Записки научных
семинаров ПОМИ
Том 256, 1999 г.

А. Л. Чистов

СИЛЬНАЯ ВЕРСИЯ ОСНОВНОГО РАЗРЕШАЮЩЕГО АЛГОРИТМА ДЛЯ ЭКЗИСТЕНЦИОНАЛЬНОЙ ТЕОРИИ ПЕРВОГО ПОРЯДКА ВЕЩЕСТВЕННО ЗАМКНУТЫХ ПОЛЕЙ

Введение

Пусть U – вещественное алгебраическое многообразие в n-мерном аффинном пространстве, которое является множеством нулей семейства многочленов степени меньше d. Пусть U_i, $i \in I$ – семейство всех неприводимых компонент U. Обозначим через $U_i^{(s)}$ замыкание в классической топологии множества всех гладких точек размерности s многообразия U_i. В статье описывается алгоритм для построения конечного множества точек S, которое имеет непустое пересечение с каждой связной компонентой $U_i^{(s)}$ для каждого $i \in I$, $0 \leqslant s \leqslant n$. Число точек S ограничено сверху многочленом от d^n. Аналогичный результат справедлив для базисных полуалгебраических множеств. Время работы алгоритма (для случая алгебраического многообразия) полиномиально от длины записи входных данных и d^n. Более точные результаты формулируются с привлеченем триангуляции U, если U ограничено (соответственно компактификации по Александрову многообразия U, если U не ограничено).

Ранее известные алгоритмы с таким же временем работы позволяли [15, 7] построить только конечное множество S' с числом элементов ограниченным сверху полиномом от d^n, которое имеет непустое пересечение лишь с каждой связной компонентой вещественного алгебраического многообразия.

Перейдём к точным формулировкам. Пусть $k_0 = \mathbb{Q}(t_1, \dots, t_l, \theta)$ – вещественное упорядоченное поле, причём $t_1, \dots, t_l$ алгебраически независимы над $\mathbb{Q}$, и θ – алгебраический над $\mathbb{Q}$ элемент с минимальным многочленом $F \in \mathbb{Q}[t_1, \dots, t_l, Z]$. Старший коэффициент $\mathrm{lc}_Z F$ многочлена F равен 1.

Статья написана при частичной поддержке Volkswagen–Stiftung, Program on Computational Complexity.

В дальнейшем мы будем предполагать, что поле k_0 удовлетворяет следующему свойству.

(A) *Пусть конечное расширение $k_1 \supset k_0$ вещественно замкнутых полей задано своим примитивным элементом и его минимальным многочленом. Тогда для всякого элемента $a \in k_1$ можно определить верно ли, что $a > 0$ за полиномиальное время.*

Отметим, что если $k_0 = \mathbb{Q}$, то k_0 удовлетворяет этому свойству. Если $\varepsilon > 0$ – бесконечно малая величина относительно поля k_0, то вещественное упорядоченное поле $k_0(\varepsilon)$ также удовлетворяет сформулированному свойству.

Пусть даны многочлены $f_1, \dots, f_m \in k_0[X_1, \dots, X_n]$, причём $n \geqslant 1$, $m \geqslant 1$. Рассмотрим замкнутое алгебраическое множество или алгебраическое многообразие (в этой статье мы не различаем эти понятия)

$$V = \{(x_1, \dots, x_n) : f_i(x_1, \dots, x_n) = 0,\ x_i \in \overline{k_0},\ \forall 1 \le i \le m\} \subset \mathbb{A}^n(\overline{k}_0).$$

Это множество всех общих нулей многочленов $f_1, \dots, f_m$ в $\mathbb{A}^n(\overline{k})_0$, где $\overline{k}_0$ – алгебраическое замыкание k_0. В дальнейшем мы будем обозначать для краткости это множество через $\mathcal{Z}(f_1, \dots, f_m)$. Аналогичные обозначения будут также использоваться для множеств всех общих нулей (в аффинных или проективных пространствах, как это будет видно из контекста) других многочленов. Следовательно, $V = \mathcal{Z}(f_1, \dots, f_m)$.

Пусть R – вещественно замкнутое поле, содержащее вещественное замыкание $\widetilde{k}_0$ поля k_0, и $C = \overline{R}$ – алгебраическое замыкание поля R. Положим

$$V(R) = \{(x_1, \dots, x_n) : f_i(x_1, \dots, x_n) = 0, x_i \in R, \forall 1 \le i \le m\} \subset \mathbb{A}^n(R).$$

Это множество всех общих нулей многочленов $f_1, \dots, f_m$ в $\mathbb{A}^n(R)$. В дальнейшем мы будем обозначать для краткости это множество через $\mathcal{Z}_R(f_1, \dots, f_m)$. Аналогичные обозначения будут также использоваться для множеств всех общих нулей (в аффинных или проективных пространствах, как это будет видно из контекста) других многочленов. Так что $V(R) = \mathcal{Z}_R(f_1, \dots, f_m)$ является вещественным алгебраическим множеством или вещественным алгебраическим многообразием над R, см. [8]. Элементы множества $\mathcal{Z}_R(f_1, \ldots, f_m)$ суть вещественные корни многочленов $f_1, \ldots, f_m$.

Каждый многочлен $f = f_i$ будем представлять в форме

$$f = \frac{1}{a_0} \sum_{i_1,\ldots,i_n} \sum_{0 \le j < \deg F} a_{i_1,\ldots,i_n,j} \theta^j X_1^{i_1} \cdots X_n^{i_n} ,$$

где $a_0, a_{i_1,\ldots,i_n,j} \in \mathbb{Z}[t_1, \ldots, t_l]$, $\gcd_{i_1,\ldots,i_n,j}(a_0, a_{i_1,\ldots,i_n,j}) = 1$. 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 $a_0, a_{i_1,\ldots,i_n,j}$, и степень

$$\deg_{t_\alpha}(f) = \max_{i_1,\ldots,i_n,j} \{\deg_{t_\alpha}(a_0), \deg_{t_\alpha}(a_{i_1,\ldots,i_n,j})\} ,$$

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

$$\deg_{X_1,\ldots,X_n}(f_i) < d,\ \deg_{t_\alpha}(f_i) < d_2,\ l(f_i) < M,$$

$$\deg_Z(F) < d_1,\ \deg_{t_\alpha}(F) < d_1,\ l(F) < M_1 .$$

Размер (или длина записи) $L(f)$ многочлена f определяется как произведение $l(f)$ 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.

Замечание 1. В дальнейшем мы будем предполагать без ограничения общности, что многочлены $f_1, \ldots, f_m$ являются линейно независимыми над k_0. Следовательно, $\dim V \leqslant n - 1$.

Рассмотрим сначала случай, когда $V(R)$ ограничено. Рассмотрим некоторую триангуляцию вещественного алгебраического многообразия $V(R)$, см. [8], т.е. конечный симплициальный комплекс $K = \cup_{1 \leqslant i \leqslant p} \sigma_i$, определённый над полем R (здесь это означает симплициальное пространство, а не абстрактную симплициальную схему на конечных множествах, т.е. $K \subset R^N$ для некоторого N, и всякий симплекс σ_i является выпуклой оболочкой его вершин) и полуалгебраический гомеоморфизм $\phi : K \to V(R)$ относительно топологии вещественного поля. Мы будем называть для краткости симплекс σ комплекса K максимальным тогда и только тогда, когда он не является гранью какого-либо другого симплекса из K. Пусть $0 \leqslant s \leqslant n-1$. Рассмотрим ненулевой s–мерный цикл $e = \sum_{1 \leqslant j \leqslant q} \sigma_{p_j}$ с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$ симплициального комплекса K, такой что σ_{p_j} максимален для любого j, и $p_{j_1} \neq p_{j_2}$, если $j_1 \neq j_2$. Следовательно, размерность $\dim \sigma_{p_j} = s$ для каждого j. Обозначим $E = |e| = \cup_{1 \leqslant j \leqslant q} \phi(\sigma_{p_j})$.

Замечание 2. Отметим, что если имеется неприводимая компонента W многообразия $V(R)$ размерности s над R, то существует также цикл e, как выше, и такой что $|e|$ совпадает с множеством всех точек размерности s многообразия W. Это следует из того, что для всякого $(s-1)$-мерного симплекса t триангуляции W число s-мерных симплексов рассматриваемой триангуляции, содержащих t как грань, чётно, см. [8].

Пусть теперь дан ненулевой вектор $y = (y_1, \dots, y_n) \in R^n$. Согласно принципу переноса, см. [8], функция $\sum_{1 \leqslant i \leqslant n} y_i X_i$ имеет максимум и минимум на E. Обозначим

$$m' = \max(\sum_{1 \leqslant i \leqslant n} y_i X_i)(E), \quad E' = \{z \in E : (\sum_{1 \leqslant i \leqslant n} y_i X_i)(z) = m'\},$$
$$m'' = \min(\sum_{1 \leqslant i \leqslant n} y_i X_i)(E), \quad E'' = \{z \in E : (\sum_{1 \leqslant i \leqslant n} y_i X_i)(z) = m''\}$$

(чтобы избежать двусмысленности обозначений заметим, что в следующих разделах статьи мы будем также рассматривать случаи, когда координаты y принадлежат некоторому расширению R).

Теорема 1. *Пусть $V(R)$ – ограниченное вещественное многообразие в аффинном пространстве, заданное как множество нулей многочленов $f_1, \dots, f_m$. Тогда для заданного вектора $y \in k_0^n$ можно построить конечное множество S_y точек $V(R)$, такое что для всякого $0 \leqslant s \leqslant n-1$, для всякой полуалгебраической триангуляции $\phi : K \to V(R)$ и всякого ненулевого s-мерного цикла e с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$, описанного выше, пересечения $S_y \cap E'$ и $S_y \cap E''$ непусты. Число точек множества S_y ограничено сверху многочленом от d^n. Время работы алгоритма для построения S_y полиномиально от d^n, d_1, d_2, M, M_1, m и длины записи вектора y.*

Теорема 1 будет выведена из нашей теоремы существования, которая формулируется и доказывается в Разделе 2. Отметим, что может случится, что $E = E' = E''$, например, когда $s = 0$, и E состоит из одной точки. Применяя Теорему 1 к n линейно независимым векторам $y^{(1)}, \dots, y^{(n)}$ и определяя $S = \cup_{1 \leqslant i \leqslant n} S_{y^{(i)}}$, мы получаем следующий результат.

Следствие 1. *Пусть $1 \leqslant s \leqslant n-1$. Тогда можно построить конечное множество S точек $V(R)$, такое что для всякой полуалгебраической триангуляции $\phi : K \to V(R)$ и всякого s-мерного цикла e с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$, такого как выше, пересечение $S \cap E$ содержит по крайней мере две различные точки. Число точек множества S ограничено сверху многочленом от d^n. Время работы алгоритма для построения S полиномиально от d^n, d_1, d_2, M, M_1, m.*

В общем случае, т.е. когда $V(R)$ необязательно ограничено, можно проверить, ограничено ли $V(R)$, за полиномиальное время от d^n, d_1, d_2, M, M_1, m. Напомним конструкцию алгебраического многообразия V_1, такого что $V_1(R)$ является компактификацией по Александрову $V(R)$, если $V(R)$ не ограничено. Именно, построим точку $x^{(0)} \notin V(R)$. Можно предполагать, не умаляя общности, что $x^{(0)} = (0, \dots, 0)$, осуществляя при необходимости подходящее линейное преобразование координат в $\mathbb{A}^n(R)$. Положим

$$g_i = (\sum_{1 \leqslant i \leqslant n} X_i^2)^{\deg f_i} f_i \left(\frac{X_1}{\sum_{1 \leqslant i \leqslant n} X_i^2}, \dots, \frac{X_n}{\sum_{1 \leqslant i \leqslant n} X_i^2} \right), \quad 0 \leqslant i \leqslant m.$$

Определим $V_1 = \mathcal{Z}(g_1, \dots, g_m)$. Так что V_1 ограничено. Имеется изоморфизм вещественных алгебраических многообразий $\iota : V(R) \to V_1(R) \setminus \{x^{(0)}\}$, индуцированный преобразованием инверсии

$$(X_1, \dots, X_n) \mapsto \left(\frac{X_1}{\sum_{1 \leqslant i \leqslant n} X_i^2}, \dots, \frac{X_n}{\sum_{1 \leqslant i \leqslant n} X_i^2} \right).$$

Пусть K, ϕ, s, e имеют смысл для $V_1(R)$ аналогичный тому, что был прежде для $V(R)$. Применяя Следствие 1 к вещественному алгебраическому многообразию $V_1(R)$, мы получаем следующий результат.

Следствие 2. *Пусть $V(R)$ – неограниченное вещественное аффинное многообразие, заданное как множество нулей многочленов $f_1, \ldots, f_m$. Тогда можно построить конечное множество S точек $V(R)$, такое что для всякого $0 \leqslant s \leqslant n-1$, для всякой полуалгебраической триангуляции $\phi : K \to V_1(R)$ многообразия $V_1(R)$ и всякого ненулевого s-мерного цикла e с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$, описанного выше, пересечение $\iota(S) \cap E$ непусто. Число точек множества S ограничено сверху многочленом от d^n. Время работы алгоритма для построения S полиномиально от d^n, d_1, d_2, M, M_1, m.*

Пусть теперь $g_1, \ldots g_s \in k_0[X_1, \ldots, X_n]$ – некоторые многочлены, удовлетворяющие тем же самым оценкам на степени и длины записи целых коэффициентов, что и $f_1, \ldots, f_m$. Рассмотрим базисное полуалгебраическое множество, см. [15, 7],

$$U = \{x \in R^n : f_1(x) = \ldots =$$
$$= f_m(x) = 0 \,\&\, g_1(x) > 0 \,\&\, \ldots \,\&\, g_s(x) > 0\}. \qquad (1)$$

Пусть $s \leqslant s'n < s+n$ и $s' \in \mathbb{Z}$. Если $s < n$ положим $g_j = 1$ для всех $s+1 \leqslant j \leqslant n$. Положим $s_j = s'j$ для $j = 0, \ldots, n-1$ и $s_n = \max\{s, n\}$. Пусть $Z_1, \ldots, Z_n$ и T – новые переменные. Рассмотрим вещественное алгебраическое многообразие $U_1 \subset \mathbb{A}^{n+2}$, которое является множеством всех общих нулей многочленов $\prod_{s_{j-1}+1 \leqslant i \leqslant s_j} g_i - Z_j$, $1 \leqslant j \leqslant n$; $f_1, \ldots, f_m$ и $T \prod_{1 \leqslant j \leqslant n} Z_j - 1$ (так что в случае, когда $s < n$, многочлены $1 - Z_j$, $s+1 \leqslant j \leqslant n$, принадлежат рассматриваемому семейству).

Обозначим через

$$\pi : R^{2n+1} \to R^n, \quad (X_1, \ldots, X_n, Z_1, \ldots, Z_n, T) \mapsto (X_1, \ldots, X_n)$$

линейную проекцию. Тогда множество U совпадает с $\pi(U_2)$, где U_2 – объединение некоторых связных компонент U_1. Следовательно, применяя Следствие 2 и Замечание 2 к алгебраическому многообразию U_1, мы получаем следующий результат.

Теорема 2. *Рассмотрим базисное полуалгебраическое множество (1). Пусть U_i, $i \in I$, – семейство всех неприводимых компонент множества U, (см., например, [16]). Пусть $U_i^{(s)}$ является замыканием в классической топологии множества всех гладких точек размерности s компоненты U_i. Тогда можно построить конечное множество S точек U, которое имеет непустое пересечение со всякой связной компонентой каждого $U_i^{(s)}$ для любых $i \in I$,*

$0 \leqslant s \leqslant n-1$. Число точек множества S ограничено сверху многочленом от $((1+s/n)d)^n$. Время работы алгоритма для построения S полиномиально от $((1+s/n)d)^n$, d_1, d_2, M, M_1, m.

Замечание 3. Время работы алгоритмов из теорем данной статьи и их следствий по-существу то же самое, что и для решения систем алгебраических уравнений с конечным числом решений в проективном пространстве над алгебраически замкнутым полем. Следовательно, эти теоремы могут быть сформулированы также и для случая, когда l не фиксировано, см. [5].

1. Один алгоритм приведения к общему положению

Пусть $V(R)$ – вещественное алгебраическое многообразие такое же, как и во Введении. Так что

$$V(R) = \mathcal{Z}_R(f_1, \dots, f_m),$$

см. Введение. Мы будем предполагать в этом разделе, что $V(R)$ непусто и ограничено, т.е. существует $a \in R$, $a > 0$, такое что

$$\emptyset \neq V(R) \subset \{(x_1, \dots, x_n) \in R^n \ : \ \sum_{1 \leqslant i \leqslant n} x_i^2 \leqslant a\} = B_a.$$

Предположим в дальнейшем также, что пересечение с границей шара B_a

$$V(R) \cap \partial B_a = V(R) \cap \mathcal{Z}_R(\sum_{1 \leqslant i \leqslant n} x_i^2 - a) = \emptyset. \qquad (2)$$

Обозначим $f = \sum_{1 \leqslant i \leqslant m} f_i^2$. Пусть $g = 1 + X_1^{2d+2} + \ldots + X_n^{2d+2}$.

