Записки научных
семинаров ПОМИ
Том 325, 2005 г.

**А. Л. Чистов**

# ВЫЧИСЛЕНИЕ СТЕПЕНИ ДОМИНАНТНОГО МОРФИЗМА В НУЛЕВОЙ ХАРАКТЕРИСТИКЕ ЗА ПОЛИНОМИАЛЬНОЕ ВРЕМЯ. II

## 1. Введение

Данная статья продолжает работу [9] и является второй её частью. Третья часть [10] будет заключительной. Данное введение можно рассматривать как совместное для настоящей статьи и [10]. Мы исследуем общие рациональные морфизмы в нулевой характеристике с алгоритмической точки зрения. Приложением результатов настоящей статьи является обоснование метода представления алгебраического многообразия при помощи систем представителей точек его неприводимых компонент, предложенного в [7]. Именно, в одной из следующих статей мы рассмотрим это обоснование, а также алгоритм для построения гладкой стратификации, описанной в [7], подробно. Теорема 1 (см. ниже) будет там основным орудием (частично при этом будут использоваться и результаты из [10]). Кроме того, мы увидим в той же последующей статье, что теорема 1 позволяет вычислять пересечения и индексы пересечений алгебраических многообразий, заданных при помощи метода из [7] (хотя неприводимые компоненты пересечений не всегда могут быть заданы методом из [7] с хорошей верхней оценкой на степени соответствующих многочленов). Результаты из [10] будут использованы в будущем при построении алгоритма для первой теоремы Бертини.

В настоящей статье нам потребовалось разработать новый метод для решения систем полиномиальных уравнений и неравенств с квадратами абсолютных величин (см. [12]) в случае, когда эти системы содержат общие линейные формы (и даже общие однородные многочлены заданных степеней; но в этой статье нам требуется только случай линейных форм). Именно, пусть это система от $(n+1)\nu$ переменных $X_{i,j}$, $0 \leqslant j \leqslant n$, $1 \leqslant i \leqslant \nu$, где $\nu = O(1)$ (рассматривается как константа, $\nu < n$), и также от линейных форм $U_\alpha = \sum_{0\leqslant j\leqslant n} u_{\alpha,j}X_{i,j}$, $1 \leqslant \alpha \leqslant \mu$, где все $u_{\alpha,j}$

являются переменными и $\mu = O(n)$. Предположим, что эта система зависит также от других $O(n)$ переменных. Так что полное число переменных может быть $\geqslant Cn^2$ для некоторой константы $C$. Следовательно, применяя общий метод для решения таких систем (см. [12]), мы получаем для времени работы алгоритма построения решения оценку, полиномиальную от $d^{n^2}$, где $d$ – оценка на степень всех уравнений и неравенств. Кратко можно сказать, что предлагаемый метод позволяет заменить общие линейные формы на линейные формы от $\nu$ переменных $X_{i,j_1}, \dots, X_{i,j_\nu}$, где $0 \leqslant j_1 < \dots < j_\nu \leqslant n$ выбраны, и получить новую систему. Следовательно, в новой системе имеется только $\mu\nu = O(n)$ переменных $u_{\alpha,j_\beta}$, соответствующих различным выборам $j_1, \dots, j_\nu$. Данный метод сводит построение решения первоначальной системы к построению решений $\binom{n+1}{\nu}$ новых систем от $O(n)$ переменных.

Результаты настоящей работы фактически основываются на этом методе (хотя мы формально и не описываем его отдельно от рассматриваемых задач). Он применяется в разделе 1 для усиления теоремы 1 из [8], а также в разделах 3 и 4 [10]. Также мы хотели бы подчеркнуть здесь важность работы [5] и ее следствия теоремы 2 из [9] для настоящей статьи. Кроме того, теперь мы используем работу [8] (исправление формулировки леммы 2 из [8] см. в [9]), [9] и другие наши предыдущие статьи.

Пусть $k$ – поле нулевой характеристики с алгебраическим замыканием $\overline{k}$. Пусть $X_0, X_1, \dots$ – независимые переменные над $k$. Обозначим через $\mathbb{P}^n(\overline{k})$, $n \geqslant 0$, проективное пространство над полем $\overline{k}$ с координатами $X_0, \dots, X_n$. Мы будем предполагать, что $\mathbb{P}^n(\overline{k})$ определено над $k$. Для произвольных однородных многочленов $g_1, \dots, g_m \in \overline{k}[X_0, \dots, X_n]$ будем обозначать через $\mathcal{Z}(g_1, \dots, g_m)$ множество всех общих нулей многочленов $g_1, \dots, g_m$ в $\mathbb{P}^n(\overline{k})$. Аналогичные обозначения будут использоваться для множеств нулей идеалов и многочленов с другими полями коэффициентов в аффинных и проективных пространствах (это будет видно из контекста). Для поля $k$ и семейства элементов $a' = \{a'_i\}_{i \in I}$ из расширения поля $k$ мы будем обозначать через $k(a')$ (соответственно $k[a']$) поле (соответственно кольцо), порождённое над $k$ всеми элементами $a'_i$, $i \in I$. Для двух (или более) семейств $a'$, $a''$ обозначения $k(a', a'')$, $k[a', a'']$ имеют аналогичный смысл. Теперь предположим, что $a'$ является семейством алгебраически независимых переменных над $k$ и $f \in k[a']$. Предположим, что $b' = \{b'_i\}_{i \in I}$ – семейство элементов из $k$ с теми же самыми индексами, что и $a'$. Тогда мы будем обозначать через $f(b')$ значение $f$ при $a'_i = b'_i$, $i \in I$, а также использовать другие аналогичные обозначения.

В алгоритмической части статьи мы будем предполагать, что $k$ является конечнопорождённым расширением поля рациональных чисел $\mathbb{Q}$. Поле $k$ снабжено вещественной структурой, если задано вложение $k \to R[\sqrt{-1}]$, где $R$ – вещественное упорядоченное поле.

Рассмотрим систему полиномиальных уравнений от $n$ переменных и фиксированного числа неравенств с квадратами абсолютных величин с коэффициентами из поля $k$. Пусть степени уравнений и неравенств меньше $d$ (см. подробности в [12], а также в [9, раздел 1]). Тогда (см. [12, предложение 1]) можно построить вещественную структуру на $k$ и выяснить, за полиномиальное время от $d^n$ и длины записи входных данных, имеет ли данная система решение в $\mathbb{A}^n(\overline{k})$ относительно этой вещественной структуры. Если такое решение существует, его можно построить за то же самое время. Координаты решения принадлежат конечному расширению поля $k$. Это конечное расширение строится и задаётся примитивным элементом и его минимальным многочленом. Мы будем использовать это предложение много раз без явной ссылки на него.

