УДК 510.52

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ О СУММЕ ПОДМНОЖЕСТВ ДЛЯ ПОЛУГРУПП ЦЕЛОЧИСЛЕННЫХ МАТРИЦ[1]

А. Н. Рыбалов

Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

В 2003 г. Каповичем, Мясниковым, Шуппом и Шпильрайном была предложена теория генерической вычислимости и сложности вычислений. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Проблема о сумме подмножеств является классической комбинаторной проблемой, изучаемой многие десятилетия. Мясников, Николаев и Ушаков в 2015 г. ввели аналог этой проблемы для произвольных групп (полугрупп). Оказалось, что для некоторых классов групп, таких, как гиперболические и нильпотентные группы, эта проблема разрешима за полиномиальное время. Для других, например групп Баумслага — Солитера и группы унимодулярных целочисленных матриц второго порядка $SL_2(\mathbb{Z})$, эта проблема NP-полна. Из работ Гуревича, Каи, Фукса, Козена и Лиу следует, что проблема о сумме подмножеств для группы $SL_2(\mathbb{Z})$ и для моноида $SL_2(\mathbb{N})$ полиномиально разрешима для почти всех входов. В работе изучается генерическая сложность проблемы о сумме подмножеств для полугрупп матриц произвольного порядка с целыми неотрицательными элементами. Эта проблема является NP-полной, а потому при условии $\mathrm{P} \neq \mathrm{NP}$ нет полиномиального алгоритма, решающего её для всех входов. Доказывается, что проблема является генерически разрешимой за полиномиальное время. Предлагается полиномиальный генерический алгоритм, основанный на методе динамического программирования.

Ключевые слова: *генерическая сложность, проблема о сумме подмножеств, полугруппы целочисленных матриц.*

DOI 10.17223/20710410/50/9

ON GENERIC COMPLEXITY OF THE SUBSET SUM PROBLEM FOR SEMIGROUPS OF INTEGER MATRICES

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

E-mail: alexander.rybalov@gmail.com

Generic-case approach to algorithmic problems was suggested by Miasnikov, Kapovich, Schupp, and Shpilrain in 2003. This approach studies behavior of an algorithm on typical (almost all) inputs and ignores the rest of inputs. The subset sum problem is a classic combinatorial problem that has been studied for many decades. Myasnikov, Nikolaev and Ushakov in 2015 introduced an analogue of this problem for arbitrary groups (semigroups). For some classes of groups, such as hyperbolic and nilpotent groups, this problem is solvable in polynomial time. For others, for example, Baumslag — Solitaire groups, group of second order integer unimodular matrices $SL_2(\mathbb{Z})$, this problem is NP-complete. From the works of Gurevich, Kai, Fuchs,

[1]Работа поддержана грантом РНФ № 18-71-10028.

Cosen, and Liu, it follows that the subset sum problem for the group $SL_2(\mathbb{Z})$ and for the monoid $SL_2(\mathbb{N})$ is polynomially solvable for almost all inputs. In the paper, we study the generic complexity of the subset sum problem for semigroups of matrices of arbitrary order with integer non-negative elements. This problem is NP-complete, and therefore for it, provided P $\neq$ NP, there is no polynomial algorithm that solves it for all inputs. We present a polynomial generic algorithm based on the dynamic programming and prove that this problem is generically solvable in polynomial time.

Keywords: *generic complexity, the subset sum problem, integer matrix semigroups.*

Введение

Проблема о сумме подмножеств является классической комбинаторной проблемой, изучаемой многие десятилетия. Она содержится в классическом списке из двадцати одной NP-полной проблемы в знаменитой работе [1]. Её формулировка состоит в следующем. Дано множество натуральных чисел $A = \{a_1, \ldots, a_n\}$ и натуральное число S. Все числа записаны в двоичном виде. Необходимо определить, можно ли в множестве A выбрать подмножество чисел, которые в сумме дают число S. Эта задача имеет родство с другой классической проблемой оптимизации — о рюкзаке, её иногда считают частным случаем проблемы о рюкзаке. Большую популярность проблема о сумме подмножеств приобрела в криптографии, где неоднократно предлагались криптосистемы, основанные на ней [2, 3]. Отметим, что Н. Н. Кузюрин доказал полиномиальную разрешимость в среднем некоторых проблем рюкзачного типа [4].

