МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52 DOI 10.17223/20710410/55/7

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ВХОЖДЕНИЯ ДЛЯ ПОЛУГРУПП ЦЕЛОЧИСЛЕННЫХ МАТРИЦ[1]

А. Н. Рыбалов

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

E-mail: alexander.rybalov@gmail.com

Проблема вхождения в конечно порождённую подгруппу (подполугруппу) для групп (полугрупп) является классической алгоритмической проблемой в алгебре, активно изучаемой многие десятилетия. Уже для достаточно простых групп и полугрупп эта проблема становится неразрешимой. Например, К. А. Михайлова в 1966 г. доказала неразрешимость проблемы вхождения в конечно порождённые подгруппы и, следовательно, подполугруппы для прямого произведения $F_2 \times F_2$ двух свободных групп ранга 2. Так как по известной теореме Санова группа F_2 имеет точное представление целочисленными матрицами порядка 2, группа $F_2 \times F_2$ является подгруппой группы $\mathrm{GL}_4(\mathbb{Z})$ целочисленных матриц порядка 4. Отсюда легко следует неразрешимость рассматриваемой проблемы для группы $\mathrm{GL}_k(\mathbb{Z})$ при $k \geqslant 4$. Неразрешимость проблемы вхождения в подполугруппы полугрупп целочисленных матриц порядка $\geqslant 3$ следует из результата М. Патерсона 1970 г. В данной работе предлагается сильно генерический алгоритм, решающий проблему вхождения в подполугруппы полугрупп целочисленных матриц произвольного порядка для подмножества входов, последовательность относительных плотностей которого при увеличении размера экспоненциально быстро сходится к 1.

Ключевые слова: *генерическая сложность, проблема вхождения, полугруппа целочисленных матриц.*

GENERIC COMPLEXITY OF THE MEMBERSHIP PROBLEM FOR SEMIGROUPS OF INTEGER MATRICES

A. N. Rybalov

Sobolev Institute of Mathematics, Novosibirsk, Russia

The membership problem for finitely generated subgroups (subsemigroups) of groups (semigroups) is a classical algorithmic problem, actively studied for many decades. Already for sufficiently simple groups and semigroups, this problem becomes undecidable. For example, K. A. Mikhailova in 1966 proved the undecidability of the membership problem for finitely generated subgroups (hence and for subsemigroups) of a direct product $F_2 \times F_2$ of two free groups of rank 2. Since, by the well-known Sanov theorem, the group F_2 has an exact representation by integer matrices of order 2,

[1]Работа выполнена в рамках государственного задания ИМ СО РАН, проект FWNF-2022-0003.

the group $F_2 \times F_2$ is a subgroup of the group $\mathrm{GL}_4(\mathbb{Z})$ of integer matrices of order 4. It easily implies the undecidability of this problem for the group $\mathrm{GL}_k(\mathbb{Z})$ for $k \geqslant 4$. Undecidability of the membership problem for finitely generated subsemigroups of semigroups of integer matrices of order $\geqslant 3$ follows from Paterson's result proved in 1970. In this paper, we propose a strongly generic algorithm deciding the membership problem for semigroups of integer matrices of arbitrary order for inputs from a subset whose sequence of frequencies exponentially fast converges to 1 with increasing size.

Keywords: *generic complexity, membership problem, semigroups of integer matrices.*