Поскольку $k$ – произвольное конечнопорождённое поле над $\mathbb{Q}$, то этот результат справедлив также в случае, если заменить поле коэффициентов $k$ на конечное расширение поля $k_i = k(\varepsilon_1, \dots, \varepsilon_i)$ для фиксированного $i$, где $\varepsilon_j > 0$ для $j \geqslant 1$ является бесконечно малой величиной относительно поля $k_{j-1}$, см. ниже. Теорема 2 из работы [9], которая основывается на работе [5], усиливает этот результат. Фактически в этой статье большая часть систем полиномиальных уравнений и неравенств решается при помощи теоремы 2 из [9].

Пусть $V \subset \mathbb{P}^n(\overline{k})$ – проективное алгебраическое многообразие, которое является множеством всех общих нулей семейства однородных многочленов от $n+1$ переменных степени меньше $d$ с коэффициентами из поля $k$. Пусть $W$ является определённой над $k$ и неприводимой над $k$ компонентой многообразия $V$, и $W$ задано своей точкой, которая принадлежит только одной неприводимой над $k$ компоненте многообразия $V$, подробности см. в [8, теорема 1], а также ниже. Пусть $e_0, \dots, e_r \in k[X_0, \dots, X_n]$ – однородные многочлены, такие, что $\deg e_i = d' \geqslant 1$ для всякого ненулевого $e_i$, $0 \leqslant i \leqslant r$. Мы будем предполагать в дальнейшем, что $\dim W \cap \mathcal{Z}(e_0, \dots, e_r) < \dim W$. Пусть

$$p : W \setminus \mathcal{Z}(e_0, \dots, e_r) \to \mathbb{P}^r, \quad (X_0 : \dots : X_n) \mapsto (e_0 : \dots : e_r) \qquad (1)$$

– регулярный морфизм. Положим $W' = \overline{p(W \setminus \mathcal{Z}(e_0, \dots, e_r))}$ (здесь и ниже в аналогичных ситуациях черта обозначает замыкание относительно топологии Зариского). Следовательно, $W'$ – неприводимое над $k$ замкнутое подмногообразие пространства $\mathbb{P}^r(\overline{k})$. Заметим, что можно рассматривать рациональный морфизм $W \to \mathbb{P}^r(\overline{k})$ проективных алгебраических многообразий, заданный по тому же самому правилу, но, чтобы быть более точными, в дальнейшем мы будем иметь дело с регулярными морфизмами квазипроективных алгебраических многообразий. Обозначим через

$$p' : W \setminus \mathcal{Z}(e_0, \dots, e_r) \to W'$$

доминантный морфизм, индуцированный $p$. Предположим, что $\dim W = n - s$ и $\dim W' = n - \sigma$ (можно вычислить $s$ и $\sigma$, используя алгоритм из [4], см. ниже). Следовательно, $0 \leqslant s \leqslant \sigma \leqslant n$. Пусть $v_j = \sum_{0 \leqslant i \leqslant n} v_{j,i} X_i$, $0 \leqslant j \leqslant n+1$, – общие линейные формы относительно $X_0, \dots, X_n$, т.е. степень трансцендентности семейства всех коэффициентов $v_{j,i}$ над $k$ равна $(n+2)(n+1)$. По определению, $v = (v_{s+1}, \dots, v_\sigma)$, $\overline{v} = (v_0, \dots, v_{n+1})$ и $k_v$ (соответственно $k_{\overline{v}}$) – поле, порождённое над $k$ элементами $v_{j,i}$, $s+1 \leqslant j \leqslant \sigma$, $0 \leqslant i \leqslant n$ (соответственно $0 \leqslant j \leqslant n+1$, $0 \leqslant i \leqslant n$). Обозначим через $\widetilde{v}$ семейство коэффициентов $v_{j,i}$, $0 \leqslant j \leqslant n+1$, $0 \leqslant i \leqslant n$. Тогда $k_{\overline{v}} = k(\widetilde{v})$. Теперь $p$ и $p'$ индуцируют морфизмы

$$p_v : (W \cap \mathcal{Z}(v_{s+1}, \dots, v_\sigma)) \setminus \mathcal{Z}(e_0, \dots, e_r) \to \mathbb{P}^r(\overline{k_v}),$$
$$p'_v : (W \cap \mathcal{Z}(v_{s+1}, \dots, v_\sigma)) \setminus \mathcal{Z}(e_0, \dots, e_r) \to W'(k_v),$$

определённые над $k_v$. Для удобства обозначений положим $q_v = p'_v$. Тогда $q_v$ является доминантным морфизмом. Положим $W_v = W \cap \mathcal{Z}(v_{s+1}, \dots, v_\sigma)$ в проективном пространстве над алгебраическим замыканием поля $k_v$. Имеем $\dim W \cap \mathcal{Z}(v_{s+1}, \dots, v_\sigma) \setminus \mathcal{Z}(e_0, \dots, e_r) = n - \sigma$. Мы вычисляем (см. [10, теорема 1]) степень $\deg p'_v$.

Применим теорему 1 из работы [9] к морфизму $p'_v$ (вместо $p'$), заменяя в формулировке этой теоремы поле $k$ на $k_v$. Обозначим через $\mathcal{V} \subset \mathbb{A}^{(r+1)(n-\sigma+1)}(\overline{k_v})$ непустое открытое в топологии Зариского подмножество всех наборов из $(n-\sigma+1)$ линейных форм из утверждения (d) теоремы 1 работы [9], применённой к $p'_v$. *Положим* $\mathcal{U}'_0 = \mathcal{V} \cap \mathbb{A}^{(r+1)(n-\sigma+1)}(\overline{k})$. Тогда $\mathcal{U}'_0$ очевидно является непустым открытым в топологии Зариского подмножеством в $\mathbb{A}^{(r+1)(n-\sigma+1)}(\overline{k})$. Следовательно, $L' \in \mathcal{U}'_0$ в том и только в том случае, если

$$\#\big((W_v \setminus \mathcal{Z}(e_0, ..., e_r)) \cap \mathcal{Z}(e'_{\sigma+1}, ..., e'_n)\big) = \deg(q_v) \deg W', \tag{2}$$

$$(W_v \setminus \mathcal{Z}(e_0, \dots, e_r)) \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_n) \cap \mathcal{Z}(e'_0) = \emptyset, \tag{3}$$

$$(W_v \setminus \mathcal{Z}(e_0, \dots, e_r)) \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_n) \cap (\overline{V_v \setminus W_v}) = \emptyset, \tag{4}$$

$$\#\big(W' \cap \mathcal{Z}(L'_{\sigma+1}, \dots, L'_n)\big) = \deg W' \tag{5}$$

в проективных пространствах над алгебраическим замыканием поля $k_v$. Множество $\mathcal{U}'_0$ инвариантно относительно действия группы Галуа $\mathrm{Gal}(\overline{k}/k)$ и, следовательно, определено над $k$. Мы построим элемент из $\mathcal{U}'_0$ в [10]. Более точно, мы определим ниже открытые в топологии Зариского множества $\mathcal{U}'''_{n+1} \subset \mathcal{U}'''_0 \subset \mathcal{U}''_0 \subset \mathcal{U}'_0$, относящиеся к морфизму $p$, и построим элемент из $\mathcal{U}'''_0$ за полиномиальное время в [10, теорема 1].

