення спектральних компонент вектора помилок в частотній області

$$E_0 = \alpha, E_1 = \alpha^2, E_2 = \alpha^8, E_3 = \alpha^4, E_4 = 1, E_5 = \alpha, E_6 = \alpha^2, E_7 = \alpha^8, E_8 = \alpha^4, E_9 = 1, E_{10} = \alpha, E_{11} = \alpha^2, E_{12} = \alpha^8, E_{13} = \alpha^4, E_{14} = 1$$

4. Для отримання значення компонентів вектора помилок в часовій області виконаємо ЗПФ ()

$$e_j = \sum_{i=0}^{14} E_i \alpha^{-ij}, j = 0, \dots, 14 ;$$

Наведемо приклади розрахунку e_j для деяких значень:

$$e_0 = \alpha \cdot 1 + \alpha^2 \cdot 1 + \alpha^8 \cdot 1 + \alpha^4 \cdot 1 + 1 \cdot 1 + \alpha \cdot 1 + \alpha^2 \cdot 1 + \alpha^8 \cdot 1 + \alpha^4 \cdot 1 + 1 \cdot 1 + \alpha \cdot 1 + \alpha^2 \cdot 1 + \alpha^8 \cdot 1 + \alpha^4 \cdot 1 + 1 \cdot 1 = 1$$

$$e_1 = \alpha \cdot 1 + \alpha^2 \cdot \alpha^{-1} + \alpha^8 \cdot \alpha^{-2} + \alpha^4 \cdot \alpha^{-3} + 1 \cdot \alpha^{-4} + \alpha \cdot \alpha^{-5} + \alpha^2 \cdot \alpha^{-6} + \alpha^8 \cdot \alpha^{-7} + \alpha^4 \cdot \alpha^{-8} + 1 \cdot \alpha^{-9} + \alpha \cdot \alpha^{-10} + \alpha^2 \cdot \alpha^{-11} + \alpha^8 \cdot \alpha^{-12} + \alpha^4 \cdot \alpha^{-13} + 1 \cdot \alpha^{-14} = 0$$

$$e_2 = \alpha \cdot 1 + \alpha^2 \cdot \alpha^{-2} + \alpha^8 \cdot \alpha^{-4} + \alpha^4 \cdot \alpha^{-6} + 1 \cdot \alpha^{-8} + \alpha \cdot \alpha^{-10} + \alpha^2 \cdot \alpha^{-12} + \alpha^8 \cdot \alpha^{-14} + \alpha^4 \cdot \alpha^{-16} + 1 \cdot \alpha^{-18} + \alpha \cdot \alpha^{-20} + \alpha^2 \cdot \alpha^{-22} + \alpha^8 \cdot \alpha^{-24} + \alpha^4 \cdot \alpha^{-26} + 1 \cdot \alpha^{-28} = 0$$

Якщо таким же чином виконати обчислення для інших коефіцієнтів, то отримуємо

$$e_0 = 1, e_1 = 0, e_2 = 0, e_3 = 0, e_4 = 0, e_5 = 0, e_6 = 1, e_7 = 0, e_8 = 0, e_9 = 0, e_{10} = 0, e_{11} = 0, e_{12} = 1, e_{13} = 0, e_{14} = 0$$

Остаточно отримуємо многочлен помилок $e(x) = 1+x^6+x^{12}$.

Висновки

Описаний алгоритм декодування БЧХ кодів в частотній області за допомогою перетворення Фур'є може працювати в системи захисту повідомлень від помилок незалежно від того в якій області був реалізована система кодування (в частотній чи часовій). Якщо кодування здійснювалося в часовій області, то для знаходження вектора помилок та відтворення кодової послідовності в часовій області необхідно використовувати алгоритм згортки складності $n \log_2 n$ та описаний рекурентний алгоритм Бєрлєкемпа-Мессі, а на заключному етапі використовувати ЗПФ. У випадку, коли кодер працює в частотній області, тоді інформаційний поліном обчислюється безпосередньо за допомогою виправленого спектру, тобто без необхідності виконувати ЗПФ.

