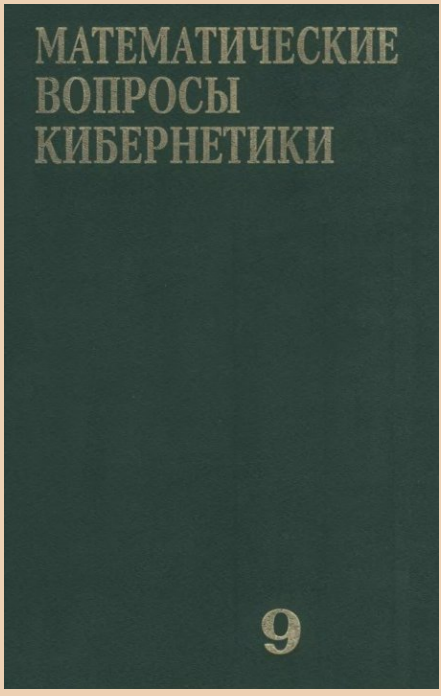
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 9



Н. К. Косовский

Сложность разрешимости некоторых дискретно нечетких систем

Рекомендуемая форма библиографической ссылки: Косовский Н. К. Сложность разрешимости некоторых дискретно нечетких систем // Математические вопросы кибернетики. Вып. 9. — М.: ФИЗМАТЛИТ, 2000. — С. 37–42. URL: http://library.keldysh.ru/mvk.asp?id=2000-37

СЛОЖНОСТЬ РАЗРЕШИМОСТИ НЕКОТОРЫХ ДИСКРЕТНО НЕЧЕТКИХ СИСТЕМ*)

Н. К. КОСОВСКИЙ

(САНКТ-ПЕТЕРБУРГ)

В математике часть усилий направлена на решение не только одной единичной задачи без параметров, но и на поиск алгоритма решения бесконечного количества задач, например, систем линейных неравенств или задач, получаемых варьированием каких-либо параметров у единичной задачи, например, уравнения второй степени.

Важным является и то, среди каких чисел ищется решение. Хорошо известно, что поиск решения в целых числах как правило более затруднителен, нежели поиск решения в рациональных числах.

Обычно алгоритмы решения систем линейных неравенств формулируются для систем нестрогих неравенств с рациональными коэффициентами. В этом случае возможно существование решения в рациональных числах и в то же время отсутствие решения в двоично рациональных числах, более удобных для компьютерного представления чисел (по определением являющихся конечными последовательностями битов, быть может разделенных точкой, отделяющей целую часть числа от дробной). В то же время, если рассматривать систему строгих неравенств, то она имеет решения в рациональных числах тогда и только тогда, когда она имеет решения в k-ично рациональных числах, каково бы ни было натуральное число $k \geqslant 2$.

Существование решения у систем неравенств может рассматриваться как задача, двойственная к существенной части задачи по проверке тождественной истинности бескванторных предикатных формул в заданной сигнатуре (т. е. формул, в которых логические связки соединяют подформулы, начиная с исходных, являющихся атомарными, содержащих только функции и предикаты, перечисленные в сигнатуре). Множество всех тождественно истинных формул такого рода в заданной сигнатуре принято называть универсальной теорией этой сигнатуры и обозначать посредством $\mathbf{UTh}S$, если посредством S обозначена рассматриваемая сигнатура.

Ниже рассматривается также более узкий класс формул, обозначаемых посредством $\mathbf{UPTh}S$ и называемый универсальной позитивной теорией. В формулах универсальной позитивной теории из логических связок разрешается использовать только конъюнкцию и дизъюнкцию.

Функция называется *определимой в теории*, если график этой функции выражается формулой, записанной в языке этой теории.

Посредством **EXPTIME** обозначается класс алгоритмов, вычислимых на машинах Тьюринга за число шагов, не превосходящее $2^{Cn^{C'}}$ при некоторых C и C', где n — длина записи аргумента алгоритма.