Пусть $\varepsilon > 0$ – бесконечно малая величина относительно поля R. Обозначим $f_\varepsilon = f - \varepsilon g$. Пусть $\varepsilon^{(0)}$ и $\varepsilon^{(1)}$ – новые переменные.

Положим $\overline{f} = X_0^{2d+2} f(X_1/X_0, \dots, X_n/X_0)$, $\overline{g} = \sum_{0 \leqslant i \leqslant n} X_i^{2d+2}$ и

$$h = \varepsilon^{(0)} \overline{f} - \varepsilon^{(1)} \overline{g} \in R[\varepsilon^{(0)}, \varepsilon^{(1)}, X_0, \dots, X_n,]$$

т.е. h является $\mathbb{P}^1 \times \mathbb{P}^n$-гомогенизацией многочлена f_ε, причём координаты $\mathbb{P}^1$ суть $(\varepsilon^{(0)} : \varepsilon^{(1)})$, $\varepsilon = \varepsilon^{(0)}/\varepsilon^{(1)}$, и координаты $\mathbb{P}^n$ суть $(X_0 : \ldots : X_n)$.

Пусть $y_2, \dots, y_n$ – элементы некоторого поля, являющегося расширением R. Обозначим $y = (y_2, \dots, y_n)$, и определим поля

$$K_1 = R(y_2, \dots, y_n), \quad C_1 = C(y_2, \dots, y_n),$$
$$K_2 = R(\varepsilon, y_2, \dots, y_n), \quad C_2 = C(\varepsilon, y_2, \dots, y_n).$$

В случае, когда $y_2, \ldots, y_n$ – элементы вещественного упорядоченного расширения R, мы будем обозначать также $R_1 = K_1$ и $R_2 = K_2$. В этом случае R_i – вещественные упорядоченные поля, и C_i имеют вещественные структуры, см. [9, 10], естественным образом. В общем случае мы будем предполагать без ограничения общности, что поле K_1 снабжено вещественной структурой. Тогда она индуцирует вещественные структуры на C_1, K_2, C_2.

Рассмотрим следующую систему полиномиальных уравнений относительно $X_0, \ldots, X_n$ и $\varepsilon^{(0)}, \varepsilon^{(1)}$

$$\begin{cases} h = 0, \\ \frac{\partial h}{\partial X_i} - y_i \frac{\partial h}{\partial X_1} = 0, \quad 2 \leqslant i \leqslant n. \end{cases} \tag{3}$$

Лемма 1. *Пусть $\varepsilon = \varepsilon^{(1)}/\varepsilon^{(0)}$. Рассмотрим (3) как систему относительно $X_0, \ldots, X_n$. Тогда система (3) имеет конечное число решений в $\mathbb{P}^n(\overline{C_2})$.*

Доказательство. Рассмотрим систему

$$\begin{cases} X_0^{2d+2} + X_1^{2d+2} + \ldots + X_n^{2d+2} = 0, \\ X_i^{2d+1} - y_i X_1^{2d+1} = 0, \qquad 2 \leqslant i \leqslant n, \end{cases} \tag{4}$$

которая получается заменой h на $\overline{g}$ в (3). Система (4) имеет конечное число решений в $\mathbb{P}^n(\overline{C_1})$. Следовательно, ср. [5] или [9], следствие 4.1, система (3) имеет конечное число решений в $\mathbb{P}^n(\overline{C_2})$. Лемма доказана.

Следствие 3. *Пусть система (3) имеет решение $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_2})$, такое что $\eta_0 = 0$. Тогда $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_1})$ является решением системы (4). Такое решение $(\eta_0 : \ldots : \eta_n)$ существует тогда и только тогда, когда существуют целые числа $j_2, \ldots, j_n$, для которых*

$$1 + \sum_{2 \leqslant i \leqslant n} \zeta_{2d+1}^{j_i} y_i^{(2d+2)/(2d+1)} = 0,$$

где ζ_{2d+1} – примитивный корень степени $2d+1$ из единицы.

Доказательство. Это следует из того, что $\deg f < 2d + 2$. Следствие доказано.

Пусть $\varepsilon^{(1)}/\varepsilon^{(0)} = \varepsilon$. Тогда решения $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_2})$ системы (3) могут быть следующих типов

(i) такие что $\eta_0 = 0$, и тогда $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_1})$ по Следствию 3,

(ii) такие что $\eta_0 = 1$, и $\sum_{1\leqslant i\leqslant n} |\eta_i|^2$ является бесконечно большой величиной относительно поля C_1,

(iii) такие что $\eta_0 = 1$, и η_i не являются бесконечно большими относительно поля C_1 для всех $1 \leqslant i \leqslant n$.

Используя алгоритмы из [5, 9, 10], в случае когда $y_2, \ldots, y_n \in k_0$, можно построить все решения системы (3) типа (i) (соответственно (ii), (iii)) за полиномиальное время от d^n, d_1, d_2, M, M_1, m и размера вектора y.

Обозначим через $\mu_2(y) = \mu_2(y_2, \ldots, y_n)$ (соответственно $\mu_0(y) = \mu_0(y_2, \ldots, y_n)$) число всех корней, учитывая кратности, типа (iii) (соответственно типа (ii) или (iii)) системы (3). Следовательно, по теореме Безу $\mu_0(y) \leqslant (2d+2)(2d+1)^{n-1}$.

Лемма 2. *Пусть $y_2, \ldots, y_n$ – элементы вещественного упорядоченного поля, которое является расширением R. Тогда система (3) имеет по меньшей мере два различных корня η' и η'' типа (iii) с координатами в вещественном замыкании $\widetilde{R_2}$ поля R_2. Все координаты корней η' и η'' не являются бесконечно большими относительно поля R.*

Доказательство. (Ср. [16, 15].) Заменим R на $\mathbb{R}$, бесконечно малую величину ε на положительное число $\varepsilon \in \mathbb{R}$, пусть $y_2, \ldots, y_n \in \mathbb{R}$. Тогда множество $\mathcal{Z}_{\mathbb{R}}(f_\varepsilon)$ для всех достаточно малых $\varepsilon > 0$ имеет связную компоненту W', которая содержится в B_a, см. (2), и не имеет никакой связной компоненты W'', которая имеет непустое пересечение со сферой ∂B_a. Обозначим через W_1 объединение всех связных компонент W' множества $\mathcal{Z}_{\mathbb{R}}(f_\varepsilon)$, таких что W' содержится в B_a. Множество

$$\mathcal{Z}_{\mathbb{R}}(f) = \mathcal{Z}_{\mathbb{R}}(f/g) \subset \mathcal{Z}_{\mathbb{R}}(\partial(f/g)/\partial X_1, \ldots, \partial(f/g)/\partial X_n) = W_2.$$

Функция f/g постоянна на всякой кусочно гладкой кривой, содержащейся в W_2. Следовательно, функция f/g постоянна на всякой связной компоненте множества W_2. Поэтому $\mathcal{Z}_{\mathbb{R}}(f)$ является объединением некоторых компактных связных компонент многообразия W_2. Следовательно, существует открытая в классической топологии окрестность U_1 множества $\mathcal{Z}_{\mathbb{R}}(f)$, такая что $U_1 \cap W_2 = \mathcal{Z}_{\mathbb{R}}(f)$. Функция f/g положительна в каждой точке компактного множества $B_a \setminus U_1$. Следовательно, для всех достаточно малых $\varepsilon > 0$ множество $W_1 \subset U_1$. Поэтому W_1 является гладкой ограниченной гиперповерхностью в $\mathbb{A}^n(\mathbb{R})$ для всех достаточно малых $\varepsilon > 0$.

Поскольку W_1 ограниченная гиперповерхность, существуют по крайней мере две различные точки η', η'' множества W_1, в которых опорные гиперплоскости имеют нормальный вектор параллельный к $(1, y_2, \dots, y_n)$. Эти опорные гиперплоскости являются касательными пространствами в точках η' и η''. Так что η' и η'' являются решениями системы (3) в $\mathbb{A}^n(\mathbb{R})$. Теперь первое утверждение следует из принципа переноса, см. [8]. Последнее утверждение леммы следует из того, что абсолютные величины координат всех точек из $V(R_2)$ ограничены сверху теми же самыми константами из R, что и абсолютные величины координат всех точек из $V(R)$. Лемма доказана.

Следствие 4. *Пусть $y_2, \dots, y_n$ – элементы вещественного упорядоченного поля, являющегося расширением R. Тогда справедливо неравенство $\mu_2(y) \geqslant 2$.*

Обозначим через

$$D(y) \in K_1[\varepsilon^{(0)}, \varepsilon^{(1)}, U_0, \dots, U_n]$$

U-результант, см., например, [4, 13], системы (3), рассматриваемой как система относительно $X_0, \dots, X_n$. Многочлен $D(y)$ равен (с точностью до множителя из $R(\varepsilon^{(0)}, \varepsilon^{(1)}, y_2, \dots, y_n)$) произведению $\prod_{j \in J}(\sum_{0 \leqslant i \leqslant n} U_i \eta_i^{(j)})$, где $\eta^{(j)} = (\eta_0^{(j)} : \ldots : \eta_n^{(j)})$, $j \in J$, – семейство всех корней (учитывая кратности) системы (3) в $\mathbb{P}^n(\overline{C_2})$. Обозначим через J' (соответственно J'', J''') подмножество J, такое что $j \in J'$ (соответственно $j \in J''$, $j \in J'''$) тогда и только тогда, когда корень $\eta^{(j)}$ системы (3) имеет тип (i) (соответственно (ii), (iii)).

Известно, что если q – коэффициент при мономе от $U_0, \dots, U_n$ U-результанта n однородных многочленов $F_1, \dots, F_n$ относительно $X_0, \dots, X_n$, то q является однородным многочленом относительно коэффициентов F_i степени $(\prod_{1 \leqslant j \leqslant n} \deg F_j)/\deg F_i$ для всякого $1 \leqslant i \leqslant n$. Следовательно, степень

$$\deg_{\varepsilon^{(1)}, \varepsilon^{(0)}} D(y) = (2dn + 2n - 1)(2d + 1)^{n-2}.$$

Пусть $L = l_0 X_0 + \ldots + l_n X_n \in \mathbb{Z}[X_0, \dots, X_n]$ – линейная форма с целыми коэффициентами l_i, $0 \leqslant i \leqslant n$, такая что L не обращается в нуль ни в какой точке типа (i) многообразия $\mathcal{W}' \subset \mathbb{P}^n(\overline{C_2})$ решений системы (3), и $L \neq l_0 X_0$. Согласно [13], см, также [5], можно проверить это условие за полиномиальное время от d^n и длины записи входных данных, включая L.

Определим множество линейных форм

$$\mathcal{L}_N = \{ \sum_{0 \leqslant i \leqslant n} c^i X_i \ : \ 1 \leqslant i \leqslant N, i \in \mathbb{Z} \}.$$

Форма L, удовлетворяющая рассматриваемому условию, может быть выбрана из множества $\mathcal{L}_N$, причём $N \leqslant \mathcal{P}(d^n)$ для некоторого полинома $\mathcal{P}$.

Линейная форма L не обращается в нуль в никакой точке типа (i) многообразия $\mathcal{W}'$ тогда и только тогда, когда многочлен

$$D(y)(1, \varepsilon, L - l_0 X_0, -l_1 X_0, \dots, -l_n X_0) \in K_1[L, X_0, \varepsilon]$$

ненулевой. Этот многочлен тождественно равен нулю на $\mathcal{W}'$.

Определим $\iota_0(y)$ (соответственно $\iota_1(L, y)$) как максимальное целое число a, такое что X_0^a (соответственно ε^a) делит многочлен $D(y)(1, \varepsilon, L - l_0 X_0, -l_1 X_0, \dots, -l_n X_0)$. Тогда $\iota_0(y)$ – число корней системы (3) типа (i) и, следовательно, не зависит от выбора L. Положим

$$G(y) = D(y)(1, \varepsilon, L - l_0, -l_1, \dots, -l_n) \in K_1[\varepsilon, L].$$

Обозначим через $H(y) \in K_1[\varepsilon, L]$ сепарабельный многочлен, который равен произведению всех различных неприводимых множителей многочлена $G(y)$, которые не принадлежат $K_1[\varepsilon]$. Согласно [13], см. также [5], многочлен $G(y)$ можно вычислить за полиномиальное время от d^n и размера входных данных, включая L.

Мы имеем $\mu_0(y) = \deg_L G(y) = \deg_{U_0, \dots, U_n} D(y) - \iota_0(y)$. Представим

$$G(y) = \varepsilon^{\iota_1(L,y)} \sum_{0 \leqslant i \leqslant \mu_0(y)} a_i L^i,$$

где $a_i \in K_1[\varepsilon]$ для всех i. Отметим, что a_i зависит от коэффициентов $l_0, \dots, l_n$ линейной формы L. Так что обозначим также $a_i = a_i(l_0, \dots, l_n)$.

Лемма 3. *Пусть L – произвольная линейная форма, не обращающаяся в нуль ни в какой точке типа* (i) *многообразия решений системы* (3). *Пусть* $\mathrm{lc}_\varepsilon(a_{\mu_0(y)}(l_0, \dots, l_n))$ – *коэффициент при старшей* *степени многочлена* $a_{\mu_0(y)}(l_0,\ldots,l_n)$ *относительно* ε. *Тогда многочлен*

$$\varepsilon^{\iota_1(L,y)}a_{\mu_0(y)}(l_0,\ldots,l_n)/\mathrm{lc}_\varepsilon(a_{\mu_0(y)}(l_0,\ldots,l_n))$$

не зависит от выбора L. *Кроме того,*

$$\iota_1(L,y)+\deg_\varepsilon a_{\mu_0(y)}(l_0,\ldots,l_n)=(2dn+2n-1)(2d+1)^{n-2}.$$

Доказательство. Представим многочлен $D(y)=D_1D_2$, где многочлен D_1 (соответственно D_2) равен $\prod_{j\in J'}\sum_{1\leqslant i\leqslant n}U_i\eta_i^{(j)}$ (соответственно $\prod_{j\in J''\cup J'''}\sum_{0\leqslant i\leqslant n}U_i\eta_i^{(j)}$) с точностью до множителя из $K_1[\varepsilon]$. Следовательно, по Следствию 3 можно выбрать эти множители так, что $D_1\in K_1[U_0,\ldots,U_n]$, и $D_2\in K_1[\varepsilon^{(0)},\varepsilon^{(1)},U_0,\ldots,U_n]$. Представим

$$D_2=\sum_{0\leqslant i\leqslant\mu_0(y)}A_iU_0^i,$$

где все $A_i\in K_1[\varepsilon^{(0)},\varepsilon^{(1)},U_1,\ldots,U_n]$ являются однородными многочленами относительно $U_1,\ldots,U_n$ степени $\deg_{U_1,\ldots,U_n}A_i=\mu_0(y)-i$. В частности $A_{\mu_0(y)}\in K_1[\varepsilon^{(0)},\varepsilon^{(1)}]$. Теперь мы немедленно получаем, что

$$\varepsilon^{\iota_1(L,y)}a_{\mu_0(y)}(l_0,\ldots,l_n)=D_1(-l_1,\ldots,-l_n)A_{\mu_0(y)}(1,\varepsilon).$$

Первое утверждение леммы следует из этого равенства. Второе утверждение следует из того, что $D(y)(0,1,U_0,\ldots,U_n)$ является U-результантом системы (4). Следовательно,

$$0\neq A_{\mu_0(y)}(0,\varepsilon^{(1)})=(\varepsilon^{(1)})^{(2dn+2n-1)(2d+1)^{n-2}}\alpha,$$

где $\alpha\in K_1$. Лемма доказана.

Положим $\mu_1(L,y)=\deg_\varepsilon a_{\mu_0(y)}$.

Определим $\mu_2(L,y)$ как максимальное i, такое что ε не делит a_i. Заметим, что $\mu_2(L,y)$ является числом корней, учитывая их кратности, типа (ii) или (iii) системы (3), таких что $|(L/X_0)(\eta)|$ не является бесконечно большой величиной относительно поля C_1. Так что $\mu_2(L,y)\geqslant\mu_2(y)$.

Положим $\mu_1(y)=\mu_1(y_2,\ldots,y_n)=\max_L\mu_1(L,y)$, где максимум берётся по всем линейным формам L, для которых определено $\mu_1(L,y)$.

Пусть L – линейная форма, не обращающаяся в нуль ни в какой точке типа (i) многообразия решений системы (3). Рассмотрим $G(y)$ как многочлен от ε, L. Пусть $(u_0, v_0), (u_1, v_1), \ldots, (u_r, v_r)$ – последовательные вершины многоугольника Ньютона $G(y)$, ср. [11], в координатах (ε, L), такие что

- $(u_0, v_0) = ((2dn + 2n + 1)(2d + 1)^{n-2}, \mu_0(y))$,
- $u_{i+1} < u_i$ для всех $0 \leqslant i \leqslant r - 1$,
- $u_r = \iota_1(L, y)$.

