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.*

ЗНАХОДЖЕННЯ СУМИ БАГАТОРОЗРЯДНИХ ЧИСЕЛ У ПАРАЛЕЛЬНІЙ МОДЕЛІ ОБЧИСЛЕННЯ

Анотація. Запропоновано новий метод реалізації операції знаходження суми двох і більше багатослівних доданків у паралельній моделі обчислення, який дає змогу звести знаходження суми великої кількості багатослівних доданків до операції знаходження двох багатослівних доданків за рахунок збереження знаків переносів для багатослівних чисел, ефективної в паралельній моделі обчислення на основі методу «прогнозування знаків переносів між групами слів». Запропоновано також алгоритми реалізації операції знаходження суми доданків на одному процесорі та k процесорах. Наведено аналіз складності таких алгоритмів.

Ключові слова: багаторозрядна арифметика, багаторозрядне додавання, знак переносу, паралельна модель обчислення.

ВСТУП

Використання нових паралельних обчислювальних систем, таких як багатоядерні процесори, графічні прискорювачі, кластери, розподілені системи, системи з розподіленою пам'яттю та інші, зумовлено потребою розв'язання складних прикладних задач у різних галузях. Серед них можна виділити задачі обчислення систем лінійних алгебричних рівнянь з кількістю невідомих 33–35 млн, моделювання фізичних процесів, аеродинаміки, захисту інформації тощо. Новітні технології значно розширюють використання багаторозрядної арифметики, тому що неврахування похибок заокруглення призводить до того, що іноді отримують комп'ютерні рішення, які не відповідають фізичному змісту. Багаторозрядна операція множення є складовою операції піднесення до степеня за модулем, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів [1–7]. У процесі реалізації операції множення час її виконання залежить від того, наскільки швидко можна додати два і більше великих чисел. У паралельній моделі обчислення час виконання операції додавання залежить від методу, на основі якого враховуються знаки переносу, які виникають в разі переповнення у відповідних розрядах (машинних словах) багаторозрядної суми двох чисел.

У роботі [8] подано аналіз імовірності появи знака переносу та запропоновано ефективний метод додавання не тільки додатних, а й від'ємних цілих чисел на основі інтерференційних суматорів, які дають змогу виконувати додавання N-бітових цілих чисел за $O(N) = N + K$ кроків, де K — кількість інтерференційних перетворень. У [9] запропоновано алгоритми ефективної реалізації