Введение

Проблема вхождения в конечно порождённую подгруппу (подполугруппу) для групп (полугрупп) является классической алгоритмической проблемой в алгебре, особенно активно изучаемой с момента появления формализации понятия алгоритма. Как оказалось, уже для достаточно простых групп и полугрупп эта проблема становится неразрешимой. Например, К. А. Михайлова [1] доказала неразрешимость проблемы вхождения в конечно порождённые подгруппы и, следовательно, подполугруппы для прямого произведения $F_2 \times F_2$ двух свободных групп ранга 2. Так как по известной теореме Санова группа F_2 имеет точное представление целочисленными матрицами порядка 2, группа $F_2 \times F_2$ является подгруппой группы $\mathrm{GL}_4(\mathbb{Z})$ целочисленных матриц порядка 4. Отсюда легко следует неразрешимость рассматриваемой проблемы для группы $\mathrm{GL}_k(\mathbb{Z})$ при $k \geqslant 4$. Неразрешимость проблемы вхождения в подполугруппы полугрупп целочисленных матриц порядка $\geqslant 3$ следует из результата М. Патерсона [2] о неразрешимости более узкой проблемы проверки принадлежности нулевой матрицы заданной подполугруппе. В литературе эта проблема называется проблемой умирающих матриц [3]. Отметим, что для полугруппы целочисленных матриц порядка 2 разрешимость проблемы умирающих матриц и проблемы вхождения в подполугруппы до сих пор не установлена [3]. Также открыт вопрос о разрешимости проблемы вхождения в конечно порождённые подгруппы группы целочисленных матриц $\mathrm{GL}_3(\mathbb{Z})$.

Генерический подход [4] — это один из подходов к изучению алгоритмических проблем для «почти всех» входов. Исследования вычислительной сложности для «почти всех» входов началось в 1970–1980-х гг., после того как был выделен огромный пласт трудноразрешимых алгоритмических проблем — NP-полных проблем, для которых не удалось найти эффективных алгоритмов, работающих за полиномиальное время для всех входов. Оказалось, что если немного ослабить требование эффективности — рассматривать не все входы, а «почти все» или случайные входы, то иногда можно быстро решать задачу для таких типичных входов. Этот подход имеет практический смысл, когда алгоритм должен решать быстро задачу для случайных входных данных: если вероятность «наткнуться» на «плохой» вход пренебрежимо мала, то алгоритм будет быстро работать практически всегда. Ярким примером такого алгоритма является симплекс-метод: этот алгоритм имеет экспоненциальную сложность в худшем случае, но за полиномиальное время решает задачу линейного программирования для почти всех входных данных. Ещё можно упомянуть алгоритм Бабаи, Эрдеша и Селкова [5], решающий за полиномиальное время знаменитую проблему изоморфизма графов для почти всех пар конечных графов. Отметим также алгоритмы Гимади, Глебова, Перепелицы [6] и Селиверстова [7] для некоторых проблем дискретной оптимизации. В теории сложности вычислений поведение алгоритмов на множестве «почти всех» входов тра-

диционно изучается в рамках подхода к сложности в среднем [8, 9], при этом время работы алгоритма усредняется по всему множеству входных данных. В отличие от сложности в среднем, генерический подход является более универсальным, так как может оказаться, что на множестве «плохих» входов даже усреднённое время работы алгоритма неполиномиально. Генерический же алгоритм просто игнорирует эти входы. Более того, генерический подход применим и к алгоритмически неразрешимым проблемам. Таким образом, может оказаться, что проблема трудноразрешима или вообще неразрешима в классическом смысле, но легкоразрешима в генерическом смысле.

В работе [10] доказано, что проблема вхождения в конечно порождённые подполугруппы полугрупп целочисленных матриц произвольного порядка генерически разрешима. В данной работе этот результат усиливается: предлагается сильно генерический алгоритм, решающий проблему для входов из подмножества, последовательность относительных плотностей которого при увеличении размера экспоненциально быстро сходится к 1.

1. Генерические алгоритмы

Пусть I — некоторое множество входов. Для подмножества $S \subseteq I$ определим последовательность

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

где I_n — множество входов размера n; $S_n = S \cap I_n$ — множество входов из S размера n. Заметим, что $\rho_n(S)$ — это вероятность попасть в S при случайной и равновероятной генерации входов из I_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. Назовём множество S *сильно пренебрежимым*, если последовательность $\rho_n(S)$ экспоненциально быстро сходится к 0, т. е. существуют константы σ, $0 < \sigma < 1$, и $C > 0$, такие, что для любого n

$$\rho_n(S) < C\sigma^n.$$

Множество S называется *сильно генерическим*, если его дополнение $\overline{S}$ сильно пренебрежимо.