А. Мясников, А. Николаев и А. Ушаков ввели аналоги проблем о рюкзаке и о сумме подмножеств для произвольных групп (полугрупп) [5]. Это является некоторым обобщением классических проблем, так как в классическом случае входные данные берутся из группы целых чисел $\mathbb{Z}$ с операцией сложения, заданной с помощью бесконечной системы порождающих $\{2^m : m = 0, 1, 2, \ldots\}$. В [5] изучена вычислительная сложность этих проблем для различных групп: доказаны полиномиальная разрешимость для гиперболических групп и NP-полнота для групп Баумслага — Солитера. Отмечена связь с классической проблемой о вхождении в подгруппу. Сложность в среднем ограниченной проблемы вхождения для группы $SL_2(\mathbb{Z})$ унимодулярных целочисленных (2×2)-матриц изучалась А. Бласcом и Ю. Гуревичем [6]. С использованием идей Гуревича из [7] в [8] предложен полиномиальный в среднем алгоритм для ограниченной проблемы вхождения в модулярной группе $PSL_2(\mathbb{Z})$. Полиномиальный в среднем алгоритм для ограниченной проблемы вхождения для полугруппы унимодулярных натуральнозначных (2×2)-матриц $SL_2(\mathbb{N})$ предложен в [9]. Эти алгоритмы без особого труда могут быть переделаны в эффективные алгоритмы, решающие проблемы рюкзака и суммы подмножеств для упомянутых групп и полугрупп матриц. Однако они не работают для полугрупп неунимодулярных матриц и матриц порядка больше 2, так как существенно используют структуру полугруппы $SL_2(\mathbb{N})$ как свободного двупорождённого моноида.

В 2003 г. в [10] предложена теория генерической вычислимости и сложности вычислений. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют генерическое множество; понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения практики алгоритмы, быстро решающие проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов.

В данной работе изучается генерическая сложность проблемы о сумме подмножеств для полугрупп матриц произвольного порядка с целыми неотрицательными элементами. Эта проблема в классическом смысле является NP-полной, а потому при условии P $\neq$ NP нет полиномиального алгоритма, решающего её для всех входов. Доказывается, что проблема является генерически разрешимой за полиномиальное время. Предлагается полиномиальный генерический алгоритм, основанный на методе динамического программирования.

1. Генерические алгоритмы

Пусть I — множество всех входов, I_n — множество входов размера $\leqslant n$. Для любого подмножества $S \subseteq I$ определим последовательность

$$\rho_n(S) = \frac{|S_n|}{|I_n|},\ n = 1, 2, 3, \ldots,$$

где $S_n = S \cap I_n$ — множество входов из S размера $\leqslant n$. *Асимптотической плотностью* S назовём предел (если он существует)

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S) = 1$, и *пренебрежимым*, если $\rho(S) = 0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо.

Алгоритм $\mathcal{A}$ с множеством входов I и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется *генерическим*, если

1) $\mathcal{A}$ останавливается на всех входах из I;
2) множество $\{x \in I : \mathcal{A}(x) = ?\}$ является пренебрежимым.

Здесь через $\mathcal{A}(x)$ обозначается результат работы алгоритма $\mathcal{A}$ на входе x. Генерический алгоритм $\mathcal{A}$ *вычисляет функцию* $f : I \to J$, если для всех $x \in I$ имеет место

$$\mathcal{A}(x) \neq ?\ \Rightarrow\ f(x) = \mathcal{A}(x).$$

Ситуация $\mathcal{A}(x) = ?$ означает, что $\mathcal{A}$ не может вычислить функцию f на аргументе x. Но условие 2 гарантирует, что $\mathcal{A}$ корректно вычисляет f на почти всех входах (входах из генерического множества).

