УДК 621.29

И.И. Дзегеленок, Ш.А. Оцоков

Метод ускорения модулярной арифметики с самоисключением ошибок округления

(Московский энергетический институт)

Разработан метод для ускорения выполнения арифметических операций без ошибок округления в системе остаточных классов на поле рациональных чисел. Данный метод позволяет существенно расширить диапазон представления дробных чисел в системе остаточных классов и повысить быстродействие вычислений за счет снижения разрядности модуля, по которому проводятся вычисления с исключением ошибок округления.

Системы компьютерной алгебры находят широкое применение во многих областях науки и техники. Возможности таких систем как, например, выполнение преобразований, упрощений произвольных математических выражений, расчеты без ошибок округления, помогают найти точные или аналитические решения многих научных задач.

В современных математических системах (Mathcad, Maple и др) для реализации вычислений, в которых исключаются ошибки округления, как правило, используется рациональная арифметика на основе схемы приведения дробей. Для выполнения арифмети-

ческих операций над дробями по этой схеме требуется определение наибольшего общего делителя.

Другой метод для реализации вычислений без ошибок округления основан на использовании арифметики системы остаточных классов (модулярная арифметика).

Все арифметические операции с дробными числами выполняются в поле целых чисел системы остаточных классов. Результаты вычислений являются целыми числами, которые можно представить в виде простых дробей. Такое представление единственно, так как существует взаимно-однозначное соответствие между целыми числами системы остаточных классов и конечным множеством несократимых дробей Фарея [2].

Численные эксперименты на ЭВМ показывают, что быстродействие вычислений в одномодульной системе остаточных классов выше чем по схеме приведения дробей.

Пусть необходимо вычислить значение некоторого арифметического выражения с исключением ошибок округления. Допустим, что в одномодульной системе остаточных классов возникла ошибка псевдопереполнения конечного результата (выход результата за пределы допустимого диапазона). Тогда, это приводит к получению неверного результата при отображении в дробь.

Рассмотрим метод организации вычислений с исключением ошибок округления и с более широким диапазоном представления дробей, чем в одномодульной системе остаточных классов.

Предлагаемый метод основан на том, что вне зависимости от ошибки псевдопереполнения искомые и полученные результаты принадлежат одному классу вычетов. В процессе вычислений найдем произведение всех знаменателей дробей модулю СОК. Можно показать, что искомый результат A / B определяется следующим образом:

$$\frac{A}{B} = N_1 \frac{\left| N_1 \cdot U \cdot B_2 \right|_m}{B_2} \qquad (1)$$

где U - конечный результат вычислений в СОК,

m - модуль СОК,

B_2 – произведение знаменателей всех дробей по модулю P ,

N_1 - знак результата.

Рассмотрим пример для вычисления 1-1/2-1/3-1/4.

$$1)\ 1 - \frac{1}{2} = \frac{1}{2}, \qquad 2)\ \frac{1}{2} - \frac{1}{3} = \frac{1}{6}, \qquad 3)\ \frac{1}{6} - \frac{1}{4} = -\frac{1}{12}$$

Пусть модуль СОК m=127, тогда

$$1)\ \left|1 - \frac{1}{2}\right|_{127} = 1 - 64 = -63\ ,$$

$$2)\ \left|\frac{1}{2} - \frac{1}{3}\right|_{127} = -63 + 42 = -21\ ,$$

$$3)\ \left|\frac{1}{6} - \frac{1}{4}\right|_{127} = -21 + 95 = 74$$

Конечное множество дробей Фарея $p\ /\ q\ ,((p,q) = 1, p\ /\ q > 0)$ соответствующих классу вычетов 74 по модулю 127 включает следующие дроби:

2/103 3/91 4/79 5/67 6/55 7/43 8/31 9/19 10/7 11/122 12/110 13/98 14/86 15/74 16/62 17/50 18/38 19/26 20/14 21/2 22/117 23/105 24/93 25/81 26/69 27/57 28/45 29/33 30/21 31/9 32/124 33/112 34/100 35/88 36/76 37/64 38/52 39/40 40/28 41/16 42/4 43/119 44/107 45/95 46/83 47/71 48/59 49/47 50/35 51/23 52/11 53/126 54/114 55/102 56/90 57/78 58/66 59/54 60/42 61/30 62/18 63/6 64/121 65/109 66/97 67/85 68/73 69/61 70/49 71/37 72/25 73/13 75/116 76/104 77/92 78/80 79/68 80/56 81/44 82/32 83/20 84/8 85/123 86/111 87/99 88/87 89/75 90/63 91/51 92/39 93/27 94/15 95/3 96/118 97/106 98/94 99/82 100/70 101/58 102/46 103/34 104/22 105/10 106/125 107/113 108/101 109/89 110/77 111/65 112/53 113/41 114/29 115/17 116/5 117/120 118/108 119/96 120/84 121/72 122/60 123/48 124/36 125/24 74/1

Докажем, что в этом списке нет двух дробей с одинаковыми знаменателями. Предположим противное, т.е. существуют две дроби $p_1\ /\ q$ и $p_2\ /\ q$, $p_1 \neq p_2$, $p_1 < m, p_2 < m$ принадлежащие одному и тому же классу вычетов r по модулю m .

