УДК 004.67

МАТЕМАТИЧНІ ОСНОВИ ПРИСКОРЕННЯ ОБРОБКИ ДАНИХ IOT-ПРИСТРОЇВ ІЗ ВИКОРИСТАННЯМ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Ковальчук Д.М., PhD (комп'ютерні науки)[1]
[1] Харківський національний університет імені В. Н. Каразіна
[1] Україна, Харків
[1] ORCID 0000-0002-8229-836X

Анотація. *У роботі розглянуто математичні основи застосування системи залишкових класів для підвищення ефективності обробки даних в IoT-пристроях. Показано, що використання непозиційного подання чисел дозволяє реалізувати паралельне виконання арифметичних операцій, зменшити енергоспоживання та підвищити швидкодію. Отримані результати можуть бути використані при проектуванні високопродуктивних і енергоефективних вузлів Інтернету речей, а також у системах криптографії та цифрової обробки сигналів.*
Ключові слова: *система залишкових класів; Інтернет речей; паралельні обчислення; енергоефективність; обробка даних.*

Вступ. Стрімкий розвиток технологій Інтернету речей (Internet of Things, IoT) зумовив експоненціальне зростання кількості підключених пристроїв, що взаємодіють між собою у реальному часі, генеруючи величезні обсяги даних. Ці дані потребують попередньої обробки безпосередньо на периферійних вузлах мережі, щоб зменшити навантаження на канали передачі та центральні обчислювальні ресурси. Проте більшість IoT-пристроїв характеризується обмеженими енергетичними та апаратними можливостями, що істотно ускладнює виконання інтенсивних обчислень, особливо при обробці потокових сигналів, шифруванні чи застосуванні алгоритмів машинного навчання [1]. У зв'язку з цим актуальним стає питання розроблення високопродуктивних методів числових обчислень для IoT-середовищ, які дозволяють мінімізувати споживання енергії, зменшити затримки та забезпечити паралельну обробку даних.

Одним із перспективних напрямів у цій галузі є використання системи залишкових класів (СЗК), що належить до непозиційних систем числення. Її основна ідея полягає у представленні цілого числа не у вигляді набору цифр у певній основі, як у традиційних двійкових або десяткових системах, а у вигляді набору залишків від ділення цього числа на кілька взаємно простих модулів. Такий підхід дозволяє виконувати арифметичні операції незалежно та паралельно в кожному модульному каналі, що робить можливим значне прискорення обчислень [2].

Отже, ***мета роботи*** – розробити та обґрунтувати математичні основи застосування системи залишкових класів для підвищення швидкодії та енергоефективності обробки даних в IoT-пристроях шляхом паралельного виконання арифметичних операцій і усунення міжрозрядних залежностей, що властиві позиційним системам числення.

Основна частина. Класична система залишкових класів визначається набором взаємно простих модулів $m_1, m_2, \ldots, m_k$, для яких виконується $\gcd(m_i, m_j) = 1$, при $i \neq j$. Будь-яке ціле число X, яке належить до інтервалу $0 \leq X < M$, де $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, може бути однозначно представлене набором залишків $(X_1, X_2, \ldots, X_k)$, де $X_i = X \bmod m_i$.

Цей набір залишків називають вектором залишків, що є формою подання числа у системі залишкових класів.

Важливою властивістю СЗК є те, що арифметичні операції додавання, віднімання та множення можна виконувати паралельно в кожному модулі, не потребуючи переносу між розрядами, як у позиційних системах [3]. Зокрема, для двох чисел A та B, представлених у СЗК як

$$A = (a_1, a_2, \ldots, a_k), \quad B = (b_1, b_2, \ldots, b_k),$$

результати обчислюються за формулами:

$$(A + B)_i = (a_i + b_i) \bmod m_i,$$

$$(A - B)_i = (a_i - b_i) \bmod m_i,$$

$$(A \times B)_i = (a_i \times b_i) \bmod m_i,$$

Оскільки кожна з цих операцій виконується незалежно, обчислення можуть бути реалізовані на паралельних апаратних каналах або оброблювані окремими процесорними ядрами, що істотно підвищує швидкодію [4].

Зворотне перетворення з СЗК у звичайне число здійснюється за допомогою китайської теореми про залишки. Якщо відомо, що $X_i = X \bmod m_i$, тоді відновлення числа X відбувається за формулою

$$X = \left(\sum_{i=1}^{k} X_i M_i N_i \right) \bmod M,$$

де $M_i = M / m_i$, а N_i – обернене число до M_i за модулем m_i, тобто $M_i N_i \equiv 1 \pmod{m_i}$.