Пусть $K$ – поле, содержащее алгебраически независимые над $k$ элементы $u_{j,w}$, $j \in \{0, \sigma+1, \dots, n\}$, $0 \leqslant w \leqslant r$, и такое, что $K$ и $k_{\overline{v}}$ являются линейно раздельными над $k$. Обозначим через $u$ семейство элементов $u_{j,w}$, $j \in \{0, \sigma+1, \dots, n\}$, $0 \leqslant w \leqslant r$. Пусть $l'_{j,w} \in \overline{k}$, $j \in \{0, \sigma+1, \dots, n\}$, $0 \leqslant w \leqslant r$. Пусть $L'_j = l'_{j,0}X_0 + \ldots + l'_{j,r}X_r$ (соответственно $U_j = u_{j,0}X_0 + \ldots + u_{j,r}X_r$), $j \in \{0, \sigma+1, \dots, n\}$, – линейные формы из $\overline{k}[X_0, \dots, X_r]$ (соответственно $K[X_0, \dots, X_n]$). Положим $e'_j = L'_j(e_0, \dots, e_r)$ (соответственно $u_j = U_j(e_0, \dots, e_r)$), $j \in \{0, \sigma+1, \dots, n\}$. Положим далее $L' = (L'_0, L'_{\sigma+1}, \dots, L'_n)$ (соответственно $U = (U_0, U_{\sigma+1}, \dots, U_n)$). В дальнейшем мы будем определять некоторые объекты, соответствующие $L'$. Аналогичные объекты, соответствующие $U$, определяются при помощи замены поля $k$ на $K$.

Пусть $L'$ – произвольное, как выше (но, возможно, $L' \notin \mathcal{U}'_0$). В дальнейшем, если не оговорено противное, мы будем предполагать, что линейные формы $L'_0, L'_{\sigma+1}, \dots, L'_n$ являются линейно независимыми. Мы будем рассматривать морфизмы

$$p_{L'}\ :\ W \setminus \mathcal{Z}(e'_0, e'_{\sigma+1}\ldots, e'_n) \to \mathbb{P}^{n-\sigma}(\overline{k}), \tag{6}$$

$$p_{v,L'}\ :\ W \cap \mathcal{Z}(v_{s+1},\ldots,v_\sigma) \setminus \mathcal{Z}(e'_0, e'_{\sigma+1}\ldots, e'_n) \to \mathbb{P}^{n-\sigma}(\overline{k_v}), \tag{7}$$

определённые над полями $k$ и $k_v$ соответственно и заданные одной и той же формулой

$$(X_0 : \ldots : X_n) \mapsto (e'_0 : e'_{\sigma+1} : \ldots : e'_n).$$

Для всякого $\sigma \leqslant i \leqslant n$ обозначим через

- $W_i(L')$ объединение всех неприводимых над $\overline{k}$ компонент $E$ многообразия $W \cap \mathcal{Z}(e'_{\sigma+1},\ldots,e'_i)$, таких, что $\dim E = n-i+\sigma-s$ и ограничение $p_{L'}|_E\ :\ E\setminus \mathcal{Z}(e'_0,\ e'_{\sigma+1},\ldots,e'_n) \to \mathcal{Z}(X_1,\ldots,X_{i-\sigma})$ является доминантным (здесь $\mathcal{Z}(X_1,\ldots,X_{i-\sigma})\ \subset \mathbb{P}^{n-\sigma}(\overline{k})$ – линейное подпространство).

Тогда $E \not\subset \mathcal{Z}(e'_0, e'_{\sigma+1}\ldots, e'_n)$. Морфизм $p_{L'}|_{W_i(L')}\ :\ W_i(L') \setminus \mathcal{Z}(e'_0, e'_{\sigma+1},\ldots,e'_n)\ \to\ \mathcal{Z}(X_1,\ldots,X_{i-\sigma})$ является доминантным, если $W_i(L') \neq \emptyset$ (здесь нельзя исключить, что $W_i(L')$ пусто для некоторого $i$). В частности, $W_\sigma(L') = W$ в том и только в том случае, если морфизм $p_{L'}$ является доминантным. Заметим, что $W_i(L')$ зависит только от $L'_{\sigma+1},\ldots,L'_i$. Так что мы будем обозначать также $W_i(L') = W(L'_{\sigma+1},\ldots,L'_i)$. Морфизм $p_{L'}|_{W_i(L')}$ является доминантным или $W_i(L') = \emptyset$, для всякого $\sigma+1 \leqslant i \leqslant n$. Следовательно,

$$\dim W(L'_{\sigma+1},\ldots,L'_{i-1}) \cap \mathcal{Z}(e'_i) \leqslant n - i + \sigma - s \tag{8}$$

и

$$\dim W(L'_{\sigma+1},\ldots,L'_n) \cap \mathcal{Z}(e'_0) \leqslant \sigma - s - 1. \tag{9}$$

Обозначим для краткости $L'_{n+1} = L'_0$, $e'_{n+1} = e'_0$, $W_{n+1}(L') = W(L'_{\sigma+1},\ldots,\ L'_{n+1}) = \emptyset$. Следовательно,

$$W_{i-1}(L') \cap \mathcal{Z}(e'_i) = W_i(L') \cup W_i^{(1)}(L') \cup W_i^{(2)}(L') \cup W_i^{(3)}(L'),\qquad \sigma+1 \leqslant i \leqslant n+1,$$

где

- $W_i^{(1)}(L')$ – объединение всех неприводимых над $\overline{k}$ компонент $E$ многообразия $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$, таких, что $E$ является неприводимой компонентой многообразия $W \cap \mathcal{Z}(e'_0, e'_{\sigma+1}\ldots, e'_n)$;

- $W_i^{(2)}(L')$ – объединение всех неприводимых над $\overline{k}$ компонент $E$ многообразия $W_{i-1}(L')\cap\mathcal{Z}(e'_i)$, таких, что $E$ содержится в $W_j^{(1)}(L')$ для некоторого $s\leqslant j<i$;
- $W_i^{(3)}(L')$ – объединение всех неприводимых над $\overline{k}$ компонент $E$ многообразия $W_{i-1}(L')\cap\mathcal{Z}(e'_i)$, таких, что $E\not\subset\mathcal{Z}(e'_0,e'_{\sigma+1}\dots,e'_n)$ и $\dim\overline{p_{L'}(E\setminus\mathcal{Z}(e'_0,e'_{\sigma+1}\dots,e'_n))}<n-i+\sigma-s$. Следовательно, $W_i^{(3)}(L')=\emptyset$ для $i=n,n+1$.

