EURASIAN NATIONAL UNIVERSITY

МАТЕМАТИКАЛЫҚ ЛОГИКА ЖӘНЕ КОМПЬЮТЕРЛІК ҒЫЛЫМДАР

Халықаралық ғылыми конференцияның еңбектері
2022 жыл, 7-8 қазан, Астана, Қазақстан

MATHEMATICAL LOGIC AND COMPUTER SCIENCE

Proceedings of the International scientific conference
October 7-8, 2022, Astana, Kazakhstan

МАТЕМАТИЧЕСКАЯ ЛОГИКА И КОМПЬЮТЕРНЫЕ НАУКИ

Труды Международной научной конференции
7-8 октября 2022 г., Астана, Казахстан

АСТАНА
2022
ASTANA

ВЫЧИСЛЕНИЯ НАД УПОРЯДОЧЕННЫМИ КОЛЬЦАМИ ПОСРЕДСТВОМ ОБОБЩЁННЫХ РЕГИСТРОВЫХ МАШИН

Латкин[(1)] И.В., Селиверстов[(2)] А.В.
[(1)]Восточно-Казахстанский технический университет им. Д. Серикбаева,
[(2)]Институт проблем передачи информации им. А.А. Харкевича

Аннотация. Рассматривается работа обобщённых регистровых машин над частично упорядоченными кольцами со вспомогательными бинарными операциями: над кольцом целых чисел, его бесконечной декартовой степенью и ультрастепенью. Обсуждается осуществимость некоторых алгоритмов и их сложность. Приводится пример нефактриального кольца элементарно эквивалентного кольцу целых чисел. Показывается, что недетерминированные вычисления над целыми числами можно реализовать как детерминированные над декартовой степенью кольца целых чисел. Используя такие машины можно также моделировать вычисления с оракулами. Это обеспечивает алгебраический подход к описанию некоторых классов вычислительной сложности. Однако эта модель вычислений существенно отличается от альтернирующих машин.

Ключевые слова: обобщённые регистровыеr машины, упорядоченные кольца, вычислительнаяl сложность, недетерминированные вычисления, модель вычислений.

Введение. Рассматривается работа обобщённых регистровых машин (ОРМ) [1,2,3] над частично упорядоченным ассоциативным и коммутативным кольцом со вспомогательными бинарными операциями вычитания и rest : $(R, 0, +, -, \mathrm{rest}, \leq)$, поскольку без подобного расширения вычислительные возможности таких машин весьма ограничены. В кольце целых чисел $\mathbb{Z}$ для любого x и для $y \geq 2$ значением $\mathrm{rest}(x, y)$ служит остаток от деления x на y из множества $\{0, \dots, y-1\}$, а для $y \leq 1$ полагаем $\mathrm{rest}(x, y) = 0$. Далее также предполагается, что

$$\exists z((x = y \cdot z + \mathrm{rest}(x, y)) \wedge (0 \leq \mathrm{rest}(x, y) < y))$$

для $y \geq 2$, где под двойкой понимается сумма нейтрального элемента по умножению с самим собой, а при нарушении условия $y \geq 2$ (в частности, если элемент y несравнимый с аналогом двойки) не обязательно будет выполняться равенство $\mathrm{rest}(x, y) = 0$. Тем не менее, требуется, чтобы для любого y было верно $\mathrm{rest}(x, y) \geq 0$ и либо $\mathrm{rest}(x, y) < y$, либо $\mathrm{rest}(x, y)$ несравним с y. Полагаем, что $\mathrm{rest}(x, y) = 0$, когда элемент x делится на y, в частности, если y обратим. Функция rest может быть корректно определена и для неевклидовых колец, как мы это увидим далее. В случае совпадения кольца R с кольцом $\mathbb{Z}$ получается консервативное расширение теории $Th(\mathbb{Z})$, так как отношение порядка и деление с остатком определяются над $\mathbb{Z}$ формулами первого порядка.

Методы: применяются обычные методы алгебры и математической логики.

