УДК 512.12

АЛГОРИТМИ ПІДБОРУ МОДУЛІВ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Касянчук М.М., Сидорчук Р.П.
Тернопільський національний економічний університет

I. Вступ

Один з можливих методів збільшення швидкодії систем пов'язаний з розпаралелюванням обчислювальних операцій [1]. Модулярне представлення [2, 3] (яке також називають представленням у системі залишкових класів (СЗК) або системі класів лишків) є одним з можливих способів побудови паралельних обчислювальних архітектур. Для ряду спеціалізованих застосувань апарат модулярної арифметики в сукупності з двійковою арифметикою може бути використаний з метою підвищення ефективності таких пристроїв [4–5].

Можна виділити дві основних "природних" переваги модулярного представлення [3]:

– по–перше, арифметичні операції додавання, віднімання і множення виконуються без переносів, на відміну від звичайного позиційного представлення чисел;

– по–друге, для кожного значення модуля арифметичні операції виконуються з парою відповідних залишків малої розрядності паралельно і незалежно один від одного, а процес обчислень із даними малої розрядності природно забезпечує збільшення швидкодії всього пристрою.

II. Теоретичні основи системи залишкових класів та постановка задачі

Фундаментальною основою СЗК є теорія чисел, зокрема, китайська теорема про залишки [2]. Будь–яке ціле додатнє число N у десятковій системі числення представляється у СЗК у вигляді залишків $(b_1, b_2, \dots, b_k)_{p1, p2, \dots, pk}$ від ділення N на кожен із попарно взаємно простих модулів: $N=(b_1, b_2, \dots, b_k)_{p1, p2, \dots, pk}$, де $b_i=N \bmod p_i$, k – кількість модулів. При цьому повинна виконуватись умова $N \le P-1$ $\left(P=\prod_{i=1}^{k} p_i\right)$.

Зворотнє перетворення із базису Крестенсона у десяткову систему числення є досить громіздке і грунтується на використанні китайської теореми про остачі [2]: $N=\left(\sum_{i=1}^{k} b_i B_i\right) mod\ P$, де $B_i=M_i m_i$, $M_i=\frac{P}{p_i}$, m_i шукається з виразу $(M_i m_i) mod\ p_i = 1$ і повинна виконуватись умова $\left(\sum_{i=1}^{k} B_i\right) mod\ P = 1$.

На даний час відомі три способи пошуку оберненого елемента $m_i = M_i^{-1} \bmod p_i$: 1) послідовним перебором m_i, поки не буде виконуватись умова $M_i m_i \bmod p_i = 1$; 2) використовуючи функцію Ейлера: $m_i = M_i^{-1} \bmod p_i = M_i^{\varphi(p_i)-1} \bmod p_i$; 3) за допомогою розширеного алгоритму Евкліда.

Всі вони досить громіздкі, потребують великих затрат обчислювальних та часових ресурсів при виконанні ділень з остачею, піднесення до степеня, знаходженні функції Ейлера (факторизації p_i). Причому всі ці операції повинні виконуватися над дуже великими числами, що може привести до переповнення розрядної сітки.

У роботі [6] було описано досконалу форму СЗК (ДФ СЗК), у якій підбір модулів такий, що $m_i=1$, тобто $M_i \bmod p_i=1$. Однак, на даний час не існує універсального методу для побудови системи будь–якої кількості модулів у ДФ СЗК а також аналітичної формули для пошуку оберненого елемента при відповідному підборі модулів, що і визначає мету нашої роботи.

III. Алгоритм підбору модулів у досконалій формі системи залишкових класів

Запишемо умову для ДФ СЗК у вигляді системи: $\begin{cases} M_1 \bmod p_1 = 1 \\ \dots \\ M_n \bmod p_n = 1. \end{cases}$ і, розв'язуючи її методами теорії чисел, можна отримати формулу для підбору модулів у ДФ СЗК:

$$\begin{cases} p_1 = 2 \\ p_i = p_1 p_2 ... p_{i-1} + 1, 1 < i < n \\ p_n = p_1 p_2 ... p_{n-1} - 1. \end{cases}$$

Слід зазначити, що запропонований метод не вичерпує всіх можливих наборів модулів для СЗК при заданих *n*. Однак набір модулів, отриманий за допомогою останньої системи, найоптимальніший, оскільки в цьому випадку величина *P* є максимальна, що дозволяє розглядати найбільший діапазон десяткових чисел. При цьому досягається зменшення розрядності приблизно вдвічі.

