Апаратно-Мінімальні Паралельні Коди CRC

Василь Семеренко
кафедра обчислювальної техніки,
Вінницький національний технічний університет
Вінниця, Україна
vpsemerenko@ukr.net

Hardware-Minimum Parallel CRC Codes

Vasyl Semerenko
Department of Computer Technique
Vinnytsia National Technical University
Vinnytsia, Ukraine,
vpsemerenko@ukr.net

***Анотація*—Запропоновано паралельні коди CRC (Cyclic Redundancy Code) для виявлення та виправлення помилок в каналах з паралельним надходженням вхідних даних. Як математичний апарат таких кодів використано теорію лінійних послідовнісних схем (ЛПІС). Досліджено властивості запропонованих паралельних кодів CRC і показана їх апаратна реалізація**

***Abstract*—Parallel CRC codes for detecting and correcting the errors in channels with parallel input data are proposed. The theory of linear finite state machine (LFSM) is used as a mathematical tools of such codes. The properties of the proposed parallel CRC codes are investigated and their hardware implementation are shown**

Ключові слова—коди CRC; лінійна послідовнісна схема; паралельні коди; завадостійке кодування

Keywords—CRC codes; linear finite state machine; parallel codes; error correcting coding

I. Вступ

Коди CRC (Cyclic Redundancy Code) належать до найбільш розповсюджених кодових методів контролю в різноманітних системах передачі, збереження та архівування даних [1].

З часу своєї появи в 1961 році ці коди були орієнтовані на виявлення помилок при послідовному надходженні вхідних даних. В сучасних інформаційних системах традиційний побітовий спосіб обчислення став головним недоліком CRC, тому стали активно розвиватись паралельні реалізації цих кодів.

Перехід до паралельних CRC вимагає розробки і відповідного теоретичного базису кодів. Більшість дослідників таким базисом вибрали теорію лінійних систем [2] і теорію автоматів [3]. Кодери та декодери послідовних кодів CRC з породжувальним поліномом

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

стали представляти у вигляді кінцевого автомату на основі так званої матриці F, а паралельних кодів CRC – на основі матриці F^r [4].

Основним недоліком такого підходу стали значні витрати пам'яті при програмній реалізації та велика кількість логічних елементів XOR при апаратній реалізації CRC.

Оскільки основною апаратною технологією були обрані ПЛІС (FPGA), тому основні зусилля зараз спрямовані на схемну оптимізацію паралельних CRC на базі ПЛІС: зменшення апаратних витрат і підвищення швидкодії. Задача мінімізації таких схем є NP-складною задачею, а різними евристичними методами можна оптимізувати схему в межах 10-20%. Навіть для нескладних 32-розрядних кодів CRC необхідно декілька сотень елементів XOR, що суттєво уповільнює роботу CRC [4, 5].

Як було показано в [6], перехід від матриці F до матриці F^r означає перехід від послідовного надходження вхідних даних до кортежно-паралельного способу реорганізації цих даних. Цей спосіб надходження даних прискорює обробку даних в рамках традиційної парадигми кодування-декодування, однак з пропорційним ускладненням апаратури.

Очевидно, необхідно шукати принципово інші варіанти паралельних кодів CRC.

II. Теоретичний базис паралельних кодів CRC

Як паралельний (n, k, ρ)-код CRC над полем $GF(2)$ будемо розуміти код CRC, який використовується для передачі по ρ паралельних каналах [7]. Такий код

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

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

Можна розрізняти два типи паралельних кодів CRC: складені та інтегровані. В подальшому будемо говорити лише про інтегровані коди CRC.

Для розуміння суті кодів CRC необхідно повернутись до основ циклічних кодів, до яких ці коди належать. Традиційні способи представлення циклічних кодів (матричне, поліноміальне, алгебраїчне) відіграли важливу роль в становленні цього класу кодів. Однак практика формує нові проблеми і для їх розв'язання найбільш придатним математичним апаратом є теорія лінійних послідовнісних схем (ЛПС) [8].

Традиційна ЛПС з одним входом і одним виходом є кінцевим автоматом лінійного типу (лінійним автоматом), який над полем Галуа $GF(2)$ описується функцією станів (переходів)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2) \qquad (3)$$

і функцією виходів.

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2),$$

де t – дискретний час; A, B, C, D – характеристичні матриці ЛПС; $S(t)$ – слово стану; $U(t)$ – вхідне слово; $Y(t)$ – вихідне слово.