Такая последовательность существует по Лемме 3 и определению $\iota_1(L, y)$. Следовательно, $r \geqslant 0$. Кроме того, из наших определений вытекает, что

- $v_1 \leqslant v_0$ и $v_{i+1} < v_i$ для всех $1 \leqslant i \leqslant r - 1$,
- $u_0 - u_r = \mu_1(L, y)$,
- $v_r = \mu_2(L, y)$, следовательно, если $y_2, \ldots, y_n$ – элементы вещественного упорядоченного поля, являющегося расширением R, то $v_r \geqslant 2$.

Определим $(u_{r+1}, v_{r+1}) = (\iota_1(L, y), 0)$. Мы будем обозначать $u_i = u_i(L, y)$, $v_i = v_i(L, y)$ и $r = r(L, y)$, когда будет существенна зависимость от L и y.

Для линейной формы L, такой как выше, и y определим $w_i = w_i(L, y) \in \mathbb{Q}$, $0 \leqslant i \leqslant \mu_0(y)$, следующими условиями:

- $w_{\mu_0(y)} = u_0$, если $v_1 < v_0$,
- $w_{\mu_0(y)} = u_1$, если $v_1 = v_0$,
- $w_i = u_{j+1} + (u_j - u_{j+1})(i - v_{j+1})/(v_j - v_{j+1})$, если $v_{j+1} \leqslant i \leqslant v_j$ и $1 \leqslant j \leqslant r$ (и $v_r \neq v_{r+1}$ при $j = r$).

Следовательно, точки с координатами (w_i, i), $\mu_2(L, y) \leqslant i \leqslant \mu_0(y)$ принадлежат ломаной Ньютона многочлена $G(y)$. Положим

$$w = w(L, y) = (w_0(L, y), \ldots, w_{\mu_0(y)}(L, y)) \in \mathbb{Q}^{\mu_0(y)+1}.$$

Определим частичный порядок на $\mathbb{Q}^{\mu_0(y)+1}$ следующим образом. Пусть $z = (z_0, \ldots, z_{\mu_0(y)})$ и $z' = (z'_0, \ldots, z'_{\mu_0(y)})$ – два элемента $\mathbb{Q}^{\mu_0(y)+1}$. Тогда $z \geqslant z'$ в том и только в том случае, если $z_i \geqslant z'_i$ для всех $0 \leqslant i \leqslant \mu_0(y)$.

Заметим, что $\mu_0(y)$, $\mu_1(L, y)$, $\mu_2(L, y)$, $r(L, y)$, все $u_i(L, y)$, $v_i(L, y)$, $w(L, y)$ могут быть вычислены за полиномиальное время от d^n и длины записи входных данных, включая L и y.

Лемма 4. *Положим* $N_1 = (2d{+}2)(2d{+}1)^{n-1}n{+}1$. *Тогда существует линейная форма* $L_1 \in \mathcal{L}_{N_1}$, *такая что* L_1 *не обращается в нуль ни в какой точке типа* (i) *многообразия решений системы* (3), *и*

$$w(L_1, y) \leqslant w(L, y)$$

для всякой линейной формы L, *такой как выше. Далее, существует семейство, состоящее из самое большее* $(2d+2)(2d+1)^{n-1}$ *гиперплоскостей в* $(n+1)$*-мерном пространстве, такое что, если коэффициенты произвольной линейной формы* L *не принадлежат объединению гиперплоскостей из этого семейства, то* L *не обращается в нуль ни в какой точке типа* (i) *многообразия решений системы* (3), *и*

$$w(L, y) = w(L_1, y).$$

Доказательство. Мы используем обозначения из доказательства Леммы 3. Форма L не обращается в нуль ни в какой точке типа (i) многообразия решений системы (3) тогда и только тогда, когда $\sum_{1\leqslant i\leqslant n} l_i\eta_i^{(j)} \neq 0$ для всех $j \in J'$. В дальнейшем в доказательстве леммы мы будем предполагать, что $L = \sum_{0\leqslant i\leqslant n} l_i X_i$ не обращается в нуль ни в какой точке типа (i) многообразия решений системы (3).

Пусть $\mathrm{ord}_\varepsilon : \overline{C_2} \to \mathbb{Q} \cup \{+\infty\}$ – функция порядка. Напомним, что $\mathrm{ord}_\varepsilon(a)$ – это показатель монома наименьшей степени в разложении a в дробно-степенной ряд относительно ε с коэффициентами в $\overline{C_1}$.

Мы имеем

$$G(y) = \varepsilon^{\iota_1(L,y)} a_{\mu_0(y)}(l_0, \ldots, l_n) \prod_{j\in J''\cup J'''} (L - (L/X_0)(\eta^{(j)})),$$

где $\eta^{(j)} = (\eta_0^{(j)} : \ldots : \eta_n^{(j)})$ – семейство всех корней, учитывая кратности, типов (ii) или (iii) системы (3) в $\mathbb{P}^n(\overline{C_2})$. Согласно Лемме 3 ломаная Ньютона (u_i, v_i), $0 \leqslant i \leqslant r$, многочлена $G(y)$ полностью определена порядками его корней $(L/X_0)(\eta^{(j)})$, $j \in J''$, и $w(L, y)$ является наименьшей тогда и только тогда, когда

$$\mathrm{ord}_\varepsilon(L/X_0)(\eta^{(j)}) = \min_{0\leqslant i\leqslant n} \mathrm{ord}_\varepsilon(\eta_i^{(j)}/\eta_0^{(j)}), \tag{5}$$

для всякого $j \in J''$. Теперь заметим, что (5) выполнено для всякого $j \in J''$ тогда и только тогда, когда коэффициенты L не принадлежат к объединению самое большее $\#J''$ гиперплоскостей в

$(n+1)$-мерном пространстве. Следовательно, требуемая линейная форма L_1 может быть выбрана из $\mathcal{L}_{N_1}$. Лемма доказана.

Определим $r(y) = r(L_1, y)$, $u_i(y) = w(L_1, y)$, $v_i(y) = w(L_1, y)$ для $1 \leqslant i \leqslant r(y) + 1$ и $w(y) = w(L_1, y)$, где L_1 – линейная форма из формулировки Леммы 4. Следовательно, $\mu_1(y) = u_0(y) - u_{r(y)}(y)$ согласно нашим определениям.

Определим $\mu(y) = (\mu_0(y), w(y)) \in \mathbb{Z} \times \mathbb{Q}^{\mu_0(y)+1}$.

Рассмотрим (3) как систему относительно $\varepsilon^{(0)}, \varepsilon^{(1)}$ и $X_0, \dots, X_n$ с коэффициентами в поле K_1. Тогда она имеет решения в произведении проективных пространств $(\mathbb{P}^1 \times \mathbb{P}^n)(\overline{C_1})$ с координатами $((\varepsilon^{(0)} : \varepsilon^{(1)}), (X_0 : \dots : X_n))$. Обозначим через $\mathcal{W}$ объединение всех неприводимых над $\overline{C_1}$ компонент W многообразия решений системы (3) в $(\mathbb{P}^1 \times \mathbb{P}^n)(\overline{C_1})$, таких что W не содержится в гиперплоскости $\mathcal{Z}(c_0\varepsilon^{(0)} + c_1\varepsilon^{(1)})$ для любых $c_0, c_1 \in \overline{C_1}$. С другой стороны, рассмотрим систему (3) над полем C_2, и напомним, что $\mathcal{W}'$ является многообразием решений системы (3) в $\mathbb{P}^n(\overline{C_2})$. Тогда, см. [5] или [9], Следствие 4.1, всякая неприводимая компонента W многообразия $\mathcal{W}$ биективно соответствует при локализации неприводимой компоненте W', определённой над полем $\overline{C_1}(\varepsilon)$, многообразия $\mathcal{W}'$. Таким образом, всякая неприводимая компонента W многообразия $\mathcal{W}$ соответствует подмножеству решений (3), содержащемуся в W'. Отметим, что если W' фиксировано, то выполнено одно из следующих условий:

- для всякого $\eta \in W'$ решение η – типа (i),
- для всякого $\eta \in W'$ решение η – типа (ii) или (iii).

Помимо этого все рассматриваемые компоненты W являются кривыми, т.е. $\dim W = 1$.

Обозначим через $\mathcal{V} = \mathcal{V}(y)$ объединение всех неприводимых компонент W многообразия $\mathcal{W}$, соответствующих решениям (3) типа (ii) или (iii). Тогда пересечение $\mathcal{V} \cap \mathcal{Z}(X_0)$ не является бесконечным по Следствию 3 и, так как $\dim \mathcal{V} = 1$.

Рассмотрим линейную форму $L \in \mathbb{Z}[X_0, \dots, X_n]$, такую что

(a) L не обращается в нуль ни в какой точке множества $\mathcal{W}'$ типа (i),

(b) L не обращается в нуль ни в какой точке множества $\mathcal{V} \cap \mathcal{Z}(X_0)$.

Лемма 5. *Пусть L – линейная форма, удовлетворяющая условию* (a), *следовательно, $w(L,y)$ определено. Тогда $w(L,y)=w(y)$ тогда и только тогда, когда L удовлетворяет условию* (b).

Доказательство. Мы используем один факт из доказательства Леммы 4. Пусть $\zeta_0^{(j)},\dots,\zeta_n^{(j)}\in\overline{K_2}$, такие что

$$\zeta^{(j)}=(\zeta_0^{(j)}:\ldots:\zeta_n^{(j)})=(\eta_0^{(j)}:\ldots:\eta_n^{(j)})\in\mathbb{P}^n(\overline{K_2}),$$

$\mathrm{ord}_\varepsilon(\zeta_i^{(j)})\geqslant 0$ для любого $0\leqslant i\leqslant n$, и существует $1\leqslant i_0\leqslant n$ (оно зависит от j), такое что $\mathrm{ord}_\varepsilon(\zeta_{i_0}^{(j)})=0$. Теперь пусть линейная форма $L=\sum_{0\leqslant i\leqslant n} l_iX_i$ удовлетворяет условиям (a) и (b). Имеем $\mathcal{V}\cap\mathcal{Z}(X_0)\subset\mathcal{Z}(\varepsilon^{(1)})$. Следовательно,

$$\mathcal{V}\cap\mathcal{Z}(X_0)=\{\mathrm{st}_\varepsilon(\zeta^{(j)})\ :\ j\in J''\},$$

где $\mathrm{st}_\varepsilon:\mathbb{P}^n(\overline{C_2})\to\mathbb{P}^n(\overline{C_1})$ – отображение стандартной части, см. [9, 10] (стандартная часть элемента $z\in\mathbb{P}^n(\overline{C_2})$ есть элемент $z'\in\mathbb{P}^n(\overline{C_1})$, который бесконечно близок к z). Следовательно, $0\notin L(\mathcal{V}\cap\mathcal{Z}(X_0))$ тогда и только тогда, когда для всякого $j\in J''$ справедливо равенство $\mathrm{ord}_\varepsilon(\sum_{0\leqslant i\leqslant n} l_i\zeta_i^{(j)})=0$, т.е. тогда и только тогда, когда

$$\mathrm{ord}_\varepsilon(\sum_{0\leqslant i\leqslant n} l_i\zeta_i^{(j)})=\min_{0\leqslant i\leqslant n}\mathrm{ord}_\varepsilon(\zeta_i^{(j)})$$

для всякого $j\in J''$. Это эквивалентно условию, что для всякого $j\in J''$

$$\mathrm{ord}_\varepsilon((L/X_0)(\eta^{(j)}))=\min_{0\leqslant i\leqslant n}\mathrm{ord}_\varepsilon((X_i/X_0)(\eta^{(j)})).$$

В доказательстве Леммы 4 установлено, что последнее эквивалентно равенству $w(L,y)=w(y)$. Лемма доказана.

Согласно [9, 10] стандартная часть элемента $\mathbb{P}^n(\overline{C_2})$ может быть вычислена за полиномиальное время от d^n и длины записи входных данных. Следовательно, можно проверить, удовлетворяет ли линейная форма L условиям (a) и (b) за полиномиальное время от d^n и длины записи входных данных. Помимо этого, для всякого y, такая линейная форма L может быть выбрана из множества $\mathcal{L}_{N_2}$ с N_2, ограниченным сверху полиномом от d^n.

Лемма 6. *Пусть L – линейная форма, удовлетворяющая условиям* (a) *и* (b)*. Обозначим через* $\Lambda_1 = K_1[\mathcal{V} \setminus \mathcal{Z}(X_0)]$ *кольцо регулярных функций на алгебраическом многообразии* $\mathcal{V} \setminus \mathcal{Z}(X_0)$ *и через* $\Lambda_2 = K_1[\varepsilon, (L/X_0)|_{\mathcal{V}\setminus\mathcal{Z}(X_0)}]$ *подалгебру алгебры* Λ_1*, порождённую функциями* ε *и* L/X_0*. Тогда* $\Lambda_2 \subset \Lambda_1$ *– конечное расширение алгебр. Кроме того, имеет место изоморфизм*

$$\Lambda_2 \longrightarrow K_1[Z_1, Z_2]/(H(y)(Z_1, Z_2)),$$

где Z_1, Z_2 *– новые переменные,* $H(y) \in K_1[\varepsilon, L]$ *– многочлен, введённый выше, и*

$$\varepsilon \mapsto Z_1 \bmod H(y)(Z_1, Z_2), \quad L \mapsto Z_2 \bmod H(y)(Z_1, Z_2)$$

при этом изоморфизме.

Доказательство. Существует целое число λ, такое что $\varepsilon^{(0)}+\lambda\varepsilon^{(1)}$ не обращается в нуль ни в какой точке многообразия $\mathcal{V} \cap \mathcal{Z}(X_0)$. Рассмотрим рациональный морфизм $\pi : \mathbb{P}^1 \times \mathbb{P}^n \to \mathbb{P}^2$, определённый формулой

$$((\varepsilon^{(0)} : \varepsilon^{(1)}), (X_0 : \ldots : X_n)) \mapsto ((\varepsilon^{(0)} + \lambda\varepsilon^{(1)})L : \varepsilon^{(1)}X_0 : \varepsilon^{(0)}X_0).$$

Согласно выбору L и λ морфизм π определён везде на $\mathcal{V}$. Прообраз $(\pi|_{\mathcal{V}})^{-1}(z)$ является конечным для всякой точки $z \in \pi(\mathcal{V})$. Таким образом, $\pi(\mathcal{V})$ замкнуто в топологии Зарисского, и морфизм

$$\pi|_{\mathcal{V}} : \mathcal{V} \to \pi(\mathcal{V})$$

конечен. Поэтому координатные функции $(X_i/X_0)|_{\mathcal{V}\setminus\mathcal{Z}(X_0)}$ на алгебраическом многообразии $\mathcal{V} \setminus \mathcal{Z}(X_0)$ (они регулярны на этом многообразии) являются целыми над алгеброй $K_1[\varepsilon, ((1 + \lambda\varepsilon)L/X_0)|_{\mathcal{V}\setminus\mathcal{Z}(X_0)}]$ для всех i. Следовательно, эти координатные функции также целы над алгеброй $K_1[\varepsilon, (L/X_0)|_{\mathcal{V}\setminus\mathcal{Z}(X_0)}]$. Последнее утверждение леммы следует непосредственно из определений алгебраического многообразия $\mathcal{V}$ и многочлена $H(y)$. Лемма доказана.

Следствие 5. *Пусть L – линейная форма, удовлетворяющая условиям* (a) *и* (b)*. Тогда* $\mu_2(L, y) = \mu_2(y)$*.*

Доказательство. Число решений η системы (3) типа (ii) или (iii), для которых $(L/X_0)(\eta)$ не является бесконечно большим относительно поля C_1 равно $\mu_2(L, y)$. Далее, согласно доказанному утверждению о целой зависимости координатных функций, если $(L/X_0)(\eta)$ не является бесконечно большим (соответственно является бесконечно большим) относительно поля C_1, то $(X_i/X_0)(\eta)$ – не бесконечно большая величина (соответственно бесконечно большая величина) для всех $1 \leqslant i \leqslant n$ (соответственно для по крайней мере одного $1 \leqslant i \leqslant n$). Таким образом, $\mu_2(y) = \mu_2(L, y)$. Следствие доказано. Данное следствие может быть доказано также, используя Лемму 5.

Лемма 7. *Пусть L – линейная форма, удовлетворяющая условиям* (a) *и* (b). *Тогда η является корнем типа* (iii) *(соответственно* (ii)*) системы* (3) *тогда и только тогда, когда $|(L/X_0)(\eta)|$ не является бесконечно большой величиной (соответственно является бесконечно большой величиной) относительно поля C_1. Кроме того, семейство корней, учитывая кратности, многочлена $G(y)$ совпадает с семейством $\{(L/X_0)(\eta^{(j)})\}_{j\in J''\cup J'''}$, где $\{\eta^{(j)}\}_{j\in J''\cup J'''}$ – семейство всех корней типа* (ii) *или* (iii) *системы* (3).

