УДК 004.9

О.І. Савчук

Розробка швидкодіючих засобів кодування циклічних кодів

Вінницький національний технічний університет, Україна

Анотація

Дано теоретичне обґрунтування на основі теорії лінійних послідовних схем, рекурентного і згорткового способів кодування циклічних кодів. Розроблено швидкодіючі програмні і апаратні засоби згорткового способу кодування циклічних кодів.

Ключові слова:

циклічні коди, лінійні послідовні схеми, кодери, декодери.

Abstract

The recurrent and convolutional methods of the encoding of cyclic codes which are based on theory of linear finite-state machine are done. High speed software and hardware of convolutional method of the encoding cyclic codes are developed.

Keywords:

cyclic codes, linear finite-state machine, encoder, decoder.

Циклічні коди одержали досить широке застосування завдяки їхній ефективності при виявленні і виправленні помилок. Схеми кодувальних і декодувальних пристроїв для цих кодів надзвичайно прості і будуються на основі звичайних регістрів зсуву.

Завадостійке кодування реалізується через різноманітні технічні компроміси. Теоретично можна виявити чи виправити будь-яку кількість помилок в даних, що передаються. Однак, підвищення коректувальної здатності коду вимагає збільшення ступеня надлишковості, тобто, зменшення частки корисної інформації в кожній порції переданих даних. У результаті знадобиться більше часу для передачі початкових даних з корисною інформацією. На практиці мінімізація часу передавання даних є важливою проблемою і виникає питання лише про те, якою ціною вона може бути вирішена.[1]

Відомо декілька представлень циклічних кодів: поліноміальне, матричне, через корені породжувального багаточлена, на основі теорії фільтрів. При поліноміальному представлені до циклічного коду буде належати множина багаточленів z(χ), які діляться без остачі на заданий породжувальний поліном g(χ) коду. За допомогою лінійних фільтрів також легко виконується обчислення остач від ділення довільного багаточлена на породжувальний багаточлен коду.

Усі згадані способи представлень циклічних кодів еквівалентні, від одного представлення можна перейти до іншого. За допомогою них організовуються алгоритми кодування та декодування.

Кодування коду будь-якого циклічного (n,k)-коду, полягає в тому, що k-розрядні інформаційні слова відображаються в n-розрядні кодові слова (n>k), які і передаються по каналу зв'язку.

Процес кодування циклічного (n,k)-коду за допомогою рекурсивної ЛПС типу Галуа може бути виконано за k тактів, або за n тактів. У першому випадку знадобиться розв’язання системи (n- k)×(n- k) лінійних рівнянь, а в другому одразу отримуємо контрольне слово.

Доведено[2], що кодування можна виконати за k тактів після подачі на її вхід інформаційного слова I, якщо компоненти ψ_j слова $\Psi=[\psi_0, \psi_{1\ldots}\psi_{r-2}, \psi_{r-1}]$ можуть бути знайдені в результаті розв’язання системи рівнянь

$$\begin{cases} \psi_0 = a_{1,1}s_{0\,k} + a^{1,2}s^{1k} + \cdots + a^{1,r-1}s^{k}, \\ \psi_1 = a_{2,1}s_{0\,k} + a^{2,2}_{\ldots}s^{1k} + \cdots + a^{2,r-1}_{r,}s^{k}_{r-1}, \\ \psi_{r-1} = a_{r,1}s_0 \end{cases}$$

де $a_{i,j}$ – компоненти r-го степеня матриці A($a_{i,j} \in A^r, i = 1 \ldots r, j = 1 \ldots r$).

Розглянемо на прикладі звичайний та метод швидкого кодування циклічних (n,k)-кодів.

Для циклічного (15,11)- коду з породжувальним багаточленом $g(x)=1+x+x^4$ виконаємо систематичне кодування на основі рекурсивної ЛПС типу Галуа.

Задані такі початкові дані:

- інформаційне слово I = [11010011001];
- характеристичні матриці ЛПС : $A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ та $B=\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$;

- початковий нульовий стан S(0).

Для обчислення сформуємо компонент інформаційного слова циклічного коду (15,11)
U(0)=1; U(1)=1; U(2)=0; U(3)=1; U(4)=0; U(5)=0; U(6)=1; U(7)=1; U(8)=0; U(9)=0; U(10)=1.

Для знаходження стану S(k) для k=4 виконаємо такі дії:

$$S(1)=A\times S(0)+B\times U(0)=\begin{bmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{bmatrix}\begin{bmatrix}0\\0\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}[1]=\begin{bmatrix}1\\0\\0\\0\end{bmatrix};$$

$$S(2)=A\times S(1)+B\times U(1)=\begin{bmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}[1]=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix};$$

…

$$S(11)=A\times S(10)+B\times U(10)=\begin{bmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{bmatrix}\begin{bmatrix}1\\1\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}[1]=\begin{bmatrix}0\\1\\0\\1\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}0\\1\\0\\1\end{bmatrix};$$

Визначимо контрольне слово Ψ, розв'язати систему рівнянь, сформувавши їх з матриці A^4.

$$A^4=\begin{bmatrix}1&0&0&1\\1&1&0&1\\0&1&1&0\\0&0&1&1\end{bmatrix};$$

$\psi_0=s_0+s_3=0+1=1;\quad \psi_1=s_0+s_1+s_3=0+0+1=1;\quad \psi_2=s_1+s_3=0+1=1;\ \psi_3=s_2+s_3=1+1=0;$

Тепер визначимо контрольне слово Ψ іншим способом. Для цього визначимо стан S(15), в який перейде ЛПС після подачі на її входи нульового слова О довжиною r =4 :

$$S(12)=A\times S(11)+B\times U(11)=\begin{bmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}[0]=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix};$$

…

$$S(15)=A\times S(14)+B\times U(14)=\begin{bmatrix}0&0&0&1\\1&0&0&1\\0&1&0&0\\0&0&1&0\end{bmatrix}\begin{bmatrix}1\\1\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}[0]=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix};$$

$\psi_0=1;\quad \psi_1=1;\ \psi_2=1;\ \psi_3=0;$

У результаті отримаємо кодове слово Z=[11010011001 0111]

Кожний тип ЛПС має свої особливості при кодуванні циклічних кодів, однак в основі всіх алгоритмів кодування лежить операція рекурсивного обчислення станів ЛПС. Ця математична операція дуже просто програмно реалізується, на відміну від традиційної операції ділення чи множення на породжувальний багаточлен коду.

Отже, процес кодування можна виконати за *k* тактів та *n* тактів. Виконуючи кодування першим способом ми витрачаємо найбільше часу, але він являється найпростішим. Знайшовши контрольне слово за допомогою системи рівнянь на *k*-ому такті, ми відчутно виграємо в часі, хоча затрачаємо більше програмних та апаратних ресурсів, тому цей спосіб є більш доцільним і раціональним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Семеренко В. П. Кодування кодів Ріда-Соломона на основі автоматних моделей / В. П. Семеренко // Вісник Хмельницького національного університету. – 2015. - № 6. - С. 196–202.
2. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей [Текст] : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.

Савчук Олександр Ігорович, студент факультету інформаційних технологій та комп'ютерної інженерії, ВНТУ, група 1КІ-13б, e-mail: savchuk.195@mail.ru
науковий керівник – к.т.н., доцент Семеренко Василь Петрович, Вінницький національний технічний університет, Україна.

Sasha I. Savchuk - Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : savchuk.195@mail.ru
Supervisor: V. Semerenko - PhD, assistant professor, Vinnytsia National Technical University, Ukraine.