Алгоритм $\mathcal{A}$ с множеством входов I называется (*сильно*) *генерическим*, если множество $\{x \in I : \mathcal{A}(x)\downarrow\}$ (сильно) генерическое. Здесь через $\mathcal{A}(x)\downarrow$ обозначается тот факт, что алгоритм $\mathcal{A}$ останавливается на входе x. (Сильно) генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если

$$\forall x \in I\ \mathcal{A}(x)\downarrow \Rightarrow\ f(x) = \mathcal{A}(x).$$

(Сильно) генерический алгоритм $\mathcal{A}$ работает за полиномиальное время, если существует полином $p(n)$, такой, что

$$\forall x \in I\ \mathcal{A}(x)\downarrow \Rightarrow t_{\mathcal{A}}(x) < p(\mathrm{size}(x)).$$

Такие алгоритмы будем называть полиномиальными генерическими.

С практической точки зрения, когда требуется построить алгоритм, решающий конкретную алгоритмическую проблему для почти всех входов, удобнее рассматривать алгоритмы следующего типа: алгоритм останавливается на всех входах, на входах из некоторого генерического множества выдаёт правильный ответ, а на пренебрежимом множестве остальных входов выдает специальный ответ «?» — «Не знаю». Определение такой эффективной генерической вычислимости можно найти в обзоре [11] и в гораздо более ранней работе [12].

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

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

Эффективно (сильно) генерический алгоритм $\mathcal{A}$ вычисляет функцию $f : I \to J$, если

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

Множество $S \subseteq I$ и соответствующая проблема распознавания (S, I) (*эффективно*) (*сильно*) *генерически разрешимы*, если существует (эффективно) (сильно) генерический алгоритм, вычисляющий характеристическую функцию S.

Легко видеть, что из эффективной генерической разрешимости следует генерическая разрешимость. Действительно, любой эффективно генерический алгоритм можно переделать в генерический, заменив выдачу ответа «?» на бесконечное зацикливание. В обратную сторону это неверно — см., например, теорему 2.22 и следствие 2.24 в [13]. Однако для полиномиальной (экспоненциальной) сложности верно и обратное: из полиномиальной (экспоненциальной) генерической разрешимости следует полиномиальная (экспоненциальная) эффективная генерическая разрешимость. Действительно, если имеется полиномиальная оценка $p(n)$ на время работы генерического алгоритма, когда он останавливается, то можно завести счётчик T числа шагов и в случае, если $T > p(n)$, можно обрывать вычисление и выдавать ответ «?» — алгоритм уже не остановится. Таким образом получается эффективно генерический полиномиальный алгоритм, решающий ту же проблему. То же верно и для сильно генерических алгоритмов.

С учётом сказанного в дальнейшем при доказательстве существования (сильно) генерического алгоритма будем строить эффективно (сильно) генерические алгоритмы. Из существования эффективного (сильно) генерического алгоритма будет следовать существование (сильно) генерического алгоритма.

2. Вспомогательный результат

Пусть $\mathrm{M}_k(\mathbb{Z})$ — полугруппа целочисленных матриц порядка k по стандартному умножению матриц. Элементы $\mathrm{M}_k(\mathbb{Z})$ будем представлять матрицами из целых чисел. Размер целого числа a, обозначаемый $\mathrm{size}(a)$, — это длина двоичной записи его модуля. Таким образом, $\mathrm{size}(a) = n$, если $2^{n-1} \leqslant |a| < 2^n$. Отдельно положим $\mathrm{size}(0) = 0$. Под размером матрицы $M = ||a_{ij}||$ будем понимать

$$\mathrm{size}(M) = \max\{\mathrm{size}(a_{ij}) : i, j = 1, \ldots, k\}.$$

Таким образом, если матрица M имеет размер n, то каждый её элемент лежит в отрезке $[-2^n + 1, 2^n - 1]$ и для него возможны $2^{n+1} - 1$ вариантов выбора.

