МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра дискретной математики и информационных технологий

ПРИЛОЖЕНИЕ P-АДИЧЕСКОЙ АРИФМЕТИКИ К ЗАДАЧАМ КОМПЬЮТЕРНОЙ АЛГЕБРЫ

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 271 группы
направления 09.04.01 — Информатика и вычислительная техника
факультета КНиИТ
Шарова Александра Вадимовича

Научный руководитель
доцент, к. ф.-м. н. _____________ Л. Б. Тяпаев

Заведующий кафедрой
доцент, к. ф.-м. н. _____________ Л. Б. Тяпаев

Саратов 2020

ВВЕДЕНИЕ

Актуальность темы.

Компьютерная алгебра – раздел математики, образовавшийся на стыке алгебры, вычислительных методов и символьных вычислений. Для данного раздела, как и для любого другого, сочетающего в себе различные области науки, трудно определить конкретные границы.

Термин "компьютерная алгебра" возник как синоним для терминов "символьные вычисления" , "аналитические вычисления" и "аналитические преобразования". На французском языке данный термин и в настоящее время означает "формальные вычисления".

Когда говорят о вычислительных методах, считается, что производимые вычисления выполняются в поле вещественных или, в ряде задач, комплексных чисел. В действительности же всякая программа для ЭВМ имеет дело только с конечным набором целых чисел, поскольку только такие числа могут быть представлены в компьютере. Для хранения целого числа отводится обычно 16 или 32 двоичных символа (бита), для вещественного - 32 или 64 бита. Это множество не замкнуто относительно арифметических операций, что может выражаться в различных переполнениях, например, при умножении достаточно больших чисел (изучаемых гугологией) или при делении на маленькое (10^{-10} и меньше) число. Еще более существенной особенностью вычислительной математики является то, что арифметические операции над этими числами, производимые компьютером, отличаются от арифметических операций в поле рациональных чисел. Более того, для компьютерных операций не выполняются основные аксиомы поля (ассоциативности и дистрибутивности). В основном в компьютерной алгебре вычисления производятся точно, без округления. Тем не менее в данном разделе математики рассматриваются и задачи, требующие приближенного решения, например, задачи из таких областей, как механика и термодинамика.

На самом деле при работе с рациональными числами вычисления происходят с приближенными значениями, которые представляют собой десятичные (или двоичные, при использовании компьютера) дроби с фиксированным числом значащих цифр. Как правило, данные вычисления являются недостаточно точными или затратными с точки зрения вычислительных ресурсов и времени. Из курса математического анализа известно, что поле вещественных чисел $\mathbb{R}$ можно определить как пополнение поля рациональных чисел $\mathbb{Q}$ по архимедовой метрике, когда расстояние между двумя рациональными числами определяется как модуль их разности. В математике, в частности в теории чисел, рассматриваются также другие метрики поля рациональных чисел, так называемые p-адические. При пополнении поля $\mathbb{Q}$ по p-адической метрике получается поле p-адических чисел, которые играют значительную роль в теории чисел.

Актуальность данной работы обусловлена исследованием как подходов использования p-адической арифметики в рамках вычислительных методов и компьютерной алгебры, так и некоторых теоретических особенностей p-адической арифметики, которые применяются к вычислениям, производимым на компьютере. Данные подходы и особенности позволяют ускорить вычисления за счет выбора правильного основания p-адического числа или же позволяют получить более точный результат за счет того, что p-адическая арифметика не накапливает арифметическую ошибку в отличие от классической арифметики (что является очень важным для многих областей прикладной математики и физики, где важны точность и время производимых вычислений).

Цель магистерской работы.

1. Дать алгоритмическое описание p-адической арифметики и реализовать ее на языке Python;
2. Составить библиотеку, которая будет базироваться на уже представленной реализации p-адической арифметики и будет содержать следующий функционал:
   — базовые математические операции над матрицами и векторами;
   — вычисление определителя матрицы;
   — алгоритм для нахождения решения СЛАУ;
3. Привести примеры применения реализованной однопоточнойбиблиотеки. Составить следующие программы:
   — для вычисления матричной экспоненты e^{Ax};
   — для нахождения решения СЛАУ методом Крамера и Гаусса;
   — для вычисления собственных значений и собственных чисел матрицы;

— для нахождения решения ОДУ;

4. Реализовать многопоточный вариант p-адической арифметики и провести сравнение с однопоточным вариантом на примерах решения прикладных задач;
5. Провести сравнение многопоточной библиотеки p-адической арифметики с классическими методами на следующих задачах:
   — нахождение решения СЛАУ;
   — нахождение решения ОДУ;
   — вычисление матричной экспоненты;
   — вычисление собственных значений и собственных векторов симметричной матрицы.

