УДК 510.51 Вестник СПбГУ. Сер. 1. Т. 3 (61). 2016. Вып. 1

УСЛОВИЯ NP-ПОЛНОТЫ ПРОВЕРКИ СОВМЕСТНОСТИ НЕСКОЛЬКИХ ВИДОВ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ ДИЗСРАВНЕНИЙ

Н. К. Косовский, Т. М. Косовская, Н. Н. Косовский

Санкт-Петербургский государственный университет,
Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7-9

В статье предлагаются две серии теоретико-числовых задач с явно выделенными параметрами, касающиеся дизсравнений по модулю m. Доказываются ограничения на параметры, при выполнении которых любая задача каждой серии NP-полна. Доказывается, что при всяком $m > 2$ задача проверки совместности системы линейных дизсравнений по модулю m, каждое из которых содержит ровно 3 переменные (даже если коэффициенты при них из $\{-1, 1\}$), NP-полна. Также доказывается, что при всяком $m > 3$ задача проверки совместности системы линейных дизсравнений по модулю m, каждое из которых содержит ровно 2 переменные, NP-полна. Если $\mathbf{P} \neq \mathbf{NP}$, то формулировки доказанных теорем не могут быть изменены путём замены термина «2-дизсравнение» на термин «1-дизсравнение». Библиогр. 6 назв.

Ключевые слова: система линейных диофантовых дизсравнений, NP-полнота.

Введение. Ценность формулировки и доказательств NP-полноты теоретико-числовых задач связана с тем, что для таких задач в настоящее время отсутствуют (и, скорее всего, будут отсутствовать в будущем) полиномиальные по времени (числу шагов на машине Тьюринга) решающие их алгоритмы.

На первый взгляд, простейшей и наиболее часто решаемой задачей математики является задача решения линейных диофантовых уравнений, сравнений и различного вида неравенств. Однако постоянно исследуются всё новые и новые методы их решения (см., например, [1]).

Для компьютерной реализации алгоритма (предиката) важно, чтобы он принадлежал классу **FP** (соответственно классу **P**). Кроме того, для многих задач полезно знать, что задача является NP-трудной (NP-полной), поскольку это условие в настоящее время не позволяет эффективно реализовать её на компьютере.

Целью настоящей работы является выявление простейших NP-полных задач, связанных с разрешимостью систем линейных диофантовых дизсравнений.

Эта цель в некоторой степени дополнительна к цели, поставленной в [2], где выявляются классы графов, в результате сужения на которые NP-трудные задачи имеют полиномиально эффективное решение, и к цели, поставленной в [3] и более тесно связанной с вычислительной сложностью алгоритмов решения систем сравнений специального вида.

Для математиков одними из наиболее простых объектов, часто возникающих в исследованиях, являются системы линейных диофантовых уравнений и сравнений. В обширном списке NP-полных задач, приведённом в [4], есть всего одна задача, относящаяся к рассматриваемым объектам. Эта задача названа переводчиком *система несравнимостей* (результат получен в [5]). К сожалению, в её формулировку на русском языке вкралась опечатка: вместо знака $\equiv$ должен быть знак $\not\equiv$. Приведём формулировку задачи без опечатки.

Система несравнимостей (в [4] под аббревиатурой АТЧ2)

УСЛОВИЕ. Задан набор $\{(a_1, b_1), \ldots, (a_n, b_n)\}$ упорядоченных пар положительных целых чисел таких, что $a_i \leq b_i$ при $1 \leq i \leq n$.

ВОПРОС. Существует ли такое целое число x, что $x \not\equiv a_i (\mathrm{mod}\ b_i)$, $1 \leq i \leq n$?

Рассмотрим частный случай этой задачи при $b_1 = \cdots = b_n = m$ и попарно различных $a_1, \ldots, a_n$, которую будем называть **Система несравнимостей по единому модулю**. В названии этой задачи полезно было бы отметить, что каждая несравнимость линейна и содержит только одну переменную с коэффициентом при ней, равным 1. Однако сохранена терминология из [4].

Новая задача может быть решена конечным перебором, но при этом алгоритм будет требовать экспоненциального числа шагов от длины исходных данных. Предложим для её решения полиномиальный алгоритм.