Основная часть. Напомним вкратце описание работы ОРМ над алгебраической системой с основным множеством A и заданными на нём операциями f_i местности $k(i)$, предикатами T_j местности $l(j)$ и выделенными элементами c_t. Машина имеет бесконечное множество (рабочих) регистров R_j, содержащих элементы из A, и бесконечно много индексных регистров $I(n)$, содержащих натуральные числа. Константы соответствуют операциям записи соответствующего элемента в регистр. Программы представляют собой конечные списки команд, часть из которых может быть помечена (или пронумерована). Выполняя эти команды, машина может за один шаг скопировать элемент из регистра $R_{I(s)}$, индексированного содержимым индексного регистра $I(s)$, и переслать его в регистр $R_{I(t)}$: $R_{I(t)} \coloneqq R_{I(s)}$. Также она может применить любую сигнатурную операцию f_j к элементам, из регистров $R_{I(n_1)}, \dots, R_{I(n_{k(j)})}$, и записать результат в $R_{I(m)}$. При проверке на истинность сигнатурного предиката T_j, применённого к элементам из $R_{I(n_1)}, \dots, R_{I(n_{l(j)})}$, машина переходит в новое состояние в зависимости от его истинности, т.е. в случае истинности

предиката T_j на наборе элементов из регистров $R_{I(n_1)}, \ldots, R_{I(n_{l(j)})}$, машина переходит к выполнению, например, команды с меткой k, а в противном случае исполняет команду t.

Над индексными регистрами выполняются обычные операции регистровых машин. В начале работы в нулевом индексном регистре записано число регистров, занятых входными данными, а в остальных индексных регистрах записаны нули. Незанятые входными данными регистры содержат некоторый фиксированный элемент основного множества A, для частично упорядоченного кольца R там естественно записать 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 $p(n)$. Задача разрешима за полиномиальное время, если имеется ОРМ, решающая эту задачу за полиномиальное время. Это определение сложности вычисления ОРМ естественно в следующем смысле: набор значений аргументов $x_1, \ldots, x_n$ (элементов основного множества системы A) отождествляется со словом $x_1 \ldots x_n$ в алфавите A, таким образом, n — это просто длина входной цепочки, которая распределена по n входным регистрам. Вычислительная сложность на рассматриваемых машинах не учитывает сложность выполнения отдельных арифметических операций, которые могут быть невычислимыми в обычном смысле. В частности, кольцо R может не быть счётным. Однако здесь учитывается время на операции над индексными регистрами.

Вслед за [1] мы не допускаем команд вида $R_{I(t)} \coloneqq a$, где a — отличный от сигнатурной константы элемент основного множества системы. Поэтому если даже кольцо $\mathbb{Z}$ вкладывается в R и $\mathbb{Z}R$ — его образ, то при некоторых условиях на R и на входные данные $x_1, \ldots, x_n$, в регистрах машины нельзя получить некоторые (или даже никакие) элементы из $\mathbb{Z}R$ отличные от констант, при условии, что они не были заданы изначально. Пример такого сорта кольца и элементов $x_1, \ldots, x_n$ возникает при доказательстве теоремы 2.

В то же время, в индексных регистрах могут вычисляться любые рекурсивные (вычислимые) функции от натуральных чисел, так как имеются функции, позволяющие вычислять результат сложения, вычитания и умножения содержимого любого индексного регистра $I(k)$ с натуральным числом a, а также функция, вычисляющая целую часть от деления на a числа из $I(k)$. Значит, можно находить значения и любых вычислимых функций над кольцом $\mathbb{Z}$, представляя целые числа в виде формальной разности двух натуральных. Для этого нужно расширить список команд обобщённых регистровых машин командами вида $\mathrm{HALT}(I(k))$, которые означают, что результат вычислений содержится в индексном регистре $I(k)$, и у нас имеется возможность его прочитать. При этом всё равно остаётся проблема определения, представляет ли элемент, содержащийся в данном регистре, аналог натурального числа из некоторого индексного регистра, если кольцо $\mathbb{Z}$ вкладывается в R, но его подмножеством не является. В лемме 1 мы увидим, что если в качестве дополнительного входа машины разрешить задавать константу 1 или она присутствует в сигнатуре, то эта проблема разрешима. В этом случае ОРМ могут вычислять любые рекурсивные (вычислимые в обычном смысле) функции внутри $\mathbb{Z}R$.

Рассмотрим вычисления над ультрастепенью кольца $\mathbb{Z}$. Пусть ω – множество натуральных чисел, начиная с нуля. а D – некоторый его ультрафильтр, расширяющий фильтр коконечных подмножеств, U – ультрастепень линейно упорядоченного кольца $\mathbb{Z}$ над ультрафильтром D. Это линейно упорядоченное кольцо – область целостности, и в нём корректно определен наибольший общий делитель, поскольку $\mathbb{Z}$ и его ультрастепень U элементарно эквивалентны [4]. Но U обладает необычными свойствами, невыразимыми в языке первого порядка теории частично упорядоченных колец.

Элементы кольца U – классы эквивалентности бесконечных последовательностей целых чисел $\boldsymbol{a} = (a_0, a_1, \ldots)$. 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 и отношение порядка в кольце U определяются покомпонентно. Кольцо $\mathbb{Z}$ вложено в U, числу a соответствует класс постоянной последовательности $\boldsymbol{a} = (a, a, \dots)$. Ввиду элементарной эквивалентности колец $\mathbb{Z}$ и U, кольцо U имеет ровно два обратимых элемента, а именно, классы последовательностей $\mathbf{1} = (1,1, \dots)$ и $-\mathbf{1} = (-1, -1, \dots)$.

Теорема 1. *Область целостности U не является факториальным кольцом, хотя в нём существует наибольший общий делитель любых двух ненулевых элементов* $\boldsymbol{a}$ *и* $\boldsymbol{b}$*, а также неполное частное от деления элемента* $\boldsymbol{a}$ *на* $\boldsymbol{b} \geq \mathbf{1}$*, то есть такой элемент* $\boldsymbol{q}$*, что* $\boldsymbol{a} = \boldsymbol{b} \cdot \boldsymbol{q} + \mathrm{rest}(\boldsymbol{a}, \boldsymbol{b})$.

Следствие 1. *Упорядоченное кольцо U не является ни архимедовым, ни плотным, ни евклидовым.*

С другой стороны, в области целостности U операция $\mathrm{rest}(\cdot,\cdot)$ ведёт себя во многом одинаково с операцией вычисления остатка в целых числах.

Теорема 2. *Наибольший общий делитель и неполное частное от деления одного элемента на другой не вычислимы над кольцом* $(U, 0, +, -, \cdot, \mathrm{rest}, \leq)$ *посредством ОРМ.*

Картина меняется, когда имеется возможность использовать константу 1. Пусть в области целостности R с нестрогим линейным порядком определена вычислимость так, что имеются алгоритмы для вычисления сложения, вычитания и умножения, вычислимыми являются константа 0 и отношение порядка. В утверждениях 1 и 2 предполагается выполнение этих свойств в кольце R. Модель вычислимости здесь никак себя не проявляет, будь то вычислимость, задаваемая некоторым абстрактным устройством, вроде ОРМ, или вычислимость, заданная подходящей нумерацией.

Утверждение 1. *Из наличия алгоритма для нахождения неполного частного любых двух элементов* a *и* $b \neq 0$ *следует существование алгоритма для вычисления остатка от деления всякого элемента* a *на любой элемент* $b \geq 1$.

Утверждение 2. *Наоборот, наличие алгоритма для вычисления функции* rest *и возможность вычислять элемент 1 (или наличие его в сигнатуре) даёт алгоритмы для выяснения обратимости любых ненулевых элементов кольца и нахождения неполного частного во многих случаях*.

Теорема 3. *Вычисление неполного частного от деления любого элемента* $\boldsymbol{a}$ *на элемент* $\boldsymbol{b} > 0$ *производится подходящей ОРМ над кольцом* $(U, 0, +, -, \cdot, \mathrm{rest}, \leq)$ *за время, ограниченное константой, если на вход машины подавать не только эти элементы, но также и запись элемента* $\mathbf{1}$ *в регистре.*

Перейдём к вычислениям над декартовой степенью $\mathbb{Z}^\omega$ кольца целых чисел, с покомпонентным определением сигнатурных операций и отношения порядка. Это кольцо имеет мощность континуума. Отождествим кольцо $\mathbb{Z}$ с образом диагонального вложения в $\mathbb{Z}^\omega$, когда целое число отождествляется с постоянной последовательностью. Кроме наличия делителей нуля и несравнимых элементов, у $\mathbb{Z}^\omega$ имеются и другие существенные отличия от кольца U. Например, в кольце $\mathbb{Z}^\omega$ для между элементами $\boldsymbol{c} = (c_0, c_1, \dots)$ и $\boldsymbol{c} + \mathbf{1} = (c_0 + 1, c_1 + 1, \dots)$ имеется бесконечно много попарно несравнимых друг с другом элементов. Однако, порядок в $\mathbb{Z}^\omega$ тоже неплотный, так как между двумя элементами, у которых проекции на все множители, кроме одного, одинаковые, а особая координата второго элемента на единицу больше соответствующей проекции у первого, ничего нет. Здесь наблюдается эффект, отмеченный во введении: остаток от деления на элемент, у которого проекции на собственную часть множителей — минус единицы, а остальные проекции — положительные, может быть несравнимым с делителем.

Далее, наряду с элементом $\mathbf{1}$, мы будем использовать элемент $\boldsymbol{d} = (0,1,2, \dots) \in \mathbb{Z}^\omega$, у которого проекция на -й декартов множитель равна k и некоторые другие.

Лемма 1. *Пусть в одном из регистров ОРМ имеется элемент* $\mathbf{1}$. *Тогда по имеющейся записи элемента* $\boldsymbol{k} = (k, k, \dots) \in \mathbb{Z}^\omega$ *можно найти запись в индексных регистрах представления числа k в двоичной системе счисления за сублинейное время от величины k. Наоборот, если в индексных регистрах имеется запись представления целого*

числа k в двоичной системе счисления или в одном из индексных регистрах записано само это число, то можно за линейное время от числа индексных регистров, содержащих цифры числа k или от величины k, соответственно, вычислить элемент $\boldsymbol{k} \in \mathbb{Z}^{\omega}$.

Пример. Рассмотрим критерий простоты числа, который основан на малой теореме Ферма: целое число $p > 2$ простое тогда и только тогда, когда для каждого $x \in \mathbb{Z}$ выполнено равенство $x^p \equiv x(\mathrm{mod} p)$. Этот критерий лежит в основе вероятностного теста Рабина–Миллера для проверки простоты натурального числа в рамках обычной тьюринговой вычислимости, когда для достаточно большого количества натуральных чисел x проверяется сравнение $x^p \equiv x(\mathrm{mod} p)$. Однако использование ОРМ над кольцом $\mathbb{Z}^{\omega}$, позволяет создать уже детерминированный тест для такой проверки.

Вместо перебора чисел x из $\mathbb{Z}$ можно запустить ОРМ над $\mathbb{Z}^{\omega}$ на независящих от входа $\boldsymbol{p}$ последовательностях $\boldsymbol{d}$ и $\mathbf{1}$. Целое число $p > 2$ простое тогда и только тогда, когда $\mathbb{Z}^{\omega} \vDash \boldsymbol{d}^p \equiv \boldsymbol{d}(\mathrm{mod}\boldsymbol{p})$. Проверка этого условия завершается за конечное число шагов над $\mathbb{Z}^{\omega}$: остаток от деления на $\boldsymbol{p} \in \mathbb{Z}^{\omega}$ вычисляется за один шаг, посредством функции rest(·,·); возведение в степень $p \in \omega$ требует $O(\log p)$ умножений, если нам известно это натуральное число. Но поскольку нам дано лишь $\boldsymbol{p} \in \mathbb{Z}^{\omega}$, то предварительно мы ищем число p, используя элемент $\mathbf{1}$, встроенные в машину операции и часть индексных регистров для хранения цифр в двоичном представлении числа p, опираясь на лемму 1. На это тратится тоже $O(\log p)$ действий. При этом на вход подаётся только три элемента $\boldsymbol{p}$, $\boldsymbol{d}$ и $\mathbf{1}$. А число шагов зависит от значения числа p и может быть сколь угодно большим. Поэтому работа ОРМ не завершается за полиномиальное время относительно количества входных регистров, которых всего только три. Но время работы машины — линейное по отношению к величине числа p.

Напомним, что множество X из класса $\boldsymbol{NP}$ называется $\boldsymbol{NP}$полным, если каждое множество из класса $\boldsymbol{NP}$ сводится по Карпу к X. Примером служит множество X_0 таких линейных диофантовых уравнений от многих переменных, что каждое из этих уравнений имеет некоторое (0,1)-решение [5,6]. Коэффициентами уравнений служат обычные целые числа. Эту задачу можно интерпретировать и следующим образом. Можно ли среди нескольких целых чисел, которые задаются в качестве коэффициентов диофантова уравнения, выбрать такие, что их сумма равна данному числу — противоположному к свободному члену уравнения? Поэтому для краткости, мы будем называть задачу распознавания множества X_0 задачей о сумме подмножества мультимножества (среди коэффициентов диофантова уравнения могут быть равные).

Теорема 4. *Задача о сумме подмножества над $\mathbb{Z}$ детерминированно разрешима за полиномиальное время посредством ОРМ над $\mathbb{Z}^{\omega}$, использующей элементы $\boldsymbol{d}$ и $\mathbf{1}$.*

Если позволить использовать не только элемент $\boldsymbol{d}$, проекции которого легко вычислимы, но и произвольные наперёд заданные элементы, то можно реализовать вычисление с оракулом.

Теорема 5. *Задача распознавания целых чисел, принадлежащих фиксированному непустому множеству $Y \subset \mathbb{Z}$ разрешима за конечное время на ОРМ над $\mathbb{Z}^{\omega}$, использующей элемент $\mathbf{1}$ и элемент $\boldsymbol{f}$, определяемый множеством Y.*

Обсуждение. Недетерминированное вычисление над $\mathbb{Z}$ превращается в параллельное вычисление на неограниченном числе копий кольца $\mathbb{Z}$, которыми служат проекции декартовой степени на множители. Выигрыш достигается, если позволить машине использовать внутренние параметры из $\mathbb{Z}^{\omega}$, которые не принадлежат кольцу $\mathbb{Z}$, как дополнительные входы. Такая модель соответствует многопроцессорному вычислительному устройству с ограниченным обменом данными между процессорами, что существенно отличает эту модель от альтернирующих машин.

Принятая для ОРМ оценка вычислительной сложности оказывается неудобной, когда на вход подаётся одно число. При работе с многочленами, рациональными функциями или матрицами эта оценка лучше соответствует обычному понятию сложности. Но в общем случае полиномиально ограниченное число арифметических

операций нельзя выполнить за полиномиальное время на обычных машинах Тьюринга из-за возникновения неожиданно больших чисел. Рассмотрим, например, вычисление наибольшего общего делителя (в кольце $\mathbb{Q}[x]$) двух многочленов с целыми коэффициентами от одной переменной на обобщённой регистровой машине над кольцом $\mathbb{Z}$. Пусть каждый многочлен задан набором коэффициентов, включая нулевые. Тогда запись одного многочлена степени d занимает $d+1$ регистров. Алгоритм Евклида требует линейного от суммы степеней числа операций. Однако возникающие на промежуточных шагах коэффициенты могут иметь очень большую длину записи [7,8,9, 10], что значительно увеличивает время вычислений при использовании многоленточных машин Тьюринга.

Заключение. Обобщённые регистровые машины – это мощное средство для изучения сложности вычислений над произвольными алгебраическими структурами, в первую очередь над кольцами и полями. Вычисления ОРМ над полем вещественных чисел подобны вычислениям на BSS-машине [11,12], а в случае линейно упорядоченных ассоциативных и коммутативных колец почти не отличаются от машин над списочной надстройкой Ашаева–Беляева–Мясникова [13] и S-машин Хеммерлинга [14].

Литература

1. E. Neumann, P. Pauly, A topological view on algebraic computation models, Journal of Complexity, 44 (2018), 1–22.

2. A.V. Seliverstov, Heuristic algorithms for recognition of some cubic hypersurfaces, Programming and Computer Software, 47 (2021), 50–55.

3. A.V. Seliverstov, Binary solutions to large systems of linear equations, Prikladnaya Diskretnaya Matematika, no. 52 (2021), 5–15.

4. C.C. Chang, H.J. Keisler, Model Theory, Elsevier, 1990.

5. K. Koiliaris, C. Xu, Faster pseudopolynomial time algorithms for subset sum, ACM Transactions on Algorithms, 15:3 (2019), 40.

6. A.V. Seliverstov, On binary solutions to systems of equations, Prikladnaya Diskretnaya Matematika, no. 45 (2019), 26–32.

7. P.E. Alaev, V.L. Selivanov, Fields of algebraic numbers computable in polynomial time. I, Algebra and Logic, 58:6 (2020), 447–469.

8. A. Sinhababu, T. Thierauf, Factorization of polynomials given by arithmetic branching programs, Computational complexity, 30:15 (2021), 1–47.

9. W. Habicht, Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens, Commentarii Mathematici Helvetici, 21 (1948), 99–116.

10. A.G. Akritas, Elements of Computer Algebra with Applications, John Wiley and Sons, NY, 1989.

11. L. Blum, M. Shub, S. Smale, On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines, Bulletin of the American Mathematical Society, 21:1 (1989), 1–46.

12. L. Blum, F. Cucker, M. Shub, S. Smale, Complexity and Real Computation, Springer, New York, 1998.

13. I.V. Ashaev, V.Ya. Belyaev, A.G. Myasnikov, Toward a Generalized Computability Theory, Algebra and Logic, 32:4 (1993), 185–205.

14. A. Hemmerling, Computability of string functions over algebraic structures, Mathematical Logic Quarterly 44:1 (1998), 1–44.