Декодування Стирань в Паралельних Циклічних Кодах

Василь Семеренко, Ольга Тарасова, Сергій Луцков
кафедра обчислювальної техніки,
Вінницький національний технічний університет
Вінниця, Україна
vpsemerenko@ukr.net, tarasovaolga016@gmail.com, lutskov 96@gmail.com

Decoding the Erasures in Parallel Cyclic Codes

Vasyl Semerenko, Olga Tarasova, Sergiy Lutskov
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, Ukraine,
vpsemerenko@ukr.net, tarasovaolga016@gmail.com, lutskov 96@gmail.com

***Анотація*—Розглядається декодування пакетів стирань в багатоканальних системах зв'язку на основі теорії паралельних лінійних послідовнісних схем (ЛПС).Пропонується метод ітеративного декодування паралельних циклічних кодів на основі степеневої перестановки.**

***Abstract*—The decoding with burst of erasures in multichannel transmission systems based on the theory of parallel linear finite-state machine (LFSM) is considered. The method of iterative decoding of the parallel cyclic codes with the help of power permutation is suggested.**

Ключові слова—циклічні коди; лінійна послідовнісна схема; ітеративне декодування; пакети стирань

Keywords—cyclic codes;linear finite-state machine (LFSM); iterative decoding; erasure burst errors

I. Вступ

Шеннонівська теорія завадостійкого кодування [1] теоретично узагальнила рівень розвитку засобів зв'язку середини 20 століття, для якого були характерні такі особливості:

- послідовне надходження даних,
- випадковий спосіб появи помилок в каналі,
- зменшення ймовірності появи помилок зі збільшенням кратності помилки,
- відсутність пам'яті в каналі зв'язку.

Сучасна передача даних може бути організована одночасно від багатьох передавачівдо багатьох приймачів по різним каналам. Така ситуація типова для комп'ютерних мереж, цифрового радіомовленняі телебачення, оптоволоконних систем зв'язку та ін.

За останні десятиріччя з'явились нові типи зв'язку, зокрема, безпровідний і мобільний зв'язок, теоретичною моделлю яких стали канали з пам'яттю. Характерною особливістю особливістю таких каналів стали нові типи помилок (стирання, пропадання символів), які часто групуються, тобто об'єднуються в пакети.

Численні дослідження показали, що в результаті опромінення світлом і радіацією динамічної напівпровідникової пам'яті в ній виникають багаторозрядні стирання даних [2,3].

Мета цієї роботи – розробка ефективних алгоритмів декодування пакетів стирань в багатоканальних системах зв'язку на основі математичного апарату лінійних послідовнісних схем.

II. Теоретичні основи паралельних циклічних кодів

В сучасних багатоканальних системах передачі даних реалізована паралельна передача даних: біти одного байту або слова (2, 4, 8 байт) поступають одночасно. Кожний байт або слово можнаінтерпретуватияк один ρ-бітовий символ (ρ=8,16,32,64).Таким чином, передачу даних будемо розглядати як передачу бітів даних по ρ паралельним каналам.Такий спосіб передавання даних є символьно-паралельним згідно[4]. Послідовність з m символів будемо розглядати як кодове слово циклічного коду, яке формується кодером на боці передавачата декодується декодером на боці приймача. В цьому випадку знадоблятьсяматематичні перетворення тільки в двійкових полях Галуа $GF(2)$.Такий спосіб інтерпретації даних означає, що паралельний циклічнийкодскладається

з ρ кодових слів z_i ($i = 1 \ldots \rho$), об'єднаних в кодову матрицю:

$$Z_{(\rho)} = \begin{bmatrix} z_1 \\ z_2 \\ \ldots \\ z_\rho \end{bmatrix} = \begin{bmatrix} z_{11} & z_{12} & \ldots & z_{1n} \\ z_{21} & z_{22} & \ldots & z_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ z_{\rho 1} & z_{\rho 2} & \ldots & z_{\rho n} \end{bmatrix}, GF(2). \quad (1)$$

Можливі два типи паралельних циклічних кодів: складенітаінтегровані [5].

В подальшому будемо використовувати лише складені паралельніциклічні коди. Кожний рядок кодової матриці (1) такого коду представляє собою звичайний циклічний (n, k)-код. Тому для кодування складеного паралельного (n, k, ρ)-коду необхідно ρ традиційних кодерів циклічного (n, k)-коду, які працюють одночасно.