Для получения полиномиального по времени алгоритма решения задачи **Система несравнимостей по единому модулю** сформулируем утверждение.

Утверждение 1. *Задача* **Система несравнимостей по единому модулю** *имеет положительное решение тогда и только тогда, когда* $n < m$.

Доказательство. Сортируем числа из $\{a_1, \ldots, a_n\}$ в порядке возрастания. Наименьшее число, отсутствующее в этом списке, является решением системы. ■

Это утверждение показывает, что при сужении единственной NP-полной задачи из [4] на системы линейных дизсравнений по единственному модулю имеет полиномиальный алгоритм решения.

Далее вместо термина «несравнимость» используется термин «дизсравнение» (более удобный, по мнению авторов).

1. Системы линейных дизсравнений. Для получения одного из результатов докажем следующую лемму.

Лемма 1. *Каковы бы ни были целые числа* k *и* m*, большие 2, задача проверки совместности в числах, сравнимых с элементами из* $\{k, k+1\}$*, систем линейных сравнений по модулю* m*, в которой каждое сравнение содержит ровно 3 различные переменные с коэффициентами при них из множества* $\{-1, 1\}$*, является NP-полной.*

Доказательство. То, что задача принадлежит классу **NP**, очевидно.

Действительно, пусть n — общее количество переменных в системе, l — количество сравнений в ней. Порождение «претендента» на решение системы (т. е. набора значений переменных из множества $\{k, k+1\}$) в недетерминированном режиме возможно не более чем за $n \log(k+1)$ шагов. Вычисление значения левой части одного сравнения требует 3 операции сложения (вычитания). Сравнение полученного числа с модулем m требует не более трёх вычитаний (так как всегда можно считать, что числа k и $k+1$ принадлежат $\{0, \ldots, m-1\}$). Операции сложения и вычитания выполняются не более чем за полином шагов от длины записи аргументов, который обозначим посредством $P(||k||, ||m||)$. Общее число шагов решения системы на недетерминированной машине Тьюринга не превосходит полинома $n \log(k+1) + P(||k||, ||m||)l$ от длины записи системы[1].

К задаче, сформулированной в лемме, полиномиально сводится задача **3-вып при одном истинном литерале** из [4] (результат получен в [6]). Действительно,

[1] Во всех следующих теоремах доказательство принадлежности задачи классу **NP** аналогично и приводиться не будет.

истинность ровно одного литерала в дизъюнкции $x_1 \vee x_2 \vee x_3$ (где x_1, x_2, x_3 — переменные или их отрицания) может быть записана с помощью сравнения $x_1 + x_2 + x_3 \equiv 3k + 1 \pmod m$ при $m > 2$. При этом вместо $\neg u_i$ подставляем $2k + 1 - u_i$. (Константа *ложь* кодируется числом k, константа *истина* кодируется числом $k + 1$.) ■

Задача из леммы 1 при $m = 3$ является одной из наиболее простых теоретико-числовых NP-полных задач, сформулированных на основе систем линейных сравнений по модулю 3. Её удобно использовать для доказательства NP-полноты разнообразных задач.

Пусть $L(x_1, \ldots, x_k)$ обозначает линейное выражение с k переменными вида $a_1x_1 + \cdots + x_ka_k + b$ с целыми ненулевыми коэффициентами. Несравнимость вида $L(x_1, \ldots, x_k) \not\equiv 0 \pmod m$ будем называть линейным k-дизсравнением.

Сформулируем серию задач по проверке совместности систем линейных дизсравнений специального вида по модулю m.

Система линейных 3-дизсравнений по модулю m

УСЛОВИЕ. Задана система линейных 3-дизсравнений

$$\begin{cases} L_1\left(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}\right) \not\equiv 0 \pmod m, \\ \qquad\qquad\qquad\quad \vdots \\ L_k\left(x_{i_k^1}, x_{i_k^2}, x_{i_k^3}\right) \not\equiv 0 \pmod m, \end{cases} \tag{1}$$

где $L_1(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}), \ldots, L_k(x_{i_k^1}, x_{i_k^2}, x_{i_k^3})$ — попарно различные линейные комбинации ровно трёх различных переменных.

