УДК 510.51
MSC 11Y16

Вестник СПбГУ. Математика. Механика. Астрономия. Т. 4 (62). 2017. Вып. 2

NP-ПОЛНЫЕ ЗАДАЧИ О СИСТЕМАХ ДЕЛИМОСТЕЙ ЗНАЧЕНИЙ ЛИНЕЙНЫХ ВЫРАЖЕНИЙ

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

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

Целью данной статьи является исследование алгоритмической сложности подзадач задачи проверки совместности систем делимостей значений линейных выражений с неотрицательными коэффициентами в положительных целых числах. В общем случае не известно, принадлежит ли она классу **NP**, но известна ее принадлежность классу **NEXPTIME**.

В работе доказывается NP-полнота двух серий сужений этой задачи, что в первом из них делителем линейного выражения является число, а во втором сужении линейное выражение является делителем числа. Установлены значения параметров, при которых задачи являются NP-полными. Для мéньших значений параметра доказана принадлежность задач классу **P**.

Доказана NP-трудность частного случая общей задачи СОВМЕСТНАЯ ДЕЛИМОСТЬ ЛИНЕЙНЫХ МНОГОЧЛЕНОВ, в котором коэффициенты при переменных могут принимать значения только из множества $\{1, 2\}$, а свободные члены линейных выражений — только из множества $\{1, 5\}$. Библиогр. 13 назв.

Ключевые слова: система делимостей значений линейных выражений, NP-трудность, NP-полнота.

Введение. Задачи, рассматриваемые в статье, связаны с задачей СОВМЕСТНАЯ ДЕЛИМОСТЬ ЛИНЕЙНЫХ МНОГОЧЛЕНОВ (СДЛМ) из [1]. Доказательство NP-трудности этой задачи в [2] стало дополнением к результату о разрешимости экзистенциальной теории натуральных чисел со сложением и делимостью [3, 4]. На основе этих результатов доказываются сложностные характеристики многих вопросов формальной верификации программ, например, NP-трудность задачи достижимости заданного состояния в параметрической автоматной односчетчиковой машине [5].

В [2] показано, что задача NP-полна для любого фиксированного числа делимостей $m \geq 5$, однако не известно, принадлежит ли СДЛМ в общем виде классу **NP**. В работе [6] приводится доказательство принадлежности этой задачи классу **NEXPTIME**, то есть доказательство существования алгоритма, решающего задачу за $2^{n^{O(1)}}$ шагов на недетерминированной машине Тьюринга.

Предметом изучения данной статьи, в частности, является проверка совместности систем произвольного числа делимостей значений линейных выражений с неотрицательными коэффициентами в положительных целых числах. Доказывается NP-полнота двух сужений этой задачи, в первом из них каждое линейное выражение является делителем одного и того же числа, а во втором сужении делителем каждого линейного выражения является одно и то же число.

Доказана NP-трудность частного случая общей задачи СДЛМ, в котором коэффициенты при переменных могут принимать значения только из множества $\{1, 2\}$, а свободные члены линейных выражений — только из множества $\{1, 5\}$. Полученные результаты могут послужить основой для дальнейшего выяснения точной алгоритмической сложности общей задачи.

DOI: 10.21638/11701/spbu01.2017.207

Отметим, что в работах [7–9] доказан ряд теорем о NP-полноте систем простейших линейных уравнений и дизуравнений специального вида. Для доказательства этих теорем, как и для некоторых теорем, установленных ниже, используется NP-полнота задачи 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ (доказана в [10] и приведена в [1]).

В оригинальном английском издании [1] задача СДЛМ названа SIMULTANIOUS DIVISIBILITY OF LINEAR POLYNOMIALS. Поскольку слова «совместная делимость» в русском языке могут трактоваться как одновременная делимость a на b и делимость b на a, а «simultanious equations» переводится обычно как «система уравнений», будем говорить о «системе делимостей». Кроме того, термин «делимость линейных многочленов» может восприниматься как их делимость нацело при любых значениях переменных. В связи с этим в названиях рассматриваемых ниже задач будут использованы слова *система делимостей значений линейных выражений.*

1. Сложность решения задач о совместности систем делимостей одного и того же числа значениями линейных выражений. В работе [11] была доказана γ-полнота задачи ЛИНЕЙНАЯ ДЕЛИМОСТЬ (ЛД), состоящей в проверке разрешимости в положительных целых числах одной делимости вида $a_1x_1 + 1 \,|\, K$, где a_1 и K — положительные целые числа. Этот результат означает отсутствие для задачи ЛД полиномиального алгоритма решения в предположении $\mathbf{NP} \neq$ co-$\mathbf{NP}$, а значит, и для систем делимостей числа на значения линейных полиномов с хотя бы одним ненулевым коэффициентом при переменных и единичными свободными членами.

