ФПМИ

62
научная
конференция
МФТИ

Министерство науки
и высшего образования
Российской Федерации

Федеральное государственное
автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный
исследовательский
университет)»

Москва, Долгопрудный,
Жуковский 2019

Тезисы.
Прикладная математика и информатика

МФТИ

5100

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение
высшего образования «Московский физико-технический институт
(национальный исследовательский университет)»

Труды

62-й Всероссийской научной конференции МФТИ

18–24 ноября 2019

Прикладные математика и информатика

Москва – Долгопрудный – Жуковский

МФТИ

2019

УДК 51+004
ББК 22.1+32.81
Т78

Труды 62-й Всероссийской научной конференции МФТИ. 18-24 ноября 2019 года. Прикладные математика и информатика. — М.: МФТИ, 2019. – 241 с.

Т78

ISBN 978-5-7417-0726-5

Включены результаты оригинальных исследований студентов, аспирантов, преподавателей и научных сотрудников МФТИ и дружественных учебных и научных организаций. Статьи представляют интерес для специалистов, работающих в области прикладных математики и информатики

УДК 51+004
ББК 22.1+32.81

ISBN 978-5-7417-0726-5

СЕКЦИЯ ТЕОРИИ ВЫЧИСЛЕНИЙ

Председатель: В.К. Леонтьев (д.ф.-м.н., профессор)

Зам. председателя: С.П. Тарасов (к.ф.-м.н.)

Секретарь: С.А. Довгаль (асс.)

Дата: 23.11.2019 Время: 12:00

Место: г. Долгопрудный, Первомайская улица, д. 3, ауд. 907 КПМ, МФТИ

УДК 519.684

Вычисление наибольшего общего делителя на обобщённых регистровых машинах

А.В. Селиверстов

Институт проблем передачи информации им. А.А. Харкевича Российской академии наук

Рассмотрим обобщённые регистровые машины [1] над частично упорядоченным ассоциативным коммутативным кольцом с единицей (R, 0, 1, +, -, ×, <). В случае, когда линейно упорядоченным кольцом служит поле вещественных чисел, эти машины тесно связаны с BSS-машинами [2]. Каждый регистр содержит элемент кольца R, над которыми за один шаг выполняются операции, перечисленные в сигнатуре. Константы соответствуют записи соответствующего элемента в регистр. В случае проверки предиката, машина переходит в новое состояние в зависимости от истинности предиката. За один шаг машина может копировать и пересылать элементы между регистрами. Также существуют индексные регистры, содержащие неотрицательные целые числа, над которыми выполняются обычные операции. В начале работы в нулевом индексном регистре записано число регистров, занятых входными данными, а в остальных индексных регистрах записаны нули. Не занятые входными данными регистры содержат нули. Время работы машины полиномиальное, если существует такой многочлен $p(n)$, что если вначале ровно n регистров занято входными данными, то полное число шагов, выполняемых машиной до остановки, ограничено значением многочлена $p(n)$.

Вычисление наибольшего общего делителя НОD двух ненулевых элементов кольца представляет собой важную задачу и, несмотря на значительное число публикаций, остаётся предметом исследования [3, 4]. Над произвольным евклидовым кольцом R для любых двух ненулевых элементов их НОD можно вычислить за полиномиальное время на обобщённых регистровых машинах, которые выполняют сравнение норм двух элементов из кольца R. При этом, если кольцо не является линейно упорядоченным, то НОD определён с точностью до умножения на обратимый элемент. Над произвольным факториальным кольцом тоже определён НОD с точностью до умножения на обратимый элемент, но вычислительная сложность может быть высокой. Например, не известен полиномиальный алгоритм для вычисления НОD для многочленов от нескольких переменных над полем. Однако НОD определён над некоторыми кольцами, которые не являются факториальными. И в этом случае НОD может быть невычислимым.

Обозначим через D ультрафильтр, расширяющий фильтр коконечных подмножеств множества натуральных чисел. В частности, для каждого подмножества либо оно само, либо его дополнение принадлежит ультрафильтру. Обозначим через (U, 0, 1, +, -, ×, <) ультрастепень линейно упорядоченного кольца целых чисел над ультрафильтром D. Это линейно упорядоченное кольцо является областью целостности. Более того, в нём корректно определен НОD, поскольку кольцо целых чисел и его ультрастепень U элементарно эквивалентны [5]. Однако U обладает необычными свойствами, невыразимыми в языке первого порядка теории частично упорядоченных колец.