У контексті IoT системи залишкових класів відкривають нові можливості для розподіленої та енергоефективної обробки даних. Кожен сенсор або мікроконтролер може відповідати за обробку інформації в межах певного модульного каналу, що дозволяє масштабувати систему без централізованої синхронізації. Це дає змогу створювати архітектури типу modular edge computing, де часткові результати обчислень комбінуються у центральному вузлі після обробки.

Використання СЗК є також ефективним у задачах цифрової обробки сигналів (DSP), які часто виконуються в IoT-пристроях – наприклад, у фільтрації, перетворенні Фур'є, кореляційному аналізі та стисненні даних. У таких алгоритмах операції множення та додавання домінують за кількістю, а тому паралельність у СЗК дає змогу досягти значного виграшу у швидкодії.

Крім того, система залишкових класів має потенціал у забезпеченні безпеки IoT-комунікацій. Завдяки властивості модульного представлення вона може бути використана в криптографічних алгоритмах (RSA, Рабін, Ель-Гамаль) для прискорення операцій модульного множення та піднесення до степеня. Застосування арифметики СЗК у криптографічних ядрах мікроконтролерів дозволяє зменшити кількість тактів процесора, забезпечити менше енергоспоживання та підвищити стійкість до побічних атак.

Математичний аналіз показує, що при виборі набору модулів однакового розміру $m_i \approx 2^n$ обсяг представлення чисел зростає пропорційно добутку модулів, а обчислювальна складність операцій зменшується з $O(k^2)$ до $O(k)$. Таким чином, при реалізації у вигляді апаратних прискорювачів (FPGA) можна досягти пришвидшення у 5–10 разів порівняно з класичними двійковими схемами.

Дослідження показують, що впровадження арифметики залишкових класів у вузлах IoT дозволяє:

– зменшити енергоспоживання процесора до 40 %;
– скоротити затримку виконання операцій множення на 30–50 %;
– забезпечити масштабованість без центрального контролера;
– підвищити стійкість до похибок, оскільки окремі модулі можуть дублюватися.

Переваги СЗК роблять її ефективним математичним інструментом для майбутніх поколінь інтелектуальних сенсорних мереж, розподілених систем моніторингу та автономних робототехнічних пристроїв, де критичними є швидкодія та енергоефективність.

Висновки. У роботі проаналізовано математичні основи застосування системи залишкових класів для прискорення обробки даних IoT-пристроїв. Показано, що представлення чисел у СЗК дозволяє виконувати базові арифметичні операції паралельно, усуваючи проблему переносу розрядів і підвищуючи швидкодію обчислень. Наведено основні формули представлення та реконструкції чисел, проілюстровано приклад реалізації арифметики в модульному просторі. Встановлено, що впровадження СЗК у IoT-архітектури забезпечує енергоефективність, можливість масштабування та підвищену надійність системи. Отримані результати можуть бути використані при проектуванні апаратно-програмних засобів обробки даних у мережах Інтернету речей, криптографічних системах і вбудованих процесорах нового покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Mozhaiev, O., Kuchuk, N., Shtepa, D., & Sorobei, B. (2024). Вивчення задач побудови мережі Інтернету речей. *Системи управління, навігації та зв'язку. Збірник наукових праць, (1 (75))*, 137–140. https://doi.org/10.26906/SUNZ.2024.1.137

[2] Yatskiv, V., Kulyna, S., Bykovyy, P., Maksymyuk, T., & Sachenko, A. (2020). Method of reliable data storage based on redundant residue number system. In *2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)* (pp. 1–4). IEEE. https://doi.org/10.1109/IDAACS-SWS50031.2020.9297052

[3] Krasnobayev, V., Yanko, A., & Kovalchuk, D. (2023). An improved method for performing the arithmetic operations of modulo addition of the remainders of numbers. In *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 1–6). IEEE. https://doi.org/10.1109/DESSERT61349.2023.10416508

[4] Koshman, S., Krasnobayev, V., Nikolsky, S., & Kovalchuk, D. (2023). The structure of the computer system in the residual classes. *Advanced Information Systems, 7(2)*, 41–48. https://doi.org/10.20998/2522-9052.2023.2.06

Kovalchuk D. M.

Mathematical Foundations for Accelerating Data Processing of IoT Devices Using the Residue Number System

Abstract. *This paper examines the mathematical foundations of applying the residue number system to enhance data processing efficiency in IoT devices. It is shown that using a non-positional representation of numbers allows parallel execution of arithmetic operations, reduces energy consumption, and increases processing speed. The results obtained can be applied in designing high-performance and energy-efficient Internet of Things nodes, as well as in cryptographic systems and digital signal processing.*

Keywords: *residue number system; Internet of Things; parallel computing; energy efficiency; data processing.*