Нестандартные представления чисел

(ИПС РАН, Переславль-Залесский)*

Григоревский И. Н. Непейвода Н. Н

*Работа выполнялась при финансовой поддержке Российской Федерации в лице Минобрнауки России (идентификатор RFMEFI61319X0092)

Введение 1

Достижения в области суперкомпьютерных технологий позволяют ставить и решать ранее «невозможные задачи». Отмечается, что в современном мире невозможно победить, не победив в вычислениях. В частности, возникают задачи, в которых по самой сути необходимы точные вычисления с большими разрядностями операндов или же вычисления с очень большой гарантированной точностью. Они принадлежат большей частью к одному из двух классов: экспериментальная математика и компьютерная криптография, прежде всего, гомоморфная.

Введение 2

Второй класс задач, в которых требуются сверхточные и надёжные вычисле-ния: практические и теоретические задачи, в которых существующие математические модели систем и алгоритмы численного моделирования оказываются почти неприемлемыми из-за недостатков в стандартном представлении чисел.

Сверхточность нужна по сути

Экспериментальная математика

Задачи, требующие для своего выполнения от нескольких десятков до нескольких тысяч и даже десятков тысяч десятичных цифр.
Методологические и обзорные материалы по экспериментальной математике даны в серии работ Bailey D. H., Borwein J. M., где показано, что они приводят и к философским, в частности, онтологически значимым выводам, в частности, что для многих задач чрезмерное увеличение точности не улучшает результатов (а иногда и ухудшает их): принцип неопределённости.

Области ЭМ

Экспериментальная статистика распределения результатов точных математических задач;
Проверка предположений, связанных с гипотезой Римана;
Символьные и рациональные вычисления, в частности, задачи символьного интегрирования

Моделирование и оптимизация

Изучение неустойчивых моделей с трением
Изучение мелкой воды при помощи точных рациональных вычислений;
Задачи целочисленной линейной оптимизации;

Комбинаторика

Подсчёт числа гамильтоновых циклов на двумерных и трёхмерных решётках, кубах, параллелепипедах и других геометрических объектах: практическое применение в физике полимеров.

Сверхточность нужна из-за дефектов

Примеры дефектов 1

Примером расчётов с катастрофической потерей точности является вычисление полинома Румпа, представленного формулой

$$f(a,b) = 333.75 \cdot b^6 + a^2 \cdot (11 \cdot a^2 \cdot b^2 - b^6 - 121 \cdot b^4 - 2) + 5.5 \cdot b^8 + \frac{a}{2} \cdot b$$

где

$$a = 77617.0, \quad b = 33096.0.$$

Точное значение $f(a,b)$ известно: около 0.8273960599. При вычислениях в стандартной арифметике IEEE 754 одинарной (single) и двойной (double) точностью получаются совершенно иные результаты не только по величине, но и по знаку: $-6.33825 \cdot 10^{29}$ для float и $-1.18059 \cdot 10^{21}$ для double.

Проблема сертификации

Одной из актуальных проблем стала проблема контроля ошибок вычислений, особенно массово возникающих при выполнении вычислений над данными большого объема или длительных итерационных вычислениях, что характерно при решении современных прикладных задач.

Проблема воспроизводимости

Стандартной проблемой современных вычислительных технологий, в особенности при использовании высокопроизводительных (HPC) платформ и альтернативных представлений для точных вычислений, является проблема «численной» воспроизводимости. Под численной воспроизводимостью понимается гарантированное получение тождественных результатов при повторном решении прикладной задачи, причём с использованием одной и той же вычислительной платформы, или, более сильное условие, других платформ. Это часто является одним из условий сертификации.

Священная корова

На самом деле, более важным и реалистичным был бы подход, связанный с получением результатов, совпадающих по модулю точности исходных данных и требуемой точности результатов.
В противном случае, возникает абсурдная, с точки зрения системного и логического анализа, ситуация: исходные данные, известные с точностью до 2–3 десятичных разрядов и результат, который требуется для оценки порядка практически нужной величины с точностью до 2 разрядов (а то и до одного), дополняются не имеющими никакого физического и математического обоснования разрядами и затем эти разряды контролируются на воспроизводимость вычислений.

Сверхточность из-за представления

Задачи волнового рассеяния из-за накопления неточностей и биения результатов сейчас считаются с использованием 32–64 десятичных цифр;
Моделирование «поведения» сверхновых звезд и чёрных дыр. По тем же причинам нужна такая же точность;
Моделирование метаболизма и конфигурации макромолекул приводит к той же ситуации, из-за чего создана система с открытым кодом SolveME;
В задачах оптимального управления иногда требуется 60–90 десятичных цифр;
Аналогичная ситуация возникает при вычислениях прямого и обратного преобразования Лапласа;

Сверхточность из-за представления 2

В астрономической одновременно теоретической и практической задаче многих тел требуется от 32 до 120 десятичных цифр;
Матричные логарифмы, интегралы Изинга и Фейнмана, встречающиеся во многих практических и теоретических задачах, требуют от 100 до 1000 десятичных цифр;
Изучение атомного уровня кулоновских систем требует использования более 100 десятичных цифр для получения корректных результатов;
Многочлены Пуассона.

Сверхточность из-за представления 3

Ангармонические осцилляторы играют ключевую роль в исследованиях молекулярных колебаний, квантовых колебаний и полупроводниковой технике. Корректное нахождение собственных значений для ангармонических осцилляторов требует вычислений с 80 и более десятичными цифрами[1];

[1] Заодно здесь пример принципа неопределённости ВВ, приведённого выше

Резюме 1

В целом, за последние два десятилетия, этим вопросам посвящено более сотни разнообразных работ.
Для решения перечисленных и задач аналогичного типа необходимо повышение точности до 100–1000 десятичных цифр (приблизительно 512–4096 бит), что требует использования методов вычислений с применением «длинной арифметики» или других альтернативных представлений чисел.
Операции с многоразрядными числами являются базовым компонентом современных криптографических систем. В связи с этим в сентябре 2019 года прошла конференция IEEE по сверхточным вычислениям, чьи материалы не выложены в открытый доступ.

