Записки научных
семинаров ПОМИ
Том 292, 2002 г.

А. Л. Чистов

МОНОДРОМИЯ И КРИТЕРИИ НЕПРИВОДИМОСТИ С АЛГОРИТМИЧЕСКИМИ ПРИЛОЖЕНИЯМИ В НУЛЕВОЙ ХАРАКТЕРИСТИКЕ

Введение

Пусть k – поле нулевой характеристики с алгебраическим замыканием $\overline{k}$. Обозначим через $\mathbb{P}^n(\overline{k})$, $n \geqslant 0$, проективное пространство над полем $\overline{k}$ с координатами $X_0, \dots, X_n$. Мы будем предполагать, что $\mathbb{P}^n(\overline{k})$ определено над k. Для произвольных однородных многочленов $g_1, \dots, g_m \in \overline{k}[X_0, \dots, X_n]$ мы будем обозначать через $\mathcal{Z}(g_1, \dots, g_m)$ множество всех общих нулей многочленов $g_1, \dots, g_m$ в $\mathbb{P}^n(\overline{k})$. Аналогичные обозначения будут использоваться для множеств нулей идеалов и многочленов с другими полями коэффициентов в аффинных и проективных пространствах (это будет видно из контекста).

В алгоритмической части статьи мы будем предполагать, что поле k является конечнопорожденным над полем рациональных чисел $\mathbb{Q}$. Пусть V – проективное алгебраическое многообразие, которое является множеством всех общих нулей семейства однородных многочленов от $n+1$ переменных степеней меньше d с коэффициентами из k. Пусть теперь $z_1, \dots, z_u \in V$ – произвольные точки. Мы построим алгоритм, который выясняет, принадлежат ли $z_1, \dots, z_u$ одной и той же неприводимой компоненте, определенной над k (соответственно $\overline{k}$), многообразия V, со временем работы, полиномиальным от d^n и длины записи входных данных (соответственно с тем же самым временем работы для фиксированного u), см. теорему 2. Кроме того, мы строим линейные формы $L_1, \dots, L_{n-1}$ от $X_0, \dots, X_n$ с целыми коэффициентами с длинами записи $O(n \log d)$, такие, что для всякого $0 \leqslant s \leqslant n$ и для всякой неприводимой над $\overline{k}$ компоненты W многообразия V размерности $\dim W = n - s$ пересечение $W \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$ трансверсально и является неприводимой над $\overline{k}$ проективной кривой, см. теорему 1.

Отметим, что даже существование требуемых линейных форм $L_1, \ldots, L_{n-1}$ с длинами записей целых коэффициентов $O(n \log d)$ нетривиально. В алгоритмах этой статьи мы существенно используем результаты работы [4]. Мы применяем также первую теорему Бертини, см. [1]. С другой стороны, для обоснования алгоритма нам потребовалось, как и в [5]), привлечь методы теории аналитических функций, а именно, группу монодромии алгебраической функции (в [5] мы использовали эти методы не только для доказательства корректности алгоритма, но и в самом алгоритме), см. теорему 3 раздела 1. Из следствия 2 этой теоремы мы получаем следующий красивый результат (основной случай здесь $n \geqslant 3$).

Критерий неприводимости. *Пусть $\Phi \in k[X_0, \ldots, X_n]$, $n \geqslant 1$ – сепарабельный однородный многочлен над полем нулевой характеристики. Пусть $\deg\Phi = \deg_{X_0}\Phi \geqslant 1$. Пусть R – дискриминант многочлена Φ относительно X_0, а R_0 – бесквадратная часть многочлена R (то есть R_0 – сепарабельный многочлен наибольшей степени, делящий R). Пусть L – ненулевая линейная форма от $X_1, \ldots, X_n$ с коэффициентами из k и $A = k[X_0, \ldots, X_n]/(L)$ (таким образом, A изоморфно кольцу многочленов от n переменных). Предположим, что многочлен $R_0 \bmod L \in A$ сепарабелен. Тогда неприводимые над k множители многочленов Φ и $\Phi \bmod L \in A$ находятся во взаимно однозначном соответствии по правилу $\Psi \mapsto \Psi \bmod L$. В частности, если Φ неприводим над k, то и $\Phi \bmod L$ неприводим над k. Кроме того, для всякого линейного подпространства $\mathcal{L}$ линейных форм от $X_1, \ldots, X_n$ размерности $\dim\mathcal{L} \geqslant 3$ существует форма $L \in \mathcal{L}$, удовлетворяющая сформулированным условиям.*

Этот критерий и следствие 2 проясняют важный случай теоремы Бертини. В одной из следующих статей мы вернемся к общему случаю первой теоремы Бертини с алгоритмической точки зрения. Результаты настоящей статьи, а именно теорема 1, будут при этом использоваться существенным образом. В следующей статье нам потребуется доказать более общую версию теоремы 3. Хотя она может быть приведена уже сейчас, мы решили сделать изложение более прозрачным и опустить подробности, относящиеся к случаю неконечных морфизмов.

Мы оставляем читателю вывести следствия данного критерия для неоднородных многочленов. Интересно доказать также аналоги этого критерия для ненулевой характеристики с произвольным n и для неоднородных многочленов с целыми коэффициентами с малыми n.

В работе [6] мы предложили новый метод представления алгебраических многообразий, основанный на системах представителей точек неприводимых компонент. Настоящая статья является важным шагом на пути построения алгоритмов для этого метода в нулевой характеристике.

Перейдем к точным формулировкам. Пусть даны однородные многочлены $f_1, \dots, f_m \in k[X_0, \dots, X_n]$, $n \geqslant 1$, $m \geqslant 1$. Рассмотрим замкнутое алгебраическое множество или алгебраическое многообразие (в данной статье мы не различаем эти понятия)

$$V = \{(x_0 : \dots : x_n) \in \mathbb{P}^n(\overline{k}) \,:\, f_i(x_0, \dots, x_n) = 0,\ x_i \in \overline{k},\ \forall 1 \leqslant i \leqslant m\}.$$

Это множество всех общих нулей многочленов $f_1, \dots, f_m$ в $\mathbb{P}^n(\overline{k})$. Следовательно, $V = \mathcal{Z}(f_1, \dots, f_m)$.

Пусть теперь $k = \mathbb{Q}(t_1, \dots, t_l, \theta)$, где $t_1, \dots, t_l$ алгебраически независимы над $\mathbb{Q}$ и θ – алгебраический над $\mathbb{Q}(t_1, \dots, t_l)$ элемент с минимальным многочленом $F \in \mathbb{Q}[t_1, \dots, t_l, Z]$. Старший коэффициент $\mathrm{lc}_Z F$ многочлена F равен 1. Каждый многочлен $f = f_i$ будем представлять в виде

$$f = \frac{1}{a_0} \sum_{i_0, \dots, i_n} \sum_{0 \le j < \deg_Z F} a_{i_0, \dots, i_n, j} \theta^j X_0^{i_0} \cdots X_n^{i_n}\,,$$

где $a_0, a_{i_0, \dots, i_n, j} \in \mathbb{Z}[t_1, \dots, t_l]$, $\gcd_{i_0, \dots, i_n, j}(a_0, a_{i_0, \dots, i_n, j}) = 1$. Определим длину записи $l(a)$ целого числа a формулой $l(a) = \min\{s \in \mathbb{Z} :: |a| < 2^{s-1}\}$. Длина записи коэффициентов $l(f)$ многочлена f определяется как максимум длин записи целых коэффициентов многочленов $a_0, a_{i_0, \dots, i_n, j}$, а его степень $\deg_{t_\gamma}(f)$ – как

$$\deg_{t_\gamma}(f) = \max_{i_0, \dots, i_n, j} \{\deg_{t_\gamma}(a_0), \deg_{t_\gamma}(a_{i_0, \dots, i_n, j})\}\,,$$

где $1 \le \gamma \le l$. Аналогичным образом определяются $\deg_{t_\gamma} F$ и $l(F)$. Мы будем предполагать, что имеются следующие оценки:

$$\deg_{X_0, \dots, X_n}(f_i) < d,\ \deg_{t_\gamma}(f_i) < d_2,\ l(f_i) < M,$$
$$\deg_Z(F) < d_1,\ \deg_{t_\gamma}(F) < d_1,\ l(F) < M_1\ .$$

Размер (или длина записи) $L(f)$ многочлена f определяется как произведение длины записи коэффициентов $l(f)$ на число всех целых коэффициентов многочлена f в плотном представлении. Имеем

$$L(f_i) < (\binom{d+n}{n} d_1 + 1) d_2^l M.$$

Аналогично $L(F) < d_1^{l+1} M_1$. В дальнейшем, если не оговорено противное, мы будем считать, что l фиксировано.

Мы будем представлять точку $z \in V$ с координатами из конечного расширения поля k следующим образом. Известен индекс $0 \leqslant i_0 \leqslant n$, такой, что $X_{i_0}(z) \neq 0$, и задан изоморфизм полей

$$k(z) = k((X_1/X_{i_0})(z), \dots, (X_n/X_{i_0})(z)) \simeq k[\eta] = k[Z]/(F_z), \qquad (1)$$

причем $\sum_{0 \leqslant i \leqslant n} c_i (X_i/X_{i_0})(z) \mapsto \eta$ под действием изоморфизма (1), коэффициенты $c_i \in \mathbb{Z}$ заданы и $F_z \in k[Z]$ – минимальный многочлен элемента η над полем k со старшим коэффициентом $\mathrm{lc}_Z F_z = 1$. Таким образом, точка z определена с точностью до сопряжения над k. Более точно, представление (1) задает определенное над k и неприводимое над k алгебраическое многообразие размерности 0.

Пусть $a \in k[\eta]$ – произвольный элемент. Тогда $a = A(\eta)$ для однозначно определенного многочлена $A \in k[Z]$, такого, что $\deg_Z A < \deg_Z F_z$. Длина записи целых коэффициентов $l(a)$, длина записи $L(a)$ и степени $\deg_{t_\alpha} a$, $1 \leqslant \alpha \leqslant l$, элемента a определены формулами

$$l(a) = l(A), \quad L(a) = L(A), \quad \deg_{t_\alpha} a = \deg_{t_\alpha} A.$$

Определим длину записи $L(z)$ точки z как $L(F_z) + \sum\limits_{0 \leqslant i \leqslant n} L(X_i/X_{i_0})$. Используя алгоритм из работы [3], можно построить систему однородных полиномиальных уравнениий с коэффициентами из k, задающую наименьшее определенное над k и неприводимое над k алгебраическое многообразие размерности 0, содержащее z, за время, полиномиальное от $L(z)$.