ВОПРОС. Совместна ли в целых числах система (1)?

При $m = 2$ система превращается в систему равенств нулю линейных полиномов Жегалкина, которая может быть решена методом исключения неизвестных за полином шагов.

На основе леммы 1 доказывается теорема.

Теорема 1. *Каково бы ни было число $m > 2$, сужение задачи* **Система линейных 3-дизсравнений по модулю** m *на случай, когда все коэффициенты при переменных принадлежат множеству $\{-1, 1\}$, является NP-полной.*

Доказательство. То, что задача принадлежит классу **NP**, очевидно.

Рассмотрим сужение этой задачи на такие системы дизсравнений, в которых каждая линейная комбинация $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3})$ более чем с одной переменной входит в систему $m-1$ раз, а именно $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \not\equiv 1 \pmod m$, $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \not\equiv 2 \pmod m$, $\ldots$, $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \not\equiv (m-1) \pmod m$. Система таких дизсравнений равносильна одному сравнению $L_j(x_{i_1^1}, x_{i_1^2}, x_{i_1^3}) \equiv 0 \pmod m$.

Кроме того, для каждой переменной x, входящей в систему, имеются дизсравнения $x \not\equiv 2 \pmod m$, $x \not\equiv 3 \pmod m$, $\ldots$, $x \not\equiv (m-1) \pmod m$. Система этих дизсравнений равносильна тому, что $x \equiv 0 \pmod m \vee x \equiv 1 \pmod m$ (и тем самым накладывает ограничение, при котором решения ищутся в множестве чисел, сравнимых по модулю m с числами из $\{0, 1\}$).

Если в сравнении число переменных меньше трёх, то добавляем фиктивные тождественно равные нулю переменные, используя следующую равносильность:

$$\begin{cases} u \equiv 0 \pmod m, \\ v \equiv 0 \pmod m \end{cases} \Leftrightarrow \exists w \begin{cases} u+v+w \equiv 0 \pmod m, \\ u-v+w \equiv 0 \pmod m, \\ u+v-w \equiv 0 \pmod m, \\ u-v-w \equiv 0 \pmod m. \end{cases} \tag{2}$$

Если m нечётно, то $\begin{cases} u+v+w \equiv 0 \pmod m, \\ u-v-w \equiv 0 \pmod m \end{cases} \Rightarrow 2u \equiv 0 \pmod m$, что в свою очередь влечёт $u \equiv 0 \pmod m$, поскольку m нечётно.

При чётном m складываем первые два сравнения и умножаем результат на $m/2$. Складываем вторые два сравнения и умножаем результат на $m/2-1$. Их сумму складываем с третьим сравнением, из результата вычитаем первое сравнение. В результате получаем сравнение $(m-1)u \equiv 0 \pmod m$, что даёт $u \equiv 0 \pmod m$.

Преобразуем систему из правой части равносильности (2) в эквивалентную ей систему посредством замены каждого сравнения вида $A \equiv 0 \pmod m$ на подсистему

$$\begin{cases} A \not\equiv 1 \pmod m, \\ A \not\equiv 2 \pmod m, \\ \qquad\vdots \\ A \not\equiv m-1 \pmod m. \end{cases}$$

Следовательно, переменную u можно добавить в качестве слагаемого в сравнения, содержащие ровно 2 переменные.

Таким образом, эквивалентность (2) позволяет вводить явно (формально необходимые, но по существу фиктивные) переменные в любые сравнения.

Хотя длина последней формулы линейно зависит от параметра m, то есть экспоненциальна от его длины, получили полиномиальную сводимость, так как m — фиксированное число для каждой задачи этой серии.

Таким образом, задача из формулировки теоремы сужена до задачи, NP-полнота которой доказана в лемме 1 при $k = 0$. ■

Следствие теоремы 1. *Каково бы ни было число $m > 2$, задача* **Система линейных 3-дизсравнений по модулю** m *является NP-полной.*

Сформулируем серию задач по проверке совместности систем линейных дизсравнений с двумя переменными по модулю m.

