також дозволяє в декілька разів зменшити число пам'яті для зберігання великого простого числа, оскільки для запису, наприклад, 16-бітного числа використовується лише його семибітне закінчення та біт синхронізації.

Список використаних джерел

1. M. Kasianchuk. Theoretical Foundations of the Modified Perfect form of Residue Number System / M. Kasianchuk, Ya. M. Nykolaychuk, , I. Z. Yakymenko // Cybernetics and Systems Analysis. – March, 2016. -Volume 52, Issue 2. – pp.219-223.
2. Karpinski M. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / M. Karpiński, S. Ivasiev, I. Yakymenko, M. Kasianchuk ,T. Gancarczyk// Proc. of 16th International Conference on Control, Automation and Systems (ICCAS–2016) – Gyeongju, Korea. – V.1. – October, 2016. – P.1484–1486.
3. Николайчук Я.М. Метод збереження простих великорозрядних чисел у базисі Радемахера / Я.М. Николайчук, І.З. Якименко, М.М. Касянчук, С.В. Івасьєв // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)". Київ: Інститут кібернетики імені В.М. Глушкова НАН України. - 2015. –С. 159-161.

УДК 681.3

МЕТОДИ ВИКОНАННЯ АРИФМЕТИЧНИХ ОПЕРЦІЙ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Івасьєв С.В.[1)], Паздрій І.Р.[2)], Петелько В.В. [3)]

Тернопільський національний економічний університет

[1)] к.т.н.; [2)] к.т.н., доцент; [3)] магістрант

I. Постановка проблеми

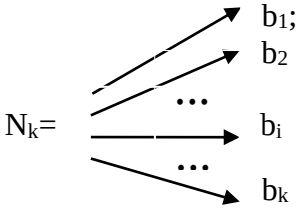
З огляду на сучасний рівень розвитку обчислювальних засобів використання непозиційних систем числення дозволяє збільшити надійність та швидкість цифрової обробки даних. Сучасні обчислювальні потужності дозволяють розв'язувати задачі оптимального вибору модулів системи та розрахунку відповідних вагових коефіцієнтів та базисних чисел, що відкриває нові можливості застосування непозиційних систем числення, в яких можлива реалізація розпаралелення процесу виконання арифметичних операцій. Однією з них є система залишкових класів (СЗК) [1-3].

II. Мета роботи

Метою роботи є дослідження методів виконання арифметичних операцій в СЗК. До недоліків існуючих рішень відносять труднощі під час виконання немодульних операцій, зокрема, порівняння чисел, ділення, визначення знаку числа, оцінка виходу результату за допустимий діапазон тощо.

III. Арифметичні операції в системі залишкових класів

В основу цілочисельного перетворення СЗК покладена Китайська теорема про залишки, згідно якої будь-яке ціле число можна однозначно перетворити набором найменших невід'ємних залишків в системі взаємно простих модулів за схемою, представленою на рисунку, та відповідною її формулою:



$$b_i = res\ N_k (mod\ p_i), \quad (1)$$

що відповідає рішенню діофантового рівняння:

$$N_k = b_i (\mathrm{mod}\ p_i) \quad (2)$$

або цілочисельному рішенню лінійного рівняння:

$$N_k = a_i p_i + b_i, \quad (3)$$

де a_i – ранг; b_i – найменший невід'ємний залишок.

При цьому діапазон кодування чисел N_k:

$$P = \prod_{i=1}^{k} p_i \; ; \; 0 \le N_k \le P\text{-}1. \tag{4}$$

Таким чином, ціле число N_k однозначно представляється набором залишків b_i.

Зворотне перетворення цілочисельної форми СЗК виконується згідно аналітичного виразу:

$$N_k = res \sum_{i=1}^{k} b_i \cdot B_i (\mathrm{mod}\, P), \tag{5}$$

де B_i – базисні числа СЗК, які обчислюються згідно діофантового рівняння:

$$B_i = \frac{P}{p_i} \cdot m_i \equiv 1 (\mathrm{mod}\, P_i). \tag{6}$$

Тобто для виконання зворотнього перетворення цілочисельної форми СЗК необхідно задати такі параметри:

1. Набір взаємно простих модулів $p_1, p_2, ..., p_i, ..., p_k$;
2. Діапазон кодування чисел P;
3. Набір базисних чисел $B_1, B_2, ..., B_i, ..., B_к$;
4. Набір коефіцієнтів, які забезпечують ортогональність перетворень: $m_1, m_2, \ldots, m_i, \ldots, m_k$;
5. Аналітичні вирази прямого і зворотнього перетворення:

$$b_i = res\, N_k (\mathrm{mod}\, p_i), \; N_k = res \sum_{i=1}^{k} b_i * B_i (\mathrm{mod}\, P). \tag{7}$$

Недоліком цілочисельної форми перетворення СЗК є практична відсутність простої операції порівняння чисел, що суттєво ускладнює реалізації алгоритмів та відповідних процесів ділення. В той же час, переваги однотактного матричного виконання інших арифметичних операцій забезпечують широкі перспективи застосування теоретичних основ цілочисельного перетворення СЗК для виконання операцій додавання та множення. Розмежовану СЗК (РСЗК) можна ефективно застосовувати для операцій додавання, множення та обчислення залишків по модулю. Типовими задачами застосування наведених операцій є шифрування та дешифрування інформаційних потоків у системах захисту інформації [4], розв'язання систем великої розмірності, задачі знаходження найбільших дільників двох великорозрядних чисел, пошуку простих чисел великої розрядності та ряд інших аналогічних задач.

