Представление данных в алгебраических вычислениях: числа

Н. Н. Непейвода
ИПС им. А.К. Айламазяна РАН

10 октября 2014 г.

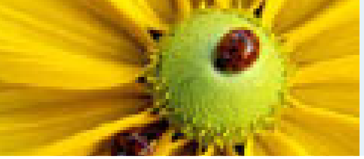
Общая постановка задачи

Данные в алгебраических вычислениях

Данные должны быть представлены как конечные алгебраические структуры, желательно группы (обратимые вычисления наиболее эффективно реализуются; оптический элемент, реализующий умножение в группе, легко модифицируется до осуществляющего деление)

Данные в алгебраических вычислениях

Данные должны быть представлены как конечные алгебраические структуры, желательно группы (обратимые вычисления наиболее эффективно реализуются; оптический элемент, реализующий умножение в группе, легко модифицируется до осуществляющего деление)
Запоминание промежуточных результатов должно быть по возможности исключено (иначе возникает эффект стены памяти, замедление вычислений и увеличение выделения тепла)



Пример с матрицами

При умножении матриц представление их как массивов действительных чисел оказывается худшим.
В частности, матрицы 2*2 можно расслоить по «двоичным разрядам» и умножение невырожденных матриц (иначе необратимо) представляет из себя группу положений куба, которая, в свою очередь, реализуется преобразованиями света в кристалле парателлурита TeO_2.

Пример с матрицами 2

Но при сложении чисел в обычном позиционном представлении обязательно возникает стена памяти (необходимость переносов на заранее непредсказуемое количество разрядов; вдобавок переносы вычисляются последовательно).

Пример с матрицами 2

Но при сложении чисел в обычном позиционном представлении обязательно возникает стена памяти (необходимость переносов на заранее непредсказуемое количество разрядов; вдобавок переносы вычисляются последовательно).
Тем самым теряется весь выигрыш, полученный на умножении.

Где неизбежно нарушается обратимость

Ввод-вывод и преобразования данных из одной алгебраической структуры в другую (поскольку последнее требуется, лишь если структуры не изоморфны).

Где неизбежно нарушается обратимость

Ввод-вывод и преобразования данных из одной алгебраической структуры в другую (поскольку последнее требуется, лишь если структуры не изоморфны).

Как показывает пример со сложением, даже в идеале обратимое действие при реализации на стандартных структурах представления часто становится нереализуемым на алгебраических элементах.

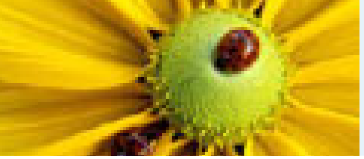
Где неизбежно нарушается обратимость

Ввод-вывод и преобразования данных из одной алгебраической структуры в другую (поскольку последнее требуется, лишь если структуры не изоморфны).
Как показывает пример со сложением, даже в идеале обратимое действие при реализации на стандартных структурах представления часто становится нереализуемым на алгебраических элементах.
В этом случае необходимо хотя бы избежать стены памяти и минимизировать эффекты необратимости.

Теоретические предпосылки

Браудр 1922

Брауэр: для эффективных действий с числами теоретически необходима другая структура представления.



Брауэр 1922

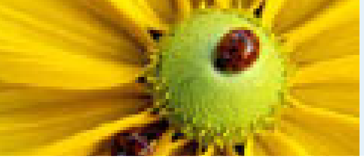
Брауэр: для эффективных действий с числами теоретически необходима другая структура представления.
Представление Брауэра чисел на отрезке [0,1]: двоичное дерево, двоичная позиционная, но необычная, система.

Брауэр 1922

Брауэр: для эффективных действий с числами теоретически необходима другая структура представления.
Представление Брауэра чисел на отрезке [0,1]: двоичное дерево, двоичная позиционная, но необычная, система.
$[0,1]$ делится на два *пересекающихся* отрезка: $[0,2/3]$, $[1/3,1]$.

Брауэр 1922

Брауэр: для эффективных действий с числами теоретически необходима другая структура представления.
Представление Брауэра чисел на отрезке [0,1]: двоичное дерево, двоичная позиционная, но необычная, система.
$[0, 1]$ делится на два *пересекающихся* отрезка: $[0, 2/3]$, $[1/3, 1]$.
Каждый из них в такой же пропорции опять на два. Например, первый на $[0, 4/9]$, $[2/9, 2/3]$.