Як математичну модель циклічних кодів можнавикористати автоматну модель [6], яка базується на теорії лінійних послідовнісних схем (ЛПС). Згідно [7], ЛПС – це лінійний скінчений автомат з ρ входами, m виходами і r комірками пам'яті. Найпростішою апаратною реалізацією ЛПС є звичайний регістр зсуву з лінійним оберненим зв'язком. Таким чином, теоретичноюосновою паралельних циклічних кодів при декодуванні кодової матриці (1) може бути паралельна ЛПС, функціонування якої визначається функцією станів (переходів)

$$S(t+1) = A \times S(t) + B_{(\rho)} \times Z_{(\rho)}(t), \quad GF(2) \quad (2)$$

де t – дискретний час, $A = \lfloor a_{ij} \rfloor_{r \times r}$, $B_{(\rho)} = \lfloor b_{ij} \rfloor_{r \times \rho}$ – характеристичні матриці ЛПС, $S = \lfloor s_i \rfloor_r$ – слово стану, $Z_{(\rho)} = \lfloor z_{ij} \rfloor_{n \times \rho}$ – вхідне слово.

Матриця A визначає внутрішню структуру ЛПС. Серед різних типів ЛПС найбільш розповсюдженою є рекурсивна ЛПС типу 1 (типу Галуа) з матрицею

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & g_0 \\ 1 & 0 & 0 & \ldots & g_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 1 & \ldots & g_{r-2} \\ 0 & 0 & 0 & 1 & g_{r-1} \end{bmatrix}. \quad (3)$$

Елементи останнього стовпця матриці A із (3) представляють собою коефіцієнти породжувального поліному

$$g(x) = g_0 + g_1 x + \cdots + g_{r-1} x^{r-1} + x^r, \quad GF(2). \quad (4)$$

Длядекодування складеного паралельного (n, k, ρ)-коду знадобиться один декодер (паралельний декодер), побудований на основі характеристичних матриць A і $B_{(\rho)}$ (рис.1).

Максимальна кількість каналів, яка може бути представлена з використанням математичного апарату ЛПС з функцією (2), дорівнює r, тому далі будемо розглядати складений паралельний циклічний (n, k, r)-код, кодові слова якого поступають по r входам (каналам), а його кодова матриця (1) містить r рядків ($r = \rho$). Для опису структури входів ЛПС використовується характеристична матриця $B_{(r)}$, тому у випадку r-входової паралельної ЛПС над полем $GF(2)$ має бути така одинична ($r \times r$)-матриця B:

$$B_{(r)} = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

III. Принципи декодування стирань за допомогою паралельних циклічних кодів

Розряди кодової матриці (1), яка формується передавачем, можуть приймати значення з множини $M = \{0,1\}$. Розрядикодової матриці (1), яка формується на виході демодулятора на боці приймача, можуть приймати значення з множини $M_x = \{0,1,x,\bar{x}\}$. Символи x та $\bar{x}$ можна використовувати для позначення стираньвідповідних розрядів.

Для виконання операцій над кодовоюматрицею (1) з використанням ЛПС в алфавіті значень множини M_x необхідно перейти від поля Галуа до іншої алгебраїчної структури – комутативного кільця R з відповідними операціями додавання і множення [6].

Якщо у різних рядках кодової матриці (1) може зустрічатись до m стирань, тоді необхідно розрізняти значення кожного стирання, тобто використовуватирозширений алфавіт значень множину $M_{ext} = \{0,1,x_1,\overline{x_1},\ldots,x_m,\overline{x_m}\}$.

В загальному випадку, окрім випадкових стирань, можуть зустрічатись також традиційні помилки типу логічної інверсії.

В результаті декодування всіх зазначених помилок буде отримано слово помилки $S_{err}(n)$ згідно (2), яке буде містити як ненульові, так і невизначені значення x або $\bar{x}$. Для виявлення кожного типу помилок виконується окрема процедура, зокрема для випадкових стирань необхідно розв'язати алгебраїчну систему рівнянь методом Гауса.

Розглянемо окремо тип помилок, які ефективно декодуються за допомогою паралельних циклічних кодів – пакети стирань в кодовій матриці (1).

повинна перевищувати половині розрядності синдрому, тобто $r/2$.