Оскільки вхідні дані паралельного коду CRC поступають по паралельних каналах, тому необхідно використати багатовходову ЛПС. В [8] представлено багатоканальний аналог традиційної ЛПС, математична модель якої базується на функції станів (переходів)

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

і функції виходів

$$Y_{(\rho)}(t) = C_{(\rho)} \times S(t) + D_{(\rho)} \times U_{(\rho)}(t), \quad GF(2).$$

Характеристичні матриці $A_{(\rho)}$, $B_{(\rho)}$, $C_{(\rho)}$, $D_{(\rho)}$ такої ЛПС мають значно складнішу структуру, ніж відповідні матриці A, B, C, D одновходової ЛПС в (3). Наприклад, матриця $A_{(\rho)}$ дорівнює степені ρ від A: $A_{(\rho)} = A^\rho$. Вхідні та вихідні дані представляються як матриці $U_{(\rho)}(t)$ і $Y_{(\rho)}(t)$, які містять масиви слів $U(t)$ і $Y(t)$.

Оскільки матриця $A_{(\rho)}$ описує внутрішню структуру ЛПС, тому апаратна реалізація багатоканальної ЛПС також буде складною. Саме ця обставина є причиною громіздкої структури відомих варіантів паралельних CRC. Розглянемо можливість створення апаратно простих кодерів та декодерів паралельних кодів CRC [7].

Теоретичною основою таких кодів CRC може бути паралельна ЛПС, функціонування якої описується функцією станів (переходів)

$$S(t+1) = A \times S(t) + B_{(\rho)} \times U_{(\rho)}(t), \quad GF(2) \qquad (4)$$

і функцією виходів

$$Y_{(\rho)}(t) = C \times S(t) + D_{(\rho)} \times U_{(\rho)}(t), \quad GF(2),$$

Функція станів в (4), як і в (3), базується на одній і тій же самій матриці A, тобто внутрішня апаратна реалізація паралельної ЛПС буде такою ж, як і в одновходової ЛПС.

Паралельна ЛПС може бути побудована на основі трьох різних типів послідовних ЛПС:
рекурсивної ЛПС типу 1 з матрицями

$$A = \begin{bmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 1 & \dots & g_{r-2} \\ 0 & 0 & 0 & 1 & g_{r-1} \end{bmatrix} \quad B = \begin{bmatrix} 1 \\ 0 \\ \dots \\ 0 \\ 0 \end{bmatrix}, \qquad (5)$$

рекурсивної ЛПС типу 2 з матрицями

$$A = \begin{bmatrix} g_{r-1} & 1 & 0 & \dots & 0 \\ g_{r-2} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & 0 \\ g_1 & 0 & 0 & \dots & 1 \\ g_0 & 0 & 0 & \dots & 0 \end{bmatrix}, \quad B = \begin{bmatrix} g_{r-1} \\ g_{r-2} \\ \dots \\ g_1 \\ g_0 \end{bmatrix}, \qquad (6)$$

та рекурсивної ЛПС типу 3 з матрицями

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ g_0 & g_1 & g_2 & \dots & g_{r-1} \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \end{bmatrix}. \qquad (7)$$

Елементи останнього стовпця матриці A із (5), першого стовпця матриці A із (6), і елементи останнього рядка матриці A із (7), представляють собою коефіцієнти породжувального поліному (1).

Паралельна ЛПС відрізняється від вказаних послідовних ЛПС лише матрицею B, яка матиме вигляд одиничної матриці.

Помилки в паралельному циклічному коді мають решіткову конфігурацію і математичною моделлю помилок може бути матриця помилок

$$\mathrm{E}_{(\rho)} = \begin{bmatrix} \varepsilon_{11} & \varepsilon_{12} & \dots & \varepsilon_{1n} \\ \varepsilon_{21} & \varepsilon_{22} & \dots & \varepsilon_{2n} \\ \dots & \dots & \dots & \dots \\ \varepsilon_{\rho 1} & \varepsilon_{\rho 2} & \dots & \varepsilon_{\rho n} \end{bmatrix},$$

в якій ненульові елементи відповідають спотвореним позиціям в кодовій матриці (2). В результаті впливу завад в паралельних каналах в приймачі буде отримано кодову матрицю з помилками:

$$Z_{(\rho)err} = Z_{(\rho)} + \mathrm{E}_{(\rho)}, \quad GF(2)$$

На Рис. 1 представлена загальна схема r-розмірної паралельної ЛПС типу 1 з r входами і одним виходом.

III. Кодування паралельного коду CRC

Для отримання CRC як контрольної суми достатньо обчислити протягом k тактів роботи стан $S(k)$ паралельної ЛПС згідно (4).

Якщо необхідно не тільки виявляти, але і виправляти деякі класи помилок, тоді робота паралельної ЛПС продовжується ще протягом r тактів для отримання CRC як циклічного коду, тобто здійснюється процес кодування.