Из совпадения классов **NP** и co-**NP** непосредственно не следует равенство классов **P** и **NP**. Кроме того, известно не так много γ-полных задач в сравнении с обширным классом NP-полных проблем. В связи с этим, доказательство отсутствия полиномиального алгоритма решения данной задачи в предположении $\mathbf{P} \neq \mathbf{NP}$ является общепринятым признаком отсутствия для нее какого-либо полиномиального алгоритма. Поэтому далее будет рассмотрен вопрос, при каком числе ненулевых коэффициентов при переменных и для каких чисел K задача совместности системы делимостей числа K на значения заданных линейных выражений является NP-полной. Сформулируем общую задачу.

Совместность системы делимостей числа K на значения линейных выражений (**СД**K).

УСЛОВИЕ: Задан набор векторов $a_i = (a_{i,0}, \ldots, a_{i,n})$ с неотрицательными целыми координатами, представляющих линейные выражения вида $a_{i,0} + \sum_{j=1}^{n} a_{i,j}x_j$ при $1 \leq i \leq m$, и целое положительное число K.

ВОПРОС: Существуют ли такие положительные целые числа $x_1, x_2, \ldots, x_n$, что $a_{i,0} + \sum_{j=1}^{n} a_{i,j}x_j$ делит K для всех $1 \leq i \leq m$?

Докажем, что эта задача уже NP-полна в таком частном случае, когда в каждом линейном выражении имеется ровно три ненулевых коэффициента при переменных.

Теорема 1.1. *При любом целом $K \geq 4$, задача* **СД**K *при условии, что в каждом линейном выражении имеется ровно три ненулевых коэффициента при переменных, является NP-полной.*

Доказательство. То, что задача принадлежит классу **NP**, очевидно, поскольку значения всех переменных x_i принадлежат множеству целых чисел из отрезка $[1, K]$.

К данной проблеме сводится задача 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ, при этом каждой пропозициональной переменной u_i из этой задачи ставятся в соответствие две числовые переменные x_i и x'_i и дополнительно вводятся три переменные w_1, w_2, w_3.

Для того чтобы обеспечить условия, при которых переменные x_i и x'_i принимают ровно одно из двух значений 1 или 2 и значения переменных различны, запишем систему из двух делимостей

$$\begin{cases} (K-4) + x_i + x'_i + w_1 \,|\, K, \\ (K-4) + 2w_1 + w_2 + w_3 \,|\, K. \end{cases}$$

Каждому предложению $z_1 \vee z_2 \vee z_3$ (где z_j — пропозициональная переменная или ее отрицание) из условия задачи 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ ставим в соответствие делимость $(K-4) + y_1 + y_2 + y_3 \,|\, K$, где $y_j = x_i$, если $z_j = u_i$, и $y_j = x'_i$, если $z_j = \neg u_i$ $(j = 1, 2, 3)$.

Так получим систему делимостей требуемого вида, совместную тогда и только тогда, когда задача 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ имеет решение. □

Так как для всякого $K \geq 4$ задача **СД**K принадлежит классу **NP** и задача, сформулированная в теореме 1.1, является ее сужением, имеет место следующий результат.

Следствие теоремы 1.1. *Для всякого $K \geq 4$ задача* **СД**K *является NP-полной.*

Задачи о совместности системы делимостей числа K при $0 < K \leq 3$ линейными многочленами принадлежат классу **P**. Для значений $K = 1$ и $K = 2$ доказательство очевидно. Случай $K = 3$ сформулируем в виде утверждения.

Утверждение 1.1. *Задача* **СД**3 *разрешима за полиномиальное время.*

Доказательство. Для задачи **СД**3 имеют решения только системы с делимостями следующих видов:

(1) $x_1 + x_2 + x_3 \,|\, 3$;
(2) $1 + x_1 + x_2 \,|\, 3$;
(3) $2x_1 + x_2 \,|\, 3$;
(4) $x_1 + x_2 \,|\, 3$;
(5) $2 + x_1 \,|\, 3$;
(6) $1 + x_1 \,|\, 3$;
(7) $3x_1 \,|\, 3$;
(8) $x_1 \,|\, 3$.

Если в системе имеются выражения иного вида, такая система несовместна.

За исключением случаев (4) и (8) значения x_i определяются однозначно: $x_i = 2$ для (6) и $x_i = 1$ для остальных случаев.