Методологические основы p-адической арифметики представлены в работах В.С. Анашина, А. Ю. Хренникова, В.С. Владимирова, И.В. Воловича, Е.И. Зеленова и С. В. Козырева. Среди зарубежных учёных можно выделить таких ученых как X.Li, C. Lu, A. Sjogren, A. Miola, R. Gregory а также I.Ojalvo и M. Newman.

Теоретическая и практическая значимость магистерской работы. Проблема увеличения точности и уменьшения времени вычислений на ЭВМ стояла всегда и ученые до сих пор продолжают изобретать все более совершенные алгоритмы для решения популярных прикладных задач физики и математики. Использование p-адической арифметики является новых подходом для вычислений производимых на компьютере и позволяет достичь лучших результатов в ряде прикладных задач как по времени выполнения алгоритмов, так и в точности получаемых вычислений. Нельзя переоценить важность этих результатов особенно в прикладных областях науки которые оперируют огромными массивами входящих данных и требуют сложных вычислений производимых с высокой точностью.

Структура и объем работы. Магистерская работа состоит из введения, 5 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 99 страниц, из них 63 страницы – основное содержание, включая 13 рисунков и список использованных источников информации – 40 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первый раздел «p-адические числа» посвящен теоретическим основам p-адической арифметики и p-адического анализа. В данном разделе приведены основные теоретические сведения такие как определение p-адической нормы, пространства p-адических чисел $\mathbb{Q}_p$ и его свойств, а также ряд определений и лемм имеющих отношение к p-адической дифференцируемости.

Второй раздел «Представления p-адических чисел и арифметические операции» посвящен описанию представлению рациональных чисел в p-адической форме. В данном разделе введены такие теоретические сведения как определение канонической формы p-адического числа и способ вычисления p-адического представления для некоторого рационального числа α. Кроме того, рассмотрены основные арифметические операции для p-адических чисел и приведены примеры. Помимо этого, введены понятия кода и псевдокода Гензеля которые позволяют представлять p-адические числа в компьютере. Для кода Гензеля также рассмотрены такие основные арифметические операции как сложение, вычитание, умножение и деление.

Третий раздел «Разработка однопоточной библиотеки для работы с p-адической арифметикой» посвящен описанию разработки однопоточной библиотеки на ЯП Python позволяющей представлять p-адические числа в компьютере, а также производить базовые арифметические операции над ними. В данном разделе дано описание всех методов для разработанных классов `Padic` и `Matrix`, описаны основные особенности разработанных типов данных, такие как:

— Вычисления, производимые в поле $\mathbb{Q}$, не накапливают ошибку с увеличением числа операций. Каждое рациональное число представляется в качестве конечной последовательности целых чисел и при увеличении числа операций арифметическая ошибка не накапливается.

— Целочисленные вычисления происходят с максимально возможным использованием классической архитектуры компьютера. Обычно вычисления, оперирующие с рациональными числами, используют представление числа в виде числителя и знаменателя.

— Параллельная структура, которая позволяет полноценно и равномерно использовать многоядерную систему. Вне зависимости от алгоритма, работающего с базовыми арифметическими операциями, будет использоваться параллельная реализация алгоритма работы с базовой арифметикой.

— Структура данных, готовая для равномерного распределения задач в облачной среде. При операциях представленным типом данных общая нагрузка на центральный процессор может равномерно распределяется на мелкие части. Кроме того, в рациональной арифметике такой процесс, как вычисление числа, сильно увеличивает потребление памяти, в то время как в p-адическом типе данных такой проблемы нет. Количество памяти не будет расти в процессе работы, потому память для p-адического типа данных выделяется всего один раз при создании объекта класса. Благодаря этому легко рассчитать приблизительное количество потребляемой памяти перед запуском программы в случае необходимости.

— cloud-ready тип данных. При использовании данного типа его модули имеют слабую связность. Исходя из этого каждый модуль может быть рассчитан параллельно на различных узлах кластера или на различных машинах в облаке.

Для наглядности приведены базовые примеры использования библиотеки. Для тестирования полученной библиотеки были решены задачи нахождения решения СЛАУ и вычисления определителя матрицы. Для данных прикладных задач были произведены замеры производительности на основании которых было произведено сравнение с аналогичными методами из популярных математических библиотек для ЯП Python.

Четвертый раздел «Разработка многопоточной библиотеки для работы с p-адической арифметикой» посвящен описанию разработки многопоточной библиотеки. В данном разделе приведено описание многопоточной p-адической арифметики и приведен алгоритм для кодирования и декодирования p-адических чисел. Кроме этого приведены многопоточные алгоритмы для нахождения решения СЛАУ и вычисления собственных чисел и собственных векторов матрицы.