Пусть $W_1, W_2 \subset \mathbb{P}^n(\overline{k})$ (соответственно $W_1, W_2 \subset \mathbb{A}^n(\overline{k})$) – два проективных (соответственно аффинных) алгебраических многообразия. Предположим, что все неприводимые компоненты многообразия W_i имеют одну и ту же размерность $n - s_i$, $i = 1, 2$. Пусть W_3 – неприводимая компонента многообразия $W_1 \cap W_2$. Мы будем говорить, что пересечение $W_1 \cap W_2$ трансверсально в W_3 тогда и только тогда, когда $\dim W_3 = n - s_1 - s_2$ и существует точка $x \in W_3$, такая, что x – гладкая точка каждого W_i, $i = 1, 2$, и пересечение касательных пространств $T_{x,W_1} \cap T_{x,W_2}$ многообразий W_1 и W_2 в точке x трансверсально, то есть $\dim(T_{x,W_1} \cap T_{x,W_2}) = n - s_1 - s_2$. Мы будем говорить, что пересечение $W_1 \cap W_2$ трансверсально тогда и только тогда, когда оно трансверсально в каждой своей компоненте. Аналогичным образом определяется трансверсальность для пересечения конечного числа равноразмерностных алгебраических многообразий.

Теорема 1. *Пусть заданы, как и выше, поле k, алгебраическое многообразие V и многочлены F, $f_1, \dots, f_m$. Тогда можно построить линейные формы $L_0, L_1, \dots, L_{n+1}$ от $X_0, \dots, X_n$ с целыми коэффициентами с длинами записи $O(n \log d)$ и конечные определенные над k множества A_s, $V_{s,0}$, $0 \leqslant s \leqslant n$, точек многообразия V, удовлетворяющие следующим свойствам. Для всякого $0 \leqslant s \leqslant n$ обозначим через V_s объединение всех неприводимых компонент размерности $n - s$ многообразия V.*

(a) *Тогда для всякого $0 \leqslant s \leqslant n$ множество $A_s = V_s \cap \mathcal{Z}(L_{s+1}, \dots, L_n)$ конечно (или пусто, если $V_s = \emptyset$), состоит из гладких точек многообразия V и пересечения касательных пространств V_s и $\mathcal{Z}(L_{s+1}, \dots, L_n)$ во всех этих точках трансверсальны. Линейная форма L_0 не обращается в нуль ни в какой точке из A_s, то есть $0 \notin L_0(A_s)$, и $\#L_{n+1}(A_s) = \#A_s = \deg V_s$.*

(b) *Для всякого $0 \leqslant s \leqslant n - 1$ (случай $s = n - 1$ тривиален) неприводимые над $\overline{k}$ (соответственно над k) компоненты алгебраических многообразий V_s и $V_s \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$ находятся во взаимно однозначном соответствии по правилу $W \mapsto W \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$. Последнее пересечение является неприводимой над $\overline{k}$ (соответственно над k) кривой. Кроме того, если W неприводимо над $\overline{k}$, то минимальные поля определения многообразий W и $W \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$, содержащие k, совпадают.*

(c) *Для всякого $0 \leqslant s \leqslant n - 1$ обозначим через $\Phi_s \in k[L_0, L_{s+1}, L_{s+2}, \dots, L_{n+1}] = B_s$ (здесь все L_j рассматриваются как переменные) ненулевой сепарабельный многочлен минимальной степени, такой, что Φ_s обращается в нуль тождественно на V_s. Обозначим через R_s дискриминант многочлена Φ_s относительно L_{n+1} и через $R_{s,0}$ – бесквадратную часть многочлена R_s (то есть $R_{s,0}$ – сепара-*

бельный многочлен наибольшей степени, делящий R_s). Тогда $\deg_{L_{n+1}}\Phi_s = \deg\Phi_s = \deg V_s$ и многочлен

$$R_{s,0} \bmod (L_{s+1}, \ldots, L_{n-1}) \in B_s/(L_{s+1}, \ldots, L_{n-1})$$

является ненулевым сепарабельным. Мы выбираем и фиксируем Φ_s таким образом, что старший коэффициент Φ_s относительно L_{n+1} равен 1.

(d) *Для всякого $0 \leqslant s \leqslant n$ неприводимые над k компоненты алгебраических многообразий V_s и $V_{s,0}$ находятся во взаимно однозначном соответствии по правилу $W \mapsto W \cap V_{s,0}$. Кроме того, $V_{s,0} \subset A_s$ и $V_{n,0} = A_n = V_n$.*

(e) *Для всякого $0 \leqslant s \leqslant n-1$ и для всякой точки $z \in V_{s,0}$ строится представление (1). Обозначим через W_z однозначно определенную неприводимую над $\overline{k}$ компоненту V, такую, что $z \in W_z$, и обозначим через $k_z \supset k$ минимальное поле определения компоненты W_z. Тогда $k(z) \supset k_z$ и поле k_z строится алгоритмом. Оно задано своим базисом и таблицей умножения. Две точки из $V_{s,0}$ принадлежат W_z тогда и только тогда, когда они сопряжены элементу z над k_z. Следовательно, можно легко определить систему представителей (мы не строим ее) $V'_{s,0} \subset V_{s,0}$ точек неприводимых над $\overline{k}$ компонент многообразия V_s. Если $a \subset V_{s,0}$ – произвольная определенная над k и неприводимая над k компонента и $z \in a$, то $V'_{s,0} \cap a$ состоит из $[k_z : k]$ точек.*

Алгоритм для построения линейных форм $L_0, L_1, \ldots, L_{n+1}$, конечных множеств A_s, $V_{s,0}$, $0 \leqslant s \leqslant n$, и всех полей $k_z \subset k(z)$, $z \in V_{s,0}$, является полиномиальным от d^n, d_1, d_2, M, M_1 и m. Отметим, что для всякой точки $z \in A_s$ в представлении (1), полученном алгоритмом, $\deg_Z F_z \leqslant \deg V_n \leqslant d^n$ согласно теореме Безу.

В следующей теореме заданы u точек $z_1, \ldots, z_u \in V$. Именно, мы заменяем в представлении (1) z, η, F_z на z_i, η_i, F_{z_i} и получаем представление для z_i, $1 \leqslant i \leqslant u$. Кроме того, в утверждении (b) этой теоремы мы будем предполагать, что композит полей $k[\eta_1, \ldots, \eta_u]$ задан явно (базисом и таблицей умножения над k). Здесь следует зафиксировать u точек и, следовательно, задать не только точки $z_1, \ldots, z_u$, но также и наборы из u точек $(z_1, \ldots, z_u)$, однозначно с точностью до сопряжения над k. Заметим, что можно построить все возможные композиты полей $k[\eta_i]$, $1 \leqslant i \leqslant u$, над полем k за время, полиномиальное от

$L(z_1), \dots, L(z_2)$ и $\prod_{1 \leqslant i \leqslant u} \deg F_{z_i}$, см. [3]. При этом длина записи базиса и таблицы умножения любого построенного композита полиномиальна от сумм длин записи базисов и таблиц умножения полей $k[\eta_i]$, $1 \leqslant i \leqslant u$, и степени расширения этого композита над k. В дальнейшем мы будем считать, что эта оценка всегда справедлива для данного нам представления композита $k[\eta_1, \dots, \eta_u]$.

Теорема 2. *Пусть, как и выше, заданы поле k, алгебраическое многообразие V и многочлены F, $f_1, \dots, f_m$. Пусть даны $u \geqslant 2$ точек $z_1, \dots, z_u \in V$.*

(a) *Тогда для всякого $0 \leqslant s \leqslant n-1$ можно вычислить количество неприводимых над k компонент W многообразия V с размерностью $\dim W = n - s$, таких, что $z_i \in W$ для всех $1 \leqslant i \leqslant u$. Время работы этого алгоритма полиномиально от d^n, d_1, d_2, M, M_1, m и суммы длин записи $\sum_{1 \leqslant i \leqslant u} L(z_i)$ точек z_i, $1 \leqslant i \leqslant u$.*

(b) *Предположим, что задан композит полей $k[\eta_1, \dots, \eta_u]$. Тогда для всякого $0 \leqslant s \leqslant n-1$ можно вычислить количество неприводимых над $\overline{k}$ компонент W многообразия V с размерностью $\dim W = n - s$, таких, что $z_i \in W$ для всех $1 \leqslant i \leqslant u$. Время работы этого алгоритма полиномиально от d^n, d_1, d_2, M, M_1, m, суммы длин записи $\sum_{1 \leqslant i \leqslant u} L(z_i)$, точек z_i, $1 \leqslant i \leqslant u$, и степени $[k[\eta_1, \dots, \eta_u] : k]$ расширения поля.*

Замечание 1. Теоремы 1 и 2 тривиальны при $s = 0$: можно взять $L_i = X_i$, $0 \leqslant i \leqslant n$, и $L_{n+1} = X_n$ для $s = 0$. Так что в дальнейшем мы будем предполагать без ограничения общности, что многочлены $f_1, \dots, f_m$ линейно независимы над k. Таким образом, $\dim V \leqslant n - 1$, и мы будем считать, не умаляя общности, что $1 \leqslant s$ в условиях Теорем 1 и 2.

1. Монодромия и неприводимость

Пусть $n \geqslant 1$ и $1 \leqslant s \leqslant n$ – целые числа. Пусть k – произвольное поле нулевой характеристики, V_s – определенное над k проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$ и все неприводимые компоненты V_s имеют одну и ту же размерность $n - s$. Предположим, что $\deg V_s = D \geqslant 1$ (здесь и далее D зависит от s). Пусть $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$ – линейные формы от $X_0, \dots, X_n$ с коэффициентами из k. Пусть

$$A^{(s)} = V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_n) \,\&\, 0 \notin T_0(A^{(s)}) \\ \& \,\#(T_{n+1}/T_0)(A^{(s)}) = \deg V_s, \tag{2}$$

где пересечение рассматривается в $\mathbb{P}^n(\overline{k})$ и $\#$ обозначает число элементов множества. В частности, $\#A^{(s)} = D$, и пересечение $V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_n)$ трансверсально в каждой точке по теореме Безу.