*) Работа выполнена при частичной финансовой поддержке Российского гуманитарного научного фонда (проект 97-05-12048) и Федеральной целевой программы «Интеграция» (проект 0145)

Лемма. *Пусть универсальная теория сигнатуры S, содержащей предикат равенства, разрешима алгоритмом из класса* **EXPTIME**. *Тогда универсальная теория сигнатуры S', получаемой добавлением в сигнатуру S этой теории функций, определимых в ней, также разрешима алгоритмом из класса* **EXPTIME**.

Доказательство леммы основывается на сведении формулы новой теории к формуле первоначальной теории с длиной, ограниченной сверху полиномом от длины исходной формулы. Такое сведение можно осуществить путем введения новых переменных и замены суперпозиции с помощью эквивалентности $y=f(g(x))\Leftrightarrow\forall z(z=g(x)\Rightarrow y=f(z))$.

В случае универсальной позитивной теории это доказательство может не пройти при отсутствии предиката $\neq$.

Пусть Q_0 — подмножество множества всех рациональных чисел Q и содержит числа c и c', такие что $0<c<c'$. Пусть $\overline{Q}_0$ — замыкание множества Q_0 относительно сложения и умножения его элементов. Множество $\overline{Q}_0$ совпадает с Q_0, если в качестве Q_0 рассматривается множество всех k-ично рациональных чисел при любом $k\geqslant 2$ или подмножество всех положительных чисел из этого множества.

Легко убедиться, что $N^c\subseteq\overline{Q}_0\subseteq Q$, где N^c — множество всех положительных натуральных чисел не меньших c.

Пусть Pol_{Q_0} — множество всех полиномов с коэффициентами из Q_0, а $|\mathrm{Pol}_{Q_0}$ — их бесконечный список. Корень нечетной степени $2k+3$ из натурального числа при $k\geqslant 2$ выразим в универсальной позитивной теории $\mathbf{UPTh}\langle R;|\mathrm{Pol}_{Q_0},\leqslant\rangle$, так как $y=\sqrt[2k+1]{x}\Leftrightarrow y^{2k+1}=x$. В то же время суперпозиция корней не может быть промоделирована в этой теории по обычной схеме

$$y=f(g(x))\Leftrightarrow\exists z(y=f(z)\,\&\,z=g(x))$$

(из-за отсутствия квантора существования) или по схеме

$$y=f(g(x))\Leftrightarrow\forall z(z=g(x)\Rightarrow y=f(z))$$

(из-за отсутствия логических операций следования и отрицания равенства).

Наличие в сигнатуре двуместных функций max и min и одноместного минуса (или выразимость этих функций в ней) позволяет говорить о расширенно нечеткой теории некоторых сигнатур, поскольку max соответствует дизъюнкции, min — конъюнкции, а одноместный минус — отрицанию. Расширенная нечеткость позволяет использовать любые числа из промежутка $(-\infty,\ \infty)$ вместо чисел отрезка $[0,\ 1]$ как у Л. Заде [5]. В этом случае 0 соответствует значению $1/2$ у Л. Заде, положительные числа — истине различной степени уверенности (т. е. числу из $(1/2,\ 1)$ у Л. Заде при предположении, что абсолютной истины не существует) и, наконец, отрицательные числа соответствуют лжи различной степени уверенности (т. е. числу из $(0,\ 1/2)$ у Л. Заде при предположении, что абсолютной лжи не существует). Поэтому нечеткую (универсальную) теорию сигнатуры $\langle R;|\mathrm{Pol}_{Q_0},\leqslant\rangle$ можно рассматривать как подтеорию теории $\mathbf{UPTh}\langle R;|\mathrm{Pol}_{Q_0},\leqslant\rangle$.

В [2] на стр. 10 под номером 89 А. И. Кокориным была поставлена задача о разрешимости универсальной теории поля рациональных чисел. В настоящей статье предлагается решение некоторых близких задач.

Доказана разрешимость универсальной позитивной теории кольца всех рациональных чисел алгоритмом из класса **EXPTIME**. Доказана также **NP**-трудность этой задачи (этот результат анонсирован автором в [1]). Кроме этого, доказана разрешимость универсальной позитивной теории колец всех k-ично рациональных чисел, больших заданной константы, и всех

k-ично рациональных чисел, не больших заданной константы. Доказана **NP**-трудность всех этих задач.