2. Полугруппа натуральнозначных матриц

Обозначим через $\mathbb{N}$ множество натуральных чисел, начинающееся с единицы, а через ω — множество натуральных чисел с нулём. Будем работать в основном с полугруппой матриц $Mat(k, \omega)$ порядка k с целыми неотрицательными элементами с обычной операцией умножения матриц. Иногда будем использовать полугруппу $Mat(k, \mathbb{N})$. Порядок матриц k фиксирован. Очевидно, $Mat(k, \mathbb{N}) \subseteq Mat(k, \omega)$. Элементы $Mat(k, \omega)$ будем представлять матрицами из целых неотрицательных чисел. Размер целого положительного числа a, обозначаемый $\mathrm{size}(a)$, — это длина его двоичной записи. Таким образом, $\mathrm{size}(a) = n$, если $2^{n-1} \leqslant a < 2^n$. Отдельно положим $\mathrm{size}(0) = 0$. Легко видеть, что для любых натуральных $a, b \neq 0$ выполнено $\mathrm{size}(ab) = \mathrm{size}(a) + \mathrm{size}(b)$ и $\mathrm{size}(a) \leqslant \mathrm{size}(a + b)$. Под размером матрицы $M = ||a_{ij}||$ будем понимать $\mathrm{size}(M) = \max\limits_{i,j=1,\ldots,k} \{\mathrm{size}(a_{ij})\}$.

Лемма 1. Для любого n имеет место

$$|Mat(k,\omega)_n| = 2^{nk^2},\ |Mat(k,\mathbb{N})_n| = (2^n-1)^{k^2}.$$

Доказательство. На каждом из k^2 мест матрицы из множества $Mat(k,\omega)_n$ может стоять число от 0 до (2^n-1), то есть 2^n вариантов. Всего получаем 2^{nk^2} различных матриц. Аналогично производится подсчёт $|Mat(k,\mathbb{N})_n|$. ■

Докажем несколько фактов о полугруппах матриц, которые используются при построении и обосновании генерического полиномиального алгоритма для проблемы о сумме подмножеств.

Лемма 2.

1) Пусть Z — множество матриц в $Mat(k,\omega)$, содержащих хотя бы один нулевой элемент. Тогда Z пренебрежимо в $Mat(k,\omega)$.
2) Пусть $S \subseteq Mat(k,\mathbb{N})$. Если S пренебрежимо в $Mat(k,\mathbb{N})$, то S пренебрежимо в $Mat(k,\omega)$.

Доказательство.

1) Оценим число матриц из Z_n. Нуль можно поставить на одно из k^2 мест, остальные k^2-1 мест заполняются произвольно. Таким образом, $|Z_n| \leqslant k^2 2^{n(k^2-1)}$ и

$$\rho(Z) = \lim_{n\to\infty} \frac{|Z_n|}{|Mat(k,\omega)_n|} \leqslant \lim_{n\to\infty} \frac{k^2 2^{n(k^2-1)}}{2^{nk^2}} = \lim_{n\to\infty} \frac{k^2}{2^n} = 0.$$

2) Пусть

$$\rho(S) = \lim_{n\to\infty} \frac{|S_n|}{|Mat(k,\mathbb{N})_n|} = \lim_{n\to\infty} \frac{|S_n|}{(2^n-1)^{k^2}} = 0.$$

Тогда

$$\rho(S) = \lim_{n\to\infty} \frac{|S_n|}{|Mat(k,\omega)_n|} = \lim_{n\to\infty} \frac{|S_n|}{2^{nk^2}} \leqslant \lim_{n\to\infty} \frac{|S_n|}{(2^n-1)^{k^2}} = 0.$$

Лемма 2 доказана. ■

Лемма 3. Множество матриц из $Mat(k,\omega)$ с определителем 0 пренебрежимо.