Брауэр 1922 продолжение

Это связано с тем, что конструктивно можно доказать

$$\forall \varepsilon (\varepsilon > 0 \Rightarrow \forall x, y (y > x - \varepsilon \vee y < x + \varepsilon)$$

Брауэр 1922 продолжение

Это связано с тем, что конструктивно можно доказать

$$\forall\varepsilon(\varepsilon > 0 \Rightarrow \forall x, y(y > x - \varepsilon \vee y < x + \varepsilon)$$

но не трихотомию

$$\forall x, y(y > x \vee y = x \vee y < x)$$

Брауэр 1922 продолжение

Это связано с тем, что конструктивно можно доказать

$$\forall\varepsilon(\varepsilon > 0 \Rightarrow \forall x, y(y > x - \varepsilon \vee y < x + \varepsilon)$$

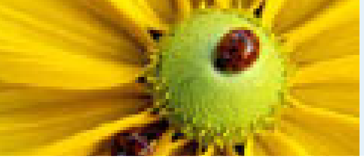
но не трихотомию

$$\forall x, y(y > x \vee y = x \vee y < x)$$

Брауэр не интересовался конкретными деталями действий в его системе. Ему достаточно было принципиальной вычислимости.

Банах Мазур 1938

Используя точное понятие алгоритма, было доказано, что в традиционных позиционных системах счисления сложение и умножение невычислимы.

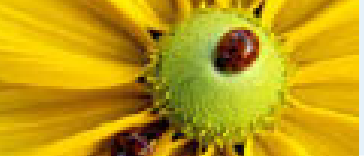


Банах Мазур 1938

Используя точное понятие алгоритма, было доказано, что в традиционных позиционных системах счисления сложение и умножение невычислимы.
Результат независимо получил и усилил В. А. Успенский (1956), систематически рассмотревший различные теоретические представления чисел с алгоритмической точки зрения

Где неизбежно нарушается обратимость

Ввод-вывод и преобразования данных из одной алгебраической структуры в другую (поскольку последнее требуется, лишь если структуры не изоморфны).



Где неизбежно нарушается обратимость

Ввод-вывод и преобразования данных из одной алгебраической структуры в другую (поскольку последнее требуется, лишь если структуры не изоморфны).
Как показывает пример со сложением, даже в идеале обратимое действие при реализации на стандартных структурах представления часто становится нереализуемым на алгебраических элементах.

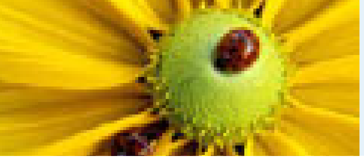
Где неизбежно нарушается обратимость

Ввод-вывод и преобразования данных из одной алгебраической структуры в другую (поскольку последнее требуется, лишь если структуры не изоморфны).
Как показывает пример со сложением, даже в идеале обратимое действие при реализации на стандартных структурах представления часто становится нереализуемым на алгебраических элементах.
В этом случае необходимо хотя бы избежать стены памяти и минимизировать эффекты необратимости.

Базовые определения

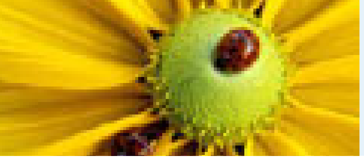
Абстрактная вычислимость

Поскольку обычное понятие алгоритма адекватно лишь для случаев. когда ресурсы неограничены, язык полон по Тьюрингу и нет физических источников и преобразователей информации, мы максимально абстрагируемся от конкретных понятий алгоритма. Накладываем лишь некоторые ограничения на возможности эффективных преобразований, которые выглядят почти абсолютными.



Принцип конечной информации [1]

Пусть Φ — эффективное преобразование объекта α в объект β. Тогда всякая конечная информация, которую можно вычислить по β, может быть вычислена с помощью Φ и конечной информации об α.



Общее представление действительных чисел

Что мы считаем конечной информацией о действительном числе? Как самое общее из конструктивных определений действительного числа (согласно анализу В. А. Успенского) рассмотрим следующее.

Общее представление действительного числа x — эффективная функция, сопоставляющая каждому положительному рациональному числу ε рациональный сегмент длины не больше ε, такая, что все вырабатываемые ею сегменты попарно пересекаются.

Представления называются *эквивалентными*, если любые два сегмента из них пересекаются.