Положим также $W^{(\beta)}(L')=W_\sigma^{(\beta)}(L')=\emptyset$, $W_0^{(\beta)}(L')=W_{n+1}^{(\beta)}(L')$, $\beta=1,2,3$.

Заметим, что если $L'\in\mathcal{U}'_0$, то $W'\cap\mathcal{Z}(L'_0,L'_{\sigma+1},\dots,L'_n)=\emptyset$ в $\mathbb{P}^n(\overline{k})$. Согласно лемме 4 из [10], если $W'\cap\mathcal{Z}(L'_0,L'_{\sigma+1},\dots,L'_n)=\emptyset$, то $W\cap\mathcal{Z}(e_0,\dots,e_r)=W\cap\mathcal{Z}(e'_0,e'_{\sigma+1},\dots,e'_n)$ (фактически в этой лемме мы имеем более сильное утверждение). Следовательно, размерность всякой неприводимой компоненты многообразия $W\cap\mathcal{Z}(e_0,\dots,e_r)$ не меньше $\sigma-s-1$. Отсюда для произвольного $L'$ (возможно, $W'\cap\mathcal{Z}(L'_0,L'_{\sigma+1},\dots,L'_n)\neq\emptyset$) всякая неприводимая компонента многообразия $W_{n+1}^{(1)}(L')$ является неприводимой компонентой размерности $\sigma-s-1$ многообразия $W\cap\mathcal{Z}(e_0,\dots,e_r)$. Если $L'\in\mathcal{U}'_0$, то для всякого $\sigma+1\leqslant i\leqslant n$ всякая неприводимая компонента многообразия $W_i^{(1)}(L')$ является неприводимой компонентой размерности $n-\sigma-s-i$ пересечения $W\cap\mathcal{Z}(e_0,\dots,e_r)$. Если $L'\in\mathcal{U}'_0$ и $\bigcup_{\sigma+1\leqslant j\leqslant i-1}W_j^{(3)}(L')$ не содержит никакую неприводимую компоненту $E$ многообразия $W\cap\mathcal{Z}(e_0,\dots,e_r)$, такую, что $\dim E=n-\sigma+s-i$ (в частности, если $\bigcup_{\sigma+1\leqslant j\leqslant i-1}W_j^{(3)}(L')=\emptyset$ или если $L'\in\mathcal{U}''_0$, см. ниже), то, обратно, всякая неприводимая компонента размерности $n-\sigma-s-i$ пересечения $W\cap\mathcal{Z}(e_0,\dots,e_r)$ является неприводимой компонентой многообразия $W_i^{(1)}(L')$.

Далее, для всякого $z\in W'$ всякая неприводимая компонента $E$ слоя $p^{-1}(z)$ является неприводимой компонентой $p_{L'}^{-1}p_{L'}p^{-1}(z)$, если $L'\in\mathcal{U}'_0$. Поэтому $\dim E\geqslant\sigma-s$. Последнее неравенство – это теорема о размерности слоёв для морфизма $p'$, ср. [1]. Кроме того, для всякого $\sigma+1\leqslant i\leqslant n+1$

- если $W'\cap\mathcal{Z}(L'_0,L'_{\sigma+1},\dots,L'_n)=\emptyset$, то $W_i^{(1)}(L')$ является объединением всех неприводимых над $\overline{k}$ компонент $E$ многообразия $W_{i-1}(L')\cap\mathcal{Z}(e'_i)$, таких, что $E$ является неприводимой компонентой многообразия $W\cap\mathcal{Z}(e_0,\dots,e_r)$;

- если $W' \cap \mathcal{Z}(L'_0, L'_{\sigma+1}, \dots, L'_n) = \emptyset$, то $W_i^{(3)}(L')$ является объединением всех неприводимых над $\overline{k}$ компонент $E$ многообразия $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$, таких, что $E \not\subset \mathcal{Z}(e_0, \dots, e_r)$ и $\dim \overline{p(E \setminus \mathcal{Z}(e_0, \dots, e_r))} < n - i + \sigma - s$.

*В дальнейшем во введении мы предполагаем, что* $W' \cap \mathcal{Z}(L'_0, L'_{\sigma+1}, \dots, L'_n) = \emptyset$. Представим $W_i(L')$ и $W_i^{(\beta)}(L')$, $\beta = 1, 2, 3$, как объединения попарно различных неприводимых над $\overline{k}$ алгебраических многообразий:

$$W_i(L') = \bigcup_{j \in J_i(L')} W_j, \quad \sigma \leqslant i \leqslant n,$$

$$W_i^{(\beta)}(L') = \bigcup_{j \in J_i^{(\beta)}(L')} W_j, \quad \sigma \leqslant i \leqslant n+1,\ \beta = 1, 2, 3$$

(в действительности $J_{\sigma+1}^{(2)}(L') = \emptyset$ и $W_{\sigma+1}^{(2)}(L') = \emptyset$). Обозначим через $W_i^{(1)}$ объединение всех неприводимых компонент размерности $n - i + \sigma - s$ многообразия $W \cap \mathcal{Z}(e_0, \dots, e_r)$. Пусть $W_j$, $j \in J_i^{(1)}$, – семейство всех неприводимых компонент многообразия $W_i^{(1)}$. В дальнейшем мы будем предполагать без ограничения общности, что $J_i^{(1)}(L') \subset J_i^{(1)}$.