Рассмотрим морфизмы

$$p : V_s \to \mathbb{P}^{n-s}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (T_0 : T_{s+1} : T_{s+2} : \ldots : T_n), \tag{3}$$

$$V_s \to \mathbb{P}^{n-s+1}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (T_0 : T_{s+1} : T_{s+2} : \ldots : T_{n+1}). \tag{4}$$

Мы будем предполагать, что $T_0, T_{s+1}, T_{s+2}, \dots, T_n$ (соответственно $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$) являются координатными функциями на $\mathbb{P}^{n-s}(\overline{k})$ (соответственно $\mathbb{P}^{n-s+1}(\overline{k})$). Тогда (ср., напр., [4]) морфизм p является доминантным, образ морфизма (4) есть $\mathcal{Z}(\Phi)$, где $\Phi \in k[T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}]$ – однородный сепарабельный многочлен, $\deg_{T_{n+1}} \Phi = D$ и старший коэффициент $\mathrm{lc}_{T_{n+1}} \Phi$ многочлена Φ относительно T_{n+1} равен 1. Обозначим через $q : V_s \to \mathcal{Z}(\Phi)$ морфизм, индуцированный морфизмом (4). Тогда $q(V_s) = \mathcal{Z}(\Phi)$ и $\deg q(V_s) = D$. Обозначим через $k(V_s)$ и $k(q(V_s))$ алгебры определенных над k рациональных функций на V_s и $q(V_s)$ соответственно (по определению эти алгебры изоморфны прямым произведениям полей рациональных функций всех определенных над k компонент V_s и $q(V_s)$ соответственно). Морфизм q является конечным доминантным и определенным над k. Кроме того, q является бирациональным в том смысле, что он индуцирует изоморфизм $k(q(V_s)) \simeq k(V_s)$. Пусть $r : q(V_s) \to \mathbb{P}^{n-s}$ – морфизм линейной проекции на координаты $T_0, T_{s+1}, T_{s+2}, \dots, T_n$. Тогда $p = r \circ q$. Морфизм r определен над k и является конечным доминантным, поскольку $\mathrm{lc}_{T_{n+1}} \Phi = 1$.

Обозначим через

$$R = \mathrm{Res}_{T_{n+1}}(\Phi, \, \partial\Phi/\partial T_{n+1}) \in k[T_0, T_{s+1}, T_{s+2}, \dots, T_n]$$

дискриминант многочлена Φ относительно T_{n+1}. Тогда $0 \neq R$ – однородный многочлен степени $D(D-1)$ относительно

$T_0, T_{s+1}, T_{s+2}, \dots, T_n$. Пусть R_0 – бесквадратная часть R, то есть R_0 – сепарабельный многочлен и $\mathcal{Z}(R) = \mathcal{Z}(R_0)$. Многочлен R_0 определен однозначно с точностью до ненулевого множителя из k. Мы выбираем и фиксируем R_0.

Отождествим $\mathcal{Z}(T_{s+1}, \dots, T_n) \subset \mathbb{P}^n(\overline{k})$ (соответственно в $\mathbb{P}^{n-s+1}(\overline{k})$, $\mathbb{P}^{n-s}(\overline{k})$) с $\mathbb{P}^{s+1}(\overline{k})$ (соответственно $\mathbb{P}^2(\overline{k})$, $\mathbb{P}^1(\overline{k})$). Рассмотрим проективную алгебраическую кривую $V_{s,*} = V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1}) \subset \mathbb{P}^{s+1}(\overline{k})$. Повторим описанную конструкцию для $V_{s,*} \subset \mathbb{P}^{s+1}(\overline{k})$ вместо $V_s \subset \mathbb{P}^n(\overline{k})$. Теперь n и s заменяются на $s+1$ и s соответственно. Линейные формы $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$ заменяются на T_0, T_n, T_{n+1}. Новое множество $A^{(s)}$ является тем же самым, что и первоначальное. Мы получаем объекты p_*, q_*, r_*, Φ_*, R_*, $R_{0,*}$, которые аналогичны p, q, r, Φ, R, R_0 и удовлетворяют подобным же свойствам по аналогичным причинам. Отметим, что $\Phi_* = \Phi(T_0, 0, \dots, 0, T_n, T_{n+1})$, $R_* = R(T_0, 0, \dots, 0, T_n)$.

Следующая лемма известна.

Лемма 1. *Пусть Z – новая переменная. Пусть $g = Z^\nu + g_{\nu-1}Z^{\nu-1} + \dots + g_0 \in \mathbb{C}[Z]$ – многочлен степени $\nu \geqslant 1$ с комплексными коэффициентами $g_i \in \mathbb{C}$, $0 \leqslant i \leqslant \nu - 1$. Пусть $z_1, \dots, z_\nu \in \mathbb{C}$ – все корни многочлена g с учетом кратности. Тогда для всякого $0 < \varepsilon \in \mathbb{R}$ существует $0 < \delta \in \mathbb{R}$, удовлетворяющее следующему условию. Пусть $\widetilde{g}_0, \dots, \widetilde{g}_{\nu-1} \in \mathbb{C}$. Предположим, что $|\widetilde{g}_i - g_i| < \delta$ для всех $0 \leqslant i \leqslant \nu - 1$. Пусть $\widetilde{z}_1, \dots, \widetilde{z}_\nu \in \mathbb{C}$ – все корни многочлена $\widetilde{g} = Z^\nu + \widetilde{g}_{\nu-1}Z^{\nu-1} + \dots + \widetilde{g}_0 \in \mathbb{C}[Z]$ с учетом кратности. Тогда существует перестановка σ индексов $1, \dots, \nu$, такая, что $|\widetilde{z}_{\sigma(i)} - z_i| < \varepsilon$.*

В дальнейшем, применяя эту лемму мы будем предполагать без ограничения общности, что σ является тождественной перестановкой: $\sigma = 1$. Теперь мы можем сформулировать наш критерий неприводимости.

Теорема 3. *Пусть $n \geqslant 3$ и $1 \leqslant s \leqslant n-2$ – целые числа. Пусть V_s – равноразмерностное проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$, причем $\dim V_s = n - s$. Пусть $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$ – линейные формы из $k[X_0, \dots, X_n]$, удовлетворяющие условию (2). Пусть многочлен Φ и его дискриминант R – такие же, как выше. Предположим, что пересечение $\mathcal{Z}(R) \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$ (рассматриваемое в $\mathbb{P}^{n-s}(\overline{k})$) трансверсально, то есть многочлен $R_0(T_0, 0, \dots, 0, T_n)$ сепарабелен. Тогда неприводимые над $\overline{k}$ (со-*

ответственно k) компоненты алгебраических многообразий V_s и $V_{s,*}$ находятся во взаимно однозначном соответствии по правилу $W \mapsto W \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$.

Доказательство. Поскольку V_s и $V_{s,*}$ определены над k, достаточно доказать только утверждение, относящееся к компонентам, неприводимым над $\overline{k}$. Обозначим через N (соответственно N_*) число всех неприводимых над $\overline{k}$ компонент многообразия V_s (соответственно $V_{s,*}$). Из условия (2) следует, что пересечение $V_s \cap \mathcal{Z}(T_{s+1}, \dots, T_{n-1})$ трансверсально в каждой его неприводимой компоненте. Следовательно, по теореме Безу справедливо неравенство $N_* \geqslant N$, и если $N_* = N$, то имеет место требуемое взаимно однозначное соответствие. Таким образом, достаточно доказать, что $N = N_*$. Заметим, что N (соответственно N_*) есть число неприводимых над $\overline{k}$ компонент $\mathcal{Z}(\Phi)$ (соответственно $\mathcal{Z}(\Phi_*)$), поскольку q (соответственно q_*) является конечным бирациональным изоморфизмом.

Мы будем предполагать без ограничения общности, что k – подполе поля комплексных чисел $\mathbb{C}$. Напомним,что $R_* \in k[T_0, T_n]$ – ненулевой однородный многочлен. Мы будем предполагать, не умаляя общности, что T_0 не делит R_*, заменяя при необходимости T_0 на $T_0 + \lambda T_n$ с подходящим целым числом λ. Пусть $y_1, \dots, y_u$ – все попарно различные корни многочлена $R_*(1, T_n)$. Тогда $u = \deg R_{0,*} = \deg R_0$ по условию леммы. Выберем точку $y \in \mathbb{C}$, такую, что $R_*(y) \neq 0$ и для всех $1 \leqslant i_1 \neq i_2 \leqslant u$ точки y, y_{i_1}, y_{i_2} не принадлежат одной и той же прямой в $\mathbb{C}$ (рассматриваемой как $\mathbb{R}^2$). Пусть $0 < m_1 \in \mathbb{R}$. Обозначим через b_i замкнутый круг с радиусом m_1 и центром y_i, $1 \leqslant i \leqslant u$. Выберем m_1 таким малым, что всякая прямая в $\mathbb{C}$, проходящая через точку y, пересекает самое большее один круг b_i, $1 \leqslant i \leqslant u$, и $|y_i - y_j| > 3m_1$, $|y - y_i| > m_1$ для всех $1 \leqslant i \neq j \leqslant u$. Обозначим через c_i, $1 \leqslant i \leqslant u$, окружность с радиусом m_1 и центром y_i. Обозначим через z_i пересечение интервала $[y, y_i]$ с c_i. Обозначим через e_i объединение интервала $[y, z_i]$ с c_i. Обозначим через γ_i, $1 \leqslant i \leqslant u$, путь из y в z_i вдоль $[y, z_i]$, затем по c_i вокруг y_i против часовой стрелки и обратно из z_i в y вдоль интервала $[z_i, y]$. Положим $e = \cup_{1 \leqslant i \leqslant u} e_i$ и $E_z = (T_{n+1}/T_0)(r_*^{-1}(1 : z))$ для всякого $z \in \mathbb{C}$. Заметим, что для всякого $z \in \mathbb{C} \setminus \mathcal{Z}(R)$ выполнено равенство $\# E_z = D$.

Положим $E = E_y$. Тогда $\# E = D$. Пусть $a \in E$. Обозначим через ξ_a аналитическую функцию от Z, определенную в окрестности y, такую, что $\Phi_*(1,Z,\xi_a)=0$ и $\xi_a(y)=a$. Результат аналитического продолжения функции ξ_a вдоль γ_i есть $\xi_{\sigma_i(a)}$, где σ_i – однозначно определенная перестановка множества E. Обозначим через S_D группу перестановок множества E и через G – подгруппу в S_D, порожденную всеми σ_i, $1\leqslant i\leqslant u$. Тогда известно (см., напр., [2], [9]), что число N_* неприводимых над $\overline{k}$ компонент $V_{s,*}$ совпадает с числом классов транзитивности группы G на E.

Пусть $\mu_i,\nu_i\in k$, $s+1\leqslant i\leqslant n-1$ и $0<\delta\in\mathbb{R}$. Обозначим через $\mathcal{A}_\delta$ условие $\sum_{s+1\leqslant i\leqslant n-1}(|\mu_i|^2+|\nu_i|^2)<\delta$. Положим $\widetilde{T}_i=T_i$, $i=0,n,n+1$, и $\widetilde{T}_i=T_i-\mu_iT_0-\nu_iT_n$ для всех $s+1\leqslant i\leqslant n-1$. Существует такое $0<\delta_0\in\mathbb{R}$, что при условии $\mathcal{A}_{\delta_0}$ линейные формы $\widetilde{T}_i$ удовлетворяют тем же самым свойствам (рассмотренным выше), что и T_i, $i\in\{0,s+1,s+2,\dots,n+1\}$. В дальнейшем мы будем предполагать, что условие $\mathcal{A}_{\delta_0}$ выполнено. Тогда для $\widetilde{T}_i$ определены объекты $\widetilde{A}^{(s)}$, $\widetilde{\Phi}$, $\widetilde{R}$ и т. д. Они соответствуют объектам $A^{(s)}$, Φ, R и т. д. Отметим, что $\Phi=\widetilde{\Phi}$, $R=\widetilde{R}$ (как многочлены от $X_0,\dots,X_n$), $N=\widetilde{N}$, $u=\widetilde{u}=\deg R_0$ и

$$\widetilde{\Phi}_*=\Phi(T_0,\mu_{s+1}T_0+\nu_{s+1}T_n,\dots,\mu_{n-1}T_0+\nu_{n-1}T_n,T_n,T_{n+1}),\quad(5)$$
$$\widetilde{R}_*=R(T_0,\mu_{s+1}T_0+\nu_{s+1}T_n,\dots,\mu_{n-1}T_0+\nu_{n-1}T_n,T_n).\quad(6)$$

Следовательно, по лемме 1, примененной к многочлену $R_*(1,Z)/\mathrm{lc}_Z(R_*(1,Z))$, существует $0<\delta_1<\delta_0$, такое, что $\mathcal{A}_{\delta_1}$ влечет $|\widetilde{y}_i-y_i|<m_1/2$ для всех $1\leqslant i\leqslant u$. В дальнейшем мы будем предполагать, что условие $\mathcal{A}_{\delta_1}$ выполнено. Теперь мы выбираем $\widetilde{y}=y$ и $\widetilde{m}_1=m_1/2$.

Пусть $m_2=\inf\{|a_1-a_2| : a_1,a_2\in E_z\ \&\ a_1\neq a_2\ \&\ z\in e\}$. Тогда $m_2>0$ в силу компактности множества e. Ввиду леммы 1, примененной к многочлену $\Phi_*(1,z,Z)$, $z\in e$, формулы (5) и компактности множества e, существует $0<\delta_2\leqslant\delta_1$, такое, что из условия $\mathcal{A}_{\delta_2}$ следует, что для всякого $z\in e$ и для всякого $a\in E_z$ существует единственное $\widetilde{a}\in\widetilde{E}_z$, такое, что $|a-\widetilde{a}|<m_2/3$. В дальнейшем мы будем предполагать, что условие $\mathcal{A}_{\delta_2}$ выполнено.

Теперь существует биекция $\tau : E\to\widetilde{E}$, $a\mapsto\widetilde{a}$, $|a-\widetilde{a}|<m_2/3$. Следовательно, τ индуцирует изоморфизм $S_D\to\widetilde{S}_D$. Согласно нашей конструкции путь γ_i гомотопен пути $\widetilde{\gamma}_i$ в $\mathbb{C}\setminus\mathcal{Z}(\widetilde{R}_*)$ для всякого $1\leqslant i\leqslant u$. Следовательно, $\widetilde{\sigma}_i=\tau\circ\sigma_i\circ\tau^{-1}$ для всякого $1\leqslant i\leqslant u$. Таким образом, $G\simeq\widetilde{G}$ и $N_*=\widetilde{N}_*$.

Обозначим через $\mathcal{L}_{n-s+1}$ (соответственно $\mathcal{L}_{n-s-1}$) векторное пространство линейных форм с коэффициентами из $\overline{k}$ с базисом $T_0, T_{s+1}, \dots, T_n$ (соответственно $T_{s+1},, \dots, T_{n-1}$). Согласно первой теореме Бертини (см. [1]), примененной последовательно $n-s-1$ раз, в каждой окрестности векторного подпространства $\mathcal{L}_{n-s-1} \subset \mathcal{L}_{n-s+1}$ (окрестность подпространства $\mathcal{L}_{n-s-1}$ рассматривается в соответствующем грассмановом многообразии с классической топологией) существует $(n-s-1)$-мерное векторное подпространство $\mathcal{L} \subset \mathcal{L}_{n-s+1}$, такое, что $\dim q(V_s) \cap \mathcal{Z}(\mathcal{L}) = 1$, $\deg q(V_s) \cap \mathcal{Z}(\mathcal{L}) = D$ и для всякой неприводимой над $\overline{k}$ компоненты W многообразия $q(V_s)$ алгебраическое многообразие $W \cap \mathcal{Z}(\mathcal{L})$ является неприводимым над $\overline{k}$. Следовательно, можно выбрать в качестве $\mathcal{L}$ линейное подпространство, порожденное $\widetilde{T}_{s+1}, \dots, \widetilde{T}_{n-1}$ для некоторых μ_i, ν_i, $s+1 \leqslant i \leqslant n-1$, удовлетворяющих условию $\mathcal{A}_{\delta_2}$. В этом случае $\widetilde{N}_* = \widetilde{N}$. Таким образом, $N = \widetilde{N} = \widetilde{N}_* = N_*$. Теорема доказана.

Следствие 1. *Пусть $1 \leqslant s \leqslant n-1$. Отождествим множество всех наборов $(L_0, L_{s+1}, \dots, L_n)$ из $n-s+1$ линейных форм $L_j \in \overline{k}[X_0, \dots, X_n]$ с аффинным пространством $\mathbb{A}^{(n-s+1)(n+1)}(\overline{k})$. Тогда множество всех $(L_0, L_{s+1}, \dots, L_n)$, таких, что для рассматриваемого фиксированого s выполняются утверждения (a) и (b) теоремы 1, является непустым определенным над k открытым в топологии Зарисского подмножеством пространства $\mathbb{A}^{(n-s+1)(n+1)}(\overline{k})$.*

Доказательство. Случай $s = n-1$ является легким. Так что мы будем предлагать, что $s \leqslant n-2$. Рассмотрим аффинное пространство однородных многочленов заданной степени от $n-s+2 \geqslant 3$ переменных с коэффициентами из $\overline{k}$. Известно (см., напр., [1]), что множество всех неприводимых над $\overline{k}$ однородных многочленов из этого аффинного пространства является непустым открытым в топологии Зарисского подмножеством рассматриваемого аффинного пространства. Теперь следствие вытекает из первого абзаца доказательства (подробности мы оставляем читателю).

Следствие 2. *Пусть $n \geqslant 2$ и $1 \leqslant s \leqslant n-1$ – целые числа. Пусть V_s – равноразмерностное проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$ и $\dim V_s = n-s$. Пусть $T_0, T_{s+1}, T_{s+2}, \dots, T_{n+1}$ – линейные формы из $k[X_0, \dots, X_n]$, удовлетворяющие условию (2). Пусть многочлен Φ и его дискриминант R – такие же, как выше. Пусть $L \in k[T_0, T_{s+1}, T_{s+2}, \dots, T_n]$ – ненулевая линейная форма. Предпо-*

ложим, что пересечение $\mathcal{Z}(R)\cap\mathcal{Z}(L)$ трансверсально в $\mathbb{P}^{n-s}(\overline{k})$ (или, что эквивалентно, $\deg\mathcal{Z}(R)=\deg(\mathcal{Z}(R)\cap\mathcal{Z}(L))$ в $\mathbb{P}^{n-s}(\overline{k})$). Тогда пересечение $V_s\cap\mathcal{Z}(L)$ трансверсально, $\deg V_s=\deg V_s\cap\mathcal{Z}(L)$ в $\mathbb{P}^n(\overline{k})$ и неприводимые над $\overline{k}$ (соответственно над k) компоненты многообразий V_s и $V_s\cap\mathcal{Z}(L)$ находятся во взаимно однозначном соответствии по правилу $W\mapsto W\cap\mathcal{Z}(L)$

Доказательство. Пусть $\mathbb{P}^{n+1}(\overline{k})$ имеет однородные координаты $X_0,\dots,X_{n+1}$. Отождествим $\mathbb{P}^n(\overline{k})=\mathcal{Z}(X_{n+1})\subset\mathbb{P}^{n+1}(\overline{k})$. Тогда $V_s\subset\mathbb{P}^{n+1}(\overline{k})$. Заменяя при необходимости n на $n+1$ и $T_0,T_{s+1},\dots,T_n$ на $T_0,T_{s+1},\dots,T_n,\ X_{n+1}$, мы будем предполагать без ограничения общности, что $n\geqslant 3$ и $1\leqslant s\leqslant n-2$. Положим $\widetilde{T}_{s+1}=L$ (не следует путать волну здесь и далее с волной из доказательства теоремы). Мы имеем $R \bmod L\neq 0$. Следовательно, существуют линейные формы $\widetilde{T}_0,\widetilde{T}_{s+2},\dots,\widetilde{T}_n$ от $T_0,T_{s+1},\ T_{s+2},\dots,T_n$ с коэффициентами из k, такие, что $\widetilde{T}_0,\widetilde{T}_{s+1},\dots,\widetilde{T}_n$ линейно независимы, $\#r^{-1}(\mathcal{Z}(\widetilde{T}_{s+1},\dots,\widetilde{T}_n))=\deg\Phi$, $0\notin\widetilde{T}_0(\#r^{-1}(\mathcal{Z}(\widetilde{T}_{s+1},\dots,\widetilde{T}_n)))$ и пересечение $\mathcal{Z}(R)\cap\mathcal{Z}(\widetilde{T}_{s+1},\dots,\widetilde{T}_{n-1})$ трансверсально. Заменим в условии (2) $T_0,\ T_{s+1},\dots,T_n$ и T_{n+1} на $\widetilde{T}_0,\ \widetilde{T}_{s+1},\dots,\widetilde{T}_n$ и T_{n+1} соответственно. Тогда полученное условие выполнено. Далее мы получаем многочлены $\widetilde{\Phi}$, $\widetilde{R}$, соответствующие новым линейным формам согласно конструкции, описанной перед теоремой 3. Теперь, применяя теорему 3 в рассматриваемой ситуации, мы устанавливаем все утверждения следствия. Следствие доказано.

2. Доказательство теоремы 1

Сначала наша цель – построить для всякого $1\leqslant s\leqslant n$ некоторые линейные формы $Y_{s,0},\dots,Y_{s,n+1}$ от $X_0,\dots,X_n$. Пусть s – произвольное, но фиксированное на некоторое время число, $1\leqslant s\leqslant n$. Согласно [4], раздел 2, можно построить линейные формы $L_{s,0},L_{s,s+1},L_{s,s+2},\dots,L_{s,n}$ с целыми коэффициентами с длинами записи $O(n\log d)$ и конечное множество A_s''', такие, что $A_s'''=V_s\cap\mathcal{Z}(L_{s,s+1},\dots,L_{s,n})$, последнее пересечение является трансверсальным, состоит из $D=\deg V_s$ гладких точек алгебраического многообразия V и $0\notin L_{s,0}(A_s''')$. Построим линейную форму $L_{s,n+1}$ с целыми коэффициентами с длинами записи $O(n\log d)$, такую, что $\#(L_{s,n+1}/L_{s,0})(A_s''')=D$. Построим линейные формы $L_{s,i}$, $1\leqslant i\leqslant s$, с целыми коэффициентами с длинами записи $O(n \log d)$, такие, что формы $L_{s,0}, \dots, L_{s,n}$ линейно независимы. Для краткости положим $Z_j = L_{s,j}$ для всех j. Пусть $T_j = Z_j$ для всех $0 \leqslant j \leqslant n+1$.

Положим для краткости $T = (T_0, \dots, T_{n+1})$. Пусть $\mathcal{B}'_s(T)$ означает, что для T выполнено условие (2) и все точки из $A^{(s)}$ являются гладкими точками многообразия V, причем $\mathcal{B}'_s$ рассматривается как функция от T и все T_j могут иметь коэффициенты из расширения поля $\overline{k}$.

Предположим на некоторое время, что $s \leqslant n-2$ и $V_s \neq \emptyset$. В этом случае линейные формы T_j будут преобразовываться алгоритмом рекурсивным образом. Наша цель – построить в конце рекурсии линейные формы T_j с целыми коэффициентами с длинами записи $O(n \log d)$, такие, что $T_0, T_{s+1}, \dots, T_{n+1}$ удовлетворяют условиям теоремы 3. На всех шагах описываемой рекурсии $T_0, T_{s+1}, \dots, T_n$ являются линейными формами с целыми коэффициентами от $Z_0, Z_{s+1}, \dots, Z_n$, и $T_j = Z_j$ для $1 \leqslant j \leqslant s$, $j = n, n+1$.

Пусть Φ, R, q, r – такие же, как в разделе 1. Используя алгоритм из работы [3], построим кривую $V_{s,*}$ и многочлены Φ_*, R_*, см. раздел 1. Обозначим через $R_{*,0}$ бесквадратную часть многочлена R_*. Положим

$$v_s(T) = \deg R_0, \quad u_s(T) = \deg R_{*,0}.$$

Тогда $v_s(T) \geqslant u_s(T)$. Как и в доказательстве теоремы 3, мы можем предполагать без ограничения общности, что T_0 не делит R_*, заменяя при необходимости T_0 на $T_0 + \lambda T_n$, где λ – целое число с длиной записи $O(n \log d)$. Теперь $\mathrm{lc}_{T_n} R_* \in k$, $\deg R_* = \deg R$ и R является однородным многочленом. Следовательно, $\mathrm{lc}_{T_n} R \in k$. Вычислим все попарно различные корни $y_1, \dots, y_u$ многочлена $R_*(1, Z)$ (то есть все поля $k[y_i]$; здесь следует разложить $R_*(1, Z)$ на неприводимые множители над k, используя [3]). Тогда $u_s(T) = u$. Теперь $\mathcal{Z}(R_*, T_0) = \emptyset$ в $\mathbb{P}^1(\overline{k})$. Далее, $\mathrm{lc}_{T_n} R_* \in k$, $\deg R_* = \deg R$ и R является однородным многочленом. Следовательно, $\mathrm{lc}_{T_n} R \in k$. Значит, морфизм $r_0 : \mathcal{Z}(R) \to \mathbb{P}^{n-s-1}(\overline{k})$ линейной проекции на координаты $T_0, T_{s+1}, \dots, T_{n-1}$ является конечным доминантным. Следовательно, $\deg r_0 = \deg R_0$.

Пусть $\varepsilon_i > 0$ – бесконечно малая величина относительно поля $k_{i-1} = k(\varepsilon_1, \dots, \varepsilon_{i-1})$, $1 \leqslant i \leqslant 5$. Мы будем предполагать, что алгебраическое замыкание поля $k_4 = k(\varepsilon_1, \dots, \varepsilon_4)$ снабжено вещественной структурой, см. [8]. Следовательно, можно рассматривать полиномиальные уравнения и неравенства с квадратами абсолютных величин над k_4. Пусть $X_{i,0}, \dots, X_{i,n}$, $1 \leqslant i \leqslant 4$, – новые переменные. Положим для краткости $X^{(i)} = (X_{i,0}, \dots, X_{i,n})$ для $1 \leqslant i \leqslant 4$ и $b(X^{(i)}) = b(X_{i,0}, \dots, X_{i,n})$ для произвольного многочлена b от $n+1$ переменных. Рассмотрим систему уравнений и неравенств

$$\begin{cases} \sum_{s+1 \leqslant i \leqslant n-1} |T_i(X^{(1)})|^2 < \varepsilon_1, & \\ \varepsilon_3 < |T_n(X^{(1)}) - T_n(X^{(3)})|^2 < \varepsilon_2, & \\ |T_{n+1}(X^{(i)}) - T_{n+1}(X^{(i+1)})|^2 = \varepsilon_4, & i = 1, 3, \\ T_j(X^{(i_1)}) = T_j(X^{(i_2)}), & 1 \leqslant i_1 < i_2 \leqslant 4, s+1 \leqslant j \leqslant n-1, \\ T_n(X^{(i)}) = T_n(X^{(i+1)}), & i = 1, 3, \\ T_0(X^{(i)}) = 1, & 1 \leqslant i \leqslant 4, \\ f_j(X^{(i)}) = 0, & 1 \leqslant j \leqslant m, \quad 1 \leqslant i \leqslant 4. \end{cases} \tag{7}$$

Лемма 2. *Система (7) имеет решение в* $\mathbb{A}^{4n+4}(\overline{k}_4)$ *тогда и только тогда, когда* $u_s(T) < \deg r_0$.

Доказательство. Пусть $u_s(T) < \deg r_0$. Тогда по лемме 1 и принципу переноса (см. [7]), примененным к многочлену $R_*(1, Z)/\mathrm{lc}_Z R_*(1, Z)$, существуют $z_{s+1}, \dots, z_{n-1}, z_{1,n}, z_{3,n} \in \overline{k_3}$, такие, что $\sum_{s+1 \leqslant i \leqslant n-1} |z_i|^2 < \varepsilon_1$, $\varepsilon_3 < |z_{1,n} - z_{3,n}|^2 < \varepsilon_2$ и $R(1, z_{s+1}, \dots, z_{n-1}, z_{n,\alpha}) = 0$, $\alpha = 1, 3$. Мы имеем $R(1, z_{s+1}, \dots, z_{n-1}, T_n) \neq 0$, поскольку $\mathrm{lc}_{T_n} R \in k$. Напомним, что $\mathrm{lc}_{T_{n+1}} \Phi = 1$. Следовательно, по лемме 1 и принципу переноса, примененным к двум многочленам $\Phi(1, z_{s+1}, \dots, z_{n-1}, z_{n,\alpha}, Z)$, $\alpha = 1, 3$, существуют $\widetilde{z}_{\alpha,n}, \widetilde{z}_{\beta,n+1} \in \overline{k_4}$, $\alpha = 1, 3$, $\beta = 1, 2, 3, 4$, такие, что $\widetilde{z}_{\alpha,n} - z_{\alpha,n}$, $\alpha = 1, 3$, – бесконечно малые величины относительно поля k_3, $|\widetilde{z}_{\beta,n+1} - \widetilde{z}_{\beta+1,n+1}|^2 = \varepsilon_4$, $\beta = 1, 3$, и $\Phi(1, z_{s+1}, \dots, z_{n-1}, \widetilde{z}_{\alpha,n}, \widetilde{z}_{\beta,n+1}) = 0$ для $\alpha = 1, 3$, $\beta = \alpha, \alpha + 1$. Положим $\widetilde{z}_{\beta,n} = \widetilde{z}_{\alpha,n}$ для $\alpha = 1, 3$, $\beta = \alpha, \alpha + 1$. Морфизм q является конечным доминантным. Следовательно, существует решение системы (7) с дополнительными уравнениями $T_j(X^{(\beta)}) = z_j$, $s + 1 \leqslant j \leqslant n - 1$, $T_j(X^{(\beta)}) = \widetilde{z}_{\beta,j}$, $j = n, n + 1$, $\beta = 1, 2, 3, 4$.

Обратно, если система (7) имеет решение, то, как это видно из описания алгоритма (см. ниже), $u_s(T) < \deg r_0$. Лемма доказана.

Выясним (см. [8]) верно ли, что система (7) имеет решение. Предположим, что система (7) не имеет решения. Тогда

$u_s(T) = \deg r_0 = \deg R_0$ по лемме 2, и линейные формы T_i, удовлетворяющие условию теоремы 3, построены. Предположим, что система (7) имеет решение. В этом случае мы строим, см. [8], такое решение $X_{i,j} = x_{i,j} \in \overline{k}_4$, $1 \leqslant i \leqslant 4$, $0 \leqslant j \leqslant n$. Для всякого $a \in \overline{k}_4$, которое не является бесконечно большим относительно поля k_3, обозначим (см. [8], раздел 1), через $\mathrm{st}_{\varepsilon_4} a \in \overline{k}_3$ такой элемент, что $(a - \mathrm{st}_{\varepsilon_4} a)$ – бесконечно малая величина относительно k_3. Вычислим, см. [8], $x_j = \mathrm{st}_{\varepsilon_4} x_{1,j}$, $0 \leqslant j \leqslant n$. Положим $T'_j = T_j - T_j(x_0, \dots, x_n)T_0$, $s+1 \leqslant j \leqslant n-1$, и $T'_j = T_j$, $j = 0, \dots, s, n, n+1$. Пусть T' обозначает для T'_j то же, что T обозначает для T_j. Тогда свойство $\mathcal{B}'_s(T')$ истинно. Пусть число $u(T')$ определяется для T', как $u(T)$ – для T. Из (7) мы получаем, что $u' = u_s(T') > u_s(T) = u$.

Пусть $T''_0, T''_{s+1}, \dots, T''_{n+1}$ – линейные формы от $Z_0, Z_{s+1}, \dots, Z_{n+1}$. Положим $v_s = v_s(T)$. Пусть $0 \leqslant a$ – целое число. Свойство $\mathcal{B}'_s(T'')\&(u_s(T'') \geqslant a)$ является хорошим свойством аргумента T'' в смысле, аналогичном [8] (см. также [4]). Для краткости обозначим рассматриваемое свойство через $\mathcal{B}_s(T'', a)$ и положим $\mathcal{B}_s(T'') = \mathcal{B}_s(T'', v_s)$. Тогда (читатель может увидеть это и непосредственно), можно последовательно заменить ненулевые коэффициенты линейных форм $T'_{s+1}, \dots, T'_{n-1}$ при Z_j целыми числами с длиной записи $O(n \log d)$ и получить новые линейные формы T'', для которых выполнено свойство $\mathcal{B}_s(T'', u')$ и $T''_j = T_j$ для $j = 0, \dots, s, n, n+1$. Теперь мы заменяем T на T'' и переходим к следующему шагу рекурсии. Число таких шагов с заменой T на T'' в конце ограничено сверху величиной d^{n-s} по теореме Безу.

Новый морфизм r_0 отличается от старого только на автоморфизм пространства $\mathbb{P}^{n-s-1}(\overline{k})$. Морфизм r_0 – конечный доминантный. Следовательно, T_0 может делить R_* только на первом шаге рекурсии. Так что после первого шага формы T_j, $j = 0, \dots, s$, $n, n+1$, не изменяются.

Таким образом, в завершение мы получим линейные формы T, такие, что $T_0, T_{s+1}, \dots, T_{n+1}$ удовлетворяют условиям теоремы 3. В дальнейшем мы не будем предполагать, что $s \leqslant n-2$ и $V_s \neq \emptyset$. Пусть $\mathcal{B}_{n-1} = \mathcal{B}'_{n-1}$. Положим $Y_{s,j} = T_j$ для всех $0 \leqslant j \leqslant n+1$. В дальнейшем мы не будем предполагать, что s фиксировано. Положим $Y_s = (Y_{s,0}, \dots, Y_{s,n+1})$, $1 \leqslant s \leqslant n$. Тогда $\mathcal{B}_s(Y_s)$ истинно для всякого $1 \leqslant s \leqslant n-1$. Пусть $0 \leqslant j \leqslant n-1$. Рассмотрим свойство $\mathcal{C}_j = \mathcal{B}_1 \& \dots \& \mathcal{B}_j$ линейных форм от $X_0, \dots, X_n$ (таким образом,

$\mathcal{C}_0$ тождественно истинно). Пусть $L' = (L'_0, \dots, L'_{n+1})$, где все L'_i являются линейными формами от $X_0, \dots, X_n$. По определению $\mathcal{C}_n(L')$ истинно тогда и только тогда, когда $\mathcal{C}_{n-1}(L')$ истинно и справедливо утверждение (a) теоремы 1 для $L'_0, \dots, L'_{n+1}$ вместо $L_0, \dots, L_{n+1}$. Заметим, что $\mathcal{C}_j$ – хорошее свойство (см. [8], [4]) для всякого $0 \leqslant j \leqslant n$.

Положим $Y_i^{(0)} = X_i$, $0 \leqslant i \leqslant n$, и $Y_{n+1}^{(0)} = X_n$. Пусть $0 \leqslant j \leqslant n - 1$ – целое число. Предположим, что мы рекурсивно построили $Y^{(j)} = (Y_0^{(j)}, \dots, Y_{n+1}^{(j)})$, где все $Y_i^{(j)}$ – линейные формы от $X_0, \dots, X_n$ с целыми коэффициентами с длиной записи $O(n \log d)$, такие, что выполнено свойство $\mathcal{C}_j(Y^{(j)})$. Пусть ε – трансцендентный элемент над полем k. Положим $Y^{(j)} + \varepsilon Y_{j+1} = (Y_0^{(j)} + \varepsilon Y_{j+1,0}, \dots, Y_{n+1}^{(j)} + \varepsilon Y_{j+1,n+1})$ (мы расширяем здесь k до $k(\varepsilon)$). Тогда выполнено свойство $\mathcal{C}_{j+1}(Y^{(j)} + \varepsilon Y_{j+1})$. Поскольку $\mathcal{C}_{j+1}$ является хорошим свойством, можно последовательно заменить ненулевые коэффициенты при X_i, $0 \leqslant i \leqslant n$, линейных форм из $Y^{(j)} + \varepsilon Y_{j+1}$ целыми числами с длинами записи $O(n \log d)$ и получить новые линейные формы $Y^{(j+1)}$, для которых выполнено $\mathcal{C}_{j+1}(Y^{(j+1)})$.

В конце мы проверяем, верно ли, что $v_s(Y^{(n)}) = v_s$ для всякого $1 \leqslant s \leqslant n-2$, такого, что $V_s \neq \emptyset$. Если это не верно, то $v_s(Y^{(n)}) > v_s$ для некоторого s. В этом случае мы полагаем $L_{s,i} = Y_i^{(n)}$ для всякого $1 \leqslant s \leqslant n$, $0 \leqslant i \leqslant n+1$, и возвращаемся к началу описанной конструкции.

Поскольку $v_s \leqslant d^s(d^s - 1)$ для всех s, то в заключение мы придем к случаю, когда $v_s(Y^{(n)}) = v_s$ для всех $1 \leqslant s \leqslant n-2$, таких, что $V_s \neq \emptyset$. Поскольку $u_s(Y^{(n)}) \geqslant v_s$ согласно описанной конструкции, то $u_s(Y^{(n)}) = v_s(Y^{(n)})$ для всех рассмотренных s и можно применить теорему 3 с $Y^{(n)}$ вместо T. В завершение мы полагаем $L = Y^{(n)}$. Теперь выполняются утверждения (a), (b) и (c) теоремы 1.

Докажем утверждения (d) и (e). Пусть $s = n$. Тогда мы положим $V_{n,0} = A_n$. Для всякого $1 \leqslant s < n - 1$ мы строим, используя алгоритм из работы [3], все определенные над k и неприводимые над k компоненты размерности 1 пересечения $V \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$. Обозначим полученные кривые через W_j, $j \in J_s$. Опять пользуясь алгоритмом из [3], мы выбираем для всякого $j \in J_s$ определенную над k и неприводимую над k компоненту $a_j \subset A_s \cap W_j$. Положим $V_{s,0} = \cup_{j \in J_s} a_j$. Теперь выполнено утверждение (d).

Пусть $z \in A_s$ и σ является k–автоморфизмом поля $\overline{k}$. Тогда $\sigma(z) = z$ влечет, что $\sigma(W_z) = W_z$ согласно нашей конструкции. Следовательно, $k_z \subset k(z)$. Кроме того, $\sigma(W_z) = W_z$ тогда и только тогда, когда $\sigma(W_z \cap \mathcal{Z}(L_1, \dots, L_{n-1})) = W_z \cap \mathcal{Z}(L_1, \dots, L_{n-1})$, согласно (b). Следовательно, минимальные поля определения многообразий W_z и $W_z \cap \mathcal{Z}(L_1, \dots, L_{n-1})$, содержащие k, совпадают.

Используя алгоритм из работы [3], мы строим все определенные над $\overline{k}$ и неприводимые над $\overline{k}$ компоненты алгебраических многообразий W_j, $j \in J_s$, и их минимальные поля определений. Более точно, эти минимальные поля определений сопряжены над k полю k_j, которое строится алгоритмом. Алгоритм строит также конечное семейство многочленов $\psi_{j,i} \in k_j[X_0, \dots, X_n]$, $i \in I_j$, такое, что $\mathcal{Z}(\psi_{j,i}, i \in I_j)$ сопряжено над k каждой неприводимой над $\overline{k}$ компоненте многообразия W_j. Пусть $z \in a_j \subset W_j$. Для всякого $j \in J_s$, снова используя алгоритм из [3], мы строим все вложения $\tau : k_j \to k(z)$ над k (существует самое большее $[k_j : k]$ таких вложений). Продолжим τ на кольцо многочленов от $X_0, \dots, X_n$ тривиально, то есть по правилу $\tau(X_i) = X_i$ для всякого i. Тогда существует только одно τ, такое, что $\tau(\psi_{j,i})(z) = 0$ для всякого $i \in I_j$. Мы вычисляем это τ и полагаем $k_z = \tau(k_j)$. Теперь выполняется утверждение (e). Требуемая оценка времени работы описанного алгоритма немедленно следует из оценок на время работы использованных алгоритмов. Теорема 1 доказана.

Замечание 2. Пусть L – такое же, как в доказательстве теоремы 1, и ε – трансцендентный элемент над k. Пусть $L'_0, \dots, L'_n \in k[X_0, \dots, X_n]$ – произвольные линейные формы. Положим $\widetilde{L}_j = L_j + \varepsilon L'_j$ для $0 \leqslant j \leqslant n$ и $\widetilde{L}_{n+1} = L_{n+1}$, $\widetilde{L} = (\widetilde{L}_0, \dots, \widetilde{L}_{n+1})$. Заменим поле k на $k(\varepsilon)$ и L на $\widetilde{L}$. Тогда (см. формулировку теоремы 1) определены многочлены $\widetilde{\Phi}_s$, $\widetilde{R}_s$, $\widetilde{R}_{s,0}$, соответствующие форме $\widetilde{L}$. Они аналогичны многочленам Φ_s, R_s, $R_{s,0}$. Рассмотрим $\widetilde{\Phi}_s$, $\widetilde{R}_s$, $\widetilde{R}_{s,0}$ как многочлены от $X_0, \dots, X_n$ с коэффициентами из $k(\varepsilon)$. Тогда наименьший общий знаменатель из $k[\varepsilon]$ коэффициентов многочлена $\widetilde{\Phi}_s$ не обращается в нуль при $\varepsilon = 0$. Подставляя $\varepsilon = 0$, мы получаем $\widetilde{\Phi}_s|_{\varepsilon=0} = \Phi_s$ и $\widetilde{R}_s|_{\varepsilon=0} = R_s$. Далее,

$$v_s(\widetilde{L}) \geqslant v_s(L) \tag{8}$$

для всякого $1 \leqslant s \leqslant n-2$, такого, что $V_s \neq \emptyset$. Если по крайней мере одно из неравенств (8) – строгое, то, расширяя поле k до $k(\varepsilon)$ и применяя конструкцию из доказательства теоремы к $L_{s,i} = \widetilde{L}_i$, $1 \leqslant s \leqslant n$, $0 \leqslant i \leqslant n+1$, мы получаем новые линейные формы $\overline{L}$, аналогичные L, такие, что $v_s(\overline{L}) \geqslant v_s(L)$ для всех рассматриваемых s, и по крайней мере одно из последних неравенств является строгим. Следовательно, заменяя L на $\overline{L}$, можно итерировать указанную процедуру до тех пор, пока все неравенства в (8) не превратятся в равенства.

Предположим, что (8) – равенства. Тогда согласно нашим определениям $\widetilde{R}_{s,0}|_{\varepsilon=0} = R_{s,0}$. Следовательно, условия теоремы 3 (соответственно теоремы 1) выполнены для линейных форм $\widetilde{L}_j$ вместо T_j (соответственно L_j), $0 \leqslant j \leqslant n+1$, и $k(\varepsilon)$ вместо k.

Замечание 3. Мы не строим линейные формы L в общем положении с максимально возможными $v_s(L)$. Так что нам требуется формулировать и использовать предыдущее замечание как некоторое слабое приведение к общему положению. Фактически, ниже можно также использовать следствие 1 вместо замечания 2.

3. Доказательство теоремы 2

Докажем утверждение (b) теоремы 2. Расширяя поле k до $k[\eta_1, \dots, \eta_u]$, мы будем предполагать в дальнейшем, что $k = k[\eta_1, \dots, \eta_u]$. Отметим, что если $z_1, \dots, z_u$ принадлежат неприводимой над $\overline{k}$ компоненте W многообразия V, то они принадлежат каждой компоненте, сопряженной компоненте W над k. Пусть ε – бесконечно малая величина относительно поля k. Тогда (см. [8], раздел 1) определено отображение $\mathrm{st}_\varepsilon : \mathbb{P}^n(\overline{k(\varepsilon)}) \to \mathbb{P}^n(\overline{k})$, такое, что $\mathrm{st}_\varepsilon(z)$ – бесконечно близкий элемент к z.

Построим линейные формы $L_0, \dots, L_{n+1}$ из теоремы 1. Пусть $1 \leqslant s \leqslant n-1$. Построим для всякого $2 \leqslant i \leqslant u$ линейно независимые линейные формы $L_{i,0}, \dots, L_{i,n}$ от $L_0, \dots, L_n$ с коэффициентами из k с длинами записи, полиномиальными от n, $L(z_1)$, $L(z_i)$, такие, что $L_{i,j}(z_\alpha) = 0$ для $1 \leqslant j \leqslant n-1$, $\alpha = 1, i$, и $L_{i,0}(z_\alpha) \neq 0$ для $\alpha = 1, i$. Для $\alpha = 1, i$ положим $\lambda_{i,\alpha} = (L_{i,n}/L_{i,0})(z_\alpha) \in k$. Пусть $L'_{i,j} = L_{i,j} + \varepsilon L_j$, $0 \leqslant j \leqslant n$. Согласно замечанию 2, примененному к ε^{-1} вместо ε, мы можем предполагать без ограничения общности, что $v_s(L) = v_s(L'_{i,0}, \dots, L'_{i,n}, L_{n+1})$ для всех $2 \leqslant i \leqslant u$ и $1 \leqslant s \leqslant n-2$, таких, что $V_s \neq \emptyset$. Тогда, согласно теоремам 3 и 1, для всякого $1 \leqslant s \leqslant n-1$ неприводимые над k (соответственно над $\overline{k}$) компоненты многообразия V_s и неприводимые над $k(\varepsilon)$ (соответственно над $\overline{k}(\varepsilon)$) компоненты размерности 1 многообразия $V \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})$ находятся во взаимно однозначном соответствии по правилу

$$W \mapsto W \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1}) = W_{s,i}, \tag{9}$$

и, кроме того, $\deg W = \deg W_{s,i}$ в формуле (9) для всякой неприводимой над $\overline{k}$ компоненты W многообразия V_s. Кроме того, по теореме 1 для всякого $1 \leqslant s_1 \leqslant n$ пересечение $V_{s_1} \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})$ непусто тогда и только тогда, когда $s_1 \leqslant s+1$ и $V_{s_1} \neq \emptyset$. В последнем случае $\dim(V_{s_1} \cap \mathcal{Z}(L_{s+1}, \dots, L_{n-1})) = s - s_1 + 1$. Следовательно (см., напр., [3]),

(*) для всякого $1 \leqslant s_1 \leqslant n$ пересечение $V_{s_1} \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})$ непусто тогда и только тогда, когда $s_1 \leqslant s+1$ и $V_{s_1} \neq \emptyset$. В последнем случае $\dim(V_{s_1} \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})) = s - s_1 + 1$.

Предположим, что $z_\alpha \in W$. Тогда (см., напр., [8], предложение 6), множество $W_{s,i} \cap \mathcal{Z}(L_{i,n} - \lambda_{i,\alpha} L_{i,0})$ конечно и $z_\alpha \in \mathrm{st}_\varepsilon(W_{s,i} \cap \mathcal{Z}(L_{i,n} - \lambda_{i,\alpha} L_{i,0}))$. Обратно, если $z_\alpha \in \mathrm{st}_\varepsilon(W_{s,i})$, то $z_\alpha \in W$.

Теперь мы собираемся вычислить все $W_{s,i}$ и выбрать среди них такие, что $z_\alpha \in \mathrm{st}_\varepsilon(W_{s,i})$ для $\alpha = 1, i$. Рассмотрим ε как переменную. Пусть $\mathbb{A}^{n+2}(\overline{k})$ определено над k и имеет координаты $X_0, \dots, X_{n+1}$, ε. Используя алгоритм из работы [3], мы строим все определенные над k и неприводимые над k компоненты W'' размерности 3 пересечения $\mathcal{Z}(f_1, \dots, f_m) \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})$ в $\mathbb{A}^{n+2}(\overline{k})$. Для всякой W'' построим точку из этой компоненты и $\lambda_0 \in \overline{k}$ (зависящее от W''), такое, что $W'' \cap \mathcal{Z}(\varepsilon - \lambda_0) \neq \emptyset$. Далее, используя результаты работы [3], мы строим $W'' \cap \mathcal{Z}(\varepsilon - \lambda_0)$ и выясняем, верно ли, что $\dim W'' \cap \mathcal{Z}(\varepsilon - \lambda_0) = \dim W''$. Таким образом мы выберем среди компонент W'' все компоненты, не содержащиеся ни в каком конечном объединении гиперплоскостей $\mathcal{Z}(\varepsilon - \lambda)$, $\lambda \in \overline{k}$. Обозначим через $\widetilde{W}_j$, $j \in J_{s,i}$, семейство полученных алгебраических многообразий. Более точно, для всякого $j \in J_{s,i}$ алгоритм строит конечное семейство многочленов $\varphi_{j,v} \in k[X_0, \dots, X_n, \varepsilon]$, $v \in I_j$, такое, что $\widetilde{W}_j = \mathcal{Z}(\varphi_{j,v}, v \in I_j)$ в $\mathbb{A}^{n+2}(\overline{k})$. Алгоритм находит также число μ_j всех неприводимых над $\overline{k}$ компонент многообразия $\widetilde{W}_j$ для всякого $j \in J_{s,i}$.

Положим $W_j = \mathcal{Z}(\varphi_{j,v}, v \in I_j)$ в $\mathbb{P}^n(\overline{k(\varepsilon)})$. Тогда (ср., напр., [3]) W_j, $j \in J_{s,i}$, – семейство определенных над $k(\varepsilon)$ и неприводимых над $k(\varepsilon)$ компонент размерности 1 многообразия $V_s \cap \mathcal{Z}(L'_{i,s+1}, \dots, L'_{i,n-1})$. Далее μ_j – число определенных над $\overline{k}(\varepsilon)$ и неприводимых над $\overline{k}(\varepsilon)$ компонент многообразия W_j, $j \in J_{s,i}$. Заметим, что если $W_{s,i} = W_j$ в (9), то μ_j – число неприводимых над $\overline{k}$ компонент многообразия W. Справедливо равенство $\mathrm{st}_\varepsilon(W_j) = \mathcal{Z}(\varphi_{j,v}|_{\varepsilon=0}, v \in I_j)$, $j \in J_{s,i}$. Построим для всякого $2 \leqslant i \leqslant u$ подмножество $J''_{s,i} \subset J_{s,i}$ всех таких j, что $(\varphi_{j,v}|_{\varepsilon=0})(z_\alpha) = 0$ для всех $v \in I_j$, $\alpha = 1, i$.

Обозначим через W_j, $j \in J_s$, семейство определенных над k компонент размерности $n-s$ многообразия V. Пусть $W = W_j$ в (9). Тогда $W_{s,i} = W_{j_1}$ для однозначно определенного индекса $j_1 \in J_{s,i}$. Положим $j_1 = \gamma_{s,i}(j)$. Тогда $\gamma_{s,i} : J_s \to J_{s,i}$ – биекции для всех $2 \leqslant i \leqslant u$. Отождествим J_s и $J_{s,2}$, то есть будем предполагать, что $\gamma_{s,2}$ – тождественное отображение. Теперь мы собираемся построить все $\gamma_{s,i}$, $2 \leqslant i \leqslant u$. Если $s = n-1$, то $J_s = J_{s,i}$ и $\gamma_{s,i}$ – тождественное отображение для всякого $2 \leqslant i \leqslant u$.

Пусть $s \leqslant n-2$. Положим $i_2 = 2$. Для всех $3 \leqslant i_1 \leqslant u$ и $\nu = 1, 2$ мы строим линейно независимые линейные формы $L''_{i_1,i}$, $s+1 \leqslant i \leqslant n-2$, и $L'''_{i_1,\nu}$ с коэффициентами из $k(\varepsilon)$ с длинами записи, полиномиальными от n и $L(z_1)$, $L(z_2)$, $L(z_{i_1})$, такие, что

$$\begin{aligned}
&\mathcal{Z}(L''_{i_1,i},\ s+1 \leqslant i \leqslant n-2) \supset \mathcal{Z}(L'_{i_\nu,i},\ s+1 \leqslant i \leqslant n-1),\ \nu = 1, 2\\
&\mathcal{Z}(L''_{i_1,i},\ s+1 \leqslant i \leqslant n-2) \cap \mathcal{Z}(L'''_{i_1,\nu}) = \mathcal{Z}(L'_{i_\nu,i},\ s+1 \leqslant i \leqslant n-1),\\
&\qquad \nu = 1, 2. \qquad (10)
\end{aligned}$$

Обозначим через V'_{s,i_1} объединение всех неприводимых над $k(\varepsilon)$ компонент W' размерности 2 многообразия $V \cap \mathcal{Z}(L''_{i_1,i}, s+1 \leqslant i \leqslant n-2)$. Согласно (*) и (10) алгебраическое многообразие V'_{s,i_1} является объединением неприводимых над $k(\varepsilon)$ компонент W' размерности 2 многообразия $V_s \cap \mathcal{Z}(L''_{i_1,i}, s+1 \leqslant i \leqslant n-2)$. Пересечение $V \cap \mathcal{Z}(L'_{2,s+1}, \dots, L'_{2,n-1})$ трансверсально в каждой кривой, и (9) – биекция для $i = 2$. Следовательно, включение из формулы (10) с $\nu = 2$ влечет, что неприводимые над k компоненты многообразия V_s и неприводимые над $k(\varepsilon)$ компоненты многообразия V'_{s,i_1} находятся во взаимно однозначном соответствии по правилу

$$W \mapsto W \cap \mathcal{Z}(L''_{i_1,i},\ s+1 \leqslant i \leqslant n-2) = W'_{s,i_1}, \qquad (11)$$

и $W'_{s,i_1} \cap \mathcal{Z}(L'''_{i_1,\nu}) = W_{s,i_\nu}$, $\nu = 1, 2$. Используя алгоритм из работы [3], мы строим все определенные над $k(\varepsilon)$ и неприводимые над $k(\varepsilon)$ компоненты многообразия V'_{s,i_1}. Обозначим через W'_j, $j \in J'_{s,i_1}$, семейство полученных компонент. Более точно, для всякого $j \in J'_{s,i_1}$ алгоритм строит семейство многочленов $\varphi_{j,v} \in k(\varepsilon)[X_0, \ldots, X_n]$, $v \in I_j$, таких, что $W'_j = \mathcal{Z}(\varphi_{j,v},\, v \in I_j)$. Для всякого $j \in J'_{s,i_1}$ имеем $\mathcal{Z}(\varphi_{j,v},\, v \in I_j) \cap \mathcal{Z}(L'''_{i_1,\nu}) = \mathcal{Z}(\varphi_{j_\nu,i},\, i \in I_{j_\nu})$ для однозначно определенного индекса $j_\nu \in J_{s,i_\nu}$, $\nu = 1, 2$. Используя алгоритм из [3], мы строим эти j_1, j_2. Теперь $(\gamma_{s,i_1} \circ \gamma_{s,2}^{-1})(j_2) = j_1$. Таким образом мы можем построить все $\gamma_{s,i}$, $2 \leqslant i \leqslant u$.

В заключение для всякого $1 \leqslant s \leqslant n-1$ мы вычисляем пересечение $\bigcap_{2 \leqslant i \leqslant u} \gamma_{s,i}^{-1}(J''_{s,i}) = J''_s$. Согласно нашей конструкции число неприводимых над $\overline{k}$ компонент многообразия V размерности $n-s$, содержащих $z_1, \ldots, z_u$, есть $\sum_{j \in J''_s} \mu_j$ (напомним, что $J''_s \subset J_s = J_{2,s}$) для всякого $1 \leqslant s \leqslant n-1$. Алгоритм для утверждения (b) описан. Требуемая оценка для времени работы этого алгоритма немедленно следует из оценок на время работы использованных алгоритмов. Утверждение (b) теоремы 2 доказано.

Для доказательства утверждения (a) мы строим конечные множества $V_{s,0}$ из теоремы 1 и все их определенные над k и неприводимые над k компоненты a_j, $j \in J_s$. Тогда определенные над k и неприводимые над k компоненты многообразий V_s и $V_{s,0}$ находятся во взаимно однозначном соответствии по правилу $W \mapsto W \cap V_{s,0}$. Пусть $z^{(j)} \in a_j$ и $W \cap V_{s,0} = a_j$. Положим $W_j = W$. Мы вводим представления для $z^{(j)}$, $j \in J_s$, заменяя в (1) z, η, F_z на $z^{(j)}, \eta^{(j)}, F_{z^{(j)}}$. Тогда $k(z^{(j)}) \simeq k[\eta^{(j)}]$. Используя алгоритм из [3], мы строим для всякого $1 \leqslant i \leqslant u$, $j \in J_s$, все попарно неизоморфные композиты $k_{j,w}$, $w \in I_{j,i}$, полей $k[\eta_i]$ и $k[\eta^{(j)}]$ над k. Теперь $z_i \in W_j$ тогда и только тогда, когда существует $w \in I_{j,i}$, такое, что точки z_i и $z^{(j)}$ с полем $k[\eta_i, \eta^{(j)}] \simeq k_{j,w}$ принадлежат одной и той же неприводимой над $\overline{k}$ компоненте многообразия V_s (которая содержится в W_j). Пользуясь описанным алгоритмом для утверждения (b), можно выяснить, существует ли $w \in I_{j,i}$, удовлетворяющее сформулированному условию, и, следовательно, построить алгоритм для утверждения (a). Требуемая оценка для времени работы этого алгоритма немедленно следует из оценок на время работы использованных алгоритмов. Теорема доказана.

Литература

1. М. Бальдассарри, *Алгебраические многообразия.* М., Издательство иностранной литературы, 1961.
2. Н. Г. Чеботарев, *Теория алгебраических функций.* М.–Л., ОГИЗ, 1948.
3. А. Л. Чистов, *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время.* — Зап. научн. семин. ЛОМИ **137** (1984), 124–188.
4. А. Л. Чистов, *Вычисление степеней алгебраических многообразий над полем нулевой характеристики за полиномиальное время и его приложения.* — Зап. научн. семин. ПОМИ **258** (1999), 7–59.
5. А. Л. Чистов, *Вычисление группы Галуа над функциональным полем характеристики нуль с алгебраически замкнутым полем констант за полиномиальное время.* — В кн.: Математические методы построения и анализа алгоритмов. Л., Наука, 1990, с. 200–232.
6. А. Л. Чистов, *Эффективная гладкая стратификация алгебраического многообразия в нулевой характеристике и ее приложения.* — Зап. научн. семин. ПОМИ **266** (2000), 254–311.
7. J. Bochnak, M. Coste, M.–F. Roy, *Géométrie algébrique réelle.* Berlin–Heidelberg –New York, Springer–Verlag, 1987.
8. A. L. Chistov, *Polynomial–time computation of the dimensions of components of algebraic varieties in zero–characteristic.* — J. Pure Appl. Algebra **117 & 118** (1997), 145–175.
9. C. Jordan, *Traité des substitutions et des équations algébriques.* Paris, 1870.

Chistov A. L. Monodromy and irreducibility criteria with algorithmic applications in zero characteristic.

Consider a projective algebraic variety V which is the set of all common zeroes of homogeneous polynomials of degrees less than d in $n{+}1$ variables in zero-characteristic. We suggest an algorithm to decide whether two (or more) given points of V belong to the same irreducible component of V. Besides that we show how to construct for each $s < n$ an $(s+1)$-dimensional plane in the projective space such that the intersection of every irreducible component of dimension $n-s$ of V with the constructed plane is transversal and is an irreducible curve. These algorithms are deterministic and polynomial in d^n and the size of input.

С.-Петербургский институт
информатики и автоматизации
Российской академии наук

E-mail: labta@iias.spb.su or sliss@iias.spb.su

Поступило 30 мая 2002 г.