Терещенко Андрій Миколайович

кандидат фізико-математичних наук, докторант Інституту кібернетики імені В.М. Глушкова НАН України

Ефективні за швидкодією алгоритми виконання операцій багаторозрядної арифметики у послідовній та паралельній моделях обчислень

У рамках доповіді розглядаються послідовна та паралельні моделі обчислень для реалізації багаторозрядних операцій для розв'язання задач інформаційної безпеки за рахунок розробки нових методів реалізації та тестування багаторозрядних операцій, пошуку областей ефективного їх використання.

У доповіді розглядаються нові методи реалізації операцій багатослівного додавання, віднімання, порівняння у паралельній моделі обчислень. Методи оперують словами та групами слів та дають змогу "передбачити" знаки переносу між групами слів. Методи базується на векторних операціях, що значно зменшує кількість задіяних паралельних процесорів.

У рамках доповіді розглядається новий метод реалізації операції знаходження суми трьох і більше багатослівних чисел у паралельній моделі. Метод дає змогу звести операцію знаходження суми великої кількості N–розрядних доданків до операції додавання двох доданків (одного N–розрядного доданку та одного N+1–розрядного доданку), яку в паралельній моделі обчислень можна ефективно реалізувати на основі «методу передбачення знаків переносів між групами слів».

Наводяться результати проведеного аналізу складності алгоритму множення методами «у стовпчик», множення NM–розрядних чисел та Карацуби-Офмана з розпаралелюванням виконання однослівних операцій додавання та множення між процесорами без врахування знаків переносів. Наводяться оцінки складності для паралельної моделі обчислень за умови необмеженої кількості задіяних процесорів та за умови, коли кількість процесорів є обмеженою. Проведено аналіз залежності кількості задіяних процесорів від кількості операцій алгоритму та різної довжини багаторозрядних чисел.

Для реалізації операції обчислення багаторозрядної згортки пропонується нова ефективна схема перерозподілу обчислень на основі використання циклічних згорток меншої розрядності. Така схема може бути використана для реалізації багаторозрядної операція множення у паралельній моделі обчислень на основі векторних операцій.

Розглядається новий метод обчислення циклічної згортки довжиною, яка дорівнює добутку взаємно простих чисел. Метод дозволяє звести обчислення згортки певної дожини до обчислення циклічних згорток меншої довжини. Циклічні згортки меншої довжини потребують нескладних перед- та післяобчислень зі застосуванням циклічних зсувів для реалізації обчислення.

Наводяться апріорні оцінки складності обчислення згорток довжиною, яка дорівнює добутку взаємно простих чисел.

Наводиться модифікація алгоритму реалізації операції множення двох N-розрядних чисел на основі ШПФ та попереднім обчисленням коефіцієнтів ДПФ. У новій модифікації використовується корегуючий доданок та операції виконуються над сигналами розрядності N замість розрядності $2N$, що дозволяє зменшити у два рази кількість задіяних процесорів у паралельній моделі.

Розглядається обчислення циклічної згортки, кожна точка якої є багаторозрядним числом. Для реалізації операцій множення та додавання такої згортки пропонується використання ШПФ невеликої довжини. Наводиться аналіз складності за кількістю однорозрядних операцій у випадку використання ШПФ різної довжини для циклічних згорток з різною кількістю точок, який показую з якої кількості точок циклічної згортки та довжини ШПФ запропонований метод є ефективним ніж метод, заснований на методі множення «у стовпчик».

Розглядається новий метод множення багаторозрядних чисел на основі дискретного косинусного перетворення (ДКП) та дискретного синусного перетворення (ДСП), у якому розділено обчислення для дійсної та уявної частин ДПФ, що дозволяє перевести обчислення з поля комплексних чисел у поле дійсних та цілих чисел та зменшити складність багаторозрядної операції множення до лінійної складності за кількістю однорозрядних множень.

Наводиться модифікація методу множення на основі ДКП та ДСП, яка дає змогу використовувати дискретне перетворення двічі меншої розрядності. Запропонований алгоритм множення чисел зберігає симетрію у дійсній та уявній частинах багаторозрядних комплексних чисел, що дає змогу задіяти вдвічі більшу кількість ДКП та ДСП з вдвічі меншими розрядностями.

Пропонується метод піднесення до степеня n багаторозрядного числа. Наводиться аналіз складності за кількістю бітових операцій додавання, віднімання та множення. У наведеній реалізації операції обчислення кореня степені n великого числа показано, яким чино можна уникнути операції ділення у разі, коли довжина слова не перевищує 32 біти.

У доповіді розглядаються методи генерації вхідних та вихідних багаторозрядних чисел для перевірки правильності обчислень багаторозрядних операцій додавання, віднімання, множення, множення за модулем та піднесення до степеня за модулем, що значно зберігає час, необхідний для підготовки тестових даних та тестування. Наводяться прості залежності генерування вхідних та вихідних багаторозрядних даних для візуальної перевірки. Залежності надаються у загальному вигляді, що дозволяє генерувати вхідні дані та результати для пристроїв, які оперують словами різної довжини (8, 16, 32, 64, 128, 256, і. д. бітів).

У доповіді розглядаються методи представлення чисел у системах числення для тестування операцій у послідовній та паралельній моделях обчислень. Пропонуються методи, які дозволяють розпаралелити алгоритм представлення числа у системі числення з іншою основою. Надається аналіз складності алгоритмів за кількістю однорозрядних операцій на основі ітераційного та рекурсивного методів, які враховують довжину машинного слова у бітах за рахунок розбиття на групи цифр, кожну з яких опрацьовує окремий процесор.