Подсистему делимостей только из выражений вида (4) $x_i + x_j \,|\, 3$ можно, например, интерпретировать как граф с ребрами $\{x_i, x_j\}$ и за полиномиальное число шагов на машине Тьюринга проверить, является ли он 2-раскрашиваемым, с помощью алгоритма поиска в глубину за полином шагов от числа переменных, входящих в эту подсистему (и, следовательно, от длины записи подсистемы). Переменным, соответствующим вершинам одной доли, присваиваем значение 1, а соответствующим вершинам другой доли — значение 2. Получили два варианта возможных решений подсистемы делимостей только из выражений вида (4). Значения 2 возможны только

для переменных, входящих в выражения вида (6). Если в основной системе в выражениях вида (6) присутствуют переменные, соответствующие вершинам из обеих долей, система решений не имеет. Если в основной системе в выражениях вида (6) присутствуют переменные, соответствующие вершинам только из одной доли, у подсистемы из выражений вида (4) принимается только одно решение.

Выражения вида (8) имеют два решения: $x_i = 1$ или $x_i = 3$. Если переменная x_i имеется в какой-либо другой делимости вида, отличного от (8), (4) и (6), то $x_i = 1$. Если переменная x_i имеется как в делимости вида (8), так и в делимости вида (6), система несовместна. Если переменные x_i и x_j имеются как в делимости вида (8), так и в делимости вида (4), причем при анализе подсистемы из делимостей вида (4) эти переменные получили разные значения, то система несовместна. □

2. Сложность решения задач о совместной делимости значений линейных выражений на одно и то же число. Определим задачу, симметричную сформулированной в разделе 1. Пусть имеем целое число, большее единицы. Какова алгоритмическая сложность задачи проверки совместности в положительных целых числах системы делимостей на это число значений линейных выражений с неотрицательными коэффициентами?

Если на значения переменных не наложено ограничение, каждую делимость можно переписать в виде линейного сравнения по модулю K, где K — число из условия задачи. Проверка совместности системы сравнений выполняется за полиномиальное время даже в том случае, когда мы не знаем разложения K на простые множители [12, раздел 2.3.4].

В дальнейшем вопросы совместности систем в данном разделе будут рассматриваться на отрезке положительных целых чисел.

Совместность на отрезке системы делимостей значений линейных выражений на число K (СДнаK).

УСЛОВИЕ: Пусть заданы положительное целое число K, отрезок положительных целых чисел $[D, D']$ при $0 < D,\ D' < K$ и набор векторов $a_i = (a_{i,0}, \ldots, a_{i,n})$ с неотрицательными целыми координатами, представляющих линейные выражения вида $a_{i,0} + \sum_{j=1}^{n} a_{i,j}x_j$, при $1 \le i \le m$.

ВОПРОС: Существуют ли числа $x_1, x_2, \ldots, x_n$ из отрезка $[D, D']$ такие, что K делит $a_{i,0} + \sum_{j=1}^{n} a_{i,j}x_j$ для всех $1 \le i \le m$?

Здесь K является параметром сформулированной серии задач. Докажем, что некоторые задачи этой серии, имеющие делитель вида kD при целом $k \ge 3$, являются NP-полными.

Теорема 2.1. *При любом целом $k \ge 3$, задача* **СДна**(kD) *на невырожденном отрезке положительных целых чисел $[D, D']$ при условии, что в каждом линейном выражении имеется ровно три ненулевых коэффициента при переменных, является NP-полной.*

Доказательство. То, что задача принадлежит классу **NP**, очевидно, поскольку на отрезке конечное число целых чисел.

Построим полиномиальное сведение задачи 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ к данной задаче.

Каждой пропозициональной переменной u_i из этой задачи поставим в соответствие две числовые переменные x_i и x'_i. Дизъюнкции вида $z_1 \vee z_2 \vee z_3$ поставим в

соответствие делимость $kD \,|\, (2kD - 3D - 1) + y_1 + y_2 + y_3$, где $y_j = x_i$, если $z_j = u_i$, и $y_j = x'_i$, если $z_j = \neg u_i$ $(j = 1, 2, 3)$. Логические константы *истина* и *ложь* кодируются числами $D + 1$ и D соответственно.

Для обеспечения условия, при котором переменные x_i и x'_i соответствуют пропозициональной переменной u_i и ее отрицанию, введем новые переменные w_1, w_2, w_3 и запишем систему делимостей

$$\begin{cases} kD \,|\, (2kD - 3D - 1) + w_1 + x_i + x'_i, \\ kD \,|\, (2kD - 3D - 1) + w_2 + x_i + x'_i, \\ kD \,|\, (2kD - 3D - 1) + w_1 + w_2 + w_3. \end{cases}$$

Значение D' возьмем из отрезка $\left[D + 1, D + \left\lfloor \frac{k}{3} D \right\rfloor\right]$.