Сверхточность из-за представления 3

В целом, проблемы с числами вызвали общую проблему проверки адекватности результатов вычислений.
В частности, министерство энергетики США назвало проблему высокоточных вычислений в числе девяти областей вычислительной математики, наряду с комбинаторными задачами, решением систем линейных алгебраических уравнений, приемлемое решение которых необходимо для вычислений эксамасштаба (ExaScale).

Инструменты

Множество библиотек

Всё множество предлагаемых библиотек для арифметики произвольной точ-ности можно разделить на коммерческие (IMSL), бесплатные для некоммерческого использования (LiDIA, MIRACL) и открытые (GMP, NTL, CLN, MPI, Imath). Вторым важным моментом, определяющим область применения библиотек, является перечень поддерживаемых типов и структур данных.

Какие структуры?

Это: целые числа произвольной длины (знаковые и беззнаковые); рациональные дроби; числа с плавающей точкой произвольной точности; комплексные числа; векторы; матрицы; полиномы. В частности, в задачах современной криптографии наиболее востребованными являются расчеты целочисленных значений произвольной длины и полиномиальная арифметика.

Базовый открытый инструмент

GMP — это открытая библиотека длинной арифметики, поддерживающая работу со знаковыми целыми числами, рациональными числами и числами с плавающей запятой.

Открытая платформа

CLN — это библиотека для расчетов с использованием всех существующих числовых типов. В этой библиотеке реализованы классы таких типов данных, как целые числа, рациональные дроби, числа с плавающей точкой, комплексные числа, инвариантные полиномы, вычисления по модулю, имеет удобный интерфейс, поддерживает механизмы взаимодействия и преобразования друг в друга различных структур. CLN использует GMP в качестве вычислительного ядра. CLN лежит в основе многих программных продуктов, связанных с научными исследованиями и математическими расчетами: Scilab, Octave, maxima и любимая мною SageMath.

Для любящих исходники

NTL —- это высокопроизводительная библиотека C++, предоставляющая структуры данных и алгоритмы для работы с целыми числами произвольной длины, векторами, матрицами, полиномами, числами с плавающей точкой произвольной точности. Все алгоритмы NTL реализованы на C++ с открытым кодом, что обеспечивает кросс-платформенность и позволяет использовать библиотеку GMP.

Другие жители зоопарка

В качестве примера можно перечислить также следующий набор приложений и прикладных областей, в которых используется длинная арифметика:
Пакет KDE Abakus поддерживает вычисления произвольной точности; библиотека APRON обеспечивает решение задач линейной алгебры и статического анализа данных;
Arb-библиотека применяется для поддержки интервальной арифметики с произвольной точностью и с плавающей точкой;
Библиотека CGAL применяется для решения задач вычислительной геометрии;
FLINT библиотека ориентирована на решение задач из области теории чисел.

Как с языками?

Вычисления произвольной точности сегодня поддерживаются такими языками программирования, как Julia и C#.
Для других языков разработаны специальные библиотеки длинной арифметики: mpmath и SymPy для Python; GNU MP и GNU MPFR для C; BOOST , CLN и NTL для C++; ARPREC, MPFUN2015 и QD для языков C++ и Fortran, и т.д.
Основные характеристики современных пакетов и библиотек, поддерживающих вычисления в длинной арифметике, приведены на рисунке Неласой, вставить который в слайды невозможно без нарушения читаемости. Смотрите его в буклете.
Таблица осталась актуальной не менее чем на 90% (проверяли).

Наследство: обзор теории

Классификация представлений

1. Позиционные системы традиционного типа.
2. Вариации позиционных систем
3. Аддитивные системы.
4. Представления, принципиально отличающиеся от систем счисления.

Позиционные системы

Позиционная система традиционного типа задаётся основанием ϖ и количеством цифр в разряде. Основание может быть натуральным, действительным и даже комплексным числом. Если количество цифр по модулю меньше основания, то система без избыточности. Если цифры начинаются с 0, то система без сдвига.
Сколько цифр необходимо?
Критерии, когда нецелое основание позволяет задать все целые числа конечными выражениями.
Критерии, когда мнимое основание позволяет задать все мнимые числа (обобщённая теорема Фруньи).

Позиционные системы 2

Теорема о системах со сдвигом.
Теорема о системах с избыточностью.
Теорема о невычислимости операций над действительными числами.
Теорема о вычислимости операций над p-адическими числами.
Теорема об автоматности операций над целыми числами в системах с целым основанием и избыточностью.
Теорема о локальной замене отрезков цифр в избыточных системах (Непейвода).
Следствия этих результатов для вычислений и для аппаратуры.

Вариации

Системы с неоднородными основаниями. Их применения.
Системы с необычными цифрами. Их применение.
Интервальные системы.
Теоремы Непейвода о вычислимости операций и Шворина о критериях автоматности сложения.
Оптимальность системы «три половинки»

Аддитивные системы

Фибоначчиева система как пример аддитивной.
Общая концепция аддитивной системы.
Условия представимости числе в аддитивной системе.
Египетские дроби: древнейшая аддитивная система.

Принципиально другие представления

Остаточные классы и их использовыание.
Биномиальное представление.
Непрерывные дроби и интеллектуальное округление.
Логарифмическое представление.