Обозначим через $\iota_j(L')$, $j \in J_{i+1}(L')$ (соответственно $\iota_j(L')$, $j \in J_{i+1}^{(\beta)}(L')$, $\beta = 1, 2, 3$), $\sigma \leqslant i \leqslant n$, индекс пересечения $i(W_i(L'), \mathcal{Z}(e'_{i+1}); W_j)$ алгебраических многообразий $W_i(L')$ и $\mathcal{Z}(e'_{i+1})$ в $W_j$, см. [2]. Тогда по теореме Безу (см. [2])

$$\begin{aligned} d' \deg W_i(L') = \sum_{j \in J_{i+1}(L')} \iota_j(L') \deg W_j + \\ + \sum_{1 \leqslant \beta \leqslant 3} \sum_{j \in J_i^{(\beta)}(L')} \iota_j(L') \deg W_j. \end{aligned} \tag{10}$$

Положим

$$D_i(L') = \deg W_i(L') = \sum_{j \in J_i(L')} \deg W_j, \quad \sigma \leqslant i \leqslant n+1,$$

$$D_i^{(\beta)}(L') = \deg W_i^{(\beta)}(L') = \sum_{j \in J_i^{(\beta)}(L')} \deg W_j,$$

$\sigma \leqslant i \leqslant n+1$, $\beta = 1, 2, 3$.

Мы будем обозначать также $D_\alpha(L') = D(L'_{\sigma+1},\dots,L'_\alpha)$, $J_\alpha(L') = J(L'_{\sigma+1},\dots, L'_\alpha)$, $W_\alpha(L') = W(L'_{\sigma+1},\dots,L'_\alpha)$ для $\sigma \leqslant \alpha \leqslant n+1$; и $W^{(\beta)}_\alpha(L') = W^{(\beta)}(L'_{\sigma+1},\dots, L'_\alpha)$, $D^{(\beta)}_\alpha(L') = D^{(\beta)}(L'_{\sigma+1},\dots,L'_\alpha)$, $J^{(\beta)}_\alpha(L') = J^{(\beta)}(L'_{\sigma+1},\dots, L'_\alpha)$ для $\sigma+1 \leqslant \alpha \leqslant n+1$, $\beta = 1,2,3$.

Положим

$$D_i = D_i(U),\ J_i = J_i(U), \quad \sigma \leqslant i \leqslant n+1,$$

$$D^{(\beta)}_i = D^{(\beta)}_i(U),\ J^{(\beta)}_i = J^{(\beta)}_i(U), \quad \sigma \leqslant i \leqslant n+1,\ \beta = 1,2,3,$$

$$\iota_j = \iota_j(U), \quad j \in J^{(\beta)}_i,\ \sigma \leqslant i \leqslant n+1,\ \beta = 1,2,3, \tag{11}$$

и $D_0 = D_{n+1}$, $D^{(\beta)}_0 = D^{(\beta)}_{n+1}$, $J^{(\beta)}_0 = J^{(\beta)}_{n+1}$, $\beta = 1,2,3$. Справедливо неравенство $D_i(L') \leqslant D_i$ для всякого $\sigma \leqslant i \leqslant n$, см. [10, лемма 8]. *Если $L' \in \mathcal{U}'_0$, то по лемме 11 из* [9] *индекс пересечения $\iota_j(L')$ равен 1 для всякого $j \in J_i(L')$, $\sigma+1 \leqslant i \leqslant n$.* В частности, $\iota_j = 1$ для всякого $j \in J_i$, $\sigma+1 \leqslant i \leqslant n$. Далее, если $L' \in \mathcal{U}'_0$ и $J^{(1)}_i(L') = J^{(1)}_i$, то $\iota_j(L') \geqslant \iota_j$ для всякого $j \in J^{(1)}_i$, см. [10, лемма 7] (фактически последнее неравенство выполнено при более слабых условиях из этой леммы). Кроме того, если дополнительно $i = n+1$, то $\iota_j(L') = \iota_j$, см. [10, лемма 8].

Обозначим через $W'''$ замыкание в топологии Зариского всех точек $z \in W'$, таких, что $\dim p^{-1}(z) > s - \sigma$. Обозначим через $W^{(4)}$ замыкание относительно топологии Зариского объединения всех неприводимых компонент $E$ обратного образа $p^{-1}(W''')$, таких, что $\dim \overline{p(E)} < \sigma - s + \dim E$. По теореме о размерности слоёв (см. [1] или выше) для всякого $z \in W'''$ размерность всякой неприводимой компоненты (если она существует; $p^{-1}(z)$ может быть пустым) обратного образа $p^{-1}(z)$ не меньше $\sigma - s + 1$. Следовательно, квазипроективное алгебраическое многообразие $W^{(4)} \setminus \mathcal{Z}(e_0,\dots,e_r)$ есть в точности множество всех точек $x \in W \setminus \mathcal{Z}(e_0,\dots,e_r)$, таких, что для всякой неприводимой компоненты $E$ слоя $p^{-1}p(x)$, если $x \in E$, то $\dim E > \sigma - s$. Следовательно, если $L' \in \mathcal{U}'_0$, то $W^{(3)}_i(L') \subset W^{(4)}$, $\sigma+1 \leqslant i \leqslant n-1$.

Пусть $\sigma \leqslant i \leqslant n$ – целое число. Нам потребуются также следующие условия (здесь, если размерность отрицательна, многообразие пусто):

$$\dim(\, W^{(4)} \setminus \mathcal{Z}(e_0,\dots,e_r)\,) \cap \mathcal{Z}(e'_{\sigma+1},\dots,e'_i) \leqslant n - i + \sigma - s - 1, \tag{12}$$

$$\dim W(L'_{\sigma+1},\dots,L'_i) \cap (\overline{V \setminus W}) \leqslant n - i + \sigma - s - 1. \tag{13}$$

Согласно теореме 1 из работы [9], если $L' = (L'_0, L'_{\sigma+1}, \dots, L'_n) \in \mathcal{U}'_0$, то выполняется неравенство (13) (напомним, что неравенства (8), (9) всегда выполняются), $W_n(L')$ является замыканием относительно топологии Зариского многообразия $W \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_n) \setminus \mathcal{Z}(e_0, \dots, e_r)$ и $D_n(L') = D_n = \deg p'_v \deg W'$. По лемме 11 из [9], если $L' \in \mathcal{U}'_0$, то $W_i(L')$ есть в точности объединение всех неприводимых над $\overline{k}$ компонент $E$ многообразия $W \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_i)$, таких, что $E(\overline{k_v})$ содержит по крайней мере одну из $\deg p'_v \deg W'$ точек многообразия $W_v \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_n) \setminus \mathcal{Z}(e_0, \dots, e_r)$ (или, что эквивалентно, $E$ содержит неприводимую компоненту многообразия $W_n(L')$).

Далее, пусть $\sigma \leqslant \alpha \leqslant n$ – целое число и $L' \in \mathcal{U}'_0$. Согласно лемме 11 из работы [9], условие (12) выполняется для всех $\sigma \leqslant i \leqslant \alpha$ тогда и только тогда, когда

$$W_i(L') = \overline{W \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_i) \setminus \mathcal{Z}(e_0, \dots, e_r)} \tag{14}$$

для всех $\sigma \leqslant i \leqslant \alpha$. В этом случае $W_i^{(3)}(L') = \emptyset$ для всех $\sigma + 1 \leqslant i \leqslant \alpha$, и, следовательно, в силу (8) и (9) алгебраическое многообразие $W_i^{(1)}(L')$, $\sigma + 1 \leqslant i \leqslant \alpha$, совпадает с объединением всех неприводимых компонент размерности $n - i + \sigma - s$ пересечения $W \cap \mathcal{Z}(e_0, \dots, e_r)$. Следовательно, $W_i^{(1)}(L')$ и $J_i^{(1)}(L') = J_i^{(1)}$ не зависят от $L'$ при рассматриваемых условиях.

Согласно лемме 20 ([10, раздел 3]), можно выяснить, верно ли, что $L' \in \mathcal{U}'_0$, за полиномиальное время от длины записи входных данных и $(dd')^n$, т.е. за полиномиальное время от длины записи $L'$ и от величин из оценки на время работы алгоритма из теоремы 1 работы [10].

Пусть $\sigma \leqslant \alpha \leqslant n + 1$ – целое число. Отождествим множество всех $(\alpha - \sigma)$-наборов $(L'_{\sigma+1}, \dots, L'_\alpha)$ линейных форм $L'_j \in \overline{k}[X_0, \dots, X_r]$ (соответственно $L'_j \in \overline{k_v}[X_0, \dots, X_r]$) с $\mathbb{A}^{(r+1)(\alpha-\sigma)}(\overline{k})$ (соответственно $\mathbb{A}^{(r+1)(\alpha-\sigma)}(\overline{k_v})$). Для удобства обозначений, если $\alpha = \sigma + 1$, то мы будем отождествлять 1-набор $(L'_{\sigma+1})$ с линейной формой $L'_{\sigma+1}$. Напомним, что $L'_0 = L'_{n+1}$. *Обозначим через* $\mathcal{U}'_\alpha$, $\sigma \leqslant \alpha \leqslant n + 1$, *образ множества* $\mathcal{U}'_0$ *относительно линейного отображения* $\pi_\alpha : \mathbb{A}^{(r+1)(n-\sigma+1)}(\overline{k}) \to \mathbb{A}^{(r+1)(\alpha-\sigma)}(\overline{k})$, $L' \mapsto (L'_{\sigma+1}, \dots, L'_\alpha)$. Тогда $\mathcal{U}'_\alpha$ – открытое в топологии Зариского множество, так как образ открытого множества относительно линейной проекции открыт. Кроме того, $\pi_{n+1}$ является изоморфизмом.

*Пусть $\sigma \leqslant \alpha \leqslant n+1$ – целое число. Обозначим через $\mathcal{U}''_\alpha \subset \mathcal{U}'_\alpha$ подмножество всех $(L'_{\sigma+1}, \dots, L'_\alpha)$, таких, что*

$$D(L'_{\sigma+1}, \dots, L'_i) = D_i \tag{15}$$

*для всякого $\sigma+1 \leqslant i \leqslant \alpha$. Положим также $\mathcal{U}''_0 = \mathcal{U}'_0 \cap \pi_n^{-1}(\mathcal{U}''_n) = \pi_{n+1}^{-1}(\mathcal{U}''_{n+1})$.* Если $(L'_{\sigma+1}, \dots, L'_\alpha) \in \mathcal{U}''_\alpha$, то (см. [10, раздел 2, лемма 8]) индексы пересечения $\iota_j(L'_{\sigma+1}, \dots, L'_i)$ равны $\iota_j$ для всех $j \in J_i^{(1)}$, $\sigma+1 \leqslant i \leqslant \alpha$, и, как мы отметили, $\iota_j = 1$ для всех $j \in J_i(L'_{\sigma+1}, \dots, L'_i)$, $\sigma+1 \leqslant i \leqslant \alpha$. Далее, $\mathcal{U}''_\alpha$ – непустое открытое в топологии Зариского подмножество в $\mathbb{A}^{(r+1)(\alpha-\sigma)}(\overline{k})$, см. [10, раздел 2, лемма 9]. По лемме 14 из [9], применённой к $W_v$, $p'_v$, $\alpha$ вместо $W$, $p'$, $i+1$, если $D_i(L') = D_i$ для всех $\sigma+1 \leqslant i \leqslant \alpha$, то $W_i^{(3)}(L') = \emptyset$ для всех $\sigma+1 \leqslant i \leqslant \alpha$. Следовательно, если $L' \in \mathcal{U}''_0$, то выполняются условия (12) и (14) для всех $\sigma \leqslant i \leqslant n-1$.

Если расширить основное поле, то $U \in \mathcal{U}''_0$. Следовательно, из (10) следует, что

$$(d')^{n-\sigma+1} \deg W = \sum_{\sigma+1 \leqslant i \leqslant n+1} \Big( \sum_{j \in J_i^{(1)}} (d')^{n-i+1} \iota_j \deg W_j + \sum_{j \in J_i^{(2)}} (d')^{n-i+1} \iota_j \deg W_j \Big). \tag{16}$$

*Пусть $\sigma \leqslant \alpha \leqslant n+1$ – целое число. Обозначим через $\mathcal{U}'''_\alpha \subset \mathcal{U}''_\alpha$ подмножество всех $(L'_{\sigma+1}, \dots, L'_\alpha)$, таких, что*

$$D^{(2)}(L'_{\sigma+1}, \dots, L'_i) = D_i^{(2)} \tag{17}$$

*для всех $\sigma+1 \leqslant i \leqslant \alpha$. Положим также $\mathcal{U}'''_0 = \mathcal{U}''_0 \cap \pi_n^{-1}(\mathcal{U}'''_n)$, т.е. $\mathcal{U}'''_0$ – множество всех $L' \in \mathcal{U}''_0$, таких, что $(L'_{\sigma+1}, \dots, L'_n) \in \mathcal{U}'''_n$.* Тогда $\mathcal{U}'''_\alpha$ – непустое открытое в топологии Зариского подмножество $\mathbb{A}^{(r+1)(\alpha-\sigma)}(\overline{k})$, см. [10, раздел 2, лемма 12]. Далее, $U \in \mathcal{U}'''_{n+1}(\overline{K})$. Очевидно, $\pi_{n+1}(\mathcal{U}'''_0) \supset \mathcal{U}'''_{n+1}$ и, если $s = \sigma$, то последнее включение становится равенством.

*Обозначим для краткости $\mathcal{U}' = \mathcal{U}'_{\sigma+1}$ (соответственно $\mathcal{U}'' = \mathcal{U}''_{\sigma+1}$, $\mathcal{U}''' = \mathcal{U}'''_{\sigma+1}$).*

Чтобы сформулировать теорему 1 из работы [10] без всяких ограничений на $s$ и $\sigma$, нам требуется рассмотреть также случай, когда $W$ является объединением некоторых определённых над $k$

и неприводимых над $k$ компонент многообразия $V$ (т.е. $W$ не обязательно неприводимо над $k$) и $\dim W = n-s = 0$ (фактически для $n = s$ теорема 1 из [10] тривиальна). В рассматриваемом случае $p$, $p'$, $W'$, определяются как выше. Мы имеем $W \cap \mathcal{Z}(e_0, \ldots, e_r) = \emptyset$, $\dim W' = n - \sigma = 0$. Пусть $L' = (L'_0)$, где $L'_0$ – линейная форма из $\overline{k}[X_0, \ldots, X_r]$. Элемент $L' = (L'_0)$ лежит в $\mathcal{U}'_0$ тогда и только тогда, когда $W' \cap \mathcal{Z}(L'_0) = \emptyset$ в $\mathbb{P}^r(\overline{k})$. Морфизм $p'$ – доминантный в том и только в том случае, если $L' \in \mathcal{U}'_0$. Для произвольного $L' \in \mathcal{U}'_0$ положим $W_n(L') = W$, $W_{n+1}(L') = \emptyset$, $W_n^{(j)}(L') = \emptyset$, $W_{n+1}^{(j)}(L') = \emptyset$ для $j = 1, 2, 3$. Положим $\mathcal{U}'''_0 = \mathcal{U}''_0 = \mathcal{U}'_0 = \mathcal{U}'''_{n+1} = \mathcal{U}''_{n+1} = \mathcal{U}'_{n+1}$. Все другие объекты, определённые выше для неприводимого $W$, определяются в рассматриваемом случае аналогичным образом.

**Замечание 1.** Из теоремы Безу вытекает, что если $L' \in \mathcal{U}'_0$, $J_i^{(2)}(L') = \emptyset$ для всех $s + 2 \leqslant i \leqslant n$ и выполняется условие (14) для всех $\sigma + 1 \leqslant i \leqslant n - 1$, то для всякого $\sigma + 1 \leqslant i \leqslant n + 1$ имеем $D_i(L') = D_i$ и $\iota_j(L') = \iota_j$ для всякого $j \in J_i^{(1)}$.

**Замечание 2.** Пусть $K_1$ – алгебраически замкнутое поле, $K_1 \supset k$, линейно раздельное с $k(W)$ над $k$. Выберем расширение $K_2 \supset k$, такое, что $W$ неприводимо над $K_2$ и $\overline{K_2} = K_1$ (например, $K_2$ может быть произвольным чисто трансцендентным расширением $k$, таким, что $\overline{K_2} = K_1$). Определим множества $\mathcal{U}'_\alpha$, $\mathcal{U}''_\alpha$, $\mathcal{U}'''_\alpha$ для основного поля $K_1$ (а также $K_2$), заменяя в определениях этих множеств основное поле $k$ на $K_2$. Для краткости обозначим полученные множества через $\mathcal{U}'_{K_1,\alpha}$, $\mathcal{U}''_{K_1,\alpha}$, $\mathcal{U}'''_{K_1,\alpha}$ (мы используем эти более подробные обозначения только в этом замечании). Тогда, очевидно, $\mathcal{U}'_{K_1,\alpha}$, $\mathcal{U}''_{K_1,\alpha}$, $\mathcal{U}'''_{K_1,\alpha}$ не зависят от выбора поля $K_2$, такого, как выше. В частности, первоначальные $\mathcal{U}'_\alpha$, $\mathcal{U}''_\alpha$, $\mathcal{U}'''_\alpha$, определённые для основного поля $k$, зависят только от $\overline{k}$. Далее, очевидно, $\mathcal{U}'_\alpha = \mathcal{U}'_{K_1,\alpha}(\overline{k})$, $\mathcal{U}''_\alpha = \mathcal{U}''_{K_1,\alpha}(\overline{k})$, $\mathcal{U}'''_\alpha = \mathcal{U}'''_{K_1,\alpha}(\overline{k})$ для всех $\alpha$. С другой стороны, вероятно также $\mathcal{U}'_\alpha(K_1) = \mathcal{U}'_{K_1,\alpha}$, $\mathcal{U}''_\alpha(K_1) = \mathcal{U}''_{K_1,\alpha}$, $\mathcal{U}'''_\alpha(K_1) = \mathcal{U}'''_{K_1,\alpha}$. Мы оставляем доказательство последних трех равенств читателю. В этой статье они нам не потребуются. Аналогично читатель может доказать, что если $V$ и $W$ определены над подполем $k'$ поля $k$ (расширение $k \supset k'$ может быть трансцендентным), то $\mathcal{U}'_\alpha$, $\mathcal{U}''_\alpha$, $\mathcal{U}'''_\alpha$ также определены над $k'$.

Напомним некоторые детали из [8]. Пусть $\overline{\lambda} = (L_0, \ldots, L_{n+1})$ и все $L_j \in k[X_0, \ldots, X_n]$, $0 \leqslant j \leqslant n + 1$, являются линейными формами. Предположим, что $\overline{\lambda}$ (т.е. линейные формы $L_0, \ldots, L_{n+1}$)

удовлетворяют утверждению теоремы 1 из [8] для алгебраического многообразия $V$. Тогда (см. [8, раздел 2]) для всякого $1 \leqslant j \leqslant n-2$, такого, что $V$ имеет неприводимую компоненту размерности $n-j$, справедливо равенство $v_j(\overline{\lambda}) = u_j(\overline{\lambda})$, где $v_j(\overline{\lambda}), u_j(\overline{\lambda}) \leqslant d^j(d^j-1)$ – целые числа, определённые в [8]. Однако сейчас обозначения $v_j$ и $u_j$ уже используются в другом смысле. Так что в настоящей статье мы будем обозначать эти числа через $b_j(\overline{\lambda}), a_j(\overline{\lambda})$ вместо обозначений $v_j(\overline{\lambda}), u_j(\overline{\lambda})$ из [8] соответственно. Более точно, в разделе 1 для произвольных $\overline{\lambda}$ и $V$, удовлетворяющих свойству (B) (см. начало раздела 1), мы определяем целые числа $b_j(\overline{\lambda}) = b_j(\overline{\lambda}, V)$, $a_j(\overline{\lambda}) = a_j(\overline{\lambda}, V)$ для всех $0 \leqslant j \leqslant n$.