Доказана также алгоритмическая неразрешимость универсальных теорий колец всех k-ично рациональных чисел при $k \geqslant 2$. Последняя задача может рассматриваться как компьютерно ориентированная модификация упомянутой задачи А. И. Кокорина [2].

Разрешимость рассматриваемых теорий

Под k-ично рациональными числами при $k \geqslant 2$ понимаем последовательности цифр $0, 1, ..., k-1$, возможно разделенные точкой на две части (целую и дробную). Эти последовательности интерпретируются как числа, записанные в k-ичной системе счисления.

Пусть T — $\mathbf{UPTh}\langle \overline{Q_0}; |\mathrm{Pol}_{Q_0}, \max, \min, \leqslant\rangle$, в которой коэффициенты и степень полиномов записываются в двоичной системе счисления.

Пусть $\overline{Q_0} \subseteq (c_0, +\infty)$ и $\overline{Q_0}$ всюду плотно на интервале $(c_0, +\infty)$, где c_0 — неотрицательное рациональное число или $-\infty$, т. е. каковы бы ни были a, b, принадлежащие $\overline{Q_0}$, если $a < b$, то $\exists c \in \overline{Q_0}(a < c < b)$. Множества всех рациональных чисел, всех k-ично рациональных чисел всюду плотны на интервале $(c_0, +\infty)$.

Теорема 1. *Теория T и ее расширение непрерывными функциями, определимыми в ней, являются* **NP**-*трудными и разрешимы алгоритмами из класса* **EXPTIME**.

Доказательство. Сначала докажем, что теория T и ее расширение разрешимы алгоритмами из класса **EXPTIME**. Существование решения у системы строгих неравенств полиномов с непрерывными функциями в числах из $\overline{Q_0}$ эквивалентно существованию решения в вещественных числах из интервала $(c_0, +\infty)$, поскольку полиномы — непрерывные функции. Такая эквивалентность сохранится, если системы заменить на дизъюнкцию таких систем, а также и на результат неоднократного использования дизъюнкций и конъюнкций строгих неравенств указанного вида, поскольку конъюнкция и дизъюнкция здесь соответствуют объединению и пересечению открытых множеств.

Поэтому отсутствие решения в числах из $\overline{Q_0}$ у отрицания формулы в сигнатуре теории T эквивалентно принадлежности самой формулы теории T к теории $\mathbf{UTh}\langle (c_0, +\infty); |\mathrm{Pol}_{Q_0}, \max, \min, \leqslant\rangle$. Здесь интервал $(c_0, +\infty)$ задает все вещественные числа, входящие в него.

Основываясь на этом, из формул в сигнатуре расширения теории T с помощью леммы, исключаем все функции, определимые в T, включая max и min, так как

$$\max(x, y) = z \Leftrightarrow (x \leqslant y \ \&\ z = y) \vee (y \leqslant x \ \&\ z = x),$$
$$\min(x, y) = z \Leftrightarrow (x \leqslant y \ \&\ z = x) \vee (y \leqslant x \ \&\ z = y).$$

(Считаем, что $a = b$ является сокращением для формулы $a \leqslant b \ \&\ b \leqslant a$.)

Далее аналогично доказательству леммы устраняем подстановки одних полиномов в другие путем введения дополнительных переменных. В результате длина преобразованной формулы будет ограничена сверху полиномом от длины исходной формулы.

После этого можно провести поиск вывода полученной формулы в многосукцедентном секвенциальном исчислении с обратимыми правилами без структурных правил и без правила сечения. Длина каждой секвенции в выводе не будет превышать полинома от длины исходной формулы. Таким образом, для поиска вывода достаточно пространства памяти полиномиального от длины исходной формулы. Отрицание логической интерпретации

секвенции может рассматриваться как система строгих неравенств, к которой если $c_0 \neq -\infty$, то для каждой переменной добавлено неравенство $x > c_0$.