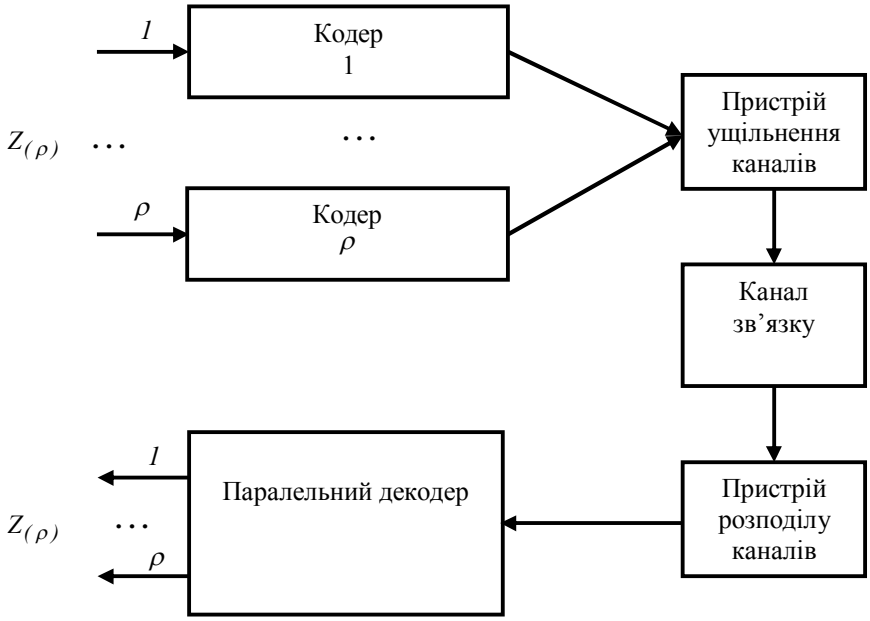

Рис. 1. Апаратна реалізація складеного паралельного циклічного коду

ОЗНАЧЕННЯ 1. Циклічним розрідженим пакетом Δ_{any}^{ers} стирань складеного паралельного циклічного (n, k, r)-коду називається такий тип помилок, коли з j-го по $((j+r-1) \bmod n)$-й розряди i-го рядка кодової матриці (1) можуть бути як стерті, так і безпомилкові символи.

ОЗНАЧЕННЯ 2. Циклічним суцільним пакетом Δ_{sol}^{ers} стирань складеного паралельного циклічного (n, k, r)-коду називається такий тип помилок, коли з j-го по $((j+r-1) \bmod n)$-й розряди i-го рядка кодової матриці (1) розташовані лише стерті символи.

Як випливає з наведених означень розглядаться пакети стирань довжини $\rho = r$.

Як і для одно канального зв'язку, розріджений пакет Δ_{any}^{ers} стирань можна також розглядатияк деяку сукупність стертих символів і декодувати кожний стертий символ окремо. В цьому випадку коректуюча здатність коду буде обмежена мінімальною кодовою відстанню цього коду.

Можна також декодувати розріджений пакет Δ_{any}^{ers} стирань подібно декодуванню розріджених пакетів інверсних помилок. Тоді коректуюча здатність коду буде обмежена відомою границею Рейгера [8], згідно якої максимальна довжина виправленого пакету помилок не

І лише для циклічнихсуцільних пакетів Δ_{sol}^{ers} стирань максимальна довжина виправленого пакету дорівнює розрядності синдрому, тобто r [9]. Тому доцільно розріджені пакети стирань переводити в суцільні пакети стирань. Саме з цих міркувань далі розглядаються лише суцільні пакети стирань (рис. 2, символом "X" позначено стерті розряди).

Для декодувань суцільних пакетів стирань зручним способом їх виявлення є заміна всіх стертих символів нулями. Це дає можливість виконувати всі математичні розрахунки в двійкових полях Галуа.

IV. Локалізація суцільних пакетів стирань за допомогою паралельних циклічних кодів

Нехай в кожному каналі є суцільний пакет стирань довжиною r, причому в першому каналі пакет стирань починається в розряді j, а в кожному наступному каналі початок пакету зсувається на один розряд ($j = 1 \div n$).

В результаті, в i-му каналі суцільний пакет стирань Δ_{sol}^{ers} починається в розряді $(j+i-1) \bmod n$, а закінчується в розряді $(j+r+i-2) \bmod n$. Тоді має місце така теорема.

ТЕОРЕМА1. Якщо в складеному паралельномуциклічному (n, k, r)-коді суцільний пакет

стирань Δ_{sol}^{ers} довжиною r починається в розряді $n-r+1$, тоді після подачі на вхід ЛПС, яка знаходиться в нульовому початковому стані $S(0)$, кодової матриці (1), значення

$z_{1,1}$	$z_{1,2}$	...	X	X	X	X	...	$z_{n-2,1}$	$z_{n-1,1}$	$z_{n,1}$
$z_{2,1}$	$z_{2,2}$	...	...	X	X	X	X	...	$z_{n-1,2}$	$z_{n,2}$
...	...	...	...	...	X	X	X	X	...	...
$z_{r,1}$	$z_{r,2}$	$z_{r,3}$	$z_{r,4}$	$z_{r,5}$	...	X	X	X	X	$z_{n,r}$

Рис. 2. Суцільний пакет стирань в кодовій матриці

слова стану $S(n)$ ЛПС буде дорівнювати r стертим символам в першому рядку кодової матриці (1).