При систематичному кодуванні на основі інформаційної $(\rho \times k)$-матриці $I_{(\rho)}$ обчислюється контрольна $(\rho \times r)$-матриця $\Psi_{(\rho)}$ і їх об'єднання утворює кодову матрицю $Z_{(\rho)}$.

Для інтегрованого паралельного (n, k, ρ)-коду CRC матриця $\Psi_{(\rho)}$ формується на основі однієї паралельної ЛПС, тому знадобиться лише один паралельний кодер. На боці приймача необхідно мати паралельний декодер на основі такої ж паралельної ЛПС.

Основна стратегія кодування для паралельного коду CRC залишається такою ж, як і для звичайних циклічних кодів [7].

Кодування циклічних кодів на основі їх автоматного представлення базується на властивості r-керованості паралельної ЛПС, тобто існуванні вхідної послідовності довжини r, яка переводить ЛПС з одного заданого стану в інший. Для (n, k, ρ)-коду CRC ЛПС буде r-керованою, якщо ранг матриці

$$L_{(\rho),r} = [l_1 \quad l_2 \quad \dots \quad l_r],$$

де $l_j = \sum_1^r a_i$; a_i – i-й стовпець матриці $A_{(\rho)}^{r-i} \times B_{(\rho)}$, $j = 1 \dots r-1$; $l_r = \sum_1^r a_i$; a_i – i-й стовпець матриці $B_{(\rho)}$ над полем $GF(2)$ буде дорівнювати r [8].

Нехай задана r-вимірна паралельна ЛПС типу 1 і деяка інформаційна $(r \times k)$-матриця $I_{(r)}$ початкових даних, яка призначена для передачі по каналу зв'язку ($r = \rho$). Якщо ($\rho < r$), тоді $(r - \rho)$ значень можна прийняти нульовими.

Внаслідок подачі $I_{(r)}$ на r входів ЛПС через k тактів відбудеться її перехід з початкового стану $S_{beg}(0)$, зазвичай нульового, в деякий стан $S(k)$. Аналітично стан $S(k)$ можна визначити з рівняння (4).

Завдяки r-керованості паралельної ЛПС можна не більше ніж за r тактів під дією $(r \times r)$-матриці $\Psi_{(r)}$ вхідних даних перейти із стану $S(k)$ в стан $S_{end}(n)$:

$$S_{end}(n) - A_{(r)}^r \times S(k) = L_{(r),r} \times \Psi_{(r)}, \quad GF(2). \qquad (8)$$

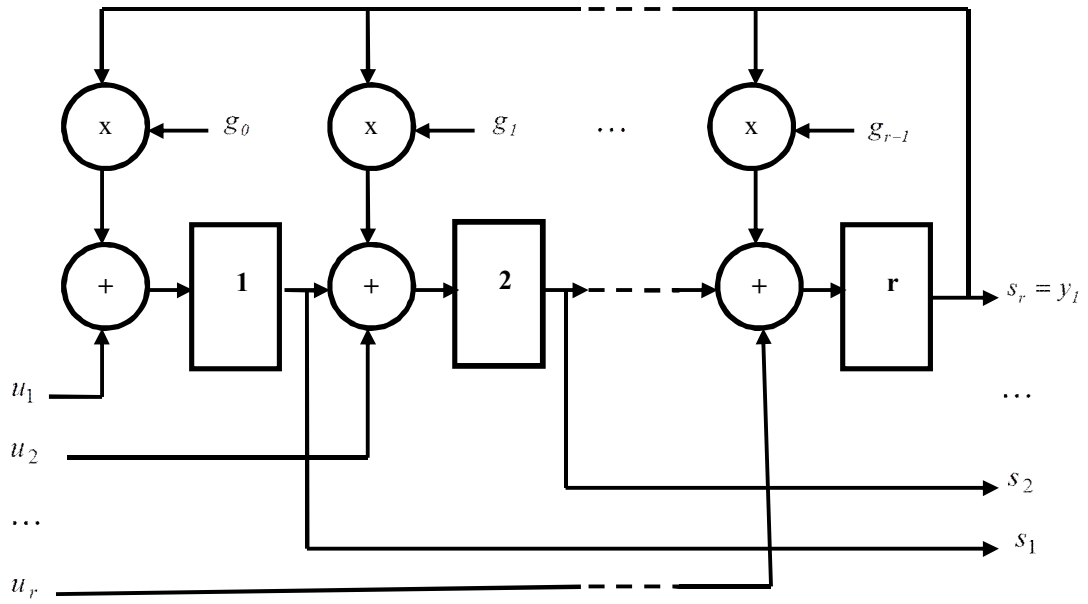

Рис. 1. Загальна схема r- розмірної паралельної ЛПС типу 1 з r входами і одним виходом (тригери позначені прямокутниками, елементи XOR – колом з символом '+')

Приймаючи кінцевий стан $S_{end}(n)$ ЛПС нульовим, запишемо рівняння (8) у вигляді

$$L_{(r),r} \times \Psi_{(r)} = S(n), \quad GF(2), \tag{9}$$

де $S(n) = A^r_{(r)} \times S(k), \quad GF(2)$.