Доказательство. Рассмотрим сначала множество $Mat(k,\mathrm{GF}(p))$ квадратных матриц порядка k с элементами из поля $\mathrm{GF}(p)$, где p — простое число. Очевидно, что $|Mat(k,\mathrm{GF}(p))| = p^{k^2}$. Найдём среди всех таких матриц долю обратимых матриц, у которых определитель отличен от нуля в $\mathrm{GF}(p)$. Такие матрицы образуют группу $\mathrm{GL}(k,\mathrm{GF}(p))$. Известно [11], что $|\mathrm{GL}(k,\mathrm{GF}(p))| = \prod_{i=1}^{k}(p^k - p^{i-1})$. Отсюда искомая доля равна

$$P = \frac{|\mathrm{GL}(k,\mathrm{GF}(p))|}{|Mat(k,\mathrm{GF}(p))|} = \frac{\prod_{i=1}^{k}(p^k - p^{i-1})}{p^{k^2}} = \prod_{i=1}^{k}(1-p^{-i}).$$

Обозначим через $Mat_0(k,\mathrm{GF}(p))$ множество матриц из $Mat(k,\mathrm{GF}(p))$ с определителем 0. Доля таких матриц равна

$$\frac{|Mat_0(k,\mathrm{GF}(p))|}{|Mat(k,\mathrm{GF}(p))|} = 1 - P = 1 - \prod_{i=1}^{k}(1-p^{-i}).$$

Вернёмся к $Mat(k,\omega)$. Согласно лемме 2, достаточно доказать, что матрицы из $Mat(k,\mathbb{N})$ с нулевым определителем образуют пренебрежимое множество в $Mat(k,\mathbb{N})$.

Зафиксируем размер матриц n. Выберем простое число p, являющееся делителем 2^n-1. Пусть $\varphi_p : \{1,\dots,2^n-1\} \to \mathrm{GF}(p)$ — отображение, определяемое для любого $a \in \{0,\dots,2^n-1\}$ как $\varphi_p(a) = a \bmod p$. Соответствующее индуцированное отображение для матриц тоже будем обозначать φ_p. Заметим, что прообраз каждого элемента из $\mathrm{GF}(p)$ при отображении φ_p состоит ровно из $(2^n-1)/p$ чисел из отрезка $1,\dots,2^n-1$. Поэтому для любого множества матриц $\mathcal{S} \subseteq Mat(k,\mathrm{GF}(p))$ имеет место

$$|\varphi_p^{-1}(\mathcal{S})| = \Big(\frac{2^n-1}{p}\Big)^{k^2}|\mathcal{S}|.$$

Пусть теперь $\mathcal{Z}$ — множество матриц из $Mat(k,\mathbb{N})_n$ с определителем 0. Так как $\mathcal{Z} \subseteq \varphi_p^{-1}(Mat_0(k,\mathrm{GF}(p))$, имеем

$$\frac{|\mathcal{Z}|}{|Mat(k,\mathbb{N})_n|} \leqslant \frac{|\varphi_p^{-1}(M_0(k,\mathrm{GF}(p))|}{|Mat(k,\mathbb{N})_n|} = \frac{\Big(\frac{2^n-1}{p}\Big)^{k^2}|Mat_0(k,\mathrm{GF}(p))|}{\Big(\frac{2^n-1}{p}\Big)^{k^2}|Mat(k,\mathrm{GF}(p))|} =$$
$$= \frac{|Mat_0(k,\mathrm{GF}(p))|}{|Mat(k,\mathrm{GF}(p))|} = 1 - \prod_{i=1}^{k}(1-p^{-i}).$$

При увеличении p значение справа стремится к нулю. Осталось доказать, при увеличении размера n значение p тоже увеличивается. Напомним, что простое число p выбиралось как делитель 2^n-1. По классической теореме Жигмонди [12], начиная с $m > 6$ каждый элемент последовательности $\{2^m-1 :\ m = 1,2,\dots\}$ имеет простой делитель, на который не делятся предыдущие члены этой последовательности. Поэтому с ростом n можно выбирать простые делители p числа 2^n-1 так, чтобы значение p неограничено увеличивалось. ■