Обозначим через $\mathrm{M}_k^r(\mathbb{Z})$ подмножество матриц в $\mathrm{M}_k(\mathbb{Z})$ с определителем, равным r.

Лемма 1. Пусть r равно 0, 1 или -1. Тогда для любого достаточно большого n имеет место оценка

$$\frac{|\mathrm{M}_k^r(\mathbb{Z})_{\leqslant n}|}{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n}|} \leqslant \frac{1}{2^n}.$$

Доказательство. Напомним лемму Шварца — Зиппеля [14–16]. Она утверждает, что если $P(x_1, x_2, \ldots, x_n)$ — ненулевой многочлен степени d над полем $\mathbb{R}$, S — конечное подмножество $\mathbb{R}$ и элементы $r_1, r_2, \ldots, r_n$ выбраны из S равномерно и независимо друг от друга, то

$$\mathsf{P}[P(r_1, r_2, \ldots, r_n) = 0] \leqslant \frac{d}{|S|}.$$

Заметим, что если положить

$$P(x_1, \ldots, x_{n^2}) = \det \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{n+1} & x_{n+2} & \ldots & x_{2n} \\ \ldots & & & \\ x_{n^2-n+1} & x_{n^2-n+2} & \ldots & x_{n^2} \end{pmatrix} - r,$$

то будет иметь место

$$\frac{|\mathrm{M}_k^r(\mathbb{Z})_{\leqslant n}|}{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n}|} = \mathsf{P}[P(r_1, r_2, \ldots, r_{n^2}) = 0],$$

где элементы $r_1, \ldots, r_{n^2}$ равновероятно и независимо друг от друга выбраны из множества $S = \{-2^n + 1, \ldots, 2^n - 1\}$. Учитывая, что степень многочлена $P(x_1, \ldots, x_{n^2})$ по любой переменной равна 1, по лемме Шварца — Зиппеля получаем

$$\frac{|\mathrm{M}_k^r(\mathbb{Z})_{\leqslant n}|}{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n}|} \leqslant \frac{1}{|S|} = \frac{1}{2^{n+1} - 1} \leqslant \frac{1}{2^n}.$$

Лемма 1 доказана. ■

3. Основной результат

Проблема вхождения для полугруппы $\mathrm{M}_k(\mathbb{Z})$ формулируется следующим образом. По произвольным заданным матрицам $M_1, \ldots, M_n, M$ из $\mathrm{M}_k(\mathbb{Z})$, таким, что $\mathrm{size}(M_1), \ldots, \mathrm{size}(M_n), \mathrm{size}(M) \leqslant n$, определить, принадлежит ли матрица M подполугруппе, порождённой матрицами $M_1, \ldots, M_n$. Другими словами, представима ли матрица M в виде некоторого произведения матриц из набора $M_1, \ldots, M_n$, возможно, с повторами? Размером входа здесь является число n.

Теорема 1. Проблема вхождения для $\mathrm{M}_k(\mathbb{Z})$ сильно генерически разрешима.

Доказательство. Эффективный сильно генерический алгоритм для проблемы вхождения работает на входе $(M_1, \ldots, M_n, M)$ размера n следующим образом:

1. Вычисляет определители $\det(M_1), \ldots, \det(M_n), \det(M)$.
2. Если среди $\det(M_1), \ldots, \det(M_n), \det(M)$ найдётся определитель, равный 0, 1 или -1, выдаёт ответ «?».
3. Иначе перебирает всевозможные наборы матриц $M_{i_1}, \ldots, M_{i_k}$, такие, что $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $\det(M_{i_1}) \ldots \det(M_{i_k}) = \det(M)$, и проверяет, выполнено ли равенство $M_{i_1} \ldots M_{i_k} = M$. Если равенство получилось, выдаёт ответ «ДА», иначе — ответ «НЕТ».