Підставляючи в (9) значення матриці $L_{(r),r}$ із (8), отримаємо систему r рівнянь для знаходження невідомих значень матриці $\Psi_{(r)}$. Але для однозначного знаходження ($r \times r$) невідомих компонент матриці $\Psi_{(r)}$ недостатньо r рівнянь системи (9). Тому необхідно прийняти однаковими значення всіх рядків матриці $\Psi_{(r)}$. В підсумку отримуємо таку систему r рівнянь для обчислення значень матриці $\Psi_{(r)}$:

$$\begin{bmatrix} l_{1,1}\psi_1 & + & l_{1,2}\psi_2 & + & \dots & + & l_{1,r}\psi_r \\ l_{2,1}\psi_1 & + & l_{2,2}\psi_2 & + & \dots & + & l_{2,r}\psi_r \\ \dots & & \dots & & \dots & & \dots \\ l_{r,1}\psi_1 & + & l_{r,2}\psi_2 & + & \dots & + & l_{r,r}\psi_r \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_r \end{bmatrix}.$$

В результаті розв'язання цієї системи рівнянь отримаємо систему перевірок, яка зв'язує компоненти контрольної матриці $\Psi_{(r)}$ і слова стану $S(n)$. Така система перевірок і застосовується в процесі кодування.

Обчислене для конкретного стану $S(n)$ слово

$$\Psi_{(r)} = [\psi_1 \quad \psi_2 \quad \dots \quad \psi_r]$$

і представляє собою CRC як код.

Далі формується контрольна ($r \times r$)-матриця $\Psi_{(r)}$ систематичного інтегрованого паралельного (n, k, r)-коду CRC.

Підкреслимо, що зазначена система рівнянь розв'язується тільки один раз для конкретного інтегрованого паралельного коду CRC.

Таким чином, при апаратній реалізації кодера інтегрованого паралельного коду CRC, (паралельної ЛПС), додатково знадобиться схема обчислення вказаної системи перевірок.

ПРИКЛАД 1. Для інтегрованого паралельного (15, 11, 4)-коду CRC з породжувальним поліномом $g(x) = 1 + x + x^4$ виконати систематичне кодування інформаційної матриці (в канал дані поступають справа)

$$I_{(4)} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

на основі рекурсивної ЛПС типу 1.

Заданому коду відповідають такі характеристичні матриці паралельної ЛПС типу 1:

$$A_{(4)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}; \quad B_{(4)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

В результаті кодування отримаємо код CRC та контрольну матрицю $\Psi_{(4)}$:

$$\text{CRC} = [1 \quad 0 \quad 1 \quad 1], \ \Psi_{(4)} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

IV. Висновки

Введено поняття (n, k, ρ)-коду CRC за допомогою кінцевих автоматів в полях Галуа – лінійних послідовнісних схем (ЛПС). Розглянуто три типу ЛПС, які відрізняються своїми характеристичними матрицями.

Основна перевага запропонованого підходу – суттєве спрощення апаратної реалізації CRC. По-перше, зменшується кількість логічних елементів XOR, оскільки матриця A має значно більше нульових елементів, ніж матриця A^r. По-друге, елементи XOR рівномірно розміщені між тригерами, що дозволяє збільшити тактову частоту і, відповідно, швидкодію всієї схеми.

Література References

[1] V. P. Semerenko. "Theory and Practice of CRC Codes Based on Automaton Models," (in Russian), *Eastern-European Journal of Enterprise Technologies*, vol. 4, issue 9 (76), pp. 38–48, 2015. doi: 10.15587/1729-4061.2015.47860

[2] G. Campobello, G. Patane, M. Russo. "Parallel CRC realization," *IEEE Transactions on Computers*, vol. 52, issue 10, pp. 1312–1319, 2003.

[3] K.V. Krishna Reddy. "An Optimization Technique for CRC Generation," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, issue 9, pp. 3260–3265, 2013.

[4] M. Grumel and S. B. Furber. "Novel Programmable Parallel CRC Circuit," *IEEE Transactions on Very Large Scale Integration (VLSI) Circuit*, vol. 4, issue 9, pp. 3260–3265, 2010.

[5] S. R. Ruckmani and P. Anbalagan. "High Speed Cyclic Redundancy Check for USB," *DSP Journal*, vol. 6, issue 1, September, pp. 45–49, 2006.

[6] 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. doi: 10.15587/1729-4061.2016.85603

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

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