В конце концов можно воспользоваться следующим результатом Д. Ю. Григорьева и Н. Н. Воробьева [3]. Пусть полиномы $f_1, ..., f_k$ принадлежат $Z[x_1, ..., x_n]$, степень их меньше d и абсолютное значение каждого коэффициента f_i меньше или равно 2^M для всех i $(1 \leqslant i \leqslant k)$. В работе [3] описан алгоритм, который распознает существование вещественных решений систем неравенств $f_1 > 0, ..., f_m > 0, f_{m+1} \geqslant 0, ..., f_k \geqslant 0$, число шагов которого ограничено сверху полиномом от $M(kd)^{n^2}$ и, следовательно, этот алгоритм принадлежит классу **EXPTIME**. Вторая часть теоремы доказана.

Докажем **NP**-трудность теории T. Формулой в сигнатуре теории T можно представить формулу, находящуюся в конъюнктивной нормальной форме следующим образом.

Пропозициональная переменная может быть представлена посредством формулы $c' \leqslant x$, а ее отрицание — посредством $x \leqslant c$. Напомним, что c и c' принадлежат Q_0 и $0 < c < c'$. «Истина» будет кодироваться числами, не меньшими, чем c', а «ложь» будет кодироваться числами, не большими, чем c.

В позитивной теории имеются конъюнкция и дизъюнкция. Следовательно, выполнимость пропозициональной формулы, находящейся в конъюнктивной нормальной форме, эквивалентна выполнимости результата ее преобразованния посредством замены пропозициональных переменных и их отрицаний на соответствующие представления, описанные выше, если к результату преобразования конъюнктивно добавлены формулы вида $(c' \leqslant x) \vee (x \leqslant c)$ для каждой переменной x.

Теперь можно воспользоваться **NP**-полнотой проблемы выполнимости формул, находящихся в конъюнктивной нормальной форме.

Следствие доказательства теоремы 1. *Пусть* $Q_k^{c_0}$ — *множество всех* k*-ично рациональных чисел из промежутка* $[c_0, +\infty)$. *Пусть* $|\mathrm{Pol}_{Q_k^{c_0}}$ — *перечень всех полиномов, у которых ненулевые коэффициенты являются элементами* $Q_k^{c_0}$. *Тогда теория* $UPTh\langle Q_k^{c_0}; |\mathrm{Pol}_{Q_k^{c_0}}, \max, \min \leqslant\rangle$ *является* **NP***-трудной и разрешима алгоритмом из класса* **EXPTIME** *при* $k \geqslant 2$.

Доказательство полностью повторяет доказательство теоремы 1 за исключением следующей ключевой фразы. Отрицание логической интерпретации секвенции может рассматриваться как система строгих неравенств, к которой, если $c_0 \neq -\infty$, для каждой переменной x добавлено неравенство $x > c_0$. В этой фразе $x > c_0$ следует заменить на $x \geqslant c_0$, что не меняет хода рассуждений, поскольку c_0 — рациональное число, а не вещественное. Поэтому добавление c_0 в область значений переменных сохраняет сведение к системе, решаемой в вещественных числах.

Отметим, что если не менять доказательство теоремы 1, а воспользоваться только ее формулировкой, то удалось бы получить в качестве разрешающего алгоритма только алгоритм из класса **EXP-EXPTIME**.

Неразрешимость некоторых универсальных теорий

Алгоритмическая неразрешимость универсальной позитивной теории $\mathbf{UPTh}\langle Z; 1, -, \cdot, \leqslant\rangle$ немедленно следует из [6].

В работе Дж. Робинсон [7] приведены следующие леммы, первые две из которых — специальный случай общей теоремы из [4], которая дает необходимые и достаточные условия рациональных представлений рационального числа заданной квадратичной формой от нескольких переменных. Остальные леммы доказаны в [7]. Ниже обозначение (k/p)

используется, как и в [7], для символа Лежандра, т. е. $(k/p)=\pm 1$ и $((k/p)=1 \Leftrightarrow \exists x(x^2 \equiv k \pmod p))$.