Доведення. Після подачі на вхід ЛПС, яка знаходиться в нульовому початковому стані $S(0)$, кодової матриці (1) без помилок, знову отримаємо нульовий стан ЛПС: $S(n)=S(0)$. Після заміни стертих позицій r старших розрядів першого рядка кодової матриці (1) нулями отримаємо кодову матрицю (1), в якій частина зазначених розрядів буде помилковою. При наявності інверсних помилок в контрольних r розрядах кодової матриці (1) їх значення будуть міститись в розрядах слова стану $S(n)$, тобто синдрому помилки $S_{err}^{(\tau)}(n)$.

Для виправлення зазначених стертих розрядів достатньо записати на їх місце отриманий синдром інверсної помилки $S_{err}^{(\tau)}(n)$ (в транспонованому вигляді: перший розряд синдрому записується в n-й розряд першого рядка кодової матриці).

Теорему 1 можна узагальнити на випадок, коли пакет стирань може знаходитися в будь-якому місці i-го рядка кодової матриці (1).

ТЕОРЕМА 2. Якщо в складеному паралельномуциклічному (n,k)-коді суцільний пакет стирань Δ_{sol}^{ers} довжиною r починається в розряді j i-го рядка кодової матриці (1), тоді після подачі на вхід ЛПС, яка знаходиться в нульовому початковому стані $S(0)$, кодової матриці (1), а потім нульового слова довжиною ϑ ($\vartheta=(j+r+i-2)$), значення слова стану $S(n+\vartheta)$ буде дорівнювати r стертим символам в i-му рядку кодової матриці (1).

Для виправлення зазначених стертих розрядів достатньо записати на їх місце отриманий синдром помилки $S_{err}^{(\tau)}(n+\vartheta)$.

Основною проблемою, яка виникає при декодуванні паралельних циклічних кодів, є розрізнення помилок в різних каналах. Як показано в [5,6], сусідні помилки і пакети інверсних помилок однакової конфігурації, якірозташовуються в сусідніх каналах з зсувом на один розряд, мають однаковий синдром помилок.

Схожа ситуація виникає і у випадку пакетів стирань після заміни їх нулями. Тоді такий пакет з нулями, який розташований в i-му рядку кодової матриці (1) з початком в розряді j, має однаковий синдром помилок з пакетом нулів, який розташований в $(i+1)$-му рядку кодової матриці (1) з початком в розряді $j+1$.

Однак, у випадку стирань ми вже знаємо область пошкоджених розрядів, тому можна точно ідентифікувати номер каналу. Проблема виникає лише тоді коли мають місце діагональні стирання в одночасно в кількох каналах, причому кількість пошкоджених каналів парна (наприклад, як на. рис.2). В цьому випадку внаслідок взаємної компенсації стирань можна отримати нульовий синдром.

Звичайно, точно ідентифікувати всі стерті розряди в таких каналах неможливо. Можна лише встановити факт такого великого пошкодження даних в каналах, що теж важливо.

Підвищити коректувальну здатність коду можна за допомогою степеневої перестановки кодової матриці (1) .

V. Степенева перестановка в паралельних циклічних кодах

Розглянутий метод локалізації пакетів стирань передбачає, що всі стерті розряди знаходяться в межах r розрядів будь-якого рядка кодової матриці (1), тобто в межах деякого r-розрядого контрольного вікна Δ. На практиці ця умова не завжди виконується.

Тому постає проблема такої перестановки кодової матриці (1), щоб всі помилкові розряди попали в межі контрольного вікна Δ. Ця проблема ефективно вирішується за допомогою операції степеневої перестановки.

Ще з робіт Прейнджа [10,11] відомо, що коли породжувальний поліном $g(x)$ циклічного коду ділить кодовий поліном $f(x)$, то він буде ділити також і поліном, символи якого переставлені у відповідності до правил:

$$i \to (2^{\upsilon} i) \bmod n \text{ або } i \to (i+\upsilon) \bmod n, \quad GF(2^m).$$

Отже, при відсутності помилок поліном $f(2^q)$ також буде кодовим. А при наявності помилок результат ділення $f(x)$ на $g(x)$ дасть одну конфігурацію помилкових розрядів кодового слова, а результат ділення поліномаз перестановками на $g(x)$ – зовсім іншу конфігурацію.

