проводиться порівняння з нулем цього значення γ_{n+1}. Якщо $\gamma_{n+1} = 0$ число А знаходиться в діапазоні [0,M)), то робиться висновок, що число А не спотворено (правильне), тобто помилок немає. Якщо $\gamma_{n+1} \neq 0$ (число А не знаходиться в діапазоні [0,M)), те число А спотворено (неправильне), тобто присутня помилка по одному з підстав (модулів) m_i МА [5].

Спільний час T_l виявлення помилки визначається як $T_l = T_{нl} + T_{cl}$, де T_{cl} –час порівняння значення γ_{n+1} з нулем. Практично час T_{cl} порівняння виконується за один такт, в цьому випадку можна вважати, що $T_l T_{Hl} = 2n \approx \tau$.

Список літератури

1. Акушский, И. Я. Машинная арифметики в остаточных класах / И. Я. Акушский, Д. И. Юдицкий. – М.: Радио и связь, 1968. – 444 с..
2. Сиора, А. А. Отказоустойчивые системы с версионно-информационной избыточностью в АСУ / А. А. Сиора, В.А Краснобаев , В.С. Харченко. – ТП: Монография. - Х.: МОН, НАУ им. Н.Е. Жуковского (ХАИ), 2009. 320с.
3. Лосев, Ю. И. Методы и модели обмена информацией в распределенных адаптивных вычислительных сетях с временной параметризацией параллельных процессов / Ю. И. Лосев, С. И. Шматков, К. М. Руккас. – Х.: ХНУ им. В. Н. Каразина, 2011. – 204 с.
4. Янко, А. С. Метод быстрого сравнения двух целых чисел в системе остаточных классов / А. С. Янко, В. Н. Курчанов, В. А. Краснобаев // ІІІ Міжнародна науково-технічна конференція «Проблеми інформатизації». Тези доповідей. – Черкаси. – 12-13 листопада 2015. – С. 45.
5. Янко, А. С. Основные свойства непозиционной системы счисления / В. А. Краснобаев, С. В. Сомов, А. С. Янко // Системи управління, навігації та зв'язку : зб. наук. пр. / Полтавський національний технічний університет імені Юрія Кондратюка. – П.: ПолтНТУ, 2013. – Вип. 1(25). – С. 110-113.

УДК 681.03

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ АРИФМЕТИЧНИХ ОПЕРАЦІЙ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

В.М. Свистун, *магістрант*
А.С. Янко, *к.т.н.*
Полтавський національний технічний університет імені Юрія Кондратюка

Відомі методи підвищення продуктивності сучасних комп'ютерних систем, які функціонують в позиційних системах числення (ПСЧ), мають загальний недолік – неможливість розпаралелення алгоритму, який розв'язується, на рівні елементарних операцій (мікрооперацій). Це обумовлено, перш за все, наявністю у ПСЧ між розрядних зв'язків між операндами системи. Розвиток сучасної мікроелектронної бази, основаної на застосуванні великих і над великих інтегральних схем, спонукає до дослідження можливості застосування табличних методів обробки інформації. Їх застосування може забезпечити надвисоку продуктивність (в результаті розпаралелення елементарних операцій) і надійність ЕОМ, а також високу степінь регулярності і однорідності структури пристроїв їх реалізації. Істотним недоліком табличних методів обробки інформації, які застосовуються в ПСЧ, залишається необхідність використання значної кількості обладнання [1], що суттєво ускладнює їх реалізацію. Тому природно, що здійснюється пошук можливостей застосування такої арифметики, в якій би порозрядні зв'язки були відсутні. У цьому плані звертає на себе увагу непозиційна система числення у системі залишкових класів (СКЗ).

Реалізація арифметичних операцій у СКЗ виконуються незалежно і паралельно над

однойменними розрядами, а структура операційного пристрою комп'ютерних засобів обробки даних (КЗОД) представляється у вигляді незалежних обчислювальних трактів, кожен з яких функціонує за своєю основою m_i СКЗ.