Теоретичною основою РСЗК є цілочисельна форма СЗК, рівняння якої представлено у вигляді суми [5]: $N_k = N_{1k} + N_{2k} + ... + N_{ik} + ... + N_{nk}$, де N_{ik} – m- розрядний (розмежований) фрагмент числа N_k, яке представлене у двійковій системі числення. Таким чином, пряме перетворення РСЗК має вигляд :

$$N_k = \begin{cases} b_1 = (b_{11} + b_{21} + ... + b_{r1} + ... + b_{n1}) \mathrm{mod} p_1 \\ b_2 = (b_{12} + b_{22} + ... + b_{r2} + ... + b_{n2}) \mathrm{mod} p_2 \\ \ldots \\ b_i = (b_{1i} + b_{2i} + ... + b_{ri} + ... + b_{ni}) \mathrm{mod} p_i \\ \ldots \\ b_k \; b_2 = (b_{1k} + b_{2k} + ... + b_{rk} + ... + b_{nk}) \mathrm{mod} p_k. \end{cases}$$

При цьому математичні операції над числами в РСЗК можуть бути розмежовані по кожному із фрагментів процесора, що забезпечує ще більш глибокий рівень розпаралелювання обробки інформації, а, відповідно, підвищення швидкодії процесора СЗК.

Висновок

Проведені в роботі дослідження показали, що недоліком цілочисельної форми перетворення СЗК є практична відсутність простої операції порівняння чисел, що суттєво ускладнює реалізації алгоритмів та відповідних процесів ділення. В той же час, виконання інших арифметичних операцій забезпечує широкі перспективи застосування теоретичних основ цілочисельного перетворення СЗК для створення та широкомасштабного впровадження спецпроцесорів в комп'ютерних мережах.

Особливу перспективу має застосування цілочисельної форми СЗК при створенні спецпроцесорів, в яких базовими операціями є додавання та множення. Прикладом таких процесорів є цифрові фільтри, обчислювачі кореляційних та спектральних характеристик випадкових процесів, а також операції над матрицями та алгебраїчними поліномами.

Список використаних джерел

1. Касянчук, М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук // Праці Міжнародного симпозіуму «Питання оптимізації обчислень (ПОО–XXXV)». Т.1. – Київ–Кацивелі. – 2009. – С. 306–310.
2. Kasianchuk, M. Algorithms of findings of perfect shape modules of remaining classes system / M. Kasianchuk, I. Yakymenko, I. Pazdriy, O. Zastavnyy // Proceedings of the XIII-th International Conference «The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)». - Polyana-Svalyava (Zakarpattya), Ukraine. - 2015. – P. 168 - 171. 10.
3. Kasianchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application / M. Kasianchuk // Proceedings of the 4-th International Conference "Advanced Computer Systems and Networks: Design and Application" (ACSN–2009). – L'viv. – 2009. – Pp. 299-301.
4. Касянчук М.М. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій системі числення Радемахера – Крестенсона / М.М. Касянчук, І.З. Якименко, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки. – 2011. – № 3. – С. 265–273.
5. Волинський О.І. Оптимізація обчислень на основі алгоритмів міжбазисних перетворень Радемахера, Крестенсона та Галуа / О.І. Волинський, О.Д. Круцкевич, П.В. Гуменний // Праці міжнародної молодіжної математичної школи “Питання оптимізації обчислень (ПОО-XXXVII)” Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2011. С. 32-33.

УДК 681.3

ПРИСТРІЙ ОБЧИСЛЕННЯ СКАЛЯРНОГО ДОБУТКУ З ФОРМУВАННЯМ ЧАСТКОВИХ РЕЗУЛЬТАТІВ НА ОСНОВІ ПОПЕРЕДНІХ ОБЧИСЛЕНЬ

Ігнатєв І.В. [1)], Пицура О.В. [2)], Карпінець Р.М. [3)]

Тернопільський національний економічний університет,

[1)]викладач, [2)]магістрант

[3)] *Національний університет «Львівська політехніка», студент*

І. Постановка проблеми

Пристрій обчислення скалярного добутку базується на використанні обчислень скалярного добутку та використовує обчислення, які здійснюються на основі однорозрядних суматорів. Скалярний добуток обчислюється у два етапи. На першому етапі за допомогою блоку БПО виконуються попередні обчислення. Дані обчислення суміщені з процесом введення множених Aj починаючи з молодших розрядів Aj Результати попередніх обчислень та вхідні дані запам’ятовуються у блоках пам’яті.

ІІ. Мета роботи

Метою дослідження є розробка структури пристрою обчислення скалярного добутку на базі попередніх обчислень, а також розробка базової структури пристрою для обчислення скалярного добутку.

ІІІ. Виклад основного матеріалу

Широке впровадження ШНМ в різних областях науки, техніки і виробництва вимагають від них високих технічних характеристик [2]. Однією з найбільш широко розповсюджених вимог, що ставиться до засобів реалізації ШНМ є забезпечення високої швидкодії. Подібна проблема виникає, як правило, при використанні ШНМ для розв’язання задач в реальному часі, який накладає певні обмеження на процес обробки інформації. Застосування ШНМ у галузях, де апаратура є бортовою, тобто такою, що возиться, носиться, літає та плаває, накладає жорсткі обмеження на їхні масогабаритні характеристики. Одночасно до засобів реалізації ШНМ висуваються жорсткі вимоги до споживаної потужності, яка впливає на габарити джерел живлення та засобів відведення тепла. Необхідність задоволення вимог забезпечення масогабаритних характеристик, енергоспоживання, вартості змушують при розробці ШНМ під заданий клас задач дуже строго підходити до вибору параметрів, що визначають апаратні затрати на їх створення.

Для обчислення часткового добутку P_{si} використовуються обчислення, які працюють на основі однорозрядних суматорів. Для визначення кількості однорозрядних суматорів визначається за допомогою формули: