НОВІ ЗАСОБИ КІБЕРНЕТИКИ, ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ТА СИСТЕМНОГО АНАЛІЗУ

УДК 519.6

В.К. ЗАДІРАКА
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *zvk140@ukr.net*.

А.М. ТЕРЕЩЕНКО
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *teramidi@ukr.net.*

ПАРАЛЕЛЬНІ МЕТОДИ ПРЕДСТАВЛЕННЯ ЧИСЕЛ ДЛЯ ТЕСТУВАННЯ ОПЕРАЦІЙ БАГАТОРОЗРЯДНОЇ АРИФМЕТИКИ

Анотація. Запропоновано методи реалізації операції представлення багаторозрядного числа у системі числення з іншою основою, потрібні для тестування арифметичних операцій у разі використання паралельних процесорів. Розглянуто представлення числа у системах числення на основі багаторозрядних операцій ділення та віднімання або багаторозрядних операцій множення та додавання. Алгоритм з розбиттям числа на групи цифр дає змогу враховувати довжину машинного слова та розподіляти обчислення між процесорами. Проаналізовано складність за кількістю операцій, обсяг додаткової пам'яті для алгоритмів на основі ітераційного та рекурсивного методів.

Ключові слова: система числення, багаторозрядна арифметика, багаторозрядне додавання, багаторозрядне множення, паралельна модель обчислень.

ВСТУП

Система числення визначає архітектуру пристрою, який реалізує операції для цієї системи. Представлення чисел залежить від конкретної фізичної реалізації елементів пристрою. Використання нових паралельних обчислювальних систем, таких як багатоядерні процесори, графічні прискорювачі, кластери, системи з розподіленою пам'яттю, розподілені системи та інші, зумовлено потребою розв'язання прикладних задач у різних галузях. Серед таких задач можна виокремити задачі обчислення оболонок ядерних реакторів, моделювання фізичних, хімічних процесів, аеродинаміки, гідродинаміки, захисту інформації, високоточних обчислень тощо. Алгоритми багаторозрядної арифметики залежать від системи числення, у якій їх використовують. Швидкодія асиметричних криптографічних програмно-апаратних комплексів [1–5] залежить від багаторозрядної операції множення, яка є складовою операції піднесення до степеня за модулем. Системи числення у залишкових класах [6, 7] мають швидкі реалізації багаторозрядної операції множення та піднесення до степеня за модулем. А для порівняння чисел у залишкових класах використовують метод, у якому багаторозрядні числа представляють у позиційній системі числення зі змішаною основою для порівняння. У логарифмічній системі числення операції додавання та віднімання відповідають операції множення та ділення у зви-