Незалежність залишків за прийнятою системою основ, дає можливість для побудови нової машинної арифметики та принципово нової схемної реалізації КЗОД. Це сприяє для вибору рішень при реалізації модульних арифметичних операцій, заснованих за допомогою методів:суматорного; табличного та методу кільцевого зсуву.

При суматорному методі використовується n (по числу основ СКЗ) малорозрядних суматорів по відповідним модулям $m_i \ (i = \overline{1,n})$. При побудові КЗОД кожен із розрядів числа обробляється незалежно, але час виконання всієї операції визначається часом необхідним для отримання результату по найбільшій основі СЗК.

У табличному операційному пристрої КЗОД для реалізації арифметичних операцій являє собою двохвходове ПЗП. Для кожного з входів кількість вхідних шин для l-байтової (8l двійкових розрядів) КЗОД рівна 2^{8l}. При цьому загальна кількість логічних схем співпадання "І" у вузлах ПЗП рівна $N_{l\ ПСЧ} = 2^{8l} \times 2^{8l} = 2^{16l}$. З цього видно, що таблична реалізація цілочисельних модульних арифметичних операцій у ПСЧ доцільна лише для значення l = 1 (є прийнятним за кількістю обладнання). Однак, для збільшення довжини розрядної сітки КЗОД зараз пропонується до практичного використання КЗОД для l = 2. Цілком прийнятно при реалізації арифметичних операцій для КЗОД у СКЗ з l = 4 і l = 8. Переваги табличного методу реалізації арифметичних операцій: табличні схеми мають високу надійність; простота табличних схем і дешифраторів; висока швидкодія (результат операції може бути отриманий в момент надходження вхідних операндів, тобто в один такт).

При суматорному методі проявляється наявність міжрозрядних зв'язків у межах даної основи m_i СЗК. При табличному методі відсутні міжрозрядні зв'язки між обробляючими операндами взагалі, однак, для достатньо великої розрядної сітки КЗОД різко збільшується кількість обладнання операційних пристроїв.

Особливість методу кільцевого зсуву в тому, що результат арифметичної операції $(a_i \pm \beta_i) \bmod m_i$ по довільному модулю КЛ, заданої сукупності $\{m_j\}, j = \overline{1,n}$, основ, визначається тільки за рахунок послідовно циклічних зсувів заданої цифрової структури. Перевага методу полягає у відсутності міжрозрядних перенесень, що істотно підвищує достовірність реалізації модульних операцій. Проте час виконання модульних операцій порівняно великий, що знижує загальну ефективність вживання КЗОД у СЗК. Дана обставина й обумовлює необхідність розробки алгоритмів підвищення швидкодії виконання даних операцій у КЗОД.

Максимальної швидкодії виконання арифметичних операцій при використанні методу кільцевого зсуву можна досягти, використовуючи програмний метод реалізації модульних операцій. використовуючи керуючі матриці, в більшості варіантів результат операції $(a_i \pm \beta_i) \bmod m_i$ можна досягти за менше, ніж $k\ \beta_i$, число зсувів двійкових розрядів.

Список літератури

1. Акушский И. Я. Машинная арифметика в остаточных классах / И. Я. Акушский, Д. И. Юдицкий. – М. : Советское радио, 1968. – 440 с.
2. Андреева Е., Фалина И. Системы счисления и компьютерная арифметика. - Учебное пособие.- БИНОМ, 2004.
3. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems (ex-tended abstract)// Advances in Cryptology— CRYPTO'90// Lecture Notes in Computer Science. Springer-Verlag. — 1991. — V. 537. — P. 2-21.
4. Янко, А. С. Метод табличной реализации операции умножения в классе вычетов / В. А. Краснобаев, А. С. Янко, С. А. Кошман // Системи обробки інформації : зб. наук. пр. / Харківський університет Повітряних Сил імені Івана Кожедуба. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 121-127.