УДК 681.32

В. П. Семеренко
Б. О. Григорчук

ШВИДКЕ ДЕКОДУВАННЯ КОДІВ CRC НА ОСНОВІ СИМЕТРІЇ ЧАСУ

Вінницький національний технічний університет

Анотація

Розглянуто теоретичні основи CRC кодів за допомогою теорії лінійних послідовнісних схем (ЛПС). Доведено, що паралельне використання прямої та оберненої ЛПС на основі математичного представлення симетрії часу дозволяє вдвічі прискорити CRC-контроль.

Ключові слова: коди CRC, контрольна сума, паралельні обчислення, лінійна послідовнісна схема, час.

Abstract

The theoretical foundations of CRC code using of the theory of linear finite-state machine (LFSM) are considered. It has been proved that the concurrent using of direct LFSM and reversible LFSM based on mathematical representation of time symmetry allows twice accelerate CRC-check.

Keywords: CRC codes, checksum, parallel computing, linear finite-state machine, time.

Вступ

При передачі даних по каналам зв'язку можливі спотворення інформації і для їх виявлення використовується завадостійке декодування. Найчастіше використовуються коди CRC (*Cyclic Redundancy Code*), для яких властива проста програмно-апаратна реалізація. Їх єдиним недоліком є повільне декодування. Традиційно вхідна послідовність M розглядається як рядок двійкових коефіцієнтів деякого полінома $f(x)$, який ділиться на заданий породжувальний поліном $g(x)$, остача від цього ділення і є CRC [1]. Такий спосіб обчислень ідеально підходить для побітової передачі даних.

Однак, в сучасних комунікаційних системах дані передаються багатобайтовими пакетами і визначити коректність прийнятого пакета можна лише прийнявши його повністю. Аналогічна проблема виникає при перевірці цілісності файлів по CRC при їх зчитуванні із запам'ятовуючих пристроїв або при їх розархівуванні.

Загальним підходом до збільшення продуктивності обчислень є перехід до паралельної обробки даних. Розглянемо можливість паралельного обчислення CRC на основі темпоральних (часових) моделей.

Паралельне обчислення бітових CRC на основі темпоральних моделей

Традиційно для опису кодів CRC використовується його породжувальний поліном

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

Для розв'язання нашої задачі доцільно розглядати CRC як автомат лінійного типу, відомого також під назвою "лінійна послідовнісна схема" (ЛПС). Згідно з [2], ЛПС з l входами, m виходами і r елементами пам'яті в дискретні моменти часу t задається функцією переходів (станів)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2), \tag{2}$$

та функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2), \qquad (3)$$

де $A = \|a_{ij}\|_{r \times r}$, $B = \|b_{ij}\|_{r \times l}$, $C = \|c_{ij}\|_{m \times r}$, $D = \|d_{ij}\|_{m \times l}$ – характеристичні матриці ЛПС, $S = \|s_i\|_r$ – слово стану, $U = \|u_i\|_l$ – вхідне слово, $Y = \|y_i\|_m$ – вихідне слово; t – такт часу.

Найчастіше використовуються ЛПС з такими матрицями:

$$A = \begin{bmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ 0 & 1 & 0 & \dots & g_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{bmatrix}, B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}, C = [0 \quad \dots \quad 0 \quad 0 \quad 1], D = [0]. \qquad (4)$$

Елементи останнього рядка матриці A із (4) представляють собою коефіцієнти полінома (1).

Відомо, що фундаментальні закони класичної та квантової динаміки обернені в часі, з чого випливає математична еквівалентність “минулого” і “майбутнього”. Іншими словами, теореми, які справедливі при зміні часу від “теперішнього” в “майбутнє”, будуть також справедливими при зміні часу від “теперішнього” в “минуле”. В [3] показано, що оберненість в часі справедлива тільки для динамічних систем з одним ступенем свободи, прикладом яких може служити ЛПС при нульовій вхідній дії (автономна ЛПС) [4].

Автономна ЛПС з матрицею A (назвемо її прямою) визначає перехід із стану $S(t)$ в момент часу t в стан $S(t+1)$ в момент часу $(t+1)$ (тобто в “майбутнє”):

$$S(t+1) = A \times S(t), \quad GF(2).$$

Для повернення назад в стан $S(t)$ (тобто в “минуле”) необхідно скористатись функцією переходів ЛПС з характеристичною матрицею A_{inv} (назвемо її оберненою):

$$S(t) = A_{inv} \times S(t+1), \qquad GF(2),$$

Правила переходу між матрицями A і A_{inv} наведено в [5].

Покажемо, що оберненість в часі справедлива і для неавтономних ЛПС, які описуються рівняннями (2) і (3). Якщо під дією ненульового $U(t)$ ЛПС перейшла зі стану $S(t)$ в стан $S(t+1)$, тоді повернення назад в стан $S(t)$ здійснюється за формулою

$$S(t) = A_{inv} \times (S(t+1) + B \times U(t)), \quad GF(2). \qquad (5)$$

Нехай потрібно перевірити коректність w-бітового блока даних, представленого вхідним словом U. Згідно з (2), в такт часу $t = w$ пряма ЛПС під дією U перейде з деякого початкового стану $S(0)$ в стан $S(w)$, який і буде представляти собою CRC.