Доказательство. Первое утверждение леммы следует непосредственно из определений. Второе было установлено в доказательстве Леммы (4). Лемма доказана.

Обозначим через $Y_2, \ldots, Y_n$ новые переменные. Положим $Y = (Y_2, \ldots, Y_n)$ Следовательно, $\mu_0(Y) \geqslant \mu_0(y)$ и, если $\mu_0(Y) = \mu_0(y)$, то $w(Y) \leqslant w(y)$ для всякого y. U-результант

$$D(Y) \in R[Y_2, \ldots, Y_n, \varepsilon^{(0)}, \varepsilon^{(1)}, U_0, \ldots, U_n]$$

является многочленом от $Y_2, \ldots, Y_n$. Заметим, что степень многочлена $D(Y)$ относительно $Y_2, \ldots, Y_n$ ограничена сверху полиномом от d^n.

Лемма 8. *Для всякого y существует многочлен $\Phi_2(y) \in R[Y_2, \ldots, Y_n]$ со степенью, ограниченной сверху многочленом от d^n, такой что $\Phi_2(y)(y_2, \ldots, y_n) \neq 0$, и, если $y' = (y'_2, \ldots, y'_n) \in \mathbb{A}^{(n-1)}(K_3)$, $\Phi_2(y)(y'_2, \ldots, y'_n) \neq 0$ (где K_3 – произвольное расширение поля C_2), то $\mu_0(y') \geqslant \mu_0(y)$ и, если $\mu_0(y') = \mu_0(y)$, то $w(y') \leqslant w(y)$.*

Доказательство. Пусть L – линейная форма, удовлетворяющая условиям (a) и (b) для y. Тогда $w(L, y) = w(y)$ по Лемме 5. Рассмотрим многочлены $G(y)$ и $G(Y)$, соответствующие L. Пусть

$$G(Y) = \sum_{i,j\geqslant 0} g_{i,j} \varepsilon^i L^j,$$

где все $g_{i,j} \in R[Y_2, \dots, Y_n]$. Тогда $G(y) = \sum_{i,j} g_{i,j}(y_2, \dots, y_n)\varepsilon^i L^j$. Пусть $r = r(y)$, $u_i = u_i(L, y)$, $v_i = v_i(L, y)$, $1 \leqslant i \leqslant r$. Положим

$$\Phi_2(y) = \prod_{0 \leqslant i \leqslant r} g_{u_i, v_i}.$$

Многочлен $\Phi_2(y)$ – требуемый согласно Лемме 4 и Лемме 5. Лемма доказана.

Следствие 6. *Для произвольного y и линейной формы L, удовлетворяющей* (a), (b) *для y существует многочлен $\Phi_3(y) \in R[Y_2, \dots, Y_n]$ со степенью, ограниченной сверху многочленом от d^n, такой что $\Phi_3(y)(y_2, \dots, y_n) \neq 0$ и, если $y' = (y'_2, \dots, y'_n) \in \mathbb{A}^{(n-1)}(K_3)$, $\Phi_3(y)(y'_2, \dots, y'_n) \neq 0$ (где K_3 – произвольное расширение поля C_2), то линейная форма L удовлетворяет условию* (a) *для y', и выполнено одно из следующих условий*

- $\mu_0(y') > \mu_0(y)$,
- $\mu_0(y') = \mu_0(y)$ *и* $w(L, y') \leqslant w(L, y)$.

Доказательство. Это было установлено в доказательстве леммы.

Лемма 9. *Существуют непустые открытые в топологии Зарисского подмножества U_0, U_1 в $\mathbb{A}^{(n-1)}(C_1)$, такие что $U_1 \subset U_0$, и*

- $y \in U_0$ *тогда и только тогда, когда* $\mu_0(y) = \mu_0(Y)$,
- $y \in U_1$ *тогда и только тогда, когда* $\mu_0(y) = \mu_0(Y)$, *и* $w(y) = w(Y)$.

Кроме того, $\mu_0(Y) = (2d + 2)(2d + 1)^{n-1}$.

Доказательство. Имеем $\mu_0(Y) = (2d+2)(2d+1)^{n-1}$ согласно нашим определениям и Следствию 3. Пусть $Y_i - y_i$, $2 \leqslant i \leqslant n$, – алгебраически независимые бесконечно малые относительно поля K_1. Тогда все требуемые утверждения следуют из Леммы 8. Лемма доказана.

Следствие 7. *Для всякого y, если $\mu_0(y) = \mu_0(Y)$, то $\iota_0(y) = 0$.*

Доказательство. Это следует из Следствия 3 и определения $\mu_0(Y)$.

Пусть $\varepsilon > 0$ – бесконечно малый элемент относительно поля R_1, элемент $\varepsilon_1 > 0$ бесконечно малый относительно поля

$R_1(\varepsilon)$ (напомним, что $R_2 = R_1(\varepsilon)$), и элемент $\varepsilon_2 > 0$ бесконечно малый относительно поля $R_1(\varepsilon, \varepsilon_1)$. Алгебраическое замыкание $\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)}$ снабжено вещественной структурой. Так что мы можем рассматривать системы полиномиальных уравнений и неравенств с квадратами абсолютных величин, см. [9, 10]. Именно, рассмотрим систему полиномиальных уравнений относительно $X_0, X_1, \ldots, X_n$, $Y_2, \ldots, Y_n$

$$\begin{cases} h = 0, & \\ \frac{\partial h}{\partial X_i} - Y_i \frac{\partial h}{\partial X_1} = 0, & 2 \leqslant i \leqslant n, \\ \sum_{2 \leqslant i \leqslant n} |Y_i - y_i|^2 = \varepsilon_2, & \\ \sum_{0 \leqslant i \leqslant n} |X_i|^2 > \varepsilon_1^{-1}, & \\ X_0 = 1. & \end{cases} \qquad (6)$$

Лемма 10.

- *Если $\mu_0(Y) > \mu_0(y)$, то система (6) имеет решение в аффинном пространстве $\mathbb{A}^{2n}(\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)})$.*
- *Пусть $(1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n}(\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)})$ – произвольное решение системы (6). Тогда $\mu_0(y') > \mu_0(y)$.*

Доказательство. Выберем элементы $y'_i \in \overline{R_1(\varepsilon_2)}$, $2 \leqslant i \leqslant n$, так что

- $\sum_{2 \leqslant i \leqslant n} (y'_i - y_i)^2 = \varepsilon_2$,
- $(y'_2, \ldots, y'_n) \in U_0$,

и положим $y' = (y'_2, \ldots, y'_n)$. Пусть L – линейная форма, удовлетворяющая условиям (a) и (b) одновременно для y, y' и переменных Y.

Пусть $\mu_0(Y) > \mu_0(y)$. Тогда степень $\deg_L G(y') > \deg_L G(y)$. Коэффициенты обоих многочленов $D(y')$ и $D(y)$ получаются из коэффициентов $D(Y)$ подстановкой значений $Y_i = y_i$ и $Y_i = y'_i$ соответственно. Коэффициент $G(Y)$ при L^i может быть представлен как многочлен $\psi_i(Z_2, \ldots, Z_n)$ от $Z_j = Y_j - y_j$, $2 \leqslant j \leqslant n$. Так что согласно нашим определениям, если $i > \deg_L G(y)$, то свободный член многочлена ψ_i равен нулю. Следовательно, существует корень $L = \lambda' \in \overline{R_1(\varepsilon, \varepsilon_2)}$ многочлена $G(y')$, такой что $|\lambda'|$ – бесконечно большая величина относительно поля $\overline{R_1(\varepsilon, \varepsilon_1)}$. По Лемме 6 существуют $\eta_1, \ldots, \eta_n \in \overline{R_1(\varepsilon, \varepsilon_2)}$, такие что $L(1, \eta_1, \ldots, \eta_n) = \lambda'$, и $(1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n)$ – требуемое решение системы (6). Утверждение (i) доказано.

Предположим, что существует решение

$$(1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n}(\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)})$$

системы (6). Мы будем предполагать без ограничения общности, что линейная форма L удовлетворяет условиям (a), (b) одновременно для Y, y и y'. Так как $y'_i - y_i$ являются бесконечно малыми, то по Лемме 8 $\mu_0(y') \geqslant \mu_0(y)$. Предположим, что $\mu_0(y') = \mu_0(y)$. Тогда существует многочлен $\Psi \in R_1(\varepsilon)[L, Z_2, \ldots, Z_n]$ степени $\deg_L \Psi \leqslant \mu_0(y)$, такой что $\Psi(L, 0, \ldots, 0) = 0$ и,

$$G(y') = G(y) + \Psi(L, y'_2 - y_2, \ldots, y'_n - y_n). \tag{7}$$

Все корни многочлена $G(y) \in R_2[L]$ (рассматриваемого как многочлен от L) не являются бесконечно большими относительно поля $R_1(\varepsilon)$. Следовательно, из (7) вытекает, что все корни многочлена $G(y')$ также не являются бесконечно большими относительно поля $R_1(\varepsilon)$. Теперь по Лемме 6 мы получаем, что $\sum_{0 \leqslant i \leqslant n} |\eta'_i|^2$ не является бесконечно большой величиной относительно поля $R_1(\varepsilon)$. Это противоречие. Утверждение (ii) и вся лемма доказаны.

Пусть теперь $\varepsilon_0 > 0$ – бесконечно малая относительно поля R_1, элемент $\varepsilon_1 > 0$ – бесконечно малый относительно поля $R_1(\varepsilon_0)$, элемент $\varepsilon_2 > 0$ – бесконечно малый относительно поля $R_1(\varepsilon_0, \varepsilon_1)$, и $\varepsilon_3 > 0$ – бесконечно малый элемент относительно поля $R_1(\varepsilon_0, \varepsilon_1, \varepsilon_2)$. Алгебраическое замыкание $\overline{R_1(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)}$ снабжено вещественной структурой.

Пусть L удовлетворяет условиям (a) и (b) для y. Обозначим $r = r(L, y)$, $0 \leqslant j \leqslant r - 1$, $u_j = u_j(L, y)$, $u_{j+1} = u_{j+1}(L, y)$, $v_j = v_j(L, y)$, $v_{j+1} = v_{j+1}(L, y)$. Рассмотрим систему полиномиальных уравнений и неравенств относительно $\varepsilon, X_0, X_1, \dots, X_n, Y_2, \dots, Y_n$

$$\begin{cases} h = 0, \\ \frac{\partial h}{\partial X_i} - Y_i \frac{\partial h}{\partial X_1} = 0, & 2 \leqslant i \leqslant n, \\ \sum_{2 \leqslant i \leqslant n} |Y_i - y_i|^2 = \varepsilon_1, \\ L\varepsilon_3 = 1, \\ \varepsilon_2 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})} < |\varepsilon|^2 < \varepsilon_0 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})}, \\ X_0 = 1. \end{cases} \tag{8}$$

Лемма 11. *Пусть* $\mu_0(y) = \mu_0(Y)$. *Пусть* $0 \leqslant j \leqslant r-1$, $j \in \mathbb{Z}$. *Пусть* $u_i = u_i(L, Y)$, $v_i = v_i(L, Y)$ *для всех* $0 \leqslant i \leqslant j$.

(i) *Пусть*

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} = \frac{v_j(L, Y) - v_{j+1}(L, Y)}{u_j(L, Y) - u_{j+1}(L, Y)},$$

и $u_{j+1} \neq u_{j+1}(L, Y)$. *Тогда система* (8) *имеет решение в* $\mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_1, \varepsilon_3)})$.

(ii) *Пусть*

$$(\varepsilon', 1, \eta_1, \dots, \eta_n, y'_2, \dots, y'_n) \in \mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)}) \tag{9}$$

– произвольное решение системы (8). *Тогда* $\mu_0(y') = \mu_0(Y)$, $u_{j+1}(L, y') < u_{j+1}$, *и* $w(L, y') < w(L, y)$.

Доказательство. Мы используем факты, установленные в доказательстве Леммы 6. Чтобы доказать (i) выберем элементы $y'_i \in \overline{R_1(\varepsilon_1)}$, $2 \leqslant i \leqslant n$, так что

- $\sum_{2 \leqslant i \leqslant n} (y'_i - y_i)^2 = \varepsilon_1$,
- $w(L, y'_2, \dots, y'_n) = w(L, Y)$

(такие элементы существуют по Следствию 6) и положим $y' = (y'_2, \dots, y'_n)$. Пусть $G(y) = \sum_{i_1, i_2 \geqslant 0} g_{i_1, i_2} \varepsilon^{i_1} L^{i_2}$, где все $g_{i_1, i_2} \in R_1$. Положим

$$B_j = \{(i_1, i_2) \in \mathbb{Z}^2 : (v_{j+1} - v_j) i_1 - (u_{j+1} - u_j) i_2 = v_{j+1} u_j - u_{j+1} v_j\},$$

$$A_j = \{(i_1, i_2) \in B_j : u_{j+1} \leqslant i_1 \leqslant u_j\},$$

$$G^*(y) = \sum_{(i_1, i_2) \in A_j} g_{i_1, i_2} \varepsilon^{i_1}.$$

Таким образом, A_j – множество всех точек с целыми координатами, содержащихся в стороне с вершинами (u_{j+1}, v_{j+1}), (u_j, v_j) ломаной Ньютона многочлена $G(y)$. Аналогично определяется многочлен $G^*(y')$. Согласно условиям леммы и, так как $w(L,y') = w(L,Y)$, существует корень $\varepsilon'_0 \in \overline{R_1(\varepsilon_1)}$ многочлена $G^*(y')$, рассматриваемого как многочлен от ε, такой что ε'_0 бесконечно малая величина относительно поля $\overline{R_1}$. Следовательно, $2\varepsilon_2 < |\varepsilon'_0|^2 < \varepsilon_0/2$.

Рассматривая многоугольник Ньютона многочлена $G(y')$ относительно переменных ε и L, мы получаем, что существует корень этого многочлена в поле дробно-степенных рядов от ε_3 с коэффициентами в $\overline{R_1(\varepsilon_1)}$, такой что

$$L = \varepsilon_3^{-1}, \quad \varepsilon = \varepsilon' = \varepsilon'_0 \varepsilon_3^{(v_j - v_{j+1})/(u_j - u_{j+1})} +$$

$$+ \sum_{1 \leqslant i \in \mathbb{Z}, i/\nu > (v_j - v_{j+1})/(u_j - u_{j+1})} \varepsilon'_i \varepsilon_3^{i/\nu}$$

где $0 < \nu \in \mathbb{Z}$ и $\varepsilon'_i \in \overline{R_1(\varepsilon_1)}$ для всех i. Следовательно, $\varepsilon_2 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})} < |\varepsilon'|^2 < \varepsilon_0 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})}$.

Многочлен $G(y')(L/X_0, \varepsilon)$, рассматриваемый как полином от $X_1/X_0, \ldots, X_n/X_0$, ε с коэффициентами в $\overline{R_1(\varepsilon_1)}$, не обращается в нуль тождественно на аффинном алгебраическом многообразии $\mathcal{V}(y') \setminus \mathcal{Z}(X_0)$. Более того, по Лемме 6 существует корень системы (8), такой что элемент ε' из (9) и (10) является одним и тем же. Утверждение (i) доказано.

Обратно, если выполнено (ii), то $\mu_0(y') = \mu_0(y)$, и $w(L,y') \leqslant w(L,y)$, поскольку y' принадлежит бесконечно малой окрестности точки y. Далее, аналогично доказательству (i) мы выводим, что $u_{j+1}(L,y') < u_{j+1}$. Следовательно, $w(L,y') < w(L,y)$. Лемма доказана.

Пусть L – линейная форма, удовлетворяющая условиям (a) и (b) для y. Обозначим $r = r(L,y)$, $0 \leqslant j \leqslant r$, $u_i = u_i(L,y)$, $v_i = v_i(L,y)$ для всех $0 \leqslant i \leqslant r+1$. Положим $u_{-1} = u_0 + 1$, $v_{-1} = v_0 - 1$. Рассмотрим систему полиномиальных уравнений и неравенств относительно $\varepsilon, X_0, X_1, \dots, X_n, Y_2, \dots, Y_n$

$$\begin{cases} h = 0, & \\ \frac{\partial h}{\partial X_i} - Y_i \frac{\partial h}{\partial X_1} = 0, & 2 \leqslant i \leqslant n, \\ \sum_{2 \leqslant i \leqslant n} |Y_i - y_i|^2 = \varepsilon_1, & \\ L\varepsilon_3 = 1, & \\ \varepsilon_2 |\varepsilon|^2 > \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})}, & \text{если } j \leqslant r-1, \\ |\varepsilon|^2 < \varepsilon_2 \varepsilon_3^{2(v_{j-1} - v_j)/(u_{j-1} - u_j)}, & \\ X_0 = 1. & \end{cases} \tag{11}$$

Лемма 12. *Пусть $\mu_0(y) = \mu_0(Y)$. Пусть $0 \leqslant j \leqslant r$, $j \in \mathbb{Z}$. Пусть $r(L, Y) \geqslant j+1$, и $u_i = u_i(L, Y)$, $v_i = v_i(L, Y)$ для всех $0 \leqslant i \leqslant j$. Пусть $v_0 \neq v_1$, если $j = 0$.*

(i) *Пусть*

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} > \frac{v_j(L, Y) - v_{j+1}(L, Y)}{u_j(L, Y) - u_{j+1}(L, Y)},$$

если $j \leqslant r-1$. Тогда система (11) имеет решение в $\mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_1, \varepsilon_3)})$.

(ii) *Пусть*

$$(\varepsilon', 1, \eta_1, \dots, \eta_n, y'_2, \dots, y'_n) \in \mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_1, \varepsilon_2, \varepsilon_3)}) \tag{12}$$

– произвольное решение системы (11). Тогда $r(L, y') \geqslant j+1$,

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} > \frac{v_j(L, y') - v_{j+1}(L, y')}{u_j(L, y') - u_{j+1}(L, y')}$$

при $j \leqslant r-1$, и

$$\frac{v_j(L, y') - v_{j+1}(L, y')}{u_j(L, y') - u_{j+1}(L, y')} > \frac{v_{j-1} - v_j}{u_{j-1} - u_j}$$

Следовательно, $\mu_0(y') = \mu_0(Y)$, и $w(L, y') < w(L, y)$.

Доказательство. Для доказательства (i) определим y' также, как в доказательстве Леммы 11. Поскольку $u_j = u_j(L, Y)$, $v_j = v_j(L, Y)$, то справедливо неравенство

$$\frac{v_j(L, Y) - v_{j+1}(L, Y)}{u_j(L, Y) - u_{j+1}(L, Y)} > \frac{v_{j-1} - v_j}{u_{j-1} - u_j}.$$

Рассматривая многоугольник Ньютона многочлена $G(y')$ относительно ε и L, мы получаем, что существует корень этого многочлена в поле дробно-степенных рядов от ε_2 с коэффициентами в $\overline{R_1(\varepsilon_1)}$, такой что

$$L = \varepsilon_3^{-1}, \quad \varepsilon = \varepsilon' = \sum_{i_0 \leqslant i \in \mathbb{Z}} \varepsilon_i' \varepsilon_3^{i/\nu}, \tag{13}$$

где $0 < \nu \in \mathbb{Z}$,

$$i_0/\nu < (v_j - v_{j+1})/(u_j - u_{j+1}), \quad \text{если} \quad j \leqslant r-1,$$
$$i_0/\nu > (v_{j-1} - v_j)/(u_{j-1} - u_j),$$

$\varepsilon_i' \in \overline{R_1(\varepsilon_1)}$ для всех i, и $0 \neq \varepsilon_{i_0}'$ является бесконечно малой величиной относительно поля R_1.

Следовательно, $\varepsilon_2|\varepsilon'|^2 > \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})}$, если $j \leqslant r-1$, и $|\varepsilon'|^2 < \varepsilon_2 \varepsilon_3^{2(v_{j-1}-v_j)/(u_{j-1}-u_j)}$. Оставшаяся часть доказательства утверждения (i) аналогична доказательству из Леммы 11.

Для доказательства (ii) рассмотрим многочлен $G(y')$, его ломаную Ньютона и корень (13) полинома $G(y')$. Мы имеем $\mu_0(y') = \mu_0(Y)$, $w(L,y') \leqslant w(L,y)$, и $u_i(L,y') = u_i(L,Y)$, $v_i(L,y') = v_i(L,Y)$ для всех $0 \leqslant i \leqslant j$, поскольку y' принадлежит бесконечно малой окрестности точки y.

Обозначим $p_j = (v_j - v_{j+1})/(u_j - u_{j+1})$, если $j \leqslant r-1$, и $q_j = (v_{j-1} - v_j)/(u_{j-1} - u_j)$. Имеем $i_0/\nu \leqslant p_j$, если $j \leqslant r-1$, и $i_0/\nu \geqslant q_j$. Далее, $i_0/\nu > q_j$, поскольку, иначе, ε_{i_0}' – бесконечно малая относительно поля R_1, что противоречит равенствам $u_j(L,y') = u_j(L,y)$, $v_j(L,y') = v_j(L,y)$.

Если $j = r$ или $j \leqslant r-1$, и $i_0/\nu < p_j$, то все требуемые утверждения леммы доказаны.

Пусть $j \leqslant r-1$, и $i_0/\nu = p_j$. Тогда ε_{i_0}' является бесконечно большой величиной относительно поля R_1. Это возможно только в случае, когда ломаная Ньютона многочлена $G(y')$ содержит сторону e', параллельную стороне e с вершинами (u_j, v_j), (u_{j+1}, v_{j+1}) ломаной Ньютона полинома $G(y)$ (так что e' и e лежат на различных параллельных прямых). Следовательно, если $(u_\alpha(L,y'), v_\alpha(L,y'))$, $(u_{\alpha+1}(L,y'), v_{\alpha+1}(L,y'))$ – вершины e, то $\alpha > j$. Отсюда следуют все утверждения леммы в рассматриваемом случае. Лемма доказана.

Положим $N_3 = 2(2d+2)(2d+1)^{n-1}n+1$. Тогда по Лемме 4 и Лемме 5 существует линейная форма $L \in \mathcal{L}_{N_3}$, удовлетворяющая условиям (a) и (b) одновременно для y и Y.

Теперь мы опишем алгоритм для построения целых чисел $z_2, \ldots, z_n$ с длинами записи $O(n \log d)$, таких что $\mu_0(Y) = \mu_0(z_2, \ldots, z_n)$, и $w(Y) = w(z_2, \ldots, z_n)$. Выберем целые числа $y_2, \ldots, y_n$ с длинами записи $O(n \log d)$, скажем, $y_i = 0$, $2 \leqslant i \leqslant n$. Так что сейчас $R_1 = R$. Построим решение системы (6) или установим, что эта система не имеет решений, см [9, 10] (здесь следует использовать условие (A) из Введения).

В случае, когда система не имеет решений, мы имеем $\mu_0(Y) = \mu_0(y)$ по Лемме 10. Пусть система (6) имеет решение $(1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n}(\overline{R(\varepsilon, \varepsilon_1, \varepsilon_2)})$. Тогда $\mu_0(y'_2, \ldots, y'_n) > \mu_0(y)$ по Лемме 10.

Покажем, что можно построить последовательно $y''_2, \ldots, y''_n \in \mathbb{Z}$, такие что $\mu_0(y''_2, \ldots, y''_i, y'_{i+1}, \ldots, y'_n) \geqslant \mu_0(y'_2, \ldots, y'_n)$ для любого $2 \leqslant i \leqslant n$, ср. со вспомогательными алгоритмами из [9, 10]. Перебирая целые значения $y''_2 = 0, \ldots, N$, где N ограничено сверху полиномом от d^n, и вычисляя каждый раз $\mu_0(y''_2, y'_3, \ldots, y'_n)$, мы найдём требуемое y''_2. Последнее следует из Леммы 8. Аналогичным образом построим $y''_3, \ldots, y''_n$. Теперь заменим $y_2, \ldots, y_n$ на $y''_2, \ldots, y''_n$ и вернёмся к началу, описываемого алгоритма.

Заметим, что $\mu_0(Y)$ ограничено сверху полиномом от d^n. Следовательно, таких возвратов к началу может быть самое большее полиномиальное от d^n число. Таким образом, в конечном счёте мы придём к случаю, когда система (6) не имеет решений, и $\mu_0(Y) = \mu_0(y)$.

Пусть $\mu_0(Y) = \mu_0(y)$. Будем перебирать все линейные формы $L \in \mathcal{L}_{N_3}$. Построим подмножество $\mathcal{L}'$ множества $\mathcal{L}$, состоящее из всех линейных форм, удовлетворяющих условиям (a) и (b). Следовательно, согласно выбору N_3 выполнено $w(L, y) = w(y)$ для любой $L \in \mathcal{L}'$, и существует $L \in \mathcal{L}'$, такая что $w(L, Y) = w(Y)$. Будем перебирать все линейные формы $L \in \mathcal{L}'$.

Для рассматриваемой линейной формы L построим многочлен $G(y)$ и $w(L, y)$. Положим $r = r(L, y)$ и $u_i = u_i(L, y)$, $v_i = v_i(L, y)$ для всех $0 \leqslant i \leqslant r+1$. Положим $u_{-1} = u_0+1$, $v_{-1} = v_0-1$. Предположим, что $0 \leqslant j \leqslant r$, $j \in \mathbb{Z}$ (база рекурсии $j = 0$), и мы уже установили, что $u_i = u_i(L, Y)$, $v_i = v_i(L, Y)$ для всех $0 \leqslant i \leqslant j$. Так что, если

$j \leqslant r-1$, то

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} \geqslant \frac{v_j(L,Y) - v_{j+1}(L,Y)}{u_j(L,Y) - u_{j+1}(L,Y)}$$

для любой $L \in \mathcal{L}'$.

Пусть $v_0 \neq v_1$, если $j = 0$. Тогда для всякой $L \in \mathcal{L}'$ построим решение системы (11) или установим, что она не имеет решений, см. [9, 10] (здесь следует использовать условие (A) из Введения).

Пусть система (11) имеет решение

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}(\overline{R(\varepsilon_1, \varepsilon_2, \varepsilon_3)})$$

для некоторой $L \in \mathcal{L}'$. Тогда $\mu_0(y') = \mu_0(Y)$, и $w(L, y') < w(L, y) = w(y)$ по Лемме 12 (ii).

Если $j = r$, и система (11) не имеет решений для всех $L \in \mathcal{L}'$, то $w(y) = w(Y)$ по Лемме 12 (i) и согласно выбору N_3. В этом случае положим $z_i = y_i$ для $2 \leqslant i \leqslant n$.

Пусть $j = 0$ и $v_0 = v_1$, или $0 \leqslant j \leqslant r-1$, и система (11) не имеет решений для всех $L \in \mathcal{L}'$. Тогда

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} = \frac{v_j(Y) - v_{j+1}(Y)}{u_j(Y) - u_{j+1}(Y)} \tag{14}$$

по Лемме 12 (i) и согласно выбору N_3. В этом случае снова будем перебирать $L \in \mathcal{L}'$. Для всякой $L \in \mathcal{L}'$ построим решение системы (8) или установим, что она не имеет решений, см. [9, 10] (здесь следует использовать условие (A) из Введения).

Пусть система (8) имеет решение

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}(\overline{R(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)})$$

для некоторого $L \in \mathcal{L}'$. Тогда $\mu_0(y') = \mu_0(Y)$, и $w(L, y') < w(L, y) = w(y)$ по Лемме 11 (ii).

Предположим, что система (8) не имеет решений для всех $L \in \mathcal{L}'$ и $j \leqslant r-1$. Тогда мы имеем $u_{j+1} = u_{j+1}(Y)$, и $v_{j+1} = v_{j+1}(Y)$ по Лемме 11 (i) и по выбору N_3. В этом случае мы заменяем j на $j+1$ и возвращаемся к началу описываемого алгоритма. Теперь j больше, чем оно было первоначально.

Таким образом, остаётся рассмотреть случаи, когда система (11) или система (8) имеет решение

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}(\overline{R(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)})$$

(для системы (11) это решение не зависит от ε_0). Следовательно, $\mu_0(y') = \mu_0(Y)$, и $w(L,y') < w(L,y) = w(y)$, см. выше. Покажем, что можно построить последовательно $y''_2,\dots,y''_n \in \mathbb{Z}$, такие что $\mu_0(y''_2,\dots,y''_i,y'_{i+1},\dots,y'_n) = \mu_0(Y)$, и

$$w(y''_2,\dots,y''_i,y'_{i+1},\dots,y'_n) \leqslant w(y'_2,\dots,y'_n)$$

для всех $2 \leqslant i \leqslant n$, ср. со вспомогательными алгоритмами из [9, 10]. Перебирая целые значения $y''_2 = 0,\dots,N$, где N ограничено сверху полиномом от d^n, и вычисляя каждый раз $\mu_0(y''_2,y'_3,\dots,y'_n)$ и $w(y''_2,y'_3,\dots,y'_n)$, мы найдём в конечном счёте требуемое y''_2. Последнее следует из Леммы 8. Аналогичным образом построим $y''_3,\dots,y''_n$. Теперь заменим $y_2,\dots,y_n$ на $y''_2,\dots,y''_n$ и вернёмся к началу описываемого алгоритма. Описание алгоритма для построение $z_2,\dots,z_n$ завершено.

Отметим, что в рекурсии описанного алгоритма частное $(v_j - v_{j+1})/(u_j - u_{j+1})$ может принимать самое большее полиномиальное от d^n число значений, и, когда выполнено равенство (14), целое число u_{j+1} также может принимать самое большее полиномиальное от d^n число значений. Следовательно, в описанном алгоритме может быть самое большее полиномиальное от d^n число возвратов к началу, когда значение j одно и то же. Поскольку имеется максимум полиномиальное от d^n число различных значений j, общее число возвратов в алгоритме ограничено сверху полиномом от d^n.

Заметим, что степени всех уравнений и неравенств систем (6), (11), (8) относительно всех переменных равны $O(d)$. Поле коэффициентов в системе (8), (соответственно (11)) является расширением $R(\varepsilon_0,\varepsilon_1,\varepsilon_2,\varepsilon_3)$ (соответственно $R(\varepsilon_1,\varepsilon_2,\varepsilon_3)$) степени полиномиальной от d^n. Согласно [15, 6], см. также [9], время работы алгоритма, который определяет, имеют ли системы (6), (11), (8) решения и строит эти решения полиномиально от d^n, d_1, d_2, M, M_1, m. Таким образом, время работы алгоритма, описанного в этом разделе полиномиально от d^n, d_1, d_2, M, M_1, m.

2. Теорема существования

Мы будем предполагать, что $R = \mathbb{R}$ в этом разделе. Пусть $V = \mathcal{Z}(f_1,\dots,f_m)$ – алгебраическое многообразие из введения, и $V(\mathbb{R})$ – соответствующее вещественное алгебраическое многообразие. Мы будем предполагать в этом разделе, что $V(\mathbb{R})$ является непустым и ограниченным.

Нам потребуются следующие леммы.

Лемма 13. *Пусть дано компактное множество $C' \subset \mathbb{C}^{m_1+1}$, $m_1 \geqslant 0$. Пусть для любой точки $(b_0, \dots, b_{m_1}) \in C'$ координата $b_0 \neq 0$. Пусть*

$$C = \{ \sum_{0 \leqslant i \leqslant m_1} b_i Z^{m_1 - i} \, : \, (b_0, \dots, b_{m_1}) \in C' \}$$

является множеством многочленов $\psi = \sum_{0 \leqslant i \leqslant m_1} b_i Z^{m_1-i} \in \mathbb{C}[Z]$ степени $\deg\psi = m_1$ с коэффициентами из C'. Пусть m_2 целое число, такое что $m_2 \geqslant m_1$, и $0 < \delta \in \mathbb{R}$. Пусть $\widetilde{\psi} \in \mathbb{C}[Z]$ – многочлен степени $\deg\widetilde{\psi} \leqslant m_2$, такой что абсолютные величины коэффициентов многочлена $\widetilde{\psi} - \psi$ меньше, чем δ. Обозначим через $z_i \in \mathbb{C}$, $1 \leqslant i \leqslant m_1$, (соответственно $\widetilde{z}_i \in \mathbb{C}$, $1 \leqslant i \leqslant \deg\widetilde{\psi}$) семейство корней, учитывая их кратности, многочлена ψ (соответственно $\widetilde{\psi}$). Тогда для всякого $\delta_0 > 0$ существует $\delta > 0$, такое что для всякого $\psi \in C$, для всякого $\widetilde{\psi}$ такого, как выше, существует перестановка σ множества $1, \dots, \deg\widetilde{\psi}$, такая что

- $|\widetilde{z}_{\sigma(i)} - z_i| < \delta_0$ *для всех* $1 \leqslant i \leqslant m_1$,
- $|\widetilde{z}_{\sigma(i)}| > \delta_0^{-1}$ *для всех* $m_1 + 1 \leqslant i \leqslant \deg\widetilde{\psi}$.

Доказательство. Поскольку C' компактно, достаточно доказать эту лемму для малой окрестности W произвольного многочлена ψ_0 вместо компакта C'. Рассмотрим конечное семейство непересекающихся окружностей c_α, $\alpha \in A$, с радиусами меньше, чем $\delta_0/2$, такое что внутри всякой окружности c_α имеется только один, может быть кратный, корень многочлена ψ_0. Рассмотрим также окружность c с центром в нуле, содержащую внутри все корни многочлена ψ_0, с радиусом больше, чем δ_0^{-1}. Пусть ψ – многочлен из достаточно малой окрестности W многочлена ψ_0. Пусть c' есть c_α для некоторого α или c. Тогда выберем δ и W такими малыми, что ψ и $\widetilde{\psi}$ не имеют какого-либо корня на c', и абсолютная величина каждого интеграла $(2\pi\sqrt{-1})^{-1} \int_{c'} (\psi'(z)/\psi(z) - \widetilde{\psi}'(z)/\widetilde{\psi}(z)) dz$ меньше, чем $1/2$. Лемма доказана.

Теперь пусть целые числа $y_2, \dots, y_n$ имеют длины $O(n \log d)$. Напомним, что в Разделе 1 были определены $\mu_0(y)$, $\mu_1(y)$, $\mu_2(y)$,

$w(y)$ и $\mu(y)$. Пусть $\mu(y_2,\dots,y_n)=\mu(Y)$, где $Y=(Y_2,\dots,Y_n)$, см. Раздел 1. Напомним,что многочлен $h\in R[\varepsilon^{(0)},\varepsilon^{(1)},X_0,\dots,X_n]$, многочлен $G(y)\in\mathbb{R}[\varepsilon,L]$. Пусть $v_2,\dots,v_n\in\mathbb{R}$, и $0\neq\delta\in\mathbb{R}$. Обозначим для краткости $v=(v_2,\dots,v_n)$ и $|v|^2=\sum_{2\leqslant i\leqslant n}|v_i|^2$. Также обозначим $\mu_i=\mu_i(Y)$, $i=1,2,3$, $\mu=\mu(Y)$ и $w=w(Y)$. Определим $F(y)=G(y)/\varepsilon^{\iota_1(L,y)}\in\mathbb{R}[\varepsilon,L]$.

Рассмотрим следующую систему полиномиальных уравнений относительно $X_0,\dots,X_n$.

$$\begin{cases} h(1,\delta,X_0,\dots,X_n)=0,\\ \frac{\partial h}{\partial X_i}(1,\delta,X_0,\dots,X_n)-y_i\frac{\partial h}{\partial X_1}(1,\delta,X_0,\dots,X_n)=0, \quad 2\leqslant i\leqslant n. \end{cases} \tag{15}$$

Лемма 14. *Пусть $\mu(y)=\mu$. Тогда существует $\nu>0$, такое что для любых $v_2,\dots,v_n\in\mathbb{R}$ для любого $0\neq\delta\in\mathbb{R}$, если $|v|^2\leqslant\nu$ и $|\delta|\leqslant\nu$, то $\mu(y+v)=\mu(y)$, и система (15) имеет конечное число решений в $\mathbb{P}^n(\mathbb{C})$.*

Доказательство. Выберем линейную форму L с целыми коэффициентами, удовлетворяющую условиям (a) и (b), см. Раздел 1. Пусть v является вектором с достаточно малым $|v|^2$. Тогда по Лемме 8 мы имеем $\mu_0(y+v)=\mu_0(y)$ и $w(L,y+v)=w(L,y)$. Следовательно, $\iota_1(L,y+v)=\iota_1(L,y)$, $\mu_2(L,y+v)=\mu_2(L,y)=\mu_2$. Следовательно,

$$D(y+v)(1,\delta,L-l_0,-l_1,\dots,-l_n)=\delta^{\iota_1(L,y)}F(y+v)(\delta,L).$$

Аналогичное равенство имеет место, если заметить $y+v$ на y. Поскольку $D(Y)$ является многочленом от $Y_2,\dots,Y_n$, и по определению $\mu_2(L,y)$ коэффициент при $L^{\mu_2(L,y)}$ многочлена $F(y+v)(\delta,L)$ – ненулевой для всех $\delta\neq0$ и v с достаточно малыми $|\delta|$ и $|v|^2$. Следовательно, при данных условиях $D(y+v)$ – ненулевой. Поэтому система (15) имеет конечное число решений. Лемма доказана.

Пусть $v_2,\dots,v_n\in\mathbb{R}$, – такие что $|v|^2\leqslant\nu$. Заменим в системе (3) y на $y+v$. Обозначим через

$$\xi^{(j)}(\varepsilon,v)=(1:\xi_1^{(j)}(\varepsilon,v):\dots:\xi_n^{(j)}(\varepsilon,v))\in\mathbb{P}^n(\overline{\mathbb{C}(\varepsilon)}),\quad 1\leqslant j\leqslant\mu_2,$$

семейство всех корней типа (iii) рассматриваемой системы. Положим

$$\xi^{(j)}(v)=(1:\mathrm{st}_\varepsilon(\xi_1^{(j)}(\varepsilon,v)):\dots:\mathrm{st}_\varepsilon(\xi_n^{(j)}(\varepsilon,v)))\in\mathbb{P}^n(\mathbb{C}),1\leqslant j\leqslant\mu_2,$$

где st_ε – стандартная часть, определённая для элементов поля $\overline{\mathbb{C}(\varepsilon)}$, которые не являются бесконечно большими относительно поля $\mathbb{C}$, см. [9, 10].

Пусть v и δ, – такие что система (15) имеет конечное число решений в $\mathbb{P}^n(\mathbb{C})$. Обозначим через $\xi^{(j)}(\delta, v) \in \mathbb{P}^n(\mathbb{C})$, $1 \leqslant j \leqslant \mu_0$, (напомним,что $\mu_0 = (2d+2)(2d+1)^{n-1}$) семейство корней системы (15), учитывая кратности. Обозначим

$$\xi^{(j)}(\delta, v) = (\xi_0^{(j)}(\delta, v) : \xi_1^{(j)}(\delta, v) : \ldots : \xi_n^{(j)}(\delta, v)),$$

где $\xi_i^{(j)}(\delta, v) \in \mathbb{C}$. Мы будем предполагать без ограничения общности, что если $\xi_0^{(j)}(\delta, v) \neq 0$, то $\xi_0^{(j)}(\delta, v) = 1$ для всех j.

Замечание 4. Пусть некоторое $\xi^{(j)}(\varepsilon, v)$ (соответственно $\xi^{(j)}(v)$, $\xi^{(j)}(\delta, v)$) не принадлежит гиперплоскости $\mathcal{Z}(X_0)$ в $\mathbb{P}^n$. Тогда мы будем использовать те же самые обозначения для этого элемента, рассматриваемого как точка из $\mathbb{A}^n$. Это не приведёт к двусмысленности.

Лемма 15. *Пусть $\mu(y) = \mu$. Пусть $\nu > 0$ – из формулировки Леммы 14. Тогда существует $0 < \nu_1 \leqslant \nu$, , такое что для всякого $\delta_1 > 0$ существует $0 < \delta_2 \leqslant \nu$, такое что для всех $v_2, \ldots, v_n \in \mathbb{R}$, удовлетворяющих неравенству $|v|^2 \leqslant \nu_1$, если $|\delta| < \delta_2$, то существует перестановка σ множества $1, \ldots, \mu_0$, такая что*

- *для любого $1 \leqslant j \leqslant \mu_2$ элемент $\xi_0^{(\sigma(j))}(\delta, v) = 1$, и $\sum_{0 \leqslant i \leqslant n} |\xi_i^{(\sigma(j))}(\delta, v) - \xi_i^{(j)}(v)|^2 < \delta_1$,*
- *для любого $\mu_2 + 1 \leqslant j \leqslant \mu_0$, если $\xi_0^{(\sigma(j))}(\delta, v) = 1$, то $\sum_{0 \leqslant i \leqslant n} |\xi_i^{(\sigma(j))}(\delta, v)|^2 > \delta_1^{-1}$.*

Доказательство. Существует семейство различных линейных форм L_u, $1 \leqslant u \leqslant (n-1)\mu_0! + 1$, такое что

$$L_u = \sum_{0 \leqslant i \leqslant n} c_u^i X_i, \quad c_u \in \mathbb{Z},$$

и для любого u форма L_u удовлетворяет условиям (a) и (b) для y. Обозначим многочлены $F(y)$ и $F(y+v)$, соответствующие линейной форме L_u, через $F_u(y)$ и $F_u(y+v)$ соответственно. Обозначим через $J_u(\delta, v) \subset \{1, \ldots, \mu_0\}$ подмножество индексов, такое что $\xi_0^{(j)}(\delta, v) \neq 0$ тогда и только тогда, когда $j \in J_u(\delta, v)$. Отметим, что число элементов $\# J_u(\delta, v) = \deg_{L_u} F_u(y+v)$. Поскольку $D(Y)$ является многочленом относительно $Y_2, \dots, Y_n$ мы можем представить

$$F_u(y+v) = \varepsilon \Psi_3(\varepsilon, L_u, v_2, \dots, v_n) + \Psi_4(L_u, v_2, \dots, v_n),$$

где многочлены $\Psi_3 \in \mathbb{R}[\varepsilon, Z, Z_2, \dots, Z_n]$, $\Psi_4 \in \mathbb{R}[Z, Z_2, \dots, Z_n]$. Согласно выбору y и L_u мы имеем $\deg_Z \Psi_4(Z, 0, \dots, 0) = \mu_2$. Кроме того,

$$\deg_Z \Psi_4(Z, v_2, \dots, v_n) = \deg_Z F_u(y+v)(0, Z) = \mu_2(L, y+v) = \mu_2$$

по Следствию 6 для всех v с достаточно малыми $|v|^2$.

По нашим определениям семейство корней многочлена $F_u(y+v)$ совпадает с $(L_u/X_0)(\xi^{(j)}(\delta, v))$, $j \in J_u(\delta, v)$. Семейство корней многочлена $\Psi_4(Z, v_2, \dots, v_n)$ совпадает с $(L_u/X_0)(\xi^{(j)}(v))$, $1 \leqslant j \leqslant \mu_2$.

Теперь Лемма 13 влечёт, что существует $\nu_1 > 0$, такое что для любого $\delta_3 > 0$ существует $\delta_2 > 0$, такое что для любого u, для любых $v_2, \dots, v_n \in \mathbb{R}$ с $|v|^2 \leqslant \nu_1$, если $|\delta| < \delta_2$, то существует перестановка $\rho = \rho_u$ (она зависит от u) множества $\{1, \dots, \mu_0\}$, такая что $\rho(j) \in J_u(\delta, v)$ для любого $1 \leqslant j \leqslant \deg_{L_u} F_u(y+v)$, и

- $|(L_u/X_0)(\xi^{(\rho(j))}(\delta, v)) - (L_u/X_0)(\xi^{(j)}(v))| < \delta_3$ для всех $1 \leqslant j \leqslant \mu_2$,
- $|(L_u/X_0)(\xi^{(\rho(j))}(\delta, v))| > \delta_3^{-1}$ для всех $\mu_2 + 1 \leqslant j \leqslant \deg_Z F_u(y+v)(\delta, Z)$.

Для всякого u рассмотрим проекцию

$$p_u : \mathbb{A}^n(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C}),\ (X_1, \dots, X_n) \mapsto L_u(1, X_1, \dots, X_n).$$

Положим для всех $\delta_1 > 0$, $\delta_3 > 0$, u и $1 \leqslant j \leqslant \mu_2$

$$W_{u,j}(\delta_3) = \{z \in \mathbb{C} : |z - (L_u/X_0)(\xi^{(j)}(v))| < \delta_3\},$$

$$W_j(\delta_1) = \{(z_1, \dots, z_n) \in \mathbb{A}^n(\mathbb{C}) : \sum_{1 \leqslant i \leqslant n} |z_i - \xi_i^{(j)}(v))|^2 < \delta_1\}.$$

Выберем δ_3 таким малым, что для всех v с $|v|^2 \leqslant \nu_1$, для всех $1 \leqslant j \leqslant \mu_2$, для всех $1 \leqslant u_1 < \ldots < u_n \leqslant (n-1)\mu_0! + 1$ пересечение

$$\bigcap_{1 \leqslant i \leqslant n} p_{u_i}^{-1}(W_{u_i,j}(\delta_3)) \subset W_j(\delta_1) \qquad (16)$$

(это возможно, так как линейные формы $L_{u_1} - X_0, \dots, L_{u_n} - X_0$ линейно независимы). Заметим, что фактически δ_3 не зависит от v, поскольку достаточно удовлетворить (16) в единственной точке. Кроме того, потребуем, может быть, выбирая меньшее δ_3, чтобы для любого u из неравенства $|(L_u/X_0)(1, z_1, \dots, z_n)| > \delta_3^{-1}$ следовало, что $\sum_{1\leqslant i\leqslant n} |z_i|^2 > \delta_1^{-1}$.

Теперь отметим, что существует перестановка σ множества $\{1, \dots, \mu_0\}$ и индексы $1 \leqslant u_1 < \dots < u_n \leqslant (n-1)\mu_0! + 1$, такие что $\sigma = \rho_{u_i}$ для любого $1 \leqslant i \leqslant n$. Перестановка σ – требуемая. Лемма доказана.

Напомним,что для всех $v_2, \dots, v_n \in \mathbb{R}$, удовлетворяющих неравенству $\sum_{2\leqslant i\leqslant n} |v|^2 \leqslant \nu$, выполнено $\mu_2(y+v) = \mu_2(y) = \mu_2$.

Лемма 16. *Пусть $\mu(y) = \mu$. Пусть $\nu > 0$ – из формулировка Леммы 14. Тогда для всякого $\delta > 0$ существует $0 < \nu_2 < \nu$, такое что для любых $v_2, \dots, v_n \in \mathbb{R}$, удовлетворяющих неравенству $|v|^2 \leqslant \nu_2$, существует перестановка σ множества $1, \dots, \mu_2$, такая что $|\xi_i^{(\tau(j))}(v) - \xi_i^{(j)}(0)|^2 < \delta$ для любого $1 \leqslant j \leqslant \mu_2$.*

Доказательство. Доказательство этой леммы аналогично доказательству Леммы 15, но является более простым. Оно следует из Леммы 13 и того, что $\deg_Z \Psi_4(Z, 0, \dots, 0) = \mu_2$, см. доказательство Леммы 15. Лемма доказана.

Замечание 5. В дальнейшем для удобства обозначений, применяя Лемму 15 или Лемму 16, мы будем предполагать без ограничения общности, что σ и τ – тождественные перестановки. Мы будем говорить в этой ситуации, что семейства $\xi^{(j)}(\delta, v)$, $1 \leqslant j \leqslant \mu_0$, и $\xi^{(j)}(v)$, $1 \leqslant j \leqslant \mu_2$, (соответственно $\xi^{(j)}(v)$, $1 \leqslant j \leqslant \mu_2$, и $\xi^{(j)}(0)$, $1 \leqslant j \leqslant \mu_2$), согласованы по Лемме 15 (соответственно Лемме 16).

Напомним,что семейство корней типа (iii) системы (3) в $\mathbb{A}^n(\overline{\mathbb{C}(\varepsilon)})$ есть $\xi^{(j)}(\varepsilon, 0)$, $1 \leqslant j \leqslant \mu_2$. Обозначим для краткости для любого $1 \leqslant j \leqslant \mu_2$

$$\xi^{(j)} = (\xi_1^{(j)}, \dots, \xi_n^{(j)}) = \xi^{(j)}(0) =$$
$$\mathrm{st}_\varepsilon(\xi^{(j)}(\varepsilon, 0)) = (\mathrm{st}_\varepsilon(\xi_1^{(j)}(\varepsilon, 0)), \dots, \mathrm{st}_\varepsilon(\xi_1^{(j)}(\varepsilon, 0))) \in \mathbb{A}^n(\mathbb{C}).$$

Для любого вектора $z = (z_1, \dots, z_n) \in \mathbb{C}^n$ обозначим $|z| = (\sum_{1\leqslant i\leqslant n} |z_i|^2)^{1/2}$. Определим также $\mathrm{Re}(z) \in \mathbb{R}^n$ и $\mathrm{Im}(z) \in \mathbb{R}^n$ равенством $z = \mathrm{Re}(z) + \sqrt{-1}\mathrm{Im}(z)$. Так что $|\xi^{(j)}|^2 = \sum_{1 \leqslant i \leqslant n} |\xi_i^{(j)}|^2$ для $1 \leqslant j \leqslant \mu_2$.

Рассмотрим некоторую полуалгебраическую триангуляцию вещественного алгебраического многообразия $V(\mathbb{R})$, см. Введение, т.е. конечный симплициальный комплекс $K = \cup_{1 \leqslant i \leqslant p} \sigma_i$ (здесь это означает симплициальное пространство, т.е. $K \subset R^N$ для некоторого N, и всякий симплекс σ_i является выпуклой оболочкой его вершин) и полуалгебраический гомеоморфизм $\phi : K \to V(R)$.