Система линейных 2-дизсравнений по модулю m

УСЛОВИЕ. Задана система линейных дизсравнений

$$\begin{cases} L_1\left(x_{i_1^1}, x_{i_1^2}\right) \not\equiv 0 \pmod m, \\ \qquad\vdots \\ L_k\left(x_{i_k^1}, x_{i_k^2}\right) \not\equiv 0 \pmod m, \end{cases} \tag{3}$$

где $L_1(x_{i_1^1}, x_{i_1^2}), \ldots, L_k(x_{i_k^1}, x_{i_k^2})$ — попарно различные линейные комбинации двух различных переменных.

ВОПРОС. Совместна ли в целых числах система (3)?

Лемма 2. *Каково бы ни было число $m > 3$, любое двухместное отношение $P(x, y)$ на множестве $\{0, 1, 2, 3\}$ может быть задано системой линейных*

2-дизсравнений по модулю m, в которых все коэффициенты при переменных принадлежат множеству $\{1, 2\}$.

Для доказательства достаточно использовать систему всех дизсравнений вида $x + 2y \not\equiv c \ (mod\ m)$, где $c = a + 2b$ для всех пар (a, b) с элементами из множества $\{0, 1, \ldots, m-1\}$, не удовлетворяющих заданному отношению.

Теорема 2. *Каково бы ни было число $m > 3$, задача* **Система линейных 2-дизсравнений по модулю** m, *в которой все коэффициенты при переменных принадлежат множеству $\{1, 2\}$, является NP-полной.*

Доказательство. То, что задача принадлежит классу **NP**, очевидно.

Докажем, что задача 3-ВЫП полиномиально сводится к задаче **Система линейных 2-дизсравнений по модулю** m. Каждому дизъюнкту c_j ставим в соответствие две переменные s_j и s'_j, принимающие одно из четырёх значений из множества $\{0, \ldots, 3\}$, а также дизсравнение $s_j + s'_j \not\equiv 0 \pmod m$.

По существу значения переменных s_j и s'_j нумеруют пары из нулей и единиц (a, b) и (b, c) посредством $a + 2b$ и $2b + c$ соответственно, где a, b, c — истинностные значения литералов, выраженные числами 0 и 1.

Для каждой пары дизъюнктов c_j и c_k, содержащих одну и ту же переменную, записываем отношение вида «$(l - j)$-й литерал дизъюнкта c_j сопадает с l_k-м литералом дизъюнкта c_k» или «$(l - j)$-й литерал дизъюнкта c_j контрарен l_k-му литералу дизъюнкта c_k». Каждое такое отношение по лемме 2 может быть задано проверкой совместности системы линейных 2-дизсравнений по модулю m, зависящих от пар переменных (s_j, s_k), (s_j, s'_k), (s'_j, s_k), (s'_j, s'_k).

Система, состоящая из всех дизсравнений вида $s_j + s'_j \not\equiv 0 \ (mod\ m)$, $s_j + s'_j \not\equiv 4 \pmod m$, $s_j + s'_j \not\equiv 4 \pmod m$, $\ldots$, $s_j + s'_j \not\equiv m - 1 \pmod m$ и всех систем, задающих все необходимые отношения описанных видов, совместна тогда и только тогда, когда задача 3-ВЫП имеет решение. ■

Следствие теоремы 2. *Каково бы ни было число $m > 3$, задача* **Система линейных 2-дизсравнений по модулю** m *является NP-полной.*

Если $\mathbf{P} \neq \mathbf{NP}$, то в теореме 2 и её следствии термин «2-дизсравнение» не может быть заменён на термин «1-дизсравнение», поскольку при этом задача из формулировки теоремы превращается в подзадачу задачи **Система несравнимостей по единому модулю**, которая принадлежит классу **P**. Алгоритм описан в доказательстве утверждения из введения к этой статье.

Можно проверить, что следствие теоремы 2 по существу усиливает следствие теоремы 1 при $m \neq 3$.

Авторам неизвестно, справедливы ли утверждения теоремы 2 и её следствий при $m = 3$.

Заключение. Такой объект исследования, как системы линейных дизсравнений, гораздо естественнее для большинства математиков, чем задачи, связанные с проверкой истинности пропозициональной формулы.