При $k \geq 3$ и $D \geq 1$ свободный член равен $2kD - 3D - 1 \geq 2$. Ограничение на значения переменных $x_i \leq D + \left\lfloor \frac{k}{3} D \right\rfloor$ таково, что значения полиномов не превосходят $2kD - 3D - 1 + 3\left(D + \left\lfloor \frac{k}{3} D \right\rfloor\right) \leq 3kD - 1$. Следовательно, получаем систему требуемого в формулировке теоремы вида, совместную тогда и только тогда, когда задача 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ имеет решение. □

Задача **СДна**2 очевидно принадлежит классу **P**. Положив значение начала отрезка $D = 1$, получим следующий результат.

Следствие 1 теоремы 2.1. *Для всякого $K \geq 3$, задача* **СДна**K *является NP-полной.*

Пусть далее параметром задачи является число ненулевых коэффициентов при переменных в каждом полиноме. Сформулируем следующую серию задач, зависящих от параметра k.

Совместность на отрезке системы делимостей значений линейных выражений с не более чем k ненулевыми коэффициентами при переменных на число (k**-СДЧ**).

УСЛОВИЕ: Пусть заданы положительное целое число K, отрезок положительных целых чисел $[D, D']$ при $0 < D,\ D' < K$ и набор векторов неотрицательных целых чисел $a_i = (a_{i,0}, \ldots, a_{i,n})$, представляющих линейные выражения вида $a_{i,0} + \sum_{j=1}^{n} a_{i,j} x_j$, при $1 \leq i \leq m$ с не более чем k ненулевыми коэффициентами при переменных.

ВОПРОС: Существуют ли положительные целые числа $x_1, x_2, \ldots, x_n$ из отрезка $[D, D']$ такие, что K делит $a_{i,0} + \sum_{j=1}^{n} a_{i,j} x_j$ для всех $1 \leq i \leq m$?

Для таким образом сформулированной задачи, получим следствие теоремы 2.1.

Следствие 2 теоремы 2.1. *Задача* 3**-СДЧ** *является NP-полной.*

Доказательство NP-полноты для случая $k = 2$ основано на сведении к 2**-СДЧ** задачи GOOD SIMULTANEOUS APPROXIMATION из [13]. Приведем формулировку этой задачи.

ПРИБЛИЖЕНИЕ ВЕКТОРА (ПВ)

УСЛОВИЕ: Задан рациональный вектор $a = (a_1/b_1, \ldots, a_n/b_n)$, положительные целые числа N и s.

ВОПРОС: Существует ли целое число $Q \in [1, N]$, что $\max\limits_{1 \leq i \leq n} \left\{ \min\limits_{k \in \mathbb{Z}} \left| Q \frac{a_i}{b_i} - k \right| \right\} \leq \frac{1}{s}$?

Теорема 2.2. *Задача* 2-**СДЧ** *является NP-полной.*

Доказательство. То, что задача принадлежит классу **NP**, очевидно, поскольку на отрезке конечное число целых чисел.

В действительности, в [13] доказана NP-полнота задачи ПВ с ограничением на значение параметра $s \geq 4(d+1)p_0^R p_1$, где d, R — некоторые положительные целые числа, p_0, p_1 — некоторые простые числа. По этой причине задача ПВ останется NP-полной, если дополнить условие неравенством $s \geq 5$.

Пусть $B = \text{НОК}(b_1, \ldots, b_n)$. Задача ПВ нетривиальна для $N < B$. Построим полиномиальное сведение задачи ПВ при $s \geq 5$ и $N < B$ к 2-**СДЧ**.

Условие $\max\limits_{1 \leq i \leq n} \left\{ \min\limits_{k \in \mathbb{Z}} |Qa_i/b_i - k| \right\} \leq 1/s$ перепишем в виде системы n неравенств вида $|Qa_i/b_i - k_i| \leq 1/s$ с целочисленными переменными $k_1, \ldots, k_n$ и переменной Q, принимающей значения из отрезка $[1, N]$.

Умножая каждое неравенство на Bs, получим $-B \leq Q(a_i/b_i)Bs - k_i Bs \leq B$. Следует заметить, что выражение $-(a_i/b_i)Bs$ является целым числом, так как $B = \text{НОК}(b_1, \ldots, b_n)$. Тогда определим $\tilde{a_i}$ как наименьшие неотрицательные числа такие, что $\tilde{a_i} \equiv (-(a_i/b_i)Bs) \pmod{Bs}$.

Пусть далее $K = Bs$ и $x_i = Q(a_i/b_i)K - k_i K$ для $1 \leq i \leq n$. Переименуем для удобства Q в x_{n+1}. Таким образом, имеем систему сравнений вида $x_i + \tilde{a_i} x_{n+1} \equiv 0 \pmod{K}$, где $x_i \in [-B, B]$ для $1 \leq i \leq n$ и $x_{n+1} \in [1, N]$.