Теорема 3. *Пусть $n \geqslant 3$, и $V(\mathbb{R})$ – ограниченное непустое вещественное аффинное алгебраическое многообразие, заданное как множество всех общих нулей многочленов $f_1, \dots, f_m \in \mathbb{R}[X_1, \dots, X_n]$, см. Введение. Пусть $\dim V(\mathbb{R}) \leqslant n - 2$. Пусть $y_1 = 1$, $y_2, \dots, y_n \in \mathbb{R}$. Пусть*

$$\mu = \mu(Y_2, \dots, Y_n) = \mu(y_2, \dots, y_n),$$

см. Раздел 1. Пусть $e = \sum_{1 \leqslant j \leqslant q} \sigma_{p_j}$ – ненулевой s-мерный цикл с коэффициентами из $\mathbb{Z}/2\mathbb{Z}$ симплициального комплекса K, причём все симплексы σ_{p_j} максимальны. Следовательно, см. Введение, $E = \cup_{1 \leqslant j \leqslant q} \phi(\sigma_{p_j}) \subset V(\mathbb{R})$, m', E', m'', E'' определены для вектора $(1, y_2, \dots, y_n)$. Предположим, что образ всякого симплекса $\phi(\sigma_{p_j})$, $1 \leqslant j \leqslant q$, не содержится в какой-либо гиперплоскости $\mathcal{Z}_{\mathbb{R}}(\sum_{1 \leqslant i \leqslant n} y_i X_i - a)$, $a \in \mathbb{R}$ (так что $s \geqslant 1$). Тогда существуют по крайней мере две различные точки $\xi^{(j)}$, $1 \leqslant j \leqslant \mu_2$, которые принадлежат E. Более точно, $E' \cup E'' \subset \{\xi^{(j)} : 1 \leqslant j \leqslant \mu_2\}$. В частности при условиях этой теоремы множества E' и E'' конечны.

Доказательство. Осуществляя линейное преобразование координат $X_1 \mapsto X_1 + \sum_{2 \leqslant j \leqslant n} y_j X_j$, $X_i \mapsto X_i$, $i = 0, 2, 3, \dots, n$, мы будем предполагать в дальнейшем, что $(y_2, \dots, y_n) = (0, \dots, 0)$, и $\mu(0, \dots, 0) = \mu$. Таким образом, (3) с $X_0 = 1$ эквивалентно системе полиномиальных уравнений относительно $X_1, \dots, X_n$ с коэффициентами из поля $\mathbb{R}(\varepsilon)$

$$\begin{cases} f_\varepsilon = 0, \\ \frac{\partial f_\varepsilon}{\partial X_i} = 0, \quad 2 \leqslant i \leqslant n. \end{cases} \tag{17}$$

Напомним,что $m' = \max X_1(E)$, и $E' = \{z \in E : X_1(z) = m'\}$. Мы будем предполагать без ограничения общности, что $m' = 0$, сделав при необходимости линейное преобразование

$X_1 \mapsto X_1 + m'$. Обозначим через W' алгебраическое многообразие, которое является замыканием в топологии Зарисского множества E'. Тогда $\dim W' < s$, поскольку каждый симплекс $\phi(\sigma_{p_j})$, $1 \leqslant j \leqslant q$, не содержится ни в какой гиперплоскости $\mathcal{Z}_{\mathbb{R}}(X_1 - a)$, $a \in \mathbb{R}$. Предположим, что существует точка $\xi^{(0)} \in E'$, и $\xi^{(0)} \neq \xi^{(j)}$ для всякого $1 \leqslant j \leqslant \mu_2$.

Обозначим через $J_1 \subset \{1, \dots, \mu_2\}$ подмножество индексов, таких что $j \in J_1$ тогда и только тогда, когда $X_1(\xi^{(j)}) = 0$, и $\xi^{(j)} \in \mathbb{R}^n$.

Обозначим через $J_2 \subset \{1, \dots, \mu_2\}$ подмножество индексов, таких что $j \in J_2$ тогда и только тогда, когда $X_1(\xi^{(j)}) \neq 0$, и $\xi^{(j)} \in \mathbb{R}^n$.

Обозначим через $J_3 \subset \{1, \dots, \mu_2\}$ подмножество индексов, таких что $j \in J_3$ тогда и только тогда, когда $\xi^{(j)} \notin \mathbb{R}^n$.

Так что $\{1, \dots, \mu_2\} = J_1 \cup J_2 \cup J_3$, и $J_i \cap J_j = \emptyset$ для всех $1 \leqslant i \neq j \leqslant 3$.

Рассмотрим проекцию

$$p_1 : \mathbb{R}^n \to \mathbb{R}^{n-1},\ (X_1, \dots, X_n) \mapsto (X_2, \dots, X_n).$$

Отметим, что точка $p_1(\xi^{(0)})$ отлична от всякой точки $p_1(\xi^{(j)})$, $j \in J_1$. Следовательно, существует C^∞-функция $\beta : \mathbb{R}^{n-1} \to \mathbb{R}$, такая что $\beta(p_1(\xi^{(j)})) < 0$ для всех $j \in J_1$, и $\beta(p_1(\xi^{(0)})) > 0$. Определим функцию $\gamma = \beta \circ p_1$. Тогда $\gamma(\xi^{(j)}) < 0$ для всех $j \in J_1$, и $\gamma(\xi^{(0)}) > 0$.

Определение ϵ_1**.** Выберем $\epsilon_1 > 0$ таким малым, что

(1a) для всякого $j \in J_1$ справедливо неравенство $\gamma(\xi^{(j)}) < -2\epsilon_1$,

(1b) для всякого $j \in J_2$ справедливо неравенство $|X_1(\xi^{(j)})| > 2\epsilon_1$,

(1c) для всякого $j \in J_3$ справедливо неравенство $|\mathrm{Im}(\xi^{(j)})| > 2\epsilon_1$,

(1d) $\gamma(\xi^{(0)}) > 2\epsilon_1$.

Определение ϵ_2**.** Выберем $\epsilon_2 > 0$ таким малым, что

(2a) $\epsilon_2 \leqslant \nu_1$, где ν_1 – из Леммы 15.

Заметим, что существует $w > 0$ такое малое, что (1a), (1b) и (1c) имеют место, если заменить $2\epsilon_1$ на $2\epsilon_1 + w$. Следовательно, существует $\delta' > 0$, такое что, если $z \in \mathbb{C}^n$, и $|z - \xi^{(j)}|^2 \leqslant \delta'$, то для всякого $j \in J_1$ (соответственно $j \in J_2$, $j \in J_3$) справедливо неравенство $\gamma(\mathrm{Re}(z)) < -2\epsilon_1$ (соответственно $|X_1(z)| > 2\epsilon_1$, $|\mathrm{Im}(z)| > 2\epsilon_1$).

Напомним,что $\nu_1 < \nu$. Так что положим $\delta = \delta'$, применим Лемму 16 и Замечание 5. Мы будем предполагать в дальнейшем, что соответствующие семейства $\xi^{(j)}(v)$, $1 \leqslant j \leqslant \mu_2$, и $\xi^{(j)}$, $1 \leqslant j \leqslant \mu_2$, согласованы по Лемме 16. Мы требуем, чтобы

(2b) $\epsilon_2 \leqslant \nu_2$, где ν_2 соответствует $\delta = \delta'$ по Лемме 16.

Отметим, что из (2b) следует, что

(2i) для всякого $j \in J_1$, для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $\gamma(\mathrm{Re}(\xi^{(j)}(v))) < -2\epsilon_1$,
(2ii) для всякого $j \in J_2$, для всякого $v \in \mathbb{R}^{n-1}$ такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $|X_1(\xi^{(j)}(v))| > 2\epsilon_1$,
(2iii) для всякого $j \in J_3$, для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $|\mathrm{Im}(\xi^{(j)}(v))| > 2\epsilon_1$,
(2iv) существует $m_0 > 0$, такое что для всякого $1 \leqslant j \leqslant \mu_2$, для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $|\xi^{(j)}(v)|^2 < m_0$.

Определение ϵ_3**.** Пусть $r : \mathbb{R} \to \mathbb{R}$ – C^∞–функция, такая что $r(x) = 1$, если $x \leqslant -\epsilon_1$, $r(x) = 0$, если $x \geqslant \epsilon_1$, и r является монотонной убывающей функцией в открытом интервале $-\epsilon_1 < x < \epsilon_1$.

Выберем открытый n-мерный шар $B \subset \mathbb{R}^n$ с центром в точке $(0, \dots, 0)$, содержащий $V(\mathbb{R})$. Обозначим через $\overline{B}$ замыкание в классической топологии шара B. Обозначим $r' = dr/dx$. Положим

$$m_1 = \max\{r'(x) : x \in \mathbb{R}\}$$

$$m_2 = \max_{2 \leqslant i \leqslant n} \max\{|\frac{\partial \gamma}{\partial X_i}(z)| : z \in \overline{B} \,\&\, |\gamma(z)| \leqslant \epsilon_1\}.$$

Мы требуем, чтобы

(3a) $\epsilon_3 < \min\{\sqrt{\epsilon_2/(n-1)}/(m_1 m_2), \epsilon_1/2\}$.

Отсюда следует, что $(\epsilon_3 m_1 m_2)^2 (n-1) < \epsilon_2$.

Определение ϵ_4**.** Заметим, что для всякой достаточно малой окрестности U в классической топологии точки $\xi^{(0)}$ существует точка $z_0 \in U$, такая что

(4i) точка $z_0 \in E$,

(4ii) точка z_0 – гладкая размерности s на вещественном алгебраическом многообразии $V(\mathbb{R})$,

(4iii) касательное пространство $T_{z_0,V(\mathbb{R})}$ не содержится в гиперплоскости $\mathcal{Z}_{\mathbb{R}}(X_1)$, т.е. вектор $(1, 0, \dots, 0)$ не ортогонален к $T_{z_0,V(\mathbb{R})}$,

(4iv) $\gamma(z_0) > 2\epsilon_1$.

Эти требования могут быть удовлетворены в силу того, что всякий симплекс $\phi(\sigma_{p_j})$, $1 \leqslant j \leqslant q$, не содержится ни в какой гиперплоскости $\mathcal{Z}_{\mathbb{R}}(X_1 - a)$, $a \in \mathbb{R}$.

Выберем $\epsilon_4 > 0$, так что

(4a) $\epsilon_4 < \epsilon_3/2$,

(4b) пересечение $E \cap \mathcal{Z}_{\mathbb{R}}(X_1 + \epsilon_4)$ содержит точку z_0, которая удовлетворяет условиям (4i)–(4iv).

Определение ϵ_5**.** Рассмотрим n-мерный шар $B \subset \mathbb{R}^n$, введённый прежде. Положим

$$m_4 = \min\{(f/g)(z) \,:\, z \in \overline{B} \cap (\mathbb{R}^n \setminus B)\},$$

Тогда $m_4 > 0$. Обозначим через m_5 радиус B. Положим $m_6 = \max\{m_0 + 2, m_5 + 1\}$.

Обозначим $V_\epsilon = \mathcal{Z}_{\mathbb{R}}(f - \epsilon g) \cap B$, если $0 < \epsilon \in \mathbb{R}$. Мы требуем, чтобы

(5a) $0 < \epsilon_5 < m_4$,

(5b) для всякого ϵ, $0 < \epsilon < \epsilon_5$, V_ϵ является гладким многообразием, ср. с доказательством Леммы 2,

(5c) $\epsilon_5 \leqslant \nu_1$, где ν_1 – из формулировки Леммы 15.

Согласно (2i)–(2iv) существует $\delta'' > 0$, такое что для всякого $v \in \mathbb{R}^{n-1}$, для всякого $z \in \mathbb{C}^n$, если $|v|^2 \leqslant \epsilon_2$, и $|z - \xi^{(j)}(v)|^2 \leqslant \delta''$, то

- для всякого $j \in J_1$ справедливы неравенства $\gamma(\mathrm{Re}(z)) < -\epsilon_1$, и $|X_1(z) - X_1(\xi^{(j)}(v)))| < \epsilon_3/2$,
- для всякого $j \in J_2$ справедливо неравенство $|X_1(z)| > \epsilon_1$,
- для всякого $j \in J_3$ справедливо неравенство $|\mathrm{Im}(z)| > \epsilon_1$.

Таким образом, положим $\delta_1 = \min\{\delta'', m_6^{-2}\}$, применим Лемму 15 и Замечание 5. Мы будем предполагать в дальнейшем, что соответствующие семейства $\xi^{(j)}(\epsilon, v)$, $1 \leqslant j \leqslant \mu_0$, и $\xi^{(j)}(v)$, $1 \leqslant j \leqslant \mu_2$, согласованы по Лемме 15, если $0 < \epsilon < \epsilon_5$, $|v|^2 \leqslant \epsilon_2$. Мы требуем, чтобы

(5d) $\epsilon_5 \leqslant \delta_2$, где δ_2 соответствует $\delta_1 = \min\{\delta'', m_6^{-2}\}$ по Лемме 15.

Тогда (5d) влечёт, что

(5i) для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякого $j \in J_1$, для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $\gamma(\mathrm{Re}(\xi^{(j)}(\epsilon, v))) < -\epsilon_1$,

(5ii) для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякого $j \in J_1$ справедливо неравенство $|X_1(\xi^{(j)}(\epsilon, 0))| < \epsilon_3/2$,

(5iii) для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякого $j \in J_2$, для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $|X_1(\xi^{(j)}(\epsilon, v))| > \epsilon_1$,

(5iv) для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякого $j \in J_3$, для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $|\mathrm{Im}(\xi^{(j)}(\epsilon, v))| > \epsilon_1$,

(5v) для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякого $1 \leqslant j \leqslant \mu_2$ для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, справедливо неравенство $|\xi^{(j)}(\epsilon, v)|^2 < m_0 + 1$,

(5vi) для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякого $\mu_2 + 1 \leqslant j \leqslant \mu_0$, для всякого $v \in \mathbb{R}^{n-1}$, такого что $|v|^2 \leqslant \epsilon_2$, если $\xi_0^{(j)}(\epsilon, v) = 1$, то справедливо неравенство $|\xi^{(j)}(\epsilon, v)|^2 > m_6^2 - 1 > (\max\{m_0 + 1, m_5\})^2$.

Заметим, что из (5i)–(5iv) и (3a) следует, что

(5vii) для всякого ϵ, $0 < \epsilon < \epsilon_5$, если $j \in J_1 \cup J_2$, и $\gamma(\mathrm{Re}(\xi^{(j)}(\epsilon, 0))) < -\epsilon_1$, то $|X_1(\xi^{(j)}(\epsilon, 0)) - \epsilon_3| > \epsilon_3/2$,

(5viii) для всякого ϵ, $0 < \epsilon < \epsilon_5$, если $j \in J_2$, то $|X_1(\xi^{(j)}(\epsilon, 0))| > \epsilon_3/2$,

(5ix) для всякого ϵ, $0 < \epsilon < \epsilon_5$, если $j \in J_3$, то $|\mathrm{Im}(\xi^{(j)}(\epsilon, 0))| > \epsilon_3/2$.

Теперь рассмотрим точку z_0, определённую в (4i)–(4iv) и (4b). Выберем линейные формы $L_1, \dots, L_s \in \mathbb{R}[X_1, \dots, X_n]$, так что $L_1 = X_1$, и пересечение

$$T_{z_0, V(\mathbb{R})} \cap \mathcal{Z}_{\mathbb{R}}(L_1, \dots, L_s) = \{0\}.$$

Тогда по теореме о неявной функции z_0 – изолированная точка пересечения $V(\mathbb{R}) \cap \mathcal{Z}_{\mathbb{R}}(L_1 - L_1(z_0), \dots, L_s - L_s(z_0))$. Связная компонента B_1 пересечения

$$\{z : f(z) - \epsilon g(z) \leqslant 0\} \cap \mathcal{Z}_{\mathbb{R}}(L_1 - L_1(z_0), \dots, L_s - L_s(z_0)), \qquad (18)$$

содержащая точку z_0, стремится к точке z_0, когда ϵ стремится к нулю. Для всех достаточно малых $\epsilon > 0$ граница $S_1 = \partial B_1$ является гладким компактным многообразием, ср. доказательство Леммы 2. Поскольку $n - s - 1 > 0$, это многообразие является связной компонентой вещественного алгебраического многообразия

$$\mathcal{Z}_{\mathbb{R}}(f - \epsilon g) \cap \mathcal{Z}_{\mathbb{R}}(L_1 - L_1(z_0), \dots, L_s - L_s(z_0)). \qquad (19)$$

В дальнейшем мы будем предполагать, что полуалгебраическое множество B_1 триангулировано, см. [8]. Тогда эта триангуляция индуцирует триангуляцию множества S_1. Множество B_1 определяет $(n - s)$-мерную цепь b_1, и S_1 определяет $(n - s - 1)$–мерный цикл s_1, который является границей b_1, т.е. $s_1 = \partial b_1$.

В заключение мы выдвинем следующие требования.

(5e) для всякого ϵ, $0 < \epsilon < \epsilon_5$, граница $S_1 = \partial B_1$ – гладкое многообразие, являющееся связной компонентой вещественного алгебраического многообразия,

(5f) для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякой точки $z' \in B_1$ справедливо неравенство $\gamma(z') \geqslant \epsilon_1$.