В целом полученные результаты показывают, что проверка совместности в целых числах систем **линейных** дизсравнений может оказаться во многих случаях NP-полной.

Авторы благодарны рецензенту за контрпример к первоначальной формулировке утверждения из введения, позволивший авторам исправить формулировку сужения задачи из этого утверждения.

Литература

1. *Кривий С. Л.* Лінійні діофантові обмеження та їх застосування. Видавничий дім «Букрек». 2015. 224 с.

2. *Быкова В. В.* Программирование задач на графах ограниченной древовидной ширины // Программные продукты и системы. Т. 4, № 96, 2011. С. 101–106.

3. *Косовская Т. М., Косовский Н. К.* О числе шагов получения булевого решения у полиномиальных сравнений и у систем из них // Вестн. С.-Петерб. ун-та. Сер. 1. 2007. Вып. 3. С. 82–90.

4. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

5. *Stockmeyer L. J., Meyer A. R.* Word problems requiring exponential time // Proc. 5th Ann. ICM Symp. on Theory of Computing. Association of Computing Machinery. New York, 1973. P. 1–9.

6. *Shafer T. J.* The complexity of satisfiability problems // Proc. 10th Ann. ACM Symp. on Theory of Computing. Association of Computing Machinery. New York, 1978. P. 216–226.

Статья поступила в редакцию 22 октября 2015 г.

Сведения об авторах

Косовский Николай Кириллович — доктор физико-математических наук, профессор; kosov@nk1022.spb.edu

Косовская Татьяна Матвеевна — доктор физико-математических наук, доцент; kosovtm@gmail.com

Косовский Николай Николаевич — кандидат физико-математических наук, доцент; kosovnn@pdmi.ras.ru

NP-COMPLETENESS CONDITIONS FOR SOME TYPES OF SYSTEMS OF LINEAR DIOPHANTINE DIS-COMPARISONS CONSISTENCY CHECKING

Nikolay K. Kosovskii, Tatyana M. Kosovskaya, Nikolay N. Kosovskii

St. Petersburg State University, Universitetskaya nab., 7-9, St. Petersburg, 199034, Russian Federation; kosov@nk1022.spb.edu, kosovtm@gmail.com, kosovnn@pdmi.ras.ru

Two series of number-theoretic problems concerning modulo m dis-comparisons with explicitly pointed out parameters are proposed in the paper. Conditions upon the parameters implying that every problem of a series is an NP-complete one are proved. It is proved that for every $m > 2$ the consistency problem for a system of modulo m dis-comparisons every of which contains exactly 3 variables (even if every coefficient belongs to $\{-1, 1\}$) is NP-complete. It is also proved that for every $m > 3$ the consistency problem for a system of modulo m dis-comparisons every of which contains exactly 2 variables is NP-complete. If $\mathbf{P} \neq \mathbf{NP}$ then the statement of the proved theorem can not be changed by means of replacing the term «2-dis-comparison» by the term «1-dis-comparison». Refs 6.

Keywords: system of linear Diophantine dis-comparisons, NP-completeness.

References

1. Krivyi S. L., *Linear Diophantine equations and their decisions* (Publishing House "Bukrek", 2015, 224 p.) [in Ukrainian].

2. Bykova V. V., "Programming of problems for a bounded tree-type width graph", *Program products and systems* **4**(96), 101–106 (2011) [in Russian].

3. Kosovskii N. K., Kosovskaya T. M., "The Number of Steps for Construction of a Boolean Solution to Polynomial Congruences and Systems of Polynomial Congruences", *Vestnik St. Petersburg University: Mathematics* **40**(3), 218–223 (Allerton Press. Inc., 2007).

4. Garey M. R., Johnson D. S., *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman, New York, 1979).

5. Stockmeyer L. J., Meyer A. R., "Word problems requiring exponential time", *Proc. 5th Ann. ICM Symp. on Theory of Computing* (1–9) (Association of Computing Machinery, New York, 1973).

6. Shafer T. J., "The complexity of satisfiability problems", *Proc. 10th Ann. ACM Symp. on Theory of Computing* (216–226) (Association of Computing Machinery, New York, 1978).