Поскольку $K = Bs \geq 5B$, получаем, что каждое сравнение эквивалентно делимости $K \mid (K-B-1)+x_i+\tilde{a}_i x_{n+1}$ на отрезке положительных целых чисел $[1, 2B+1]$. Для того чтобы обеспечить выполнение условия $x_{n+1} \in [1, N]$, введем новую переменную x_{n+2} и дополним систему делимостью $K \mid (K - N - 1) + x_{n+1} + x_{n+2}$ для $x_{n+1}, x_{n+2} \in [1, 2B+1]$. Такое представление корректно, так как имеет место следующая цепочка неравенств $-K < -B < -N + 1 \leq x_{n+1} + x_{n+2} - N - 1 \leq 4B - N + 1 < 5B \leq K$, следовательно, $x_{n+1} + x_{n+2} = N + 1$.

Таким образом, каждой индивидуальной задаче ПВ при $s \geq 5$ и $N < B$ ставится в соответствие эквивалентная по разрешимости индивидуальная задача 2-**СДЧ** вида

$$\begin{cases} K \mid (K - B - 1) + x_1 + \tilde{a}_1 x_{n+1}, \\ \vdots \\ K \mid (K - B - 1) + x_n + \tilde{a}_n x_{n+1}, \\ K \mid (K - N - 1) + x_{n+1} + x_{n+2} \end{cases}$$

на отрезке целых чисел из $[1, 2B+1]$ при $K \geq 5B$ и $N < B$. Все шаги построения осуществляются за полиномиальное от длины исходных данных число шагов, следовательно, построенное сведение полиномиально, а задача 2-**СДЧ** NP-полна. □

В случае только одного ненулевого коэффициента при переменных в каждой делимости, получаем задачу из класса **P**.

Утверждение 2.1. *Задача* 1-**СДЧ** *разрешима за полиномиальное время.*

Доказательство. Проверка совместности системы делимостей вида

$$\begin{cases} K \mid a_{1,0} + a_{1,1}x_1, \\ K \mid a_{2,0} + a_{2,1}x_1, \\ \vdots \\ K \mid a_{i,0} + a_{i,j}x_j, \\ \vdots \\ K \mid a_{m,0} + a_{m,n}x_n \end{cases}$$

на отрезке целых чисел $[D, D']$ при $0 < D, D' < K$ выполняется за полиномиальное число шагов на машине Тьюринга. Каждую делимость перепишем в виде линейного сравнения $a_{i,j}x_j \equiv -a_{i,0} (\mathrm{mod}\, K)$ и решим его с помощью расширенного алгоритма Евклида. Получив отдельно для каждой переменной x_i систему сравнений вида $x_i \equiv a_{i_j} (\mathrm{mod}\, k_{i_j})$, воспользуемся обобщенной китайской теоремой об остатках. Либо система несовместна, либо за полиномиальное число шагов на машине Тьюринга получим единственное решение по модулю $K_i = \mathrm{НОК}(k_{i_1}, \ldots, k_{i_l})$. Так как $K_i | K$, осталось проверить для каждой переменной x_i имеется ли такое решение системы сравнений, которое принадлежит отрезку $[D, D']$. □

3. NP-трудность одной подзадачи совместной делимости линейных многочленов. Л. Липшицем в [2] установлена NP-трудность задачи СДЛМ. Формулировка этого результата приведена в [1]. Сформулируем эту задачу.

СОВМЕСТНАЯ ДЕЛИМОСТЬ ЛИНЕЙНЫХ МНОГОЧЛЕНОВ (СДЛМ)

УСЛОВИЕ: Заданы векторы $a_j = a_{j,0}, \ldots, a_{j,n}$ и $b_j = b_{j,0}, \ldots, b_{j,n}$ при $1 \le j \le m$ с положительными целыми координатами.

ВОПРОС: Существуют ли такие положительные целые числа $x_1, x_2, \ldots, x_n$, что при всех j $(1 \le j \le m)$ выполняется $a_{j,0} + \sum_{i=1}^{n} a_{j,i}x_i \mid b_{j,0} + \sum_{i=1}^{n} b_{j,i}x_i$?

Докажем NP-трудность ее подзадачи.

Теорема 3.1. *NP-трудна задача проверки совместности в положительных целых числах систем делимостей значений линейных полиномов от одних и тех же переменных с коэффициентами из {1,2} и свободными членами из {1,5}.*

Заметим, что если $P, Q \ge 1$, то $(P = Q) \Leftrightarrow (P \mid Q)\ \&\ (Q \mid P)$. Поэтому для доказательства теоремы 3.1 достаточно доказать следующую лемму.