Определим C^∞-функция $\omega : \mathbb{R}^n \to \mathbb{R}$ формулой

$$\omega(X_1, \dots, X_n) = X_1 - \epsilon_3 r(\gamma(X_1, \dots, X_n)).$$

Заметим, что $\omega(X_1, \dots, X_n) = X_1 - \epsilon_3 r(\beta(X_2, \dots, X_n))$. Мы утверждаем, что для всякого ϵ, $0 < \epsilon < \epsilon_5$, для всякой $z \in V_\epsilon$, такой что $|\omega(z)| \leqslant \epsilon_4$, точка z не является критической точкой, см. [1], функции ω на компактном гладком многообразии V_ϵ, см. (5a), (5b).

Действительно, предположим противное, что z – критическая точка функции ω. Если $|\gamma(z)| > \epsilon_1$, то градиенты функций $f - \epsilon g$

и ω в точке z параллельны вектору $(1, 0, \dots, 0)$. Следовательно, $z = \xi^{(j)}(\epsilon, 0)$ для некоторого $1 \leqslant j \leqslant \mu_0$. Условия (5v) и (5vi) влекут, что $1 \leqslant j \leqslant \mu_2$. Условие (5iv) (или (5ix)) влечёт, что $j \in J_1 \cup J_2$. Теперь из определения функции ω и условий (4a), (5vii) и (5viii) мы получаем противоречие.

Если $|\gamma(z)| \leqslant \epsilon_1$, то градиенты функций $f - \epsilon g$ и ω в точке z параллельны вектору

$$\left(1,\, -\epsilon_3\, r'(\gamma(z))\, \frac{\partial \gamma}{\partial X_2}(z),\, \dots,\, -\epsilon_3\, r'(\gamma(z))\, \frac{\partial \gamma}{\partial X_n}(z)\right).$$

Положим

$$v_i = -\epsilon_3\, r'(\gamma(z))\, \frac{\partial \gamma}{\partial X_i}(z), \quad 2 \leqslant i \leqslant n.$$

Напомним,что $V_\epsilon \subset \overline{B}$. Следовательно, (3a) влечёт, что $|v|^2 \leqslant \epsilon_2$. В этом случае $z = \xi^{(j)}(\epsilon, v)$ для некоторого $1 \leqslant j \leqslant \mu_0$. Из условий (5v) и (5vi) следует, что $1 \leqslant j \leqslant \mu_2$. Мы получаем противоречие из определения функции ω и условий (4a), (5i), (3a), (5iii) и (5iv). Требуемое утверждение доказано.

Теперь, см. [1], мы получаем, что существует диффеоморфизм

$$\alpha : [-\epsilon_4, \epsilon_4] \times (V_\epsilon \cap \{z : \omega(z) = -\epsilon_4\}) \longrightarrow V_\epsilon \cap \{z : |\omega(z)| \leqslant \epsilon_4\}, \quad (20)$$

такой что $\omega(\alpha(a, w)) = a$ для всякого $-\epsilon_4 \leqslant a \leqslant \epsilon_4$ и $w \in V_\epsilon \cap \{z : \omega(z) = -\epsilon_4\}$. Обозначим $V_{\epsilon,a} = V_\epsilon \cap \{z : \omega(z) = a\}$ для всех $-\epsilon_4 \leqslant a \leqslant \epsilon_4$. Обозначим через $i_a : V_{\epsilon,a} \to V_\epsilon \cap \{z : |\omega(z)| \leqslant \epsilon_4\}$ отображения включения. Тогда из (20) следует, что гомоморфизмы групп сингулярных гомологий, индуцированные i_a

$$i_{a\,*} : H_{n-s-1}(V_{\epsilon,a}, \mathbb{Z}/2\mathbb{Z}) \to H_{n-s-1}(V_\epsilon \cap \{z : |\omega(z)| \leqslant \epsilon_4\}, \mathbb{Z}/2\mathbb{Z})$$

имеют один и тот же образ для всех $-\epsilon_4 \leqslant a \leqslant \epsilon_4$. Следовательно, то же самое справедливо для сквозных гомоморфизмов

$$H_{n-s-1}(V_{\epsilon,a}, \mathbb{Z}/2\mathbb{Z}) \longrightarrow H_{n-s-1}(V_\epsilon \cap \{z : |\omega(z)| \leqslant \epsilon_4\}, \mathbb{Z}/2\mathbb{Z}) \longrightarrow$$
$$H_{n-s-1}(V_\epsilon, \mathbb{Z}/2\mathbb{Z}) \longrightarrow H_{n-s-1}(\mathbb{R}^n \setminus E, \mathbb{Z}/2\mathbb{Z}).$$

Обозначим через $j(a) : H_{n-s-1}(V_{\epsilon,a}, \mathbb{Z}/2\mathbb{Z}) \to H_{n-s-1}(\mathbb{R}^n \setminus E, \mathbb{Z}/2\mathbb{Z})$ этот сквозной гомоморфизм. Обозначим $j_- = j(-\epsilon_4)$ и $j_+ = j(\epsilon_4)$.

Имеем коммутативную диаграмму групп гомологий, индуцированную вложениями топологических пространств,

$$\begin{array}{ccc} H_{n-s-1}(V_{\epsilon,a},\mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H_{n-s-1}((\mathbb{R}^n\setminus E)\cap\{z:\omega(z)=a\},\mathbb{Z}/2\mathbb{Z}) \\ \downarrow & & \downarrow \\ H_{n-s-1}(V_\epsilon,\mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H_{n-s-1}(\mathbb{R}^n\setminus E,\mathbb{Z}/2\mathbb{Z}). \end{array}$$

Топологическое пространство $(\mathbb{R}^n\setminus E)\cap\{z:\omega(z)=\epsilon_4\}$ гомеоморфно $\mathbb{R}^{n-1}$, так как $E\cap\{z:\omega(z)=\epsilon_4\}=\emptyset$. Следовательно, группа гомологий $H_{n-s-1}((\mathbb{R}^n\setminus E)\cap\{z:\omega(z)=\epsilon_4\},\mathbb{Z}/2\mathbb{Z})=0$, поскольку $n-s-1>0$. Следовательно, образ $\mathrm{Im}(j_+)=0$. С другой стороны, по (5f) и (5e) образ $\mathrm{Im}(j_-)$ содержит гомологический класс цикла $s_1\in Z_{n-s-1}(\mathbb{R}^n\setminus E,\mathbb{Z}/2\mathbb{Z})$, определённого выше. Покажем, что s_1 не гомологичен нулю в $H_{n-s-1}(\mathbb{R}^n\setminus E,\mathbb{Z}/2\mathbb{Z})$. Действительно, пересечение $B_1\cap E$ состоит из одной точки и трансверсально в этой точке. Следовательно, согласно общей топологической теории двойственности, см. [2], коэффициент зацепления в $\mathbb{Z}/2\mathbb{Z}$ циклов e и s_1 отличен от нуля. Отсюда наше утверждение следует непосредственно.

Итак, $0\neq\mathrm{Im}(j_-)=\mathrm{Im}(j_+)=0$. Следовательно, первоначальное предположение, что $E'\not\subset\{\xi^{(j)}:1\leqslant j\leqslant\mu_2\}$, ведёт к противоречию. Таким образом, $E'\subset\{\xi^{(j)}:1\leqslant j\leqslant\mu_2\}$. Аналогичным образом $E''\subset\{\xi^{(j)}:1\leqslant j\leqslant\mu_2\}$. Теорема доказана.

Замечание 6. Слегка модифицируя доказательство Теоремы 3, можно рассмотреть также случай, когда $\dim V(\mathbb{R})=n-1$.

Замечание 7. Условие, что образ всякого симплекса $\phi(\sigma_{p_j})$, $1\leqslant j\leqslant q$, не содержится ни в какой гиперплоскости $\mathcal{Z}_{\mathbb{R}}(\sum_{1\leqslant i\leqslant n}y_iX_i-a)$, $a\in\mathbb{R}$, влечёт, что $\dim E'$, $\dim E''<s$, и это условие используется только для того, чтобы доказать эти неравенства.

Замечание 8. В общем случае, если выполнены условия Теоремы 3, то точки из E' и E'' могут принадлежать многим различным компонентам $V(\mathbb{R})$ даже в случае, когда E содержится только в одной неприводимой компоненте $V(\mathbb{R})$.

3. Доказательство Теоремы 1

Отметим, что случай $s=0$ известен, см. [15]. Аналогично, используя [15], можно выяснить, верно ли, что $V(R)=\emptyset$. Поэтому мы будем предполагать в дальнейшем, что $s \geqslant 1$, и $\dim V(R) \geqslant 1$. Далее, можно предполагать без ограничения общности, что $n \geqslant 3$, и $\dim V(R) \leqslant n-2$, рассматривая при необходимости вложение $\mathbb{A}^n \to \mathbb{A}^{n+2}$.

Сначала рассмотрим случай, когда $R = \mathbb{R}$. Построим при помощи алгоритма из Раздела 1 вектор $z = (1, z_2, \ldots, z_n)$ с целыми координатами с длинами записи $O(n \log d)$, такой что $\mu(z_2, \ldots, z_n) = \mu$. Сделав при необходимости линейное преобразование $\mathbb{A}^n$, мы можем предполагать без ограничения общности, что $z = (1, 0, \ldots, 0)$, и $y_1 = 1$. В этом разделе мы предполагаем, что $y_2, \ldots, y_n \in k_0$.

Пусть V_s – замыкание в топологии Зарисского множества всех гладких точек вещественного алгебраического многообразия $V(R)$. Число неприводимых компонент V_s ограничено сверху $\mathcal{P}(d^n)$, где $\mathcal{P}$ – некоторый полином, см. [16].

По Лемме 8 существует целое число $a \neq 0$, ограниченное сверху полиномом от d^n, такое что

$$\mu(ac, ac^2, \ldots, ac^{n-1}) = \mu$$

для всех целых чисел $1 \leqslant c \leqslant n\mathcal{P}(d^n) + 1$. Построим такое число a за полиномиальное время от d^n и длины записи входных данных согласно Разделу 1. Заметим, что любые n векторов из множества

$$\mathcal{C} = \{(1, ac, ac^2 \ldots, ac^{n-1}) \,:\, 1 \leqslant c \leqslant n\mathcal{P}(d^n) + 1\}$$

линейно независимы. Для любого симплекса σ_{p_j} рассматриваемого цикла e образ $\phi(\sigma_{p_j})$ содержится в некоторой неприводимой компоненте многообразия V_s, см. [8]. Следовательно, существует $c_0 \in \mathcal{C}$, такое что любой $\phi(\sigma_{p_j})$ не содержится ни в какой гиперплоскости

$$\mathcal{Z}(X_1 + ac_0X_2 + ac_0^2X_3 + \ldots + ac_0^{n-1}X_n - b), \quad b \in R.$$

Обозначим $v_c = (1, ac, ac^2 \ldots, ac^{n-1})$ для всех c и $v_0 = v_{c_0}$.

По Лемме 8 выполнено равенство $\mu(y + \delta v_0) = \mu$ для всех достаточно малых $\delta > 0$. Кроме того, каждый $\phi(\sigma_{p_j})$ не содержится ни в какой гиперплоскости

$$\mathcal{Z}((1+\delta)X_1 + (y_2 + \delta ac_0)X_2 + (y_3 + \delta ac_0^2)X_3 + \ldots$$
$$+ (y_n + \delta ac_0^{n-1})X_n - b), \quad b \in R$$

для всех достаточно малых $\delta > 0$.

Рассмотрим систему полиномиальных уравнений

$$\begin{cases} f_\varepsilon = 0, \\ (1+\delta)\frac{\partial f_\varepsilon}{\partial X_i} - (y_i + \delta a c^{i-1})\frac{\partial f_\varepsilon}{\partial X_1} = 0, \quad 2 \leqslant i \leqslant n. \end{cases} \tag{21}$$

Пусть множества E'_δ и E''_δ соответствуют вектору $y + \delta v_0$ аналогично тому, как E', E'' соответствуют y. Теорема 3 влечёт, что для всех достаточно малых $\delta > 0$ существуют точки $z'_\delta \in E'_\delta$ и $z''_\delta \in E''_\delta$, которые являются стандартными частями некоторых решений системы (21) с $c = c_0$.

Из компактности E вытекает, что существует последовательность $\delta_i > 0$, $i = 1, 2, \ldots$, которая стремится к нулю, такая что точки z'_{δ_i} и z''_{δ_i} стремятся к $z' \in E'$ и $z'' \in E''$.

Пусть теперь δ – переменная. Рассмотрим множество W всех точек, которые являются стандартными частями относительно ε решений системы (21) в $(\mathbb{A}^n \times \mathbb{A}^1)(\overline{C(\varepsilon)})$, где $\mathbb{A}^n$ имеет координаты $X_1, \ldots, X_n$, и $\mathbb{A}^1$ имеет координату δ. Тогда W является алгебраическим многообразием, и объединение всех компонент многообразия W, которые не содержатся в $\mathcal{Z}(1+\delta)$ является кривой W_c, поскольку для всякого $\delta \neq -1$ система (21) имеет конечное число решений согласно Разделу 1. Далее, $z', z'' \in W_{c_0} \cap \mathcal{Z}(\delta)$. Так что определим

$$S_y = \bigcup_{c \in \mathcal{C}} (W_c(R) \cap \mathcal{Z}(\delta)).$$

Заметим, что всякая кривая W_c может быть построена за требуемое время при помощи рассмотрения стандартных частей относительно ε решений системы (21) в $\mathbb{A}^n((\overline{C(\delta, \varepsilon)})$ согласно [5] и, используя разложения Ньютона-Пюизе, ср. [9, 10, 11, 6]. Далее, аналогичным образом можно построить множество S_y. Теорема теперь доказана в случае, когда $R = \mathbb{R}$.

В общем случае мы используем принцип переноса, см. [8]. Достаточно заметить следующее. То, что алгебраическое многообразие полуалгебраически триангулировано, может быть выражено на языке первого порядка теории вещественно замкнутых полей. Теорема доказана.

Литература

1. Дж. Милнор, *Теория Морса*. М., Мир, 1965.

2. Э. Спеньер, *Алгебраическая топология.* М., Мир, 1971.
3. Р. Хартсхорн, *Алгебраическая геометрия.* М., Мир, 1981.
4. В. Ходж, Д. Пидо, Методы алгебраической геометрии, т. 1. М., Изд-во иностр. лит., 1954.
5. 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.
6. А. Л. Чистов, *Алгоритмы полиномиальной сложности для вычислительных задач теории алгебраических кривых.* — Зап. научн. семин. ЛОМИ **176** (1989), 127–150.
7. S. Basu, R. Pollack, M. -F. Roy, *A new algorithm to find a point in every cell defined by a family of polynomials.* Quantifier Elimination and Cylindrical Algebraic Decomposition, B. Caviness and J. Johnson Eds., Springer-Verlag, to appear.
8. J. Bochnak, M. Coste, M. -F. Roy, *Géométrie algébrique réelle.* Springer–Verlag, Berlin, Heidelberg, New York, 1987.
9. A. L. Chistov, *Polynomial-Time Computation of the Dimension of Algebraic Varieties in Zero-Characteristic.* — J. Symb. Comp. **22**, No. **1** (1996), 1–25.
10. A. L. Chistov, *Polynomial–time computation of the dimensions of components of algebraic varieties in zero–characteristic.* — J. Pure App. Algebra **117 & 118** (1997), 145–175.
11. A. L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm.* — Lect. Notes Comp. Sci. **233**, Springer, New York, Berlin, Heidelberg, 1986, p. 247–255.
12. D. Lazard, *Algèbre linéaire sur* $k[x_1, \dots, x_n]$ *et élimination.* — Bull. Soc. Math. France **105** (1977), 165–190.
13. D. Lazard, *Résolution des systèmes d'équations algébrique.* — Theor. Comp. Sci. **15** (1981), 77–110.
14. J. Milnor, *On Betti numbers of real varieties.* — Proc. Amer. Math. Soc. **15** No. **2** (1964), 275–280.
15. J. Renegar, *A faster PSPACE algorithm for deciding the existential theory of reals.* Proc. 29th Annual Symp. on Foundations of Computer Sci., 1988, p. 291–295.
16. M.-F. Roy, N. Vorobjov, *Computing the Complexification of a Semi-algebraic Set.* Proc. of ISSAC'96 conference (1996), 26–34.

Chistov A. L. Strong version of the basic deciding algorithm for the existential theory of real fields.

Let U be a real algebraic variety in n-dimensional affine space which is a set of all zeroes of a family of polynomials of degrees less than d. In the case when U is bounded (it is the main case) an algorithm of polynomial complexity is described for constructing a subset of U with the number of elements bounded from above by d^n which for every s has a non–empty intersection with every cycle with coefficients from $\mathbb{Z}/2\mathbb{Z}$ of dimension s of the closure of the set of smooth points of dimension s of U.

Санкт-Петербургский институт
информатики и автоматизации
Российской академии наук

Поступило 15 января 1999 г.