Лемма 4. Пусть для матриц $A = ||a_{ij}||$ и $B = ||b_{ij}||$ из $Mat(k,\omega)$ имеет место $\mathrm{size}(A), \mathrm{size}(B) \leqslant n$ и $\mathrm{size}(AB) \leqslant n$. Тогда для любых $1 \leqslant i,j \leqslant k$ имеет место $\mathrm{size}(a_{ij}) + \mathrm{size}(b_{ji}) \leqslant n$.

Доказательство. Пусть $AB = ||c_{ij}||$. Тогда для любого $i = 1,\dots,k$

$$c_{ii} = a_{i1}b_{1i} + a_{i2}b_{2i} + \dots + a_{ij}b_{ji} + \dots + a_{ik}b_{ki}.$$

Так как $\mathrm{size}(c_{ii}) \leqslant n$, для каждого $j = 1,\dots,k$ и положительных a_{ij}, b_{ji} имеем $\mathrm{size}(a_{ij}b_{ji}) \leqslant n$, т. е. $\mathrm{size}(a_{ij}) + \mathrm{size}(b_{ji}) \leqslant n$. Если $a_{ij} = 0$ или $b_{ji} = 0$, то требуемое неравенство следует из условия $\mathrm{size}(a_{ij}), \mathrm{size}(b_{ji}) \leqslant n$. ■

Лемма 5. Пусть S_n — множество матриц M из $Mat(k,\omega)$ размера n, таких, что матричное уравнение $M = XY$ имеет более $p(n) = (2(n+1))^{k^2+1}$ различных решений $X, Y \in Mat(k,\omega)$, таких, что $\mathrm{size}(X), \mathrm{size}(Y) \leqslant n$. Тогда

$$\frac{|S_n|}{|Mat(k,\omega)_n|} < \frac{1}{2(n+1)}.$$

Доказательство. Пусть K — число различных пар матриц X, Y, таких, что $\mathrm{size}(X), \mathrm{size}(Y) \leqslant n$ и $\mathrm{size}(XY) \leqslant n$. Тогда из определения множества S_n следует

$$(2(n+1))^{k^2+1}|S_n| \leqslant K. \tag{1}$$

Оценим сверху число K. Пусть $X = ||x_{ij}||$, $Y = ||y_{ij}||$. По лемме 4 для любых i, j выполнено $\mathrm{size}(x_{ij}) + \mathrm{size}(y_{ji}) \leqslant n$. Поэтому число K не превосходит числа пар таких матриц X, Y, что $\mathrm{size}(x_{ij}) + \mathrm{size}(y_{ji}) \leqslant n$ для $1 \leqslant i, j \leqslant k$, т. е.

$$K \leqslant |\{(X,Y) : \mathrm{size}(x_{ij}) + \mathrm{size}(y_{ji}) \leqslant n,\ 1 \leqslant i,j \leqslant k\}| =$$
$$= \prod_{1\leqslant i,j\leqslant k} |\{(a,b) : \mathrm{size}(a) + \mathrm{size}(b) \leqslant n\}| = \Big(|\{(a,b) : \mathrm{size}(a) + \mathrm{size}(b) \leqslant n\}|\Big)^{k^2} =$$
$$= \Big(\sum_{m=0}^{n} |\{(a,b) : \mathrm{size}(a) + \mathrm{size}(b) = m\}|\Big)^{k^2} =$$
$$= \Big(\sum_{m=0}^{n}\sum_{l=0}^{m} |\{(a,b) : \mathrm{size}(a) = l,\ \mathrm{size}(b) = m-l\}|\Big)^{k^2} =$$
$$= \Big(\sum_{m=0}^{n}\sum_{l=0}^{m} 2^l \cdot 2^{m-l}\Big)^{k^2} = \Big(\sum_{m=0}^{n} m2^m\Big)^{k^2} < \Big((n+1)\sum_{m=0}^{n} 2^m\Big)^{k^2} =$$
$$= \Big((n+1)(2^{n+1}-1)\Big)^{k^2} < (2(n+1))^{k^2}2^{nk^2} = (2(n+1))^{k^2}|Mat(k,\omega)_n|.$$

Таким образом, получили оценку

$$K < (2(n+1))^{k^2}|Mat(k,\omega)_n|. \tag{2}$$

Допустим теперь противное, то есть что $\dfrac{|S_n|}{|Mat(k,\omega)_n|} > \dfrac{1}{2(n+1)}$. Тогда

$$(2(n+1))^{k^2+1}|S_n| > (2(n+1))^{k^2}|Mat(k,\omega)_n|.$$

Но это неравенство и оценки (1) и (2) дают противоречие

$$(2(n+1))^{k^2}|Mat(k,\omega)_n| < (2(n+1))^{k^2+1}|S_n| \leqslant K < (2(n+1))^{k^2}|Mat(k,\omega)_n|.$$

Лемма 5 доказана. ■

3. Проблема о сумме подмножеств над $Mat(k,\omega)$

Сформулируем проблему о сумме подмножеств для полугруппы $Mat(k,\omega)$. Даны матрицы $M_1, M_2, \ldots, M_n$ из $Mat(k,\omega)$, каждая размером не более n, и матрица M из $\mathcal{M}$ размера не более n^2. Определить, существуют ли степени $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{0,1\}$, такие, что имеет место

$$M_1^{\varepsilon_1} M_2^{\varepsilon_2} \ldots M_n^{\varepsilon_n} = M.$$

Размер входа $(M_1, M_2, \ldots, M_n, M)$ полагаем равным n. Условимся, что если матрица $M = E$ (единичная), то M есть произведение пустого подмножества матриц, а потому проблема суммы подмножеств с такой матрицей M разрешима. Это допущение послужит для удобства описания генерического алгоритма в дальнейшем.

Следующее утверждение говорит, что для этой проблемы при условии P $\neq$ NP не существует полиномиального алгоритма, который решает её для всех входов.

Лемма 6. Проблема о сумме подмножеств для $Mat(k,\omega)$ NP-полна.

Доказательство. Докажем, что к данной проблеме полиномиально сводится классическая проблема о сумме подмножеств для натуральных чисел. Определим

функцию $F : \omega \to Mat(k, \omega)$ следующим образом. Для любого $a \in \omega$ положим

$$F(a) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & a \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & & & & & \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Соответствующая полиномиальная сводимость сопоставляет входу $(a_1, a_2, \dots, a_n, S)$ классической проблемы о сумме подмножеств вход $(F(a_1), F(a_2), \dots, F(a_n), F(S))$ проблемы о сумме подмножеств для $Mat(k, \omega)$. Легко проверить, что для любого набора чисел $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \{0, 1\}$ равенство

$$a_1\varepsilon_1 + a_2\varepsilon_2 + \dots + a_n\varepsilon_n = S$$

выполняется тогда и только тогда, когда $F(a_1)^{\varepsilon_1} F(a_2)^{\varepsilon_2} \dots F(a_n)^{\varepsilon_n} = F(S)$. ■

Следующая теорема говорит, что для данной проблемы существует генерический полиномиальный алгоритм, решающий её для почти всех входов.

Теорема 1. Проблема о сумме подмножеств для полугруппы $Mat(k, \omega)$ является генерически разрешимой за полиномиальное время.

Доказательство. Опишем, как работает генерический полиномиальный алгоритм $\mathcal{A}$ на входе $(M_1, \dots, M_n, M)$ размера n.

1) Вычисляем определитель матрицы M. Если он равен 0, выдаём ответ «?». Из леммы 3 следует, что множество входов $(M_1, \dots, M_n, M)$, у которых $\det(M) = 0$, пренебрежимо.
2) Вычисляем определители матриц $M_1, \dots, M_n$. Выбрасывам те матрицы, у которых определитель равен 0, — они не могут участвовать в произведении, которое равно M, так как $\det(M) \neq 0$. На последующих шагах считаем, что все матрицы $M_1, \dots, M_n, M$ невырождены.
3) В дальнейшей работе алгоритм $\mathcal{A}$ осуществляет рекурсивные вызовы алгоритма $\mathcal{A}$ на других входных данных. Будем контролировать число таких вызовов, для чего заведём счётчик вызовов R, который сначала равен 0.
4) Если счётчик R стал равен $np(n^2)$, где p — полином из леммы 5, то останавливаем все рекурсивные вызовы и выдаём ответ «?».
5) Если $M = E$, то останавливаем все запущенные рекурсивные вызовы алгоритма $\mathcal{A}$ и выдаём ответ «ДА».
6) Для каждой матрицы M_i, $i = 1, \dots, n$, решаем матричное уравнение $M_i X = M$. Оно сводится к системе линейных уравнений, которое решаем методом Гаусса в рациональных числах. Если решение получается в натуральных числах, то делаем следующее:
   а) проверяем, был ли запущен рекурсивный вызов $\mathcal{A}(M_{i+1}, \dots, M_n, X)$ ранее;
   б) если нет, то запускаем рекурсивно алгоритм $\mathcal{A}$ на входе $(M_{i+1}, \dots, M_n, X)$ и увеличиваем счетчик рекурсивных вызовов: $R := R + 1$.

   Это делаем для каждого матричного уравнения $M_i X = M$, разрешимого в натуральных числах.

7) Если ни одна из этих систем неразрешима в натуральных числах, то останавливаем текущий рекурсивный вызов алгоритма $\mathcal{A}$ и выдаем ответ «НЕТ РЕШЕНИЯ НА ДАННОЙ ПОДЗАДАЧЕ».
8) Если все запущенные рекурсивные вызовы в какой-то момент остановились и выдали ответ «НЕТ РЕШЕНИЯ НА ДАННОЙ ПОДЗАДАЧЕ», то выдаём ответ «НЕТ».

Докажем полиномиальность алгоритма $\mathcal{A}$. Каждая вычислительная процедура (метод Гаусса, вычисление определителя), используемая внутри алгоритма, работает за полиномиальное время. Кроме того, число рекурсивных вызовов алгоритма $\mathcal{A}$ ограничено полиномиально — оно не превосходит $np(n^2)$, где p — полином из леммы 5.

Докажем теперь генеричность алгоритма $\mathcal{A}$. Из леммы 5 следует, что множество входов $(M_1, \ldots, M_n, M)$ проблемы суммы подмножеств размера n, в которых число решений матричного уравнения $M = XY$ в матрицах из $\mathcal{M}$ не превосходит $p(n^2)$, является генерическим. Заметим, что для любого такого входа $(M_1, \ldots, M_n, M)$ алгоритм $\mathcal{A}$ выдаст ответ, отличный от ответа «?». Для того чтобы убедиться в этом, оценим число возможных подзадач $(M_i, \ldots, M_n, M')$, для которых происходят рекурсивные вызовы алгоритма $\mathcal{A}$. Для всех матриц, кроме последней, имеется не более n вариантов выбора. Для матрицы M' всегда найдётся матрица X, такая, что $M = XM'$. Значит, число вариантов выбора матрицы M' не может быть больше числа решений матричного уравнения $M = XY$ в матрицах из $Mat(k, \omega)$, то есть, согласно лемме 5, $p(n^2)$. Итого получаем не более $np(n^2)$ вариантов для возможных подзадач $(M_i, \ldots, M_n, M')$. А так как в алгоритме счетчик числа рекурсивных вызовов ограничен как раз значением $np(n^2)$, то все эти рекурсивные вызовы происходят и соответствующие подзадачи решаются. Поэтому на таких входах алгоритм обязательно выдаёт ответ, отличный от «?». ■

ЛИТЕРАТУРА

1. *Karp R.* Reducibility among combinatorial problems // R. E. Miller and J. W. Thather (eds). Complexity of Computer Computations. IBM Research Symposia Ser. 1972. P. 85–103.
2. *Hellman M. and Merkle R.* Hiding information and signatures in trapdoor knapsacks // IEEE Trans. Inform. Theory. 1978. V. 24. No. 5. P. 525–530.
3. *Chor B. and Rivest R.* A knapsack-type public key cryptosystem based on arithmetic in finite fields // IEEE Trans. Inform. Theory. 1988. V. 34. No. 5. P. 901–909.
4. *Кузюрин Н. Н.* Полиномиальный в среднем алгоритм в целочисленном линейном программировании // Сибирский журнал исследования операций. 1994. Т. 1. № 3. С. 38–48.
5. *Miasnikov A., Nikolaev A., and Ushakov A.* Knapsack problems in groups // Math. Comput. 2015. V. 84. P. 987–1016.
6. *Blass A. and Gurevich Yu.* Matrix transformation is complete for the average case // SIAM J. Computing. 1995. V. 24. No. 1. P. 24–39.
7. *Gurevich Yu.* Matrix decomposition problem is complete for the average case // Proc. 31st Ann. Symp. Foundations of Computer Science. 1990. P. 802–811.
8. *Cai J., Fuchs W., Kozen D., and Liu Z.* Efficient average-case algorithms for the modular group // Proc. 35th Ann. Symp. Foundations of Computer Science. 1994. P. 143–152.
9. *Cai J. and Liu Z.* The bounded membership problem of the monoid $SL_2(N)$ // Math. Systems Theory. 1996. V. 29. P. 573–587.
10. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
11. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1982. 288 с.

12. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatshefte für Math. u. Phys. 1882. V. 3. P. 265–284.

REFERENCES

1. *Karp R.* Reducibility among combinatorial problems. R. E. Miller and J. W. Thather (eds.), Complexity of Computer Computations. IBM Research Symposia Ser., 1972, pp. 85–103.
2. *Hellman M. and Merkle R.* Hiding information and signatures in trapdoor knapsacks. IEEE Trans. Inform. Theory, 1978, vol. 24, no. 5, pp. 525–530.
3. *Chor B. and Rivest R.* A knapsack-type public key cryptosystem based on arithmetic in finite fields. IEEE Trans. Inform. Theory, 1988, vol. 34, no. 5, pp. 901–909.
4. *Kuzyurin N. N.* Polinomialnyi v srednem algoritm v tselochilennom lineinom programmirovanii [Polynomial on average algorithm in integer linear programming]. Sib. J. Operation Research, 1994, vol. 1, no. 3, pp. 38–48. (in Russian)
5. *Miasnikov A., Nikolaev A., and Ushakov A.* Knapsack problems in groups. Math. Comput., 2015, vol. 84, pp. 987–1016.
6. *Blass A. and Gurevich Yu.* Matrix transformation is complete for the average case. SIAM J. Computing, 1995, vol. 24, no. 1, pp. 24–39.
7. *Gurevich Yu.* Matrix decomposition problem is complete for the average case. Proc. 31st Ann. Symp. Foundations of Computer Science, 1990, pp. 802–811.
8. *Cai J., Fuchs W., Kozen D., and Liu Z.* Efficient average-case algorithms for the modular group. // Proc. 35th Ann. Symp. Foundations of Computer Science, 1994, pp. 143–152.
9. *Cai J. and Liu Z.* The bounded membership problem of the monoid $SL_2(N)$. Math. Systems Theory, 1996, vol. 29, pp. 573–587.
10. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
11. *Kargapolov M. I. and Merzlyakov Yu. I.* Osnovy teorii grupp [Elements of the Group Theory]. Moscow, Nauka Publ., 1982. 288 p. (in Russian)
12. *Zsigmondy K.* Zur Theorie der Potenzreste. Monatshefte für Math. u. Phys., 1882, vol. 3, pp. 265–284.