Заметим, что этот алгоритм всегда останавливается, так как число матриц в тестируемых наборах ограничено числом целых делителей $\det(M)$, отличных от 1 и -1.

Для доказательства эффективной сильной генеричности алгоритма нужно показать, что множество входов S, на котором алгоритм выдаёт ответ, отличный от «?», является сильно генерическим. Заметим, что

$$S_n = \{(M_1, \ldots, M_n, M) : \operatorname{size}(M_i) \leqslant n, \operatorname{size}(M) \leqslant n, \det(M_i) \neq 0, 1, -1,\ i = 1, \ldots, n\} = \\ = \Big(\mathrm{M}_k(\mathbb{Z})_{\leqslant n} \setminus \big(\mathrm{M}_k^0(\mathbb{Z})_{\leqslant n} \cup \mathrm{M}_k^1(\mathbb{Z})_{\leqslant n} \cup \mathrm{M}_k^{-1}(\mathbb{Z})_{\leqslant n}\big)\Big)^n \times \mathrm{M}_k(\mathbb{Z})_{\leqslant n}.$$

Пусть I — множество всех входов. Тогда $I_n = (\mathrm{M}_k(\mathbb{Z})_{\leqslant n})^{n+1}$. Поэтому

$$\rho_n(S) = \frac{|S_n|}{|I_n|} = \Big(\frac{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n} \setminus \big(\mathrm{M}_k^0(\mathbb{Z})_{\leqslant n} \cup \mathrm{M}_k^1(\mathbb{Z})_{\leqslant n} \cup \mathrm{M}_k^{-1}(\mathbb{Z})_{\leqslant n}|}{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n}|}\Big)^n = \\ = \Big(1 - \frac{|\mathrm{M}_k^0(\mathbb{Z})_{\leqslant n}|}{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n}|} - \frac{|\mathrm{M}_k^1(\mathbb{Z})_{\leqslant n}|}{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n}|} - \frac{|\mathrm{M}_k^{-1}(\mathbb{Z})_{\leqslant n}|}{|\mathrm{M}_k(\mathbb{Z})_{\leqslant n}|}\Big)^n.$$

По лемме 1 можно оценить

$$\rho_n(S) \geqslant \Big(1 - \frac{3}{2^n}\Big)^n = \left(\Big(1 - \frac{3}{2^n}\Big)^{2^n}\right)^{n/2^n} > e^{-3n/2^n} > 1 - \frac{3n}{2^n}$$

для достаточно больших n. Последнее выражение экспоненциально быстро стремится к 1 при стремлении n к бесконечности, следовательно, множество S сильно генерическое. ■

Автор выражает благодарность рецензенту за полезные замечания и предложения по улучшению текста статьи.

ЛИТЕРАТУРА

1. *Михайлова К. А.* Проблема вхождения для прямых произведений групп // Математический сборник. 1966. Т. 112. № 2. С. 241–251.
2. *Paterson M. S.* Unsolvability in 3×3 matrices // Studies Appl. Math. 1970. V. 49. No. 1. P. 105–107.
3. *Halava V. and Harju T.* Mortality in matrix semigroups // Amer. Math. Monthly. 2001. V. 108. No. 7. P. 649–653.
4. *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.
5. *Babai L., Erdos P, and Selkow S.* Random graph isomorphism // SIAM J. Computing. 1980. V. 9. No. 3. P. 628–635.
6. *Гимади Э. Х., Глебов Н. И., Перепелица В. А.* Алгоритмы с оценками для задач дискретной оптимизации // Проблемы кибернетики. 1975. Т. 31. С. 35–42.
7. *Селиверстов А.В.* Двоичные решения для больших систем линейных уравнений // Прикладная дискретная математика. 2021. № 52. С. 5–15.
8. *Gurevich Y.* Average case completeness // J. Computer System Sci. 1991. V. 42. P. 346–398.
9. *Levin L.* Average case complete problems // SIAM J. Computing. 1987. V. 15. P. 285–286.
10. *Рыбалов А.* Генерический алгоритм для проблемы вхождения в полугруппах целочисленных матриц // Вестник Омского университета. 2020. Т. 25. № 3. С. 8–12.
11. *Hirschfeldt D.* Some questions in computable mathematics // Computability and Complexity. 2017. P. 22–55.

12. *Meyer A.* An open problem on creative sets // Recursive Function Theory Newsletter. 1973. V. 4. P. 15–16.
13. *Jockusch C. and Schupp P.* Generic computability, Turing degrees, and asymptotic density // J. London Math. Soc. 2012. V. 85. No. 2. P. 472–490.
14. *Schwartz J.* Fast probabilistic algorithms for verification of polynomial identities // J. ACM. 1980. V. 27. No. 4. P. 701–717.
15. *Zippel R.* Probabilistic algorithms for sparse polynomials // Symbolic Algebraic Computation. 1979. V. 72. P. 216–226.
16. *DeMillo R. and Lipton R.* A probabilistic remark on algebraic program testing // Inform. Processing Lett. 1978. V. 7. P. 193–195.

REFERENCES

1. *Mikhaylova K. A.* Problema vkhozhdeniya dlya pryamykh proizvedeniy grupp [Membership problem for direct products of groups]. Matematicheskiy Sbornik, 1966, vol. 112, no. 2, pp. 241–251. (in Russian)
2. *Paterson M.S.* Unsolvability in 3×3 matrices. Studies Appl. Math., 1970, vol. 49, no. 1, pp. 105–107.
3. *Halava V. and Harju T.* Mortality in matrix semigroups. Amer. Math. Monthly, 2001, vol. 108, no. 7, pp. 649–653.
4. *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.
5. *Babai L., Erdos P, and Selkow S.* Random graph isomorphism. SIAM J. Computing, 1980, vol. 9, no. 3, pp. 628–635.
6. *Gimadi E. X., Glebov N. I., and Perepelitsa V. A.* Algoritmy s otsenkami dlya zadach diskretnoy optimizatsii [Algorithms with bounds for problems of discrete optimization]. Problemy Kibernetiki, 1975, vol. 31, pp. 35–42. (in Russian)
7. *Seliverstov A. V.* Dvoichnye resheniya dlya bol'shikh sistem lineynykh uravneniy [Binary solutions to large systems of linear equations]. Prikladnaya Diskretnaya Matematika, 2021, no. 52, pp. 5–15. (in Russian)
8. *Gurevich Y.* Average case completeness. J. Computer System Sci., 1991, vol. 42, pp. 346–398.
9. *Levin L.* Average case complete problems. SIAM J. Computing, 1987, vol. 15, pp. 285–286.
10. *Rybalov A.* Generichеskii algoritm dlya problemy vhozhdeniya v polugruppah celochislennyh matrits [A generic algorithm for the membership problem in semigroups of integer matrices] // Vestnik Omskogo universiteta. 2020. V. 25. № 3. P. 8–12.
11. *Hirschfeldt D.* Some questions in computable mathematics. Computability and Complexity, 2017, pp. 22–55.
12. *Meyer A.* An open problem on creative sets. Recursive Function Theory Newsletter, 1973, vol. 4, pp. 15–16.
13. *Jockusch C. and Schupp P.* Generic computability, Turing degrees, and asymptotic density. J. London Math. Soc., 2012, vol. 85, no. 2, pp. 472–490.
14. *Schwartz J.* Fast probabilistic algorithms for verification of polynomial identities. J. ACM, 1980, vol. 27, no. 4, pp. 701–717.
15. *Zippel R.* Probabilistic algorithms for sparse polynomials. Symbolic Algebraic Computation, 1979, vol. 72, pp. 216–226.
16. *DeMillo R. and Lipton R.* A probabilistic remark on algebraic program testing. Inform. Processing Lett., 1978, vol. 7, pp. 193–195.