Общее представление 2

Традиционный следующий шаг: действительное число — класс эквивалентности представлений — в конструктивизме некорректен. Класс эквивалентности не является эффективным объектом.

Соответственно, конечной информацией о действительном числе является любой из порождаемых его представлением сегментов.

Вычислимая функция

Функция f действительных чисел вычислима на множестве X, если для нее найдется вычислимое преобразование $\Phi(\varepsilon, [a, b]) \to [c, d]$ что для любого числа x из этого множества и для любого рационального $\varepsilon > 0$ имеется такое $\delta > 0$, что по любому рациональному сегменту $[a, b]$ длины не больше δ, содержащему x, $\Phi(\varepsilon, [a, b])$ выдает сегмент $[c, d]$, содержащий $f(x)$, длины не больше ε.

Позиционная система

Приведенное ниже определение включает в себя и такие системы, как суперэкспоненциальная и факториальные.
Позиционная система определяется бесконечной в обе стороны последовательностью натуральных чисел $n_i \geqslant 2$ (оснований). Числа от 0 до $n_i - 1$ называются цифрами i-того разряда.
Число в позиционной системе — тройка из числа цифр целой части k, знака $+$ либо $-$ и последовательности с областью определения от k до $-\infty$, исключая границы.

Диапазоны

Длина диапазона, соответствующего разряду, определяются рекурсивно. Длина диапазона нулевого разряда 1. Пусть $i > 0$. Если известна длина диапазона i-го разряда, то длина диапазона $i+1$-го в n_i раз больше. Если известна длина диапазона $-i$-го разряда, то длина диапазона $-i-1$-го в n_i раз меньше.

Диапазоны цифр

Диапазон цифры i-го разряда для положительных чисел. Пусть l_i — длина диапазона разряда.

Диапазон цифры j $k-1$-го разряда есть $[j \cdot l_{k-1}, (j+1) \cdot l_{k-1}]$.

Если известен диапазон $[a, b]$ цифры $i+1$-го разряда, то диапазон цифры j i-го разряда есть $[a + j \cdot l_{k-1}, a + (j+1) \cdot l_{k-1}]$.

Для отрицательных везде появляются минусы и a заменяется на b.

Отрезок, определяемый конечным числом цифр позиционного представления, будем называть естественным для данного представления.

Некорректность позиционных систем

Теорема. (Первые два пункта Банах, Мазур, 1938, третий Успенский, 1956. Все обобщены)
1) Имеется алгоритм преобразования чисел из любой позиционной системы в общее представление.
2) Ни для какой позиционной системы нет алгоритма преобразования числа из общего представления в данную систему.

Метод обмана

Для доказательства пункта 2 применяется общий абстрактный метод опровержения алгоритмической разрешимости.
По алгоритму Ψ, претендующему на решение проблемы, строится. используя его результаты, алгоритм χ, который его обманывает.
Мы не можем определить даже знак числа.
Алгоритм χ выдает по каждому ε отрезок $[-\varepsilon/2, \varepsilon/2]$, пока Ψ не выдаст знак. После чего начинает выдавать все меньшие отрезки другого знака.

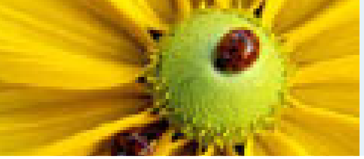
Некорректность позиционных систем 3

3) Алгоритм преобразования числа из позиционной системы α в систему β имеется в том и только в том случае, если любой естественный отрезок системы β есть конечное объединение естественных отрезков системы α.
Тогда. Каждый знак системы β может быть определен по конечному числу знаков системы α.
Только тогда. Имеется естественный отрезок системы β, один из концов которого не является концом никакого естественного отрезка α. В его окрестности применяем метод обмана.

Некорректность позиционных систем 4

4) Ни в одной позиционной системе операции сложения и умножения не вычислимы. Для десятичной системы показали Банах и Мазур (1938 г.)

Метод обмана. Идея на сложении в двоичной системе. Подаем 0.11111 и 0.0000 пока не выдаст целую часть. Затем обманываем, переходя в одном из мест с 0 на 1 или наоборот.



Брауэровы системы

Общее определение

Брауэрова система на отрезке $[a, b]$ определяется последовательностью натуральных чисел $n_i \geqslant 2$ (оснований) и числом $0 < \varepsilon < 1$ — перекрытием. Числа от 0 до $n_i - 1$ называются цифрами $-i$-того разряда.
Число в брауэровой системе — последовательность с областью определения от 0 до $-\infty$, исключая границы.