IV. Підбір модулів у випадку їх обмеженої кількості

У випадку обмеженої кількості модулів та необхідності розгляду великих чисел зручно використати іншу форму СЗК, яку назвемо напівдосконалою (НДФ), тобто підібрати такий набір модулів, що m_i=±1. Порівняно з ДФ СЗК, обчислювальну складність збільшується, але вона менша, ніж при пошуку оберненого елемента $m_i = M_i^{-1} mod\ p_i$.

Запропонований метод дозволяє побудувати систему з двох модулів, що неможливо у ДФ СЗК. Для цього необхідно вибрати два будь–які послідовні числа p_1 та p_2=p_1+1, які завжди будуть взаємно простими, оскільки для них виконується умова: $\begin{cases} (p_1 + 1) mod\ p_1 = 1 \\ p_1\ mod (p_1 + 1) = -1. \end{cases}$

Остання система дозволяє записати загальну формулу для визначення різноманітних наборів будь–якої кількості модулів, для яких коефіцієнти m_i=±1. Вважаючи p_1 найменшим у наборі модулів, можемо отримати: $\begin{cases} p_2 = p_1 + 1 \\ p_i = p_1 p_2 ... p_{i-1} \pm 1, \end{cases}$ де *i* = 3, 4, ... , *n*. Звідси видно, що для будь–якого модуля p_i виконується умова M_i mod p_i=±1.

V. Підбір модулів для аналітичного обчислення обернених чисел

Розглянемо набір модулів у такому вигляді: p_1=2^n–1; p_2=2^n+1; p_3=2^{2n} +1; p_4=2^{4n} +1; …, $p_i = 2^{n \cdot 2^{i-2}} + 1$; ..., $p_{k-1} = 2^{n \cdot 2^{k-3}} + 1$; $p_k = 2^{n \cdot 2^{k-2}} + 1$.

Неважко бачити, що кожен наступний модуль на дві одиниці більший від добутку всіх попередніх. Цим визначається їх взаємна простота. Крім того, діапазон десяткових чисел обмежується виразом $P = 2^{n \cdot 2^{k-1}} - 1$, де n – степінь двійки в модулі p_1.

Досліджуючи дані рівняння, можна отримати, що $m_i = \begin{cases} 2^{n \cdot 2^{i-2}} - 2^{n \cdot 2^{i-2} - k_i} + 1, \ a_i - непарне; \\ 2^{n \cdot 2^{i-2} - k_i}, \ a_i - парне, \end{cases}$, де k_i та a_i визначаються з рівності $k - (i-1) = 2^{i-2} n a_i + k_i$.

VI. Висновки

Отже, з вищесказаного видно, що СЗК на даний час залишається досить перспективною для застосування у сучасних обчислювальних системах, особливо під час виконання деяких операцій (додавання, віднімання та множення) з великими числами. Крім того, відповідний підбір модулів приводить до значного зменшення обчислювальної складності при переведенні чисел з СЗК в десяткову систему числення.

Список використаних джерел

1. Гофф Макс К. Сетевые распределенные вычисления: достижения и проблемы. – М.: Кудиц–образ, 2006. – 320 с.
2. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384 с.
3. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 460 с.
4. Анісімов А.В. Алгоритмічна теорія великих чисел. – К.: Академперідика, 2001. – 152 с.
5. Николайчук Я.М., Волинський О.І., Кулина С.В. Теоретичні основи побудови та структура спецпроцесорів в базисі Крестенсона. Вісник Хмельницького національного університету.– Хмельницький. – 2007. – №3. – Т1. – С.85–90.
6. Николайчук Я.М. Теорія джерел інформації. – Тернопіль: ТзОВ „Терно–граф”, 2010. – 536 с.