Лемма 3.1. *NP-полна задача проверки совместности в положительных целых числах систем вида* $\&_{j=1}^{m}(a_{j,0} + \sum_{i=1}^{n} a_{j,i}x_i = b_{j,0} + \sum_{i=1}^{n} b_{j,i}x_i)$ *с коэффициентами при переменных из {1,2} и свободными членами из {1,5}. При этом каждая переменная входит хотя бы в одно уравнение с разными коэффициентами в его правую и левую части и, кроме того, все коэффициенты переменных, равные двум, могут встретиться только в одной части уравнения.*

Доказательство. Принадлежность задачи классу **NP**, следует из того, что все коэффициенты, равные двум, могут встретиться только в одной части уравнения и каждая из переменных входит хотя бы в одно уравнение с разными коэффициентами при ней в его правой и левой частях. Поэтому после приведения подобных членов получим систему уравнений вида $\sum_i x_i = 4$, так как наличие уравнения другого вида, отличного от $0 = 0$, указывало бы на несовместность системы в положительных

целых числах. Таким образом, переменные x_i принимают целые значения из отрезка $[1, 4]$. Следовательно, недетерминированной машине для проверки совместности системы в положительных целых числах достаточно проверить 4^n кортежей n чисел из множества $\{1, 2, 3, 4\}$, представимых на ленте в виде двоичных строк длины $2n$.

Докажем, что задача 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ полиномиально сводится к задаче, сформулированной в лемме. Логические константы *истина* и *ложь* кодируются числами 2 и 1 соответственно. Каждая пропозициональная переменная кодируется переменной для положительных целых чисел. Отрицание любой переменной x кодируется новой переменной x'. То, что каждая из этих двух переменных может принимать значения только 1 или 2, причем значения переменных не совпадают, записывается с использованием новых переменных w_1, w_2, w_3 с помощью уравнений

$$\begin{cases} \sum\limits_i x_i + 2x + 2x' + 2w_1 + 1 = \sum\limits_i x_i + x + x' + w_1 + 5, \\ \sum\limits_i x_i + 2x + 2x' + 2w_2 + 1 = \sum\limits_i x_i + x + x' + w_2 + 5, \\ \sum\limits_i x_i + 2w_1 + 2w_2 + 2w_3 + 1 = \sum\limits_i x_i + w_1 + w_2 + w_3 + 5. \end{cases}$$

После приведения подобных членов получим систему

$$\begin{cases} x + x' + w_1 = 4, \\ x + x' + w_2 = 4, \\ w_1 + w_2 + w_3 = 4. \end{cases}$$

Складывая первые два уравнения и вычитая эту сумму из третьего, получим $w_3 = 2(x + x') - 4$. Решение системы в положительных целых числах возможно тогда и только тогда, когда $x + x' = 3$.

Элементарная дизъюнкция вида $x \vee y \vee z$ кодируется посредством уравнения $\sum\limits_i x_i + 2x + 2y + 2z + 1 = \sum\limits_i x_i + x + y + z + 5$, где в уравнении x — это переменная u_i, если x в дизъюнкции имеет вид u_i, либо переменная u_i', если x в дизъюнкции имеет вид $\neg u_i$. Аналогично для литералов y и z.

Получили систему требуемого вида, совместную в положительных целых числах тогда и только тогда, когда задача 3-ВЫП ПРИ ОДНОМ ИСТИННОМ ЛИТЕРАЛЕ имеет решение. □

Если в лемме 3.1 термин «NP-полная» заменить на слова «принадлежит **P**» и добавить к концу леммы фразу «в каждом уравнении *число переменных с коэффициентом 2 не превосходит двух*», получится верное утверждение.

Действительно, каждое уравнение равносильно уравнению вида $x+y = 4$, которое имеет следующее множество решений $\{(1, 3), (2, 2), (3, 1)\}$. Это означает, что выбирая одну из компонент решения, однозначно определяется вторая компонента решения. Сказанное позволяет осуществить подбор решения за полиномиальное число шагов на машине Тьюринга.

Заключение. Рассматриваемая в работе задача СДЛМ имеет существенное применение в области математических основ информатики. В общем случае она принадлежит классу **NEXPTIME**. Доказана NP-трудность и в ряде случаев NP-полнота целого ряда ее кратко формулируемых подзадач. Эти подзадачи представляют также

и самостоятельный интерес. Доказана принадлежность классу **P** некоторых частных случаев.

Доказано, что задача проверки совместности в положительных целых числах системы делимостей целого числа K на значения линейных полиномов с неотрицательными целыми коэффициентами $\exists x_1 \dots x_n \ \&_{j=1}^{m}(L_j(x_1 \dots x_n) \mid K)$ NP-полна при $K \geq 4$ и принадлежит классу **P** при $0 < K < 4$.