Під час рекурсивного обчислення CRC за формулою (2) послідовність змін станів прямої ЛПС в часі утворює деяку фазову траєкторію в просторі станів системи. Якщо кінцевий стан $S(w)$ прямої ЛПС взяти як початковий стан для оберненої ЛПС, тоді за формулою (5) ми зможемо по цій же фазовій траєкторії повернутись знову в стан $S(0)$.

В задачах підтвердження коректності пакетів переданих даних чи перевірки цілісності файлів вже є самі дані та відомі CRC-суми при відсутності помилок. Також відомі початкові значення станів ЛПС, зазвичай нульові. Таким чином, можна запустити паралельно в роботу дві ЛПС: пряма ЛПС буде функціонувати від початкового стану $S(0)$, а обернена ЛПС – від початкового стану $S(w)$. Неважко бачити, що при відсутності спотворень в даних, стани обох ЛПС в такт часу $w/2$ (при парному w) будуть рівні. Ймовірність p такого ж результату при наявності трьох та більше помилок в переданих даних не перевищуватиме величини

$$p = \frac{1}{2^w}.$$

Отже, при наявності одночасного доступу до початку та кінця масиву даних, який контролюється, перевірка коректності даних буде виконана вдвічі швидше.

Паралельне обчислення байтових CRC на основі темпоральних моделей

Більшість сучасних систем передачі даних мають байторієнтовану архітектуру, тобто одночасно передаються і обробляються блоки даних по 1, 2, 4 і 8 байт. Відповідно, контроль даних також має здійснюватись поблочно. Тому, вже більше двох десятиріч активно розвиваються методи паралельного CRC-контролю [6,7].

Основна ідея прискорення обчислення CRC-сум полягає у використанні спеціальних таблиць пошуку, які містять наперед розраховані дані про проміжні значення CRC-сум. При використанні r-розрядного породжувального CRC-поліному такий підхід дозволяє в r разів швидше отримати результат. Однак, з ростом значення r обсяг таких таблиць зростає експоненційно.

З позицій автоматної теорії ЛПС паралельне обчислення CRC може буде виконано за допомогою r-входової паралельної ЛПС, яка описується r-м степенем характеристичної матриці A. Матриця A^r дозволяє обчислювати стани ЛПС з інтервалом r, пропускаючи проміжні стани:

$$S(t+r) = A^r \times S(t) + B \times U(t), \quad GF(2) \tag{6}$$

Математичні перетворення за формулою (6) принципово не відрізняються від перетворень за формулою (2), тому, як і в попередньому випадку, можна розглянути функціонування паралельних ЛПС з позицій напрямку зміни часу.

Паралельну ЛПС, яка описується функцією переходів (6) будемо називати прямою. Обернена паралельна ЛПС описується функцією переходів:

$$S(t) = A_{inv}^r \times (S(t+r) + B \times U(t)), \quad GF(2). \tag{7}$$

Як і раніше, можна запустити одночасно пряму і обернену паралельні ЛПС, які будуть функціонувати в протилежних часових напрямках. Через $w/2$ тактів часу отримаємо результат перевірки, тобто також вдвічі швидше.

Висновки

Широке впровадження паралельних обчислень вимагає теоретичного дослідження та практичного впровадження швидкісних методів контролю інформації. Окрім традиційних способів розпаралелювання по задачам і по даним, можливий також паралелізм по протилежним осям часу. Використання обчислювальних процесів "вперед" і "назад" в часі є лише математичною абстракцією, але в кінцевому рахунку ми отримуємо подвійний виграш у фізичному часі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Столлингс В. Компьютерные системы передачи данных / В. Столлингс; изд. 6-е; пер. с англ. – М., Издательский дом «Вильямс», 2002. – 928 с.

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

3. Пригожин И. Время, хаос, квант. / И. Пригожин, И. Стенгерс; пер. с англ. – М.: Издат. группа Прогресс, 1994. – 272 с.

4. Семеренко В. П. Темпоральные модели параллельных вычислений / В. П. Семеренко // Austrian Journal of Technical and Natural Sciences. – 2014. – Vol. 1. – P. 13–25.

5. Семеренко В. П. Параллельное декодирование укороченных циклических кодов / В. П. Семеренко // Оптико-электронные информационно-энергетические технологии, 2012. – № 1. – С. 30-41.

6. Koopman, P. Effcient high hamming distance CRCs for embedded networks / J. Ray and P. Koopman // The International Conference on Dependable Systems and Networks (DSN-2006), 2006, Philadelphia PA, June 25-28. – P. 3–12.

7. Krishna Reddy K.V. An Optimization Technique for CRC Generation / International Journal of Computer Trends and Technology (IJCTT) Sep-2013. – Vol. 4, Issue 9. – P. 3260-3265.

Василь Петрович Семеренко – канд. техн. наук, доцент, кафедра обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: vasilsemerenko@gmail.com

Богдан Олексійович Григорчук – студент-магістрант групи 1КІ-16м, факультет інформаційних технологій та комп'ютерної інженерії,Вінницький національний технічний університет, Вінниця

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilsemerenko@gmail.com

Bogdan O. Grygorchuk – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia