S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 19, стр. 144–144 (2022) УДК 510.52
DOI 10.33048/semi.2022.19.xxx MSC 03D15, 68Q09

О ВЫЧИСЛЕНИЯХ НАД УПОРЯДОЧЕННЫМИ КОЛЬЦАМИ

И.В. ЛАТКИН, А.В. СЕЛИВЕРСТОВ

Abstract. We consider generalized register machines over ordered rings with an auxiliary binary operation. In particular, we consider the ring of integers, its infinite Cartesian power, and ultrapowers. The feasibility and computational complexity of some algorithms are discussed. There is also given an example of a non-factorial ring, which is elementarily equivalent to the ring of integers. It is shown that non-deterministic computations with integers can be implemented as computations over the Cartesian power of the ring of integers. It is also possible to model calculations with an oracle using such machines. This provides an algebraic approach to describing some classes of computational complexity. However, this model of computation differs significantly from alternating machines.

Keywords: generalized register machine, ring, integral domain, integers, ultrapower, polynomial time, oracle.

1. Введение

Рассмотрим обобщённые регистровые машины [1, 2, 3] над частично упорядоченным ассоциативным и коммутативным кольцом со вспомогательными бинарными операциями вычитания и rest: $(R; 0, +, -, \cdot, \mathrm{rest}, \leqslant)$, поскольку без подобного расширения вычислительные возможности таких машин весьма ограничены. В кольце целых чисел $\mathbb{Z}$ для любого x и для $y \geqslant 2$ значением $\mathrm{rest}(x, y)$ служит остаток от деления x на y из множества $\{0, \ldots, y-1\}$, а для $y \leqslant 1$ полагаем $\mathrm{rest}(x, y) = 0$. Естественно, что в других рассматриваемых кольцах тоже должно выполняться условие

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

Latkin, I.V., Seliverstov, A.V. On computations over ordered rings.

Поступила 17 января 2022 г., опубликована 31 декабря 2022 г.

для $y \geqslant 2$, где под двойкой понимается сумма нейтрального элемента по умножению с самим собой, а при нарушении условия $y \geqslant 2$ (в частности, если элемент y несравнимый с аналогом двойки) не обязательно будет выполняться равенство $\mathrm{rest}(x, y) = 0$. Тем не менее, при корректном определении этой операции, разумно потребовать выполнения более слабого свойства: для любого y верно, что $\mathrm{rest}(x, y) \geqslant 0$ и либо $\mathrm{rest}(x, y) < y$, либо $\mathrm{rest}(x, y)$ несравнимый с y. Такая ситуация возникает, например, при покомпонентном определении остатка в декартовом или прямом произведении колец, в которых эта операция уже определена (см. раздел 3 ниже). Естественно также, что во всех рассматриваемых нами кольцах $\mathrm{rest}(x, y) = 0$, когда элемент y обратим.

Хотя во всех исследуемых далее кольцах существует нейтральный элемент по умножению, единица не включена в сигнатуру в явном виде, но когда потребуется, она будет включаться в вычисления в качестве вспомогательного входа.

Отметим, что здесь мы ограничиваемся таким обогащением кольцевой сигнатуры, чтобы в случае совпадения кольца R с кольцом целых чисел $\mathbb{Z}$ получалось консервативное расширение теории $Th(\mathbb{Z})$, так как отношение порядка и деление с остатком определяются над $\mathbb{Z}$ формулами первого порядка. Например, неотрицательное целое число равно сумме четырёх квадратов целых чисел, среди которых могут быть равные. Кроме того, нам достаточно описанного выше тривиального определения операции $\mathrm{rest}(x, y)$ в кольце $\mathbb{Z}$ для случая $y < 2$ ввиду того, что в первую очередь нас интересует моделирование некоторых аспектов обычной тьюринговой вычислимости на натуральных числах средствами обобщённых регистровых машин, в частности, параллельных вычислений, см. раздел 3.

Напомним вкратце описание работы обобщённой регистровой машины. Каждый регистр может содержать какой-то элемент кольца R, над которыми за один шаг выполняются операции, перечисленные в сигнатуре. Константы соответствуют операциям записи соответствующего элемента в регистр. В случае проверки предиката на истинность, машина переходит в новое состояние в зависимости от его истинности. Также за один шаг машина может копировать и пересылать элементы между регистрами. Кроме того,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. Незанятые 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 $p(n)$.

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. В случае, когда линейно упорядоченным кольцом R служит поле вещественных чисел $\mathbb{R}$, эти машины тесно связаны с BSS-машинами [4]. Иногда

рассматривают и такие машины, время работы которых бесконечно и выражается счётным ординалом [5, 6, 7]. Однако мы предполагаем, что машина на каждом входе делает лишь конечное число шагов.

2. Вычисления над ультрастепенью кольца $\mathbb{Z}$

Обозначим через ω множество натуральных чисел, начиная с нуля. Фиксируем некоторый ультрафильтр D, расширяющий фильтр коконечных подмножеств множества ω. В частности, для каждого подмножества множества натуральных чисел либо оно само, либо его дополнение принадлежит ультрафильтру D. Обозначим через U ультрастепень линейно упорядоченного кольца целых чисел $\mathbb{Z}$ над ультрафильтром D. Это линейно упорядоченное кольцо является областью целостности. Более того, в нём корректно определен наибольший общий делитель GCD, поскольку кольцо целых чисел $\mathbb{Z}$ и его ультрастепень $U = \prod_D \mathbb{Z}$ элементарно эквивалентны [8]. Однако U обладает необычными свойствами, невыразимыми в языке первого порядка теории частично упорядоченных колец.

2.1. **Алгебраические свойства ультрастепени U.** Элементами кольца U служат классы эквивалентности бесконечных последовательностей целых чисел $\mathbf{a} = (a_0, a_1, \dots)$. 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 и отношение порядка в кольце U определяются покомпонентно. Кольцо целых чисел $\mathbb{Z}$ вложено в кольцо U, числу a соответствует класс постоянной последовательности $\mathbf{a} = (a, a, \dots)$. Каждая последовательность, содержащая нулевые элементы, либо эквивалентна последовательности из одних нулей $\mathbf{0} = (0, 0, \dots)$, либо эквивалентна последовательности, в которой нет ни одного нуля. Поэтому кольцо U не содержит делителей нуля. В кольце U ровно два обратимых элемента, а именно, классы каждой из двух постоянных последовательностей $\mathbf{1} = (1, 1, \dots)$ и $-\mathbf{1} = (-1, -1, \dots)$. Класс эквивалентности любой последовательности, состоящей из чисел 1 и -1, служит представителем обратимого элемента, но каждая из них эквивалентна либо $\mathbf{1}$, либо $-\mathbf{1}$, поскольку ультрафильтру принадлежит либо множество индексов единиц, либо множество индексов минус единиц.

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

Доказательство. Для любого натурального числа m, класс последовательности целых чисел $\mathbf{c}_m$, k-й элемент которой равен целой части $(k-m)$-й степени числа два $\lfloor 2^{k-m} \rfloor$, служит ненулевым и необратимым элементом кольца U, который делится на элемент $\mathbf{2} = (2, 2, \dots)$ без остатка, так как в этой последовательности все кроме конечного множества членов чётные. Этот класс, содержащий элементы $\mathbf{c}_m$, не разлагается в конечное произведение неприводимых элементов кольца U. Следовательно, кольцо U нефакториальное.

Существование наибольшего общего делителя и неполного частного двух элементов, удовлетворяющих условиям теоремы, вытекает из уже отмеченной элементарной эквивалентности колец $\mathbb{Z}$ и U [8]. Однако можно дать и явное

описание этих объектов, а именно, наибольший общий делитель GCD двух элементов, представителями которых служат последовательности $\mathbf{a} = (a_0, a_1, \dots)$ и $\mathbf{b} = (b_0, b_1, \dots)$, равен классу последовательности наибольших общих делителей $\mathrm{GCD}(\mathbf{a}, \mathbf{b}) = (\mathrm{GCD}(a_0, b_0), \mathrm{GCD}(a_1, b_1), \dots)$. И если все $b_i \geqslant 1$, то неполное частное от деления элемента $\mathbf{a}$ на $\mathbf{b}$ равно

$$((a_0 - \mathrm{rest}(a_0, b_0))/b_0, (a_1 - \mathrm{rest}(a_1, b_1))/b_1, \dots).$$

□

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

Доказательство. Действительно, построенный при доказательстве теоремы элемент $\mathbf{c_0}$ не может стать меньше никакой конечной суммы вида $\mathbf{2}^t + \dots + \mathbf{2}^t$. В то же время, для всякого элемента $\mathbf{a}$ из U между ним и $\mathbf{a} + \mathbf{1}$ нет никаких элементов, что следует из элементарной эквивалентности колец $\mathbb{Z}$ и U. □

2.2. **Алгоритмические свойства ультрастепени U.**

Теорема 2. *Наибольший общий делитель и неполное частное от деление одного элемента на другой невычислимы над кольцом $(U; 0, +, -, \cdot, \mathrm{rest}, \leqslant)$ посредством обобщённых регистровых машин.*

Доказательство. Очевидно, что элемент $\mathbf{c} = (2, 2^2, \dots, 2^k, \dots)$ — наибольший делитель элементов $\mathbf{a} = (2{\cdot}3, 2^2{\cdot}3^2, \dots, 2^k{\cdot}3^k, \dots)$ и $\mathbf{b} = (2{\cdot}5, 2^2{\cdot}5^2, \dots, 2^k{\cdot}5^k, \dots)$ равен также частному от деления элемента $\mathbf{a}$ на $\mathbf{e} = (3, 3^2, \dots, 3^k, \dots)$.

Индукцией по числу шагов несложно доказывается следующее утверждение. Если на вход обобщённой регистровой машины поданы элементы $\mathbf{a}$ и $\mathbf{e}$, и на каком-то шаге её работы в одном из регистров появился элемент, делящийся на $\mathbf{c}$, то этот элемент обязательно делится и на $\mathbf{3} = (3, 3, 3, \dots)$. Значит этот элемент не может быть равен $\mathbf{c}$.

Опять индукцией по числу шагов доказывается и следующая

Лемма 1. *Пусть на вход обобщённой регистровой машине подаются элементы $\mathbf{a}$ и $\mathbf{b}$. Тогда если на каком-то шаге вычислений в одном из регистров появился элемент, делящийся на $\mathbf{c}$, то*

любая его k-я компонента, начиная с какого-то номера k_0, имеет вид $2^{k+t(k)} f_k$, где $t(k+1) - t(k) = t(k+2) - t(k+1) \geqslant 0$, а множитель f_k не делится на 2^k и представим как многочлен от степеней чисел 3 и 5 вида

$$\sum m_{i,j}(k) \cdot 3^{i(k)} \cdot 5^{j(k)}.$$

В этой сумме каждое слагаемое кратно хотя бы одному из чисел 3 или 5, а множитель f_{k+1} у $(k+1)$-й компоненты представим в виде суммы с тем же числом слагаемых, что и f_k;

при этом $i(k+2) - i(k+1) = i(k+1) - i(k) \geqslant 1$ и $j(k+2) - j(k+1) = j(k+1) - j(k) \geqslant 1$;

хотя бы часть коэффициентов $m_{i,j}(k)$ не зависит от k, т.е. $m_{i,j}(k) = m_{i,j}(k+1)$, а те коэффициенты, что зависят от k имеют вид $m_{i,j}(k) = 2^{l(i,j,k)} n_{i,j}$, для некоторых констант $n_{i,j}$, где опять $l(i,j,k+2) - l(i,j,k+1) = l(i,j,k+1) - l(i,j,k) \geqslant 1$.

Разумеется, часть множителей f_k у элемента $\mathbf{r}$, делящегося на $\mathbf{c}$, может равняться степеням числа 2 даже при $k \geqslant k_0$, например, $5^2 - 3^2 = 2^4$. Тем не менее, опираясь на лемму 1, уже обычной индукцией по k несложно вывести, что при всех таких k выполнено неравенство $|f(k+1)| > |f(k)| > 0$. Это означает, что ни на каком конечном шаге мы не получим элемент $\mathbf{r}$ равный $\mathbf{c}$. □

Картина существенно меняется, когда имеется возможность использовать константу 1, как показывают следующие утверждения. Подчеркнём, что модель вычислимости здесь никак себя не проявляет, будь то вычислимость, задаваемая некоторым абстрактным вычислительным устройством, вроде обобщённых регистровых машин, или вычислимость, заданная подходящей нумерацией.

Пусть в области целостности R с нестрогим линейным порядком $\leqslant$ определена вычислимость таким образом, что имеются алгоритмы для вычисления сложения, вычитания и умножения, а также вычислимыми являются константа 0 и отношение порядка. В нижеследующих утверждениях предполагается выполнение всех этих свойств в кольце R.

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 $b \geqslant 1$.*

Доказательство. Действительно, если неполное частное от деления a на $b \geqslant 1$ равно q, то, очевидно, $\mathrm{rest}(a, b) = a - b \cdot q$. □

Утверждение 2. *Наоборот, наличие алгоритма для вычисления остатка и возможность вычислять элемент 1 влечёт существование алгоритмов для выяснения обратимости любых ненулевых элементов кольца и нахождения неполного частного во многих случаях.*

Доказательство. Очевидно, что элемент $b > 0$ из R обратим тогда и только тогда, когда $\mathrm{rest}(1, b) = 0$, а если $b < 0$, то нужно вычислить $\mathrm{rest}(1, -b)$.

Предположим, что каким-то образом можно вычислять единицу и остаток от деления всякого элемента a на любой $b \neq 0$ (или имеется способ нахождения их номеров). Чтобы вычислить неполное частное q от деления данного элемента $a > 0$ на известный элемент $b > 1$, вычислим элемент

$$c = a - \mathrm{rest}(a, b)$$

и рассмотрим три основных случая.

Если $c < b^2 - b$ и элемент $b - 1$ необратимый, то, учитывая $c = b \cdot q$, получаем $q < b - 1$ и $c = (b-1)q + q$. Следовательно, $q = \mathrm{rest}(c, b-1)$.

Когда $b^2 < c$, тогда $b < q$. Но при дополнительном предположении, что $b \geqslant 1 + 1$, элемент $c \cdot b - 1$ всё же больше, чем q; если к тому же этот элемент необратимый, то $q = \mathrm{rest}(c^2, c \cdot b - 1)$, поскольку $c^2 = (c \cdot b - 1)q + q$.

При выполнении условия $b^2 - b < c < b^2$, равносильного $b - 1 < q < b$, имеем $-c = (b+1) \cdot (-q) + q$ и $q = \mathrm{rest}(-c, b+1)$ при необратимом элементе $b + 1$.

В крайних случаях $c = b^2 - b$ или $c = b^2$ понятно, что $q = b - 1$ или $b = q$, соответственно.

При $a < 0$ поступаем почти симметричным образом. □

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

Доказательство. Напомним, что в кольце U ровно два обратимых элемента $\mathbf{1}$ и $-\mathbf{1}$, и из того, что $\mathbf{b} > \mathbf{0}$ и $\mathbf{b} \neq \mathbf{1}$ следует, что $\mathbf{b} \geqslant \mathbf{2}$, поэтому полностью применим алгоритм, описанный при доказательстве утверждения 2. □

Замечание 1. Дополнительное предположение, что $b \geqslant 1+1$, из доказательства утверждения 2 (случай $b^2 < c$) можно заменить более слабым, например, что $2 \cdot b = b + b \geqslant 1 + 1 + 1 = 3 \cdot 1$. Но для произвольной области целостности R в случае $b^2 < c$ поиск неполного частного без дополнительных ограничений вида $k \cdot b \geqslant m \cdot 1$, где $k, m \in \omega$ (или каких-то других), представляется крайне сложной задачей. На этот вывод наводит изучение делимости в кольце U_2, которое получено как ультрастепень кольца рациональных чисел, знаменатели которых в несократимой записи суть степени двойки

$$\mathbb{Q}(2) = \{m/2^t \mid m \in \mathbb{Z}, t \in \omega\},$$

по ультрафильтру D из начала этого раздела. Определим неполное частное q от деления числа x на $y > 0$ в кольце $\mathbb{Q}(2)$ как число вида $s/2$, где s — наименьшее целое со свойством $y \cdot (s+1)/2 \geqslant x$, а $\mathrm{rest}(x, y) = x - y \cdot q$. Рассмотрим в кольце U_2 множество элементов $\mathbf{b}(M)$ вида $(t_0/2^{r_0}, t_1/2^{r_1}, \ldots, t_k/2^{r_k}, \ldots)$, где последовательность $M = (\langle t_0, r_0\rangle, \langle t_1, r_1\rangle, \ldots, \langle t_k, r_k\rangle, \ldots)$ пар натуральных чисел имеет единственное ограничение $(\forall k \in \omega)(t_k \leqslant 2^{r_k})$. Несложно понять, что общего алгоритма для вычисления посредством обобщённых регистровых машин неполного частного от деления элементов $\mathbf{a} \geqslant \mathbf{2}$ на произвольный элемент вида $\mathbf{b}(M) \leqslant \mathbf{1}$ над кольцом $(U_2; 0, +, -, \cdot, \mathrm{rest}, \leqslant)$ не существует, даже тогда, когда на вход машины наряду с элементами $\mathbf{a}$ и $\mathbf{b}(M)$ подаётся элемент $\mathbf{1}$.

2.3. **Сложность вычисления наибольшего общего делителя.** Принятая для обобщённых регистровых машин 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.

Пример 1. Рассмотрим 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 коэффицентов, 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 [9, 10, 11, 12].

Чтобы преодолеть эту трудность, для вычисления наибольшего общего делителя многочленов применяются другие алгоритмы. Метод, основанный на вычислении субрезультантов, впервые предложил Дж. Сильвестр (J.J. Sylvester).

Потом этот метод улучшали Вальтер Габихт (Walter Habicht) [11] и Алкивиадис Акритас (Alkiviadis Akritas) [12]. Более эффективен алгоритм, который предложил Уильям Браун (William Brown) [13]. Этот алгоритм реализован в системах компьютерной алгебры, включая систему MathPartner [14].

3. Вычисления над декартовой степенью кольца $\mathbb{Z}$

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. Далее отождествим кольцо целых чисел $\mathbb{Z}$ с образом диагонального вложения в $\mathbb{Z}^\omega$, когда целое число m отождествляется с постоянной последовательностью. Кроме очевидного наличия делителей нуля и несравнимых элементов, у кольца $\mathbb{Z}^\omega$ имеются и другие существенные отличия от кольца U. Например, в кольце $\mathbb{Z}^\omega$ для любого элемента $\mathbf{c} = (c_0, c_1, c_2, \ldots)$ между ним и элементом $\mathbf{c} + \mathbf{1} = (c_0+1, c_1+1, c_2+1, \ldots)$ имеется бесконечно много попарно несравнимых друг с другом элементов. Тем не менее, порядок в кольце $\mathbb{Z}^\omega$ всё же неплотный, так как между двумя элементами этого кольца, у которых проекции на все множители, кроме одного, одинаковые, а особая «координата» второго элемента на единицу больше соответствующей проекции у первого, ничего нет, но первый элемент меньше второго. В этом кольце также 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.

Говоря неформально, мы покажем, что, подавая обобщённой регистровой машине над $\mathbb{Z}^\omega$ на вход числа из $\mathbb{Z}$, можно моделировать параллельные вычисления с ограниченным обменом между процессорами. Выигрыш может быть достигнут, если позволить машине использовать внутренние параметры из $\mathbb{Z}^\omega$, которые не принадлежат кольцу $\mathbb{Z}$, как дополнительные входы. Среди таких дополнительных входов-параметров, наряду с элементом $\mathbf{1} = (1, 1, \ldots)$, будем использовать элемент, обозначаемый через $\mathbf{d} = (0, 1, 2, \ldots) \in \mathbb{Z}^\omega$, чья проекция на k-й декартов множитель равна k.

Замечание 2. В дальнейшем для краткости, рассматривая вычисления над кольцом $\mathbb{Z}^\omega$, мы будем говорить, что на вход машины подано целое число a, подразумевая элемент $\mathbf{a} = (a, a, \ldots)$, так как в случае необходимости запись в индексных регистрах представления числа a в какой-либо системе счисления может быть найдена машиной за время меньшее, чем линейное от величины a, см. нижеследующий пример 2.

Пример 2. Рассмотрим тест Рабина для проверки простоты числа, который основан на малой теореме Ферма: целое число $p \geqslant 2$ простое тогда и только тогда, когда для каждого $x \in \mathbb{Z}$ выполнено равенство $x^p \equiv x \pmod{p}$. Вместо перебора чисел x из $\mathbb{Z}$ можно запустить обобщённую регистровую машину над $\mathbb{Z}^\omega$ на независящими от входа $\mathbf{p}$ последовательностями $\mathbf{d}$ и $\mathbf{1}$. Целое число $p \geqslant 2$ простое тогда и только тогда, когда

$$\mathbb{Z}^\omega \models \mathbf{d}^p \equiv \mathbf{d} \,(\mathrm{mod}\, \mathbf{p}).$$

Проверка этого условия завершается за конечное число шагов над $\mathbb{Z}^\omega$. В самом деле, остаток от деления на $\mathbf{p} \in \mathbb{Z}^\omega$ вычисляется за один шаг; для этого в сигнатуре предусмотрен функциональный символ rest. Возведение в степень

$p \in \omega$ требует $O(\log p)$ умножений, если нам известно это натуральное число. Но поскольку нам дано лишь $\mathbf{p} \in \mathbb{Z}^\omega$, 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. На это тратится тоже $O(\log p)$ действий, поскольку нахождение неполного частного от деления элемента $\mathbf{t} \leqslant \mathbf{p}$ на $\mathbf{2} = \mathbf{1}+\mathbf{1}$ осуществимо за время, ограниченное некоторой константой, согласно алгоритму, описанному при доказательстве утверждения 2. Этот алгоритм здесь применим, так как все необходимые вычисления производятся внутри образа кольца $\mathbb{Z}$ при его диагональном вложении в $\mathbb{Z}^\omega$, т.е. в некоторой области целостности. Однако можно поступить по-иному, чтобы узнать неполное частное от деления $\mathbf{p}$ на $\mathbf{2}$, для этого достаточно сделать следующее. Подряд сравниваем число $\mathbf{p}$ со степенями $\mathbf{2}^k$ до тех пор, пока не найдётся значение, превосходящее $\mathbf{p}$; число шагов при этом равно $k \leqslant 1+\log_2(1+p))$; затем находим двоичное представление числа p — это сумма некоторых степеней $\mathbf{2}^k$. Но число таких сравнений само равно $O(\log_2 p)$, поэтому второй способ немного более трудоёмкий.

При этом на вход подаётся только три элемента $\mathbf{p}$, $\mathbf{1}$ и $\mathbf{d}$. А число шагов зависит от значения числа p и может быть сколь угодно большим. Поэтому работа машины не завершается за полиномиальное время.

Отметим, что задача об определении простоты элемента может быть очень сложной, даже в случае вычислимой области целостности с однозначным разложении на множители. Например, в работе [15] строится кольцо $A(Q)$ с этими свойствами, содержащее в качестве подкольца кольцо целых чисел $\mathbb{Z}$, в котором при любом вычислимом представлении указанная задача имеет сложность вхождения в наперёд заданное Π^0_2-множество Q.

Напомним, что множество X принадлежит классу NP, если существует такой алгоритм полиномиального времени, что для каждого элемента $x \in X$ существует сертификат y полиномиальной длины, при котором этот алгоритм допускает пару $\langle x, y\rangle$, а для каждого $x \notin X$ такого сертификата не существует. Множество X соответствует задаче распознавания. Это определение легко переносится и на обобщённые регистровые машины. Но здесь мы будем рассматривать класс NP в обычном смысле.

Множество X из класса NP называется NP-полным, если каждое множество из класса NP сводится по Карпу к множеству X. Примером служит множество таких линейных диофантовых уравнений от многих переменных, что каждое из этих уравнений имеет некоторое $(0,1)$-решение [16, 17]. 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 *задачей о сумме подмножества*. Строго говоря, следовало бы говорить о мультимножестве и его подмножестве, поскольку среди коэффициентов диофантова уравнения могут быть равные.

Теорема 4. *Задача о сумме подмножества над $\mathbb{Z}$ разрешима за детерминированное полиномиальное время на обобщённой регистровой машине над $\mathbb{Z}^\omega$, использующей элементы $\mathbf{1}$ и $\mathbf{d}$.*

Доказательство. Машина получает на вход набор элементов $\mathbf{a}_0$, $\mathbf{a}_1$, …, $\mathbf{a}_n$ из кольца $\mathbb{Z}^\omega$, которые соответствуют целым коэффициентам линейного уравнения $a_0 + a_1x_1 + \cdots + a_nx_n = 0$ и элементы $\mathbf{1}$ и $\mathbf{d}$. Число регистров, занятых входом, равно $n + 3$. Это число $n + 3$ записано в нулевом индексном регистре. Работа машины состоит из трёх этапов. Реализация и сложность каждого из них описывается ниже.

Сначала машина вычисляет n различных простых натуральных чисел p_1, …, p_n, точнее соответствующие элементы из кольца $\mathbb{Z}^\omega$, а также запись в $O(n \log n)$ индексных регистрах цифр при двоичном представлении этих чисел.

Потом машина вычисляет n элементов $\mathbf{b}_1$, …, $\mathbf{b}_n$ из $\mathbb{Z}^\omega$, для каждого из которых все проекции на декартовы множители равны 0 или 1. При этом каждая из 2^n комбинаций из n нулей и единиц должна (бесконечное число раз) реализоваться как набор проекций $(b_{1,k}, \ldots, b_{n,k})$ элементов $\mathbf{b}_1$, …, $\mathbf{b}_n$ на некоторый множитель с номером k.

Наконец, вычисляется значение $\mathbf{c} = (a_0 + a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n)^2$ и за один шаг проверяется условие $\mathbf{1} \leqslant \mathbf{c}$, означающее положительность проекции элемента $\mathbf{c}$ на каждый множитель. При выполнении этого условия вход отвергается, и вход принимается, когда ответ отрицательный.

Оценим сложность этого алгоритма. При $x \geqslant 17$ количество простых чисел на отрезке $[1, x]$ удовлетворяет неравенству [18]

$$\pi(x) \geqslant \frac{x}{\ln x}$$

Поэтому для выбора простых чисел $p_1 = 2, p_2 = 3, \ldots, p_n$ достаточно проверить $O(n \log n)$ чисел. Проверка каждого из них выполняется за время, ограниченное многочленом от n, см. пример 2.

Для каждого индекса $k \leqslant n$ вычислим $\mathbf{b}_k = \mathrm{rest}(\mathbf{d}^{p_k - 1}, \mathbf{p_k})$, где через $\mathbf{d}$ обозначен фиксированный элемент $(0, 1, 2, \ldots) \in \mathbb{Z}^\omega$. Проекция k-го элемента $\mathbf{b}_k$ на m-й множитель равна нулю, когда p_k делит m, иначе она равна единице. В частности, $\mathbf{b}_1 = (0, 1, 0, 1, 0, 1, \ldots)$ и $\mathbf{b}_2 = (0, 1, 1, 0, 1, 1, 0, \ldots)$. В силу Китайской теоремы об остатках, любой набор нулей и единиц реализуется как набор проекций $(b_{1,t}, \ldots, b_{n,t})$ элементов $\mathbf{b}_1$, …, $\mathbf{b}_n$ на некоторый множитель с номером t. Например, при любом $\mathbf{b}_k$ его проекции $b_{k,0} = 0$ и $b_{k,1} = 1$. Поэтому проекции на нулевой и первый множители дают набор из нулей и набор из единиц, соответственно. Наконец, вычисление $\mathbf{c} = (a_0 + a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n)^2$ выполняется за $O(n)$ операций. □

Из теоремы 4 не следует, что за полиномиальное время разрешима задача, аналогичная задаче о сумме подмножества, когда коэффициентами уравнений служат элементы из кольца $\mathbb{Z}^\omega$.

Неформальное объяснение теоремы 4 состоит в том, что недетерминированное вычисление над $\mathbb{Z}$ превращается в параллельное вычисление на неограниченном числе копий кольца $\mathbb{Z}$, которыми служат проекции декартовой степени на множители. Такая модель соответствует многопроцессорному вычислительному устройству с ограниченным обменом данными между процессорами, что существенно отличает эту модель от альтернирующих машин.

Отметим трудную задачу, которую не удаётся решить, используя обобщённые регистровые машины над $\mathbb{Z}^\omega$. Непонятно, можно ли за полиномиальное

время, используя $\mathbf{d} = (0, 1, 2, \dots)$, найти число решений задачи о сумме подмножества. Или хотя бы проверить за полиномиальное время, что это число решений равно наперёд угаданному числу.

Если позволить использовать не только элемент $\mathbf{d}$, 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 $X \subset \mathbb{Z}$ разрешима за конечное время на обобщённой регистровой машине над $\mathbb{Z}^\omega$, использующей элемент $\mathbf{1}$ и элемент $\mathbf{f}$, определяемый множеством X.*

Доказательство. Фиксируем сюръективное отображение $\nu : \omega \to X$. Зададим проекцию элемента $\mathbf{f}$ на k-й декартов множитель равной $\nu(k)$. Машина получает на вход три элемента $\mathbf{1}$, $\mathbf{f}$ и $\mathbf{n}$, соответствующий числу $n \in \mathbb{Z}$. Это число принадлежит множеству X тогда и только тогда, когда нарушается условие $\mathbf{1} \leqslant (\mathbf{n} - \mathbf{f})^2$. Это условие проверяется за конечное число операций над $\mathbb{Z}^\omega$. □

References

[1] E. Neumann, P. Pauly, *A topological view on algebraic computation models*, Journal of Complexity, **44** (2018), 1–22. https://doi.org/10.1016/j.jco.2017.08.003

[2] A.V. Seliverstov, *Heuristic algorithms for recognition of some cubic hypersurfaces*, Programming and Computer Software, **47** (2021), 50–55. https://doi.org/10.1134/S0361768821010096

[3] A.V. Seliverstov, *Binary solutions to large systems of linear equations*, Prikladnaya Diskretnaya Matematika, no. 52 (2021), 5–15. https://doi.org/10.17223/20710410/52/1

[4] 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. https://doi.org/10.1090/S0273-0979-1989-15750-9

[5] P. Koepke, A.S. Morozov, *Characterizations of ITBM-computability. I*, Algebra and Logic, **59**:6 (2021), 423–436. https://doi.org/10.1007/s10469-021-09622-2

[6] P. Koepke, A.S. Morozov, *Characterizations of ITBM-computability. II*, Algebra and Logic, **60**:1 (2021), 26–37. https://doi.org/10.1007/s10469-021-09625-z

[7] M. Carl, *Taming Koepke's Zoo II: Register machines*, Annals of Pure and Applied Logic, **173**:3 (2022), 103041. https://doi.org/10.1016/j.apal.2021.103041

[8] C.C. Chang, H.J. Keisler, *Model Theory*, Elsevier, 1990.

[9] P.E. Alaev, V.L. Selivanov, *Fields of algebraic numbers computable in polynomial time. I*, Algebra and Logic, **58**:6 (2020), 447–469. https://doi.org/10.1007/s10469-020-09565-0

[10] A. Sinhababu, T. Thierauf, *Factorization of polynomials given by arithmetic branching programs*, Computational complexity, **30**:15 (2021), 1–47. https://doi.org/10.1007/s00037-021-00215-0

[11] W. Habicht, *Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens*, Commentarii Mathematici Helvetici, **21** (1948), 99–116. https://doi.org/10.1007/BF02568028

[12] A.G. Akritas, *Elements of Computer Algebra with Applications*, John Wiley and Sons, NY, 1989.

[13] W.S. Brown, *The subresultant PRS algorithm*, ACM Transactions on Mathematical Software, **4**:3 (1978), 237–249. https://doi.org/10.1145/355791.355795

[14] G.I. Malaschonok, A.V. Seliverstov, *Calculation of integrals in MathPartner*, Discrete and Continuous Models and Applied Computational Science, **29**:4 (2021), 337–346. https://doi.org/10.22363/2658-4670-2021-29-4-337-346

[15] D.D. Dzhafarov, J.R. Mileti, *The Complexity of Primes in Computable Unique Factorization Domains*, Notre Dame Journal of Formal Logic, **59**:2 (2018), 139–156. https://doi.org/10.1215/00294527-2017-0024

[16] K. Koiliaris, C. Xu, *Faster pseudopolynomial time algorithms for subset sum*, ACM Transactions on Algorithms, **15**:3 (2019), 40. https://doi.org/10.1145/3329863
[17] A.V. Seliverstov, *On binary solutions to systems of equations*, Prikladnaya Diskretnaya Matematika, no. 45 (2019), 26–32. https://doi.org/10.17223/20710410/45/3
[18] P. Dusart, *Explicit estimates of some functions over primes*, The Ramanujan Journal, **45** (2018), 227–251. https://doi.org/10.1007/s11139-016-9839-4

Ivan Vasilyevich Latkin
D. Serikbayev East Kazakhstan Technical University,
Protozanov Street, 69, Ust-Kamenogorsk, 070004, The Republic of Kazakhstan
E-mail address: lativan@yandex.kz

Alexandr Vladislavovich Seliverstov
Institute for Information Transmission Problems
of the Russian Academy of Sciences,
Bolshoy Karetny, 19, Moscow, 127051, Russia
E-mail address: slvstv@iitp.ru