Література

1. Blahut, R. E. (2003). *Algebraic Codes for Data Transmission*. Cambridge University Press.

2. Lin, S., & Costello, D. J. (2004). *Error Control Coding: Fundamentals and Applications*. Prentice-Hall.

3. Bardet, M., Dragoi, V., Otmani, A., & Tillich, J.-P. (2016). Algebraic Properties of Polar Codes from a New Polynomial Formalism. *Proceedings of IEEE International Symposium on Information Theory*. https://doi.org/10.1109/ISIT.2016.7541295

4. Blahut, R. E. (2008). *Algebraic Codes on Lines, Planes, and Curves: An Engineering Approach*. Cambridge University Press. https://doi.org/10.1017/CBO9780511543401

5. Wu, Y. (2008). New List Decoding Algorithms for Reed-Solomon and BCH Codes. *IEEE Transactions on Information Theory*, 54(8), 3611–3630. https://doi.org/10.1109/TIT.2008.926303

6. Wu, Y. (2012). Fast Chase Decoding Algorithms and Architectures for Reed-Solomon Codes. *IEEE Transactions on Information Theory*, 58(1), 109–129. https://doi.org/10.1109/TIT.2011.2165524

7. Trifonov, P. (2010). Efficient Interpolation in the Guruswami-Sudan Algorithm. *IEEE Transactions on Information Theory*, 56(9), 4341–4349. https://doi.org/10.1109/TIT.2010.2053901

8. Fedorenko, S. V., & Trifonov, P. V. (2002). Finding Roots of Polynomials over Finite Fields. *IEEE Transactions on Communications*, 50(11), 1709–1711.

9. Fedorenko, S. V., Trifonov, P. V., & Costa, E. (2003). Improved Hybrid Algorithm for Finding Roots of Error-Locator Polynomials. *European Transactions on Telecommunications*, 14(5), 411–416.

10. Costa, E., Fedorenko, S., & Trifonov, P. (2004). Efficient Algorithm for Computing Syndrome Polynomial in Reed-Solomon Decoder. *Proceedings of 5th International ITG Conference on Source and Channel Coding (SCC)*, 181, 179–183.

11. Freyman, V. I. (2019). Research of the Reed-Solomon Codes Characteristic for Realization within Control Systems Devices. *Radio Electronics, Computer Science, Control*, 3, 143–151.

12. Fedorenko, S. V. (2022). A Spectral Algorithm for Decoding Systematic BCH Codes. *IEEE Access*, 10, 110639–110645. https://doi.org/10.1109/ACCESS.2022.3215005

13. Liang, Z., & Zhang, W. (2017). Efficient Berlekamp-Massey Algorithm and Architecture for Reed-Solomon Decoder. *Journal of Signal Processing Systems*, 86(1), 51–65. https://doi.org/10.1007/s11265-015-1094-1

14. Almuzakkia, M. Z., & Ohara, K. (2015). Computing General Error Locator Polynomial of 3-Error-Correcting BCH Codes via Syndrome Varieties Using Minimal Polynomial. *ISCS Selected Papers*, 80–85.

15. Krylova, V. A., Tverytnykova, E. E., Vasylchenkov, O. G., & Kolisnyk, T. P. (2020). Modified Algorithm for Searching the Roots of the Error Locators Polynomial While Decoding BCH Codes. *Radio Electronics, Computer Science, Control*, 3, 150–157. https://doi.org/10.15588/1607-3274-2020-3-14

References

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*. 2016. 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. 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. September. 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. URL: http://surl.li/urqxyb.

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: https://doi.org/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. URL: http://surl.li/dujobm.

15. Krylova V. A., Tverytnykova E. E., Vasylchenkov O. G., Kolisnyk T. P. Modified algorithm for searching the roots of the error locators polynominal while decoding BCH codes. *Radio Electronics, Computer Science, Control*. 2020. Issue 3. pp. 150-157. DOI: 10.15588/1607-3274-2020-3-14.