Тогда

$p_1 \cdot q^{-1} \equiv p_2 \cdot q^{-1} (\mathrm{mod}\ m), \quad p_1 \equiv p_2 (\mathrm{mod}\ m)$,

но $p_1 \neq p_2$ по условию. Т.е. пришли к противоречию. Ч.т.д.

Таким образом, в этом списке нет двух положительных дробей с одинаковым знаменателем.

В работе [1] для вычислений с отрицательными числами в системе остаточных классов используется искусственное представление чисел. Суть которого заключается в том, что вводится дополнительное основание СОК равное двум и диапазон представления чисел в СОК удваивается. При этом положительным числам соответствует диапазон от m до $2m$, а отрицательным от 0 до $m - 1$.

В соответствии с описанными в работе [1] правилами выполнения арифмети-ческих операций с числами в искусственной форме получим результат в двухмодульной СОК. Преобразуя его в одномодульную СОК и в зависимости от диапазона определим знак результата вычислений в СОК.

Проблемой вычислений в СОК является ошибка пседопереполнения. Без обнаружения этой ошибки нет гарантий в том, что полученный результат является правильным.

Одним их возможных способов решения этой проблемы заключается в следующем. В процессе вычислений в СОК параллельно и независимо друг от друга ведутся вычисления в позиционной системе счислений (ПСС). И если результаты этих вычислений отличаются друг от друга более чем на порядок, то имеет место ошибка пседвопереполнения. В зависимости от знака результата вычислений в ПСС определяется N_1 в формуле (1). Иллюстрируем это на примере.

В данном примере $B_2 = 24$, $U = 74$ и $N_1 = -1$.

Поэтому,

$$\frac{A}{B} = -\frac{\left|-74 \cdot 24\right|_{127}}{24} = -\frac{1}{12}$$

Т.к. величины B_2, U и N_1 не зависят друг от друга их можно

вычислять параллельно.

Пусть N - порядок дроби Фарея искомого результата, тогда с использованием одномодульной СОК необходимо выбрать модуль $m \geq 2N^2 + 1$, а в предлагаемом методе - $m \geq N + 1$ [2,3].

Эффект повышения быстродействия вычислений по сравнению с одномодульной СОК достигается тем, что все арифметические операции проводятся над числами имеющими разрядность $]\log_2(N + 1)[$, в то время как в одномодульной СОК разрядность чисел будет больше чем $]\log_2(2N^2 + 1)[$.

Разработанный метод позволяет повысить быстродействие вычислений с исключением ошибок по сравнению с одномодульной системой остаточных классов за счет существенного расширения диапазона представления дробей Фарея. Хотя в данном требуется кроме U требуется определить еще и B_2, N_1, но это приводит к снижению быстродействия, т.к величины U, B_2, N_1 могут быть вычислены параллельно и независимо друг друга.

Краткое описание программного модуля безошибочной обработки чисел в одномодульной системе остаточных классов

Разработан программный модуль безошибочной обработки чисел, который может использоваться при решении различных вычислительных задач, требующих высокой точности вычислений. Основу программного модуля составляют алгоритмы преобразования и вычислений в одномодульной СОК. Рассмотрим структуру программного модуля. В его состав входят следующие процедуры:

1. Init (P) - процедура инициализации модуля, входной параметр : основание СОК - P;

2. Add_Sok (A, B ; Result) - процедура сложения двух чисел, входные параметры: два числа, выходные - результат суммирования.

3. Sub_Sok (A, B ; Result) - процедура вычитания двух чисел, входные параметры: два числа, выходные - разность двух чисел.

4. Mul_Sok(A, B ; Result) - процедура умножения двух чисел, входные параметры: два числа, выходные - результат произведения двух чисел.

5. Div_Sok(A, B ; Result) - процедура деления двух чисел, входные параметры: два числа, выходные - результат деления двух чисел.