Длина диапазона, соответствующего разряду, определяются рекурсивно. Длина диапазона -1 разряда $b-a$. Пусть $i>0$. Если известна длина диапазона $-i$-го разряда l_i, то длина диапазона $-i-1$-го

$$l_{-i-1} = \frac{l_i}{(1-\varepsilon)\cdot n_{-i}+\varepsilon}$$

Диапазоны цифр

Диапазон нулевого разряда числа $[a, b]$.
Если известен диапазон $[a_i, b_i]$ цифры $-i$-го разряда, то диапазон цифры j $-i-1$-го разряда есть
$[a + j \cdot l_{-i-1} \cdot (1 - \varepsilon), a + j \cdot l_{-i-1} \cdot (1 - \varepsilon) + l_{-i-1}]$.
Отрезок, определяемый конечным числом цифр брауэровского представления, будем называть естественным для данного представления. Его концы, не совпадающие с a, b, называются внутренними.

Корректность брауэрового представления

Любая вычислимая функция из подмножества отрезка $[a, b]$ в подмножество отрезка $[c, d]$ вычислима при любом брауэровом представлении аргумента и результата.

Однородные брауэровы системы

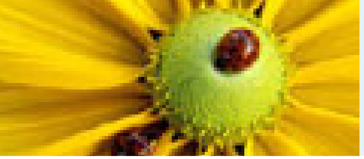
Если все n_i совпадают, то брауэрова система однородна. Она будет задаваться числом цифр и перекрытием.
В соответствии с нашей формулой, длина следующего разряда в системе $2, 1/2$ есть $2/3$ предыдущей;
длина в $3, 1/2$ половина предыдущей;
в $4, 1/2$ — $2/5$ предыдущей.
Из этого видно, что наиболее перспективны «двоичная» и «троичная» системы.

Быстрое сложение

Возможность быстрого сложения

Теорема. В однородной брауэровой системе с $n > 2$ и $\varepsilon \geqslant 1/2$ с одинаковой длиной отрезков слагаемых для вычисления i-того знака суммы достаточно знать i-тый и $i-1$-ый знаки слагаемых.

Доказательство. Длина интервала результата удваивается. Простым подсчетом длины интервалов сумм получаем, что с учетом перекрытия сумма двух $i-1$-ых интервалов обязательно попадет в один и тот же i-тый.



Таблицы сложения для двоичной и троичной систем

Как определить очередной знак для двоичной системы по трем знакам слагаемых

0+0=0 1+1=1 00+10=0 01+11=1

000+11=0 001+11=1 010+10=0 011+10=1

Пример неоднозначного представления

$1/3 = 010101\cdots = 101010\ldots$

Деление отрезка $[0, 1]$ в троичной системе:

$[0, 1/2], \ [1/4, 3/4], \ [1/2, 1]$

Таблица сложения

0+0=00+1=10+0=0;

1+1=0+2=01+1=10+2=11+0=12+0=1;

2+2=22+1=11+2=12+2=2.

Аккуратность

По таблице сложения видно, что второй знак нужен лишь в одном из слагаемых.

Определение. Число представлено *аккуратно*, если расстояние его до любой внутренней границы диапазона очередной цифры не менее половины перекрытия.

Теорема. Любое число может быть представлено аккуратно в любой равномерной брауэровой системе с $\varepsilon \geqslant 1/2$

Коварство. Для случая двоичной системы алгоритма перевода в аккуратную форму нет. Особая точка $1/2$.

Для всех остальных систем алгоритм простой.

Аккуратность 2

Теорема. Для равномерных систем с основанием больше 2 и перекрытием не меньше $1/2$ в случае, если одно из слагаемых представлено аккуратно и длины отрезков слагаемых совпадают, сложение осуществляется за один такт и полностью параллельно.

И еще один гвоздь в могилу двоичной системы

Для умножения комплексных чисел подходят лишь такие системы с простым основанием n, для которых в $\mathbb{Z}_n$ многочлен $x^2 + 1$ неприводим. Например, троичная, семеричная, с основанием 31.

1. Непейвода Н.Н.: Уроки конструктивизма. Geidelberg: Lambert Academic Publishing, 98 pp. (2011)

Вопросы????