Пятый раздел «Сравнение производительности классических и p-адических методов на примере прикладных задач» посвящен сравнению производительности p-адических и классических методов для таких задач, как: нахождение решения СЛАУ, вычисление собственных чисел и собственных значений матрицы, нахождение решения ОДУ, вычисление матричной экспоненты e^{At}. Для всех задач приведены описания экспериментов, сделаны необходимые замеры времени вычисления, а также приведены диаграммы на основании которых сделаны выводы о полученных результатах.

ЗАКЛЮЧЕНИЕ

В данной магистерской выпускной квалификационной работе представлен программный комплекс, разработанный с использованием ЯП Python и предназначенный для осуществления операций с наиболее распространенными объектами компьютерной алгебры при использовании p-адической арифметики над полем $\mathbb{Q}_p$. Представлены и описаны типы данных и алгоритмы работы с p-адическими числами как для однопоточного, так и для многопоточного случая.

Разработанный программный комплекс для работы с p-адическими числами не имеет аналогов для ЯП Python в открытом доступе, что делает его актуальным в случае необходимости применения p-адической арифметики при решении прикладных задачах с использованием данного ЯП.

Для тестирования программного комплекса было проведено решение таких популярных прикладных задач, как нахождение решения обыкновенного дифференциального уравнения, нахождение решения СЛАУ, а также вычисление собственных значений и векторов матрицы и вычисление матричной экспоненты. При проведении тестов основным рассматриваемым параметром было время вычисления для каждой из рассматриваемых задач, а на его основании производилось сравнение со временем, за которое стандартные библиотеки находили решение.

Для всех тестов были произведены замеры производительности работы как для однопоточного, так и для многопоточного варианта вычислений, а также приведены графики и диаграммы, отражающие полученные результаты. Тесты производительности многопоточной библиотеки показали, что что параллельная p-адическая арифметика сравнима с классическими методами, но, несмотря на это, является лучшей с той точки зрения, что во время вычислений не накапливает арифметическую ошибку. Очевидно, что классические методы тоже могут дать сколь угодно точный результат, но при этом время вычислений будет расти в разы, когда как в случае с p-адической арифметикой время будет константным.

Результат работы позволяет сделать вывод, что p-адическую арифметику выгодно использовать для ряда прикладных задач, которые решаются с помощью ЯП Python на распределенных кластерах или в облачной среде, так как время вычисления не уступает классическим методам, а в случае использования чисел из $\mathbb{Q}_2$ и $\mathbb{Q}_3$ даже превосходит их.

Отдельные части магистерской работы были опубликованы на студенческой научной конференции 24 апреля 2020 года где был представлен доклад о возможностях использования p-адической арифметики в ЭВМ, где были рассмотрены в том числе вопросы производительности на примере задачи вычисления матричной экспоненты.

ОСНОВНЫЕ ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1 Н., Коблиц. p-адические числа, p-адический анализ и дзета-функции / [Коблиц Н.] : М.: Мир, 1982. 192 с.

2 Владимиров, В.С. p-Адический анализ и математическая физика / [В.С. Владимиров, Волович И.В., Зеленов Е.И.] : М.: Наука, 1994. 352 с.

3 Anashin, V. Applied Algebraic Dynamics / V. Anashin, A Khrennikov. Berlin, Germany : Walter de Gruyter, 2009. 557 p.

4 Владимиров, В. С. Применение p-адических чисел в математической физике / [В. С. Владимиров, И. В. Волович] : Тр. МИАН, 1991. 200 с.

5 Хренников, А. Ю. Неархимедов анализ и его приложения / [А. Ю. Хренников] : М.: Физматлит, 2003. 216 с.

6 Gregory, R.T. The Use of Finite-segment P-adic Arithmetic for Exact Computation / R.T. Gregory // Proceedings Mathematical Sciences. 1975. Vol. 81(2). 58-79 p.

7 Li, X. A method for Hensel code overflow detection / X. Li, C. Lu, A. Sjogren // ACM SIGAPP Applied Computing Review. 2012. Vol. 12. P. 6–11.

8 Morrison, J. Parallel P-adic computation / J. Morrison // Information Processing Letters. 1988. Vol. 28.

9 Miola, A. Algebraic approach to p-adic conversion of rational numbers / A. Miola // Information Processing Letters. 1984. Vol. 18. P. 167–171.

10 Волович, И. В. p–Адическая математическая физика: основные конструкции, применения к сложным и наноскопическим системам / И. В. Волович, С. В. Козырев. 2009. Т. 12. С. 3–168.

11 Ojalvo, I. Vibration modes of large structures by an automatic matrix-reduction method / I. Ojalvo, M. Newman // Aiaa Journal - AIAA J. 1970. "— 07. Vol. 8. P. 1234–1239.