Исследована задача проверки совместности в целых числах из заданного невырожденного отрезка положительных целых чисел $[D, D']$, системы делимостей значений линейных полиномов с неотрицательными целыми коэффициентами на целое число K $\exists x_1 \dots x_n(\ \&_{i=1}^{n} x_i \in [D, D'] \ \& \ \&_{j=1}^{m} K \mid L_j(x_1 \dots x_n))$. Доказана ее NP-полнота для любого $K \geq 3$. Если параметром задачи выбрать число ненулевых коэффициентов при переменных, задача является NP-полной уже при только двух ненулевых коэффициентах. В случае, когда не равен нулю только один коэффициент, задача находится в классе **P**.

Доказана NP-трудность задачи проверки совместности в положительных целых числах системы делимостей значений линейных полиномов с положительными целыми коэффициентами на значения линейных полиномов с положительными целыми коэффициентами $\exists x_1 \dots x_n \ \&_{j=1}^{m}(L_j(x_1 \dots x_n) \mid L'_j(x_1 \dots x_n))$, если коэффициенты при переменных из $\{1, 2\}$ и свободные члены из $\{1, 5\}$.

Литература

1. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи / пер. с англ. М.: Мир, 1982.

2. *Lipshitz L.* Some remarks on the Diophantine problem for addition and divisibility // Bull. Soc. Math. Belg. Ser. B. 1981. Vol. 33, issue 1. P. 41–52.

3. *Lipshitz L.* The Diophantine problem for addition and divisibility // Transactions of the American Mathematical Society. 1976. Vol. 235. P. 271–283.

4. *Бельтюков А. П.* Разрешимость универсальной теории натуральных чисел со сложением и делимостью // Записки научных семинаров ЛОМИ. 1975. Т. 60. С. 15–28.

5. *Haase C.* On the complexity of model checking counter automata. Ph.D. Thesis, University of Oxford, 2012.

6. *Lechner A., Ouaknine J., Worrell J.* On the Complexity of Linear Arithmetic with Divisibility // Proceedings of the 30th Annual ACM/IEEE Symposium on Logic in Computer Science(LICS). 2015. P. 667–676.

7. *Косовский Н. К., Косовская Т. М., Косовский Н. Н.* Условия NP-полноты проверки совместности нескольких видов систем линейных диофантовых дизсравнений // Вестн. С.-Петерб. ун-та. Сер. 1. 2016. Т. 3(61), вып. 1. С. 25–31.

8. *Косовский Н. К., Косовская Т. М., Косовский Н. Н.* Условия NP-полноты проверки совместности нескольких видов систем линейных диофантовых сравнений и уравнений // Вестн. С.-Петерб. ун-та. Сер. 1. 2016. Т. 3(61), вып. 2. С. 198–203.

9. *Косовский Н. К., Косовская Т. М., Косовский Н. Н.* Условия NP-полноты проверки совместности нескольких видов систем линейных диофантовых дизуравнений // Вестн. С.-Петерб. ун-та. Сер. 1. 2016. Т. 3(61), вып. 3. С. 408–414.

10. *Schaefer T. J.* The complexity of satisfiability problems // Proceedings 10th Symposium on Theory of Computing, ACM Press. 1978. P. 216–226.

11. *Adleman L., Manders K.* Reducibility, randomness and intractability // Proceedings of the 9th Annual ACM Symposium on Theory of Computing. 1977. P. 151–163.

12. *Cohen H.* A Course in Computational Algebraic Number Theory, ser. Graduate Texts in Mathematics. Vol. 138. Springer-Verlag, 1993.

13. *Lagarias J. C.* The computational complexity of simultaneous diophantine approximation problems // 23th Annual Symposium on Foundations of Computer Science, IEEE. New York, 1982. P. 32–39.

Статья поступила в редакцию 9 ноября 2016 г.; рекомендована в печать 22 декабря 2016 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

Старчак Михаил Романович — аспирант; mikhstark@gmail.com

NP-COMPLETE PROBLEMS FOR SYSTEMS OF DIVISIBILITIES OF VALUES OF LINEAR POLYNOMIALS

Nikolay K. Kosovskii, Tatiana M. Kosovskaya, Nikolay N. Kosovskii, Mikhail R. Starchak

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

We study the algorithmic complexity of the subproblems of simultaneous divisibility of values of linear polynomials with non-negative coefficients in positive integers. In general, it is not known whether it is in **NP**, but it was previously proved it to be in **NEXPTIME**.

The NP-completeness is proved for such two series of this problem, that in the first of them a number divides a linear polynomial, and in the second case linear polynomial is a divisor of a number. Values for the parameters were determined, for which the problem is NP-complete. For the values less than specified, it was proved the problem to be in the class **P**.

We prove the NP-hardness of the particular case of the general problem of simultaneous divisibility of values of linear polynomials in which the coefficients of the variables may only take values from the set $\{1, 2\}$ and the constant terms of linear polynomials may only take values from the set $\{1, 5\}$. The obtained results may be useful for determining the algorithmic complexity of the general problem.