Элементами кольца U служат классы эквивалентности бесконечных последовательностей целых чисел $\boldsymbol{a}=(a_0, a_1,\dots)$. Две последовательности эквивалентны, если они совпадают на множестве индексов, принадлежащем ультрафильтру D. В частности, эквивалентны любые две последовательности, отличающиеся лишь в конечном числе позиций. Операции в кольце U определяются покомпонентно. Кольцо целых чисел вложено в кольцо U, числу a соответствует класс постоянной последовательности $\boldsymbol{a}=(a, a,\ldots)$. Каждая последовательность, содержащая нулевые элементы, либо эквивалентна последовательности из нулей $\mathbf{0}=(0, 0,\ldots)$, либо эквивалентна последовательности, в которой нет ни одного нуля. Поэтому кольцо U не содержит делителей нуля. В кольце U ровно два обратимых элемента. Обратимыми элементами кольца U служат классы каждой из двух постоянных последовательностей $\mathbf{1}=(1, 1,\ldots)$ и $\mathbf{-1}=(-1, -1,\ldots)$. Класс эквивалентности любой последовательности чисел 1 или -1 служит представителем обратимого элемента, но каждая из них эквивалентна либо **1**, либо **-1**. Поскольку ультрафильтру принадлежит либо множество индексов единиц, либо множество индексов минус единиц.

Теорема 1. Область целостности U не является факториальным кольцом, хотя в нём существует наибольший общий делитель любых двух ненулевых элементов.

Доказательство. Для любого натурального числа m, класс последовательности целых чисел, k-й элемент которой равен целой части (k-m)-й степени числа два $[2^{k-m}]$, служит ненулевым и необратимым элементом кольца U, который делится на элемент $\mathbf{2}=(2, 2,\ldots)$ без остатка. Этот элемент не разлагается в конечное произведение неприводимых элементов кольца U. Следовательно, кольцо U не факториальное.

Однако наибольший общий делитель НОD двух элементов, представителями которых служат последовательности $\boldsymbol{a}=(a_0, a_1,\ldots)$ и $\boldsymbol{b}=(b_0, b_1,\ldots)$, равен классу последовательности наибольших общих делителей НОD($\boldsymbol{a}$, $\boldsymbol{b}$)=(НОD(a_0, b_0), НОD(a_1, b_1),…). Теорема 1 доказана.

Теорема 2. Наибольший общий делитель нельзя вычислить на обобщённых регистровых машинах над линейно упорядоченным кольцом U.

Автор благодарен Сергею Давидовичу Мешвелиани (Институт программных систем им. А.К. Айламазяна РАН) за обсуждение постановки рассмотренной задачи.

Литература

1. *Neumann E., Pauly A.* A topological view on algebraic computation models // Journal of Complexity. 2018. Vol. 44. P. 1–22. DOI:10.1016/j.jco.2017.08.003
2. *Blum L., Shub M., Smale S.* On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines // Bulletin of the American Mathematical Society. 1989. Vol. 21, № 1. P. 1–46. DOI:10.1090/S0273-0979-1989-15750-9
3. *Dolgov D.A.* Polynomial greatest common divisor as a solution of system of linear equations // Lobachevskii Journal of Mathematics. 2018. Vol. 39, № 7. P. 985–991. DOI:10.1134/S1995080218070090
4. *Meshveliani S.D.* On a provable program for generic arithmetic of fractions // Компьютерная алгебра: материалы Международной конференции. Москва, 17–21 июня 2019 г. / отв. ред. С. А. Абрамов, Л. А. Севастьянов. – М.: РУДН, 2019. P. 145–153. URL: http://www.ccas.ru/ca/_media/ca-2019.pdf
5. *Кейслер Г., Чэн Ч.Ч.* Теория моделей. М.: Мир, 1977.

УДК 519.17

О трудности **решения многомерных игр вычитания**

М.Н. Вялый[1,2,3], В.А. Гурвич[3,4]

[1]Вычислительный центр им. А. А. Дородницына ФИЦ ИУ РАН
[2]Московский физико-технический институт (национальный исследовательский университет)
[3]Национальный исследовательский университет «Высшая школа экономики»
[4]Rutgers University

Одним из важных разделов алгоритмической теории игр является решение беспристрастных игр. Два основных инструмента, которые используются при этом: периодичность P-позиций и использование ним-функции (функции Шпрага-Гранди).

Игры вычитания с конечным множеством разностей являются классическим примером применения первого инструмента. Такая игра задается конечным набором D положительных целых