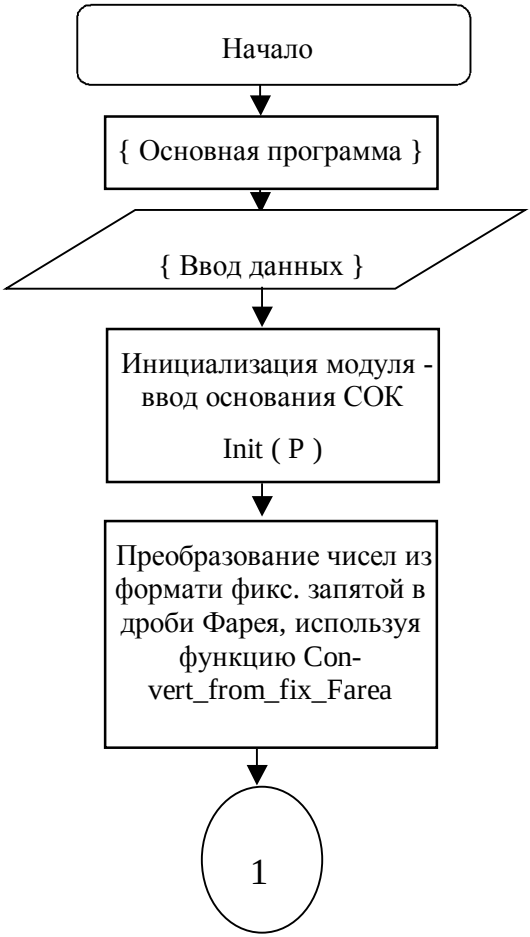
Процедуры для работы с числами сверх большой величины длиной до 100 цифр:

6. Mul_Long_Sok(A, B ; Result) - процедура умножения двух чисел A и B, входные параметры: два числа, выходные - результат произведения двух чисел.

7. Div_Long_Sok(A, B ; Result) - процедура деления двух чисел A и B, входные параметры: два числа, выходные - результат деления двух чисел.

8. Add_Long_Sok (A, B ; Result) - процедура сложения двух чисел A и B, входные параметры: два числа, выходные - результат суммирования.

9. Sub_Long_Sok (A, B ; Result) - процедура вычитания двух чисел A и B, входные параметры: два числа, выходные - разность двух чисел.



Процедуры преобразования чисел и работы с дробями Фарея:

10. Convert_from_Sok_Farea(A ; Result) - процедура преобразова-

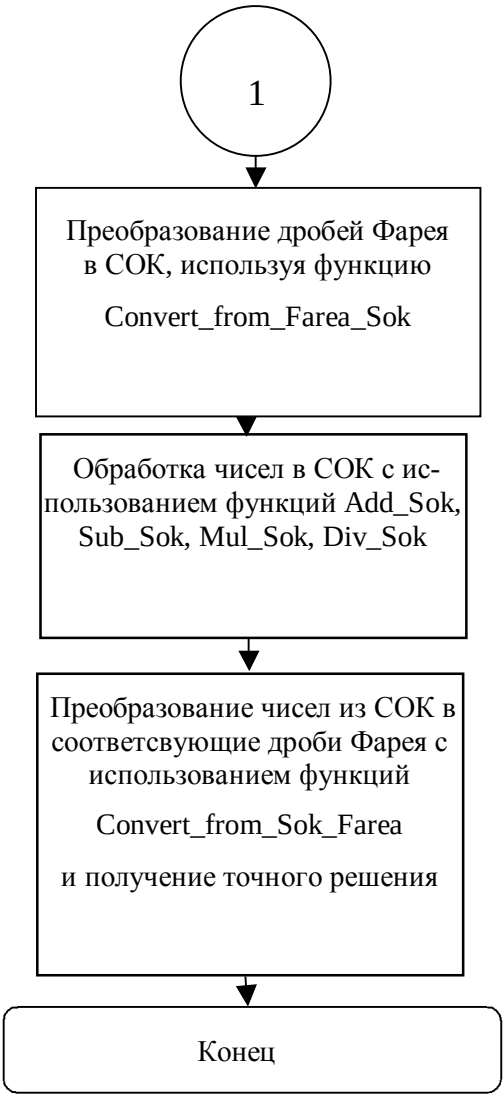
ния числа A из СОК в соответствующую дробь Фарея Result ;

11. Sokr (A; Result) - процедура для сокращения дроби A

12. Convert_from_fix_Farea (A ; Result) - процедура преобразования числа A с фиксированной запятой в дробь Фарея Result.

Для безошибочных вычислений необходим именно следующий порядок вызовов процедур программного модуля, показанный на рис 1.

Программный модуль реализованный в виде dll-библиотекии и динамически подключается к прикладной программе. Реализация в виде dll-библиотеки позволяет использовать ее практически в любых современных средах программирования для прикладных параллельных программ, в которых требуется повышенная точность вычислений.



Литература

1. *Акушский Н.Я, Юдицкий Д.И.* Машинная арифметика в остаточных классах, М. “Сов. радио ”, 1968. – 439 с.

2. *Грегори Р, Кришнамурти Е.* Безошибочные вычисления. Методы и приложения.М.:Мир,1988. –207 с.

3. *Дзегелёнок И.И, Оцоков Ш.А.* Подход к решению проблемы безошибочных вычислений с использованием ускоренного алгоритма отображения дробей Фарея. // Труды научной конференции, посвященной 75-летию со дня рождения академика В.А.Мельникова. РАН. М. 2004.