Лемма 1. *Если p — простое число, сравнимое с 3 по модулю 4, то $X^2+Y^2-pZ^2$ представляет ненулевое рациональное число M тогда и только тогда, когда M не имеет ни одного из следующих видов*

$$p \cdot k \cdot S^2 \quad \text{при} \quad (k/p)=1 \qquad \text{или} \qquad k \cdot S^2 \quad \text{при} \quad k \equiv p \pmod 8.$$

Лемма 2. *Если p и q — нечетные простые числа такие, что $p \equiv 1 \pmod 4$ и $(q/p)=-1$, то $X^2+qY^2-pZ^2$ представляет ненулевое число M тогда и только тогда, когда M не имеет ни одного из следующих видов*

$$p \cdot k \cdot S^2 \quad \text{при} \quad (k/p)=-1 \qquad \text{или} \qquad q \cdot k \cdot S^2 \quad \text{при} \quad (k/q)=-1.$$

Лемма 3. *Если p — простое число, сравнимое с 3 по модулю 4, то уравнение*

$$2+pM^2+pZ^2=X^2+Y^2$$

имеет решение относительно X, Y и Z тогда и только тогда, когда знаменатель M, взаимно простой с числителем M, взаимно прост с p и с q.

Лемма 4. *Если p и q — нечетные простые числа такие, что $p \equiv 1 \pmod 4$ и $(q/p)=-1$, то уравнение*

$$2+qpM^2+pZ^2=X^2+qY^2$$

имеет решение относительно X, Y и Z тогда и только тогда, когда знаменатель M, взаимно простой с числителем M, взаимно прост с p и с q.

Лемма 5. *Если p — простое число и $p \equiv 1 \pmod 4$, то существует такое нечетное простое число q, что $(q/p)=-1$.*

Пусть $Q_{2\ell}$ — множество всех 2ℓ-ично рациональных чисел при $\ell \geqslant 1$.

Следствие 1 леммы 3. *Каково бы ни было 2ℓ-ично рациональное число M, оно является целым тогда и только тогда, когда уравнение*

$$\begin{aligned}2+3M^2+3\big((z_1-c)^2+(z_2-c)^2+(z_3-c)^2+(z_4-c)^2\big)^2 &= \\ =\big((x_1-c)^2+(x_2-c)^2+(x_3-c)^2+(x_4-c)^2\big)^2 &+ \\ +\big((y_1-c)^2+(y_2-c)^2+(y_3-c)^2+(y_4-c)^2\big)^2 &\end{aligned}$$

разрешимо в 2ℓ-ично рациональных числах из $[c_0, +\infty)$.

Доказательство основывается на теореме Лагранжа о том, что всякое натуральное число представимо в виде суммы квадратов четырех целых чисел и лемме 3 при $p=3$. Поскольку всякое неотрицательное рациональное число представимо в виде m/n^2, оно представимо в виде суммы квадратов четырех рациональных чисел.

Пусть $Q_{p\ell}$ — множество всех $p\ell$-ично рациональных чисел при простом p, $\ell \geqslant 1$ и $p \equiv 3 \pmod 4$.

Следствие 2 леммы 3. *Каково бы ни было $p\ell$-ично рациональное число M, оно является целым тогда и только тогда, когда в $p\ell$-ично рациональных числах из $[c_0, +\infty)$ разрешимо уравнение*

$$\begin{aligned}2+pM^2+p\big((z_1-c)^2+(z_2-c)^2+(z_3-c)^2+(z_4-c)^2\big)^2 &= \\ =\big((x_1-c)^2+(x_2-c)^2+(x_3-c)^2+(x_4-c)^2\big)^2 &+ \\ +\big((y_1-c)^2+(y_2-c)^2+(y_3-c)^2+(y_4-c)^2\big)^2. &\end{aligned}$$

Пусть $Q_{p\ell}$ — множество всех $p\ell$-ично рациональных чисел при простом нечетном p, $\ell \geqslant 1$ и $p \equiv 1 \pmod 4$. По лемме 5 найдем такое простое число q, что $q/p = -1$.