Ця властивість традиційних циклічних кодів має місце і у випадку складених паралельних циклічних кодів. В найпростішому варіанті степенева перестановка полягає в тому, що спочатку записуються непарністовпці кодової матриці (1), а потім – парні (можнапочинатиіз парних стовпців). В результаті отримуємо нову ітерацію переставленої кодової матриці $Z^{(1)}_{(\rho)}$ (рис.3).

Аналогічним чином можна зробити наступні ітерації перестановок і знайти такий варіант, коли всі стерті розряди попадуть в межі контрольного вікна Δ хоча б одного рядка кодової матриці (1). Далі необхідно виправити стерті розряди вікна Δ і через обернені перестановки повернутись в початковий стан кодової матриці (1).

Звичайно, бажано мати велику кількість можливих перестановок, а ця задача вирішується оптимальним вибором породжувального поліному (4) паралельного циклічного коду.

$z_{1,1}$	$z_{1,3}$	$z_{1,5}$	...	...	$z_{1,n}$	$z_{1,2}$	...	...	$z_{1,n-2}$	$z_{1,n-1}$
$z_{2,1}$	$z_{2,3}$	$z_{2,5}$	...	...	$z_{2,n}$	$z_{2,2}$	...	...	$z_{2,n-2}$	$z_{2,n-1}$
...	...	...	...	...	...	...	...	...	...	...
$z_{r,1}$	$z_{r,3}$	$z_{r,5}$	...	...	$z_{r,n}$	$z_{r,2}$	...	...	$z_{r,n-3}$	$z_{r,n-1}$

Рис.3 Степенева перестановка кодової матриці на другій ітерації

Висновки

Багатоканальний зв'язок знаходить все більше застосування в різних сферах: в оптоволоконних системах системах передачі даних, в комп'ютерних мережах тощо. Оптимальними кодами для завадостійкого кодування при багатоканальному зв'язку є паралельні циклічні коди. Теоретичною основою таких кодів може бути теорія паралельних ЛПС. Тоді можна використати синдромний принцип декодування, що зручно для представлення пакетів стирань розрядів кодової матриці.

Основною тенденцією сучасного розвитку в завадостійких кодах є використання ітеративного (багатокрокового) декодування. Пропонується метод ітеративного декодування паралельних циклічних кодів на основі степенової перестановки. На відміну від відомих ітеративних кодів, запропоновані коди базуються лише на основі "жорстких рішень"(harddecision) при декодуванні, що дозволяє суттєво підвищити продуктивність роботи та використовувати прості апаратно-програмні засоби [12].

ЛітератураReferences

[1].К. Шеннон К. Работы по теории информации и кибернетике. – М. : Изд-во иностр. лит., 1963. – 829 с.

[2] E. Fujiwara,Code Design for Dependable Systems. Theory and Practical Applications. USA: John Willy& Sons, Inc.,

[3] Lylod W. Massengil, "Cosmic and Terrestrial Single Event RadianEffects in Dynamic Random Access Memories,"*IEEETrans. on Nuclear Science*, vol 43, No 2, pp. 576-593, April1996.

[4] V. P. Semerenko, "The Theory of Parallel CRC Codes Based on Automaton Models," *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 9 (84), pp. 45–55, 2016.

[5] В. П. Семеренко, "Паралельні циклічні коди," *Вісник ВПІ*. – № 6. – 2014. – С. 65–72.

[6] В. П. Семеренко, Теорія циклічних кодів на основі автоматних моделей : монографія. – Вінниця: ВНТУ, 2015. – 444 с.

[7] A. Gill, Linear Sequential Circuits. Analysis, Synthesis and Application. New York, London: McGraw-Hill Book Company, 1967.

[8] Р. Блейхут, Теория и практика кодов, контролирующих ошибки. – М. : Мир, 1986. – 576 с.

[9] M. Fossorier,"Universalbursterrorcorrection," in*Proc. IEEEInt. Symp. InformationTheory*, Seatle, WA,pp. 1969–1973, Jul. 2006.

[10] E. Prange. Cyclic error-correcting codes in two symbols / E. Prange. – AFCRC-TN-57-103, Air Force Cambridge Research Center. Cambridge (Mass.), Sept. 1957.

[11] Дж. Кларк мл., Дж. Кейн Кодирование с исправлением ошибок в системах цифровой связи. М. : Радиоисвязь, 1987. – 392 с.

[12] V. P. Semerenko. Iterative hard-decision decoding of combined cyclic codes, Eastern- European Journal of Enterprise Technologies. 2018. Vol. 1, issue 9 (91). P. 61–72.