In Section 1, it is proved that the problem $\exists x_1 \dots x_n \ \&_{j=1}^{m}(L_j(x_1 \dots x_n) \mid K)$ is NP-complete for $K \geq 4$ and exactly three non-zero coefficients in each linear polynomial. It is from the class **P** for $0 < K < 4$.

In Section 2, we studied the problem of simultaneous divisibility in positive integers from the non-trivial interval $[D, D']$, of values of linear polynomials with non-negative integer coefficients by a positive integer K: $\exists x_1 \dots x_n \ (\ \&_{i=1}^{n} x_i \in [D, D'] \ \& \ \ \&_{j=1}^{m} K \mid L_j(x_1 \dots x_n))$. It is proved to be NP-complete for $K \geq 3$. If the parameter of the problem is the number of non-zero coefficients in linear polynomials, the problem is NP-complete for only two non-zero coefficients. In the case of exactly one non-zero coefficient, the problem is from the class **P**.

In Section 3, it is proved NP-hardness of $\exists x_1 \dots x_n \ \&_{j=1}^{m}(L_j(x_1 \dots x_n) \mid L'_j(x_1 \dots x_n))$, the problem of simultaneous divisibility of the values of linear polynomials on the values of the linear polynomials with the coefficients of the variables from $\{1, 2\}$ and constant terms from $\{1, 5\}$. Refs 13.

Keywords: system of divisibilities of values of linear polynomials, NP-hardness, NP-completeness.

References

1. Garey M. R., Johnson D. S., "Computers and Intractability: a Guide to the Theory of NP-completeness" (Freeman, New York, 1979).

2. Lipshitz L., "Some remarks on the Diophantine problem for addition and divisibility", *Bull. Soc. Math. Belg. Ser. B* **33**, issue 1, 41–52 (1981).

3. Lipshitz L., "The Diophantine problem for addition and divisibility", *Transactions of the American Mathematical Society* **235**, 271–283 (1976).

4. Bel'tyukov A., "Decidability of the universal theory of the natural numbers with addition and divisibility", *Zapiski Nauchnyh Seminarov LOMI* **60**, 15–28 (1976) [in Russian].

5. Haase C., "On the complexity of model checking counter automata", Ph.D. Thesis (University of Oxford, 2012).

6. Lechner A., Ouaknine J., Worrell J., "On the Complexity of Linear Arithmetic with Divisibility", *Proceedings of the 30th Annual ACM/IEEE Symposium on Logic in Computer Science(LICS)*, 667–676 (2015).

7. Kosovskii N. K., Kosovskaya T. M., Kosovskii N. N., "NP-completeness conditions for verifying the consistency of several kinds of systems of linear diophantine discongruences", *Vestn. St. Petersburg Univ.: Math.* **49**, issue 1, 18–22 (2016).

8. Kosovskii N. K., Kosovskaya T. M., Kosovskii N. N., "NP-completeness conditions for verifying the consistency of several kinds of systems of linear diophantine congruences and equations", *Vestn. St. Petersburg Univ.: Math.* **49**, issue 2, 111–114 (2016).

9. Kosovskii N. K., Kosovskaya T. M., Kosovskii N. N., "NP-completeness conditions for verifying the consistency of several kinds of systems of linear diophantine dis- equations", *Vestn. St. Petersburg Univ.: Math.* **49**, issue 3, 243–247 (2016).

10. Schaefer T. J., "The complexity of satisfiability problems", *Proceedings 10th Symposium on Theory of Computing*, 216–226 (ACM Press, 1978).

11. Adleman L., Manders K., "Reducibility, randomness and intractability", *Proceedings of the 9th Annual ACM Symposium on Theory of Computing*, 151–163 (1977).

12. Cohen H., *A Course in Computational Algebraic Number Theory*, in ser. *Graduate Texts in Mathematics* (Springer-Verlag, **138**, 1993).

13. Lagarias J. C., "The computational complexity of simultaneous diophantine approximation problems", *23th Annual Symposium on Foundations of Computer Science, IEEE*, 32–39 (New York, 1982).

Для цитирования: Косовский Н. К., Косовская Т. М., Косовский Н. Н., Старчак М. Р. NP-полные задачи о системах делимостей значений линейных выражений // Вестник СПбГУ. Математика. Механика. Астрономия. 2017. Т. 4 (62). Вып. 2. С. 236–246. DOI: 10.21638/11701/spbu01.2017.207

For citation: Kosovskii N. K., Kosovskaya T. M., Kosovskii N. N., Starchak M. R. NP-complete problems for systems of divisibilities of values of linear polynomials. *Vestnik SPbSU. Mathematics. Mechanics. Astronomy*, 2017, vol. 4 (62), issue 2, pp. 236–246. DOI: 10.21638/11701/spbu01.2017.207