Следствие леммы 4. *Каково бы ни было $p\ell$-ично рациональное число M, оно является целым тогда и только тогда, когда уравнение*

$$2 + qpM^2 + p\big((z_1 - c)^2 + (z_2 - c)^2 + (z_3 - c)^2 + (z_4 - c)^2\big)^2 =$$
$$= \big((x_1 - c)^2 + (x_2 - c)^2 + (x_3 - c)^2 + (x_4 - c)^2\big)^2 +$$
$$+ q\big((y_1 - c)^2 + (y_2 - c)^2 + (y_3 - c)^2 + (y_4 - c)^2\big)^2$$

разрешимо в $p\ell$-ично рациональных числах из $[c_0, +\infty)$.

Теорема 2. *Проблема существования m-ично рациональных решений при $m \geqslant 2$ у уравнений вида $P = 0$, где P — полином с целыми коэффициентами, алгоритмически неразрешима.*

Доказательство. Пусть $2|m$. Воспользуемся следствием 1 леммы 3.

Пусть p — простое число такое, что $p \equiv 3 \pmod 4$ и $p|m$. Тогда воспользуемся следствием 1 леммы 3. Пусть p — простое число, $p \equiv 3 \pmod 4$ и $p|m$. Тогда воспользуемся следствием 2 леммы 3. Пусть $p \equiv 1 \pmod 4$ и $p|m$. Тогда воспользуемся следствием леммы 4.

Далее доказательство теоремы основывается на алгоритмической неразрешимости 10-й проблемы Гильберта [6].

Следствие теоремы 2. *Универсальная теория сигнатуры $\langle Q_m; 1, -, \cdot, \leqslant\rangle$ алгоритмически неразрешима.*

Доказанная теорема устанавливает невозможность усиления теоремы 1 при исключении буквы P в определении теории T, означающей «позитивная», если множество $\overline{Q_0}$ является множеством всех k-ично рациональных чисел из интервала $(c_0, +\infty)$ при $c < c_0$.

Универсальные теории всех рациональных чисел и всех k-ично рациональных чисел при $k \geqslant 2$ могут служить фундаментом построения дискретных и конструктивных оснований тех разделов непрерывной математики, которые используются в практике приближенных вычислений, что может уточнить концепции из [8].

СПИСОК ЛИТЕРАТУРЫ

1. Косовский Н. К. Разрешимость универсальной теории поля рациональных чисел // Материалы международной конференции по математической логике, посвященной 90-летию со дня рождения А. И. Мальцева. Тезисы докладов. — Новосибирск: Изд-во института дискретной математики и информатики, 1999. — С. 34–35.
2. Логическая тетрадь. Нерешенные проблемы математики. — Новосибирск, 1986.
3. Grigoriev D. Yu., Vorobjov N. N. Solving systems of polynomial inequalities in subexponential time // J. Symb. Comput. — 1988. — № 5. — P. 37–64,
4. Hasse H. Über die Darstellbarkeit von Zahlen durch quadratische Formen im Kőrper der rationalen Zahlen // Jurnal für die reine und angewandte Mathematik. — 1923. — V. 152. — P. 129–148.
5. Kossovski N. K., Tishkov A. V. Mathematical reasoning for fuzzy propositions // Proc. International Conference on Informatics and Control, V. 2. — St.-Petersburg. 1997. — P. 522–529.
6. Matiyasevič Yu. Enumerable sets are Diophantine // Soviet Math. Doklady. — 1970. — № 11. — P. 354–357.
7. Robinson J. Definability and decision problems in arithmetic // The Journal of Symbolic Logic. — 1949. — V. 14, № 2. — P. 98–114.
8. Suppers P., Chuaqui R. A finitarily consistent free-variable positive fragment of infinitesmall analysis // Notas de Logica matematica, Instituto de Matematica Argentina. — 1993. — № 38. — P. 1–59.

Поступило в редакцию 25 XII 1999