**Коржавина Анастасия Сергеевна Методы и алгоритмы модулярной арифметики для массовой обработки сверхдлинных чисел на гибридных вычислительных платформах**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Коржавина Анастасия Сергеевна

Введение

Глава 1. Организация массовых высокоточных арифметических вычислений

1.1 Вычислительные задачи, требующие массовых высокоточных вычислений

1.1.1 Экспериментальная математика

1.1.2 Символьные и дробно-рациональные вычисления

1.1.3 Гомоморфная криптография и гомоморфные нейронные сети

1.1.4 Библиотеки длинной арифметики

1.1.5 Аппаратные средства повышения точности вычислений

1.2 Способы представления числовой информации

1.2.1 Интервальная арифметика

1.2.2 Логарифмические системы счисления

1.2.3 Постбинарные форматы данных

1.3 Использование модулярной арифметики для решения задач высокоточной массовой обработки данных

1.3.1 Применение модулярной арифметики для специализированных устройств

1.3.2 Использование систем остаточных классов в задачах криптографии

1.3.3 Проблемы выполнения немодульных операций модулярной арифметики

1.4 Выводы по главе

Глава 2. Разработка методов и алгоритмов выполнения основных

немодульных операций модулярной арифметики

2.1 Основные принципы и особенности модулярных вычислений

2.1.1 Выбор оснований систем остаточных классов

2.1.2 Операция умножения по модулю

2.1.3 Индексные и иерархические системы счисления в остаточных классах

2.2 Точные методы выполнения немодульных операций

2.2.1 Системы счисления со смешанными основаниями

2.2.2 Алгоритм сравнения чисел в СОК

2.2.3 Алгоритм расширения базиса СОК

2.3 Метод интервальных логарифмических характеристик

2.3.1 Выполнение арифметических операций в интервально-логарифмической системе счисления

2.3.2 Алгоритм преобразования вещественных чисел в интервально-логарифмическое представление

2.3.3 Результаты экспериментальных исследований

2.4 Метод целочисленных интервалов

2.4.1 Интервальная оценка величины модулярного представления числа

2.4.2 Вычисление позиционных индексов с использованием целочисленной интервальной арифметики

2.4.3 Основные алгоритмы выполнения немодульных операций

2.4.4 Результаты экспериментальных исследований

2.5 Быстрое масштабирование модулярных чисел

2.5.1 Общая постановка задачи масштабирования

2.5.2 Метод масштабирования модулярных чисел с использованием целочисленных интервалов

2.5.3 Результаты экспериментальных исследований

2.6 Выводы по главе

Глава 3. Применение гибридной модулярно-позиционной

интервально-логарифмической арифметики для организации

массовых вычислений над числами сверхбольшой разрядности

3.1 Стандартные способы представления чисел в ЭВМ

3.1.1 Представление чисел в стандарте IEEE

3.1.2 Представление длинных чисел в ЭВМ

3.2 Гибридная модулярно-позиционная интервально-логарифмическая форма представления чисел сверхбольшой разрядности

3.2.1 Форма представления чисел RPIL с фиксированной точкой

3.2.2 Форма представления чисел RPIL с плавающей точкой

3.2.3 Алгоритм преобразования вещественного числа в RPIL-форму представления с плавающей точкой

3.3 Алгоритмы выполнения арифметических операций над целыми числами в RPIL- форме

3.3.1 Алгоритм выполнения операции целочисленного сложения

3.3.2 Алгоритм выполнения операции целочисленного вычитания

3.3.3 Алгоритм выполнения операции целочисленного умножения

3.4 Алгоритмы выполнения арифметических операций над вещественными числами в RPIL-форме

3.4.1 Алгоритм выполнения операции сложения вещественных чисел в RPIL-форме

3.4.2 Алгоритм выполнения операции умножения вещественных чисел в RPIL-форме

3.5 Выводы по главе

Глава 4. Организация процессора для массовой обработки чисел большой

разрядности с плавающей точкой в системе остаточных классов

4.1 Модулярные процессоры для высокоточных вычислений

4.2 Организация процессора-ускорителя для массовых модулярно-позиционных интервально-логарифмических вычислений

4.2.1 Блок преобразования вещественных чисел в интервально-логарифмический формат

4.2.2 Блок сложения и вычитания чисел в интервально-логарифмическом формате

4.2.3 Специализированное модулярное АЛУ

4.2.4 Преобразователь чисел из стандартного представления в форму ИРГЬ

4.2.5 Блок вычисления целочисленных интервальных оценок и позиционных индексов

4.2.6 МЯС конвейер

4.2.7 Результаты экспериментальных исследований

4.3 Организация вычислений на гибридном многоядерном модулярно-позиционном интервально-логарифмическом процессоре

4.4 Выводы по главе

Заключение

Список литературы

Перечень условных обозначений

Список рисунков

Список таблиц

Приложение А. Примеры

А.1 Пример выполнения операции модулярного умножения

А.2 Пример выполнения операции точного расширения базиса

А.3 Пример выполнения операции вычисления позиционного индекса

А.4 Пример выполнения операции сравнения с использованием целочисленных

интервалов

А.5 Пример выполнения операции масштабирования

А.6 Пример преобразования вещественного числа в гибридную форму

представления RPIL

Приложение Б. Выполнение арифметических операций в логарифмической

системе счисления

Приложение В. Вычисление интервально-логарифмической характеристики

вещественного числа

Приложение Г. Рекурсивная и иерархическая модулярная арифметика

Приложение Д. Использование систем счисления со смешенными

основаниями для организации операции расширения базиса систем остаточных классов

Приложение Е. Ошибки округления чисел в стандарте IEEE

Приложение Ж. Оценка времени выполнения арифметических операций

Приложение З. Акты о внедрении результатов диссертационного исследования