В [8] мы не строили $\overline{\lambda}$ в общем положении с максимально возможными $b_j(\overline{\lambda})$, см. [8, замечание 3]. Мы применяли [8, замечание 2] как слабое приведение к общему положению. В настоящей статье это тоже возможно, однако изложение результатов при этом становится несколько громоздким. Так что мы сумели избежать использования замечания 2 из [8]. Вместо этого мы усиливаем результат работы [8] и строим $\overline{\lambda}$ в общем положении с максимально возможными $b_j(\overline{\lambda})$ (см. раздел 1), используя разработанный метод, см. начало введения. Поэтому теперь достаточно применять простой алгоритм приведения к целым коэффициентам, см. [9, предложение 2].

Пусть $\lambda = (L_{s+1}, \dots, L_\sigma)$, где все $L_j \in k[X_0, \dots, X_n]$, $s+1 \leqslant j \leqslant \sigma$, являются линейными формами. Рассмотрим следующее свойство.

(A) Для $\lambda$ задан элемент $\overline{\lambda}$ (следовательно, линейные формы $L_w$, $s+1 \leqslant w \leqslant \sigma$, из $\lambda$ и $\overline{\lambda}$ совпадают); для алгебраического многообразия $V$ и линейных форм $L_0, \dots, L_{n+1}$ справедливы утверждения теоремы 1 из [8]; и для всякого $0 \leqslant j \leqslant n$, такого, что $V$ имеет неприводимую компоненту размерности $n-j$, целое число $b_j(\overline{\lambda}) = a_j(\overline{\lambda})$ является максимально возможным (если варьировать $\overline{\lambda}$, подробности см. в разделе 1).

В этом случае мы будем говорить для краткости, что $\lambda$ удовлетворяет условию (A) для $V$ или что (A) выполняется для $\lambda$ и $V$.

В дальнейшем, если не оговорено противное, мы будем предполагать, что $\dim W \cap \mathcal{Z}(L_{s+1}, \dots, L_\sigma) = n - \sigma$; последнее пересечение трансверсально; если $n - \sigma > 0$, то алгебраическое многообразие $W \cap \mathcal{Z}(L_{s+1}, \dots, L_\sigma)$ неприводимо над $k$. Обозначим

$W_\lambda = W \cap \mathcal{Z}(L_{s+1}, \dots, L_\sigma)$, $V_\lambda = V \cap \overline{\mathcal{Z}(L_{s+1}, \dots, L_\sigma)}$. Мы будем считать в дальнейшем, что $\dim(W_\lambda \cap (\overline{V_\lambda \setminus W_\lambda})) < \dim W_\lambda$. Заметим, что если для $\lambda$ справедливо условие (A), то все эти свойства выполняются. Обозначим через

$$p_\lambda : W_\lambda \setminus \mathcal{Z}(e_0, \dots, e_r) \to \mathbb{P}^r(\overline{k}), \tag{18}$$

$$p'_\lambda : W_\lambda \setminus \mathcal{Z}(e_0, \dots, e_r) \to W' \tag{19}$$

морфизмы, индуцированные $p$ и $p'$. Предположим, что

$$\dim W_\lambda \cap \mathcal{Z}(e_0, \dots, e_r) < \dim W_\lambda \tag{20}$$

и морфизм $p'_\lambda$ – доминантный. Отметим, что если $n - \sigma > 0$, то $W_\lambda$ неприводимо над $k$ согласно нашему предположению. Следовательно, если $n - \sigma > 0$ и морфизм $p'_\lambda$ доминантный, то выполнено условие (20). Заменим $(V, W, p, p')$ на $(V_\lambda, W_\lambda, p_\lambda, p'_\lambda)$ во всех определениях всех $W_i(L')$, $W(L'_{\sigma+1}, \dots, L_n)$, $\mathcal{U}'_\alpha$, $\mathcal{U}''_\alpha$, $\mathcal{U}'''_\alpha$, $p_{L'}$ и т. д. Мы будем обозначать полученные объекты через $W_{\lambda,i}(L')$, $W_\lambda(L'_{\sigma+1}, \dots, L_n)$, $\mathcal{U}'_{\lambda,\alpha}$, $\mathcal{U}''_{\lambda,\alpha}$, $\mathcal{U}'''_{\lambda,\alpha}$, $p_{\lambda,L'}$ и т. д. Отметим, что $k_{v_\lambda} = k$ и $p_{\lambda,v_\lambda,L'} = p_{\lambda,L'}$, так как $s_\lambda = \sigma_\lambda = \sigma$. Нам будет удобно также рассматривать морфизм $p'_\lambda$ (положим $q_\lambda = p'_\lambda$) вместе с $p'_v$, см. [10, теорема 1]. Определим $V_v$, $W_v$ и т. д., расширяя основное поле $k$ до $k_v$. Заметим, что условие (A) выполняется для $v$ и $V$, если расширить $k$ до $k_{\overline{v}}$.

После этих определений мы переходим к точным формулировкам. Пусть даны однородные многочлены $f_1, \dots, f_m \in k[X_0, \dots, X_n]$, $n \geqslant 0$, $m \geqslant 1$. Рассмотрим замкнутое алгебраическое множество или алгебраическое многообразие (в этой статье мы не различаем эти понятия)

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

Это множество всех общих нулей многочленов $f_1, \dots, f_m$ в $\mathbb{P}^n(\overline{k})$. Следовательно, $V = \mathcal{Z}(f_1, \dots, f_m)$. Пусть $e_0, \dots, e_r \in k[X_0, \dots, X_n]$ – однородные многочлены, такие, что $\deg_{X_0,\dots,X_n} e_j = d'$, если $e_j \neq 0$ для всякого $0 \leqslant j \leqslant r$.

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

(и аналогично $e_j$) будем представлять в форме

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

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

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

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

$$\begin{aligned}
&\deg_{X_0,\dots,X_n}(f_i) < d,\ \deg_{t_\gamma}(f_i) < d_2,\ \mathrm{l}(f_i) < M,\\
&\deg_{X_0,\dots,X_n}(e_j) = d' \text{ или } e_j = 0,\\
&\deg_{t_\gamma}(e_j) < d_2',\ \mathrm{l}(e_j) < M',\\
&\deg_Z(F) < d_1,\ \deg_{t_\gamma}(F) < d_1,\ \mathrm{l}(F) < M_1
\end{aligned}$$

для всех $1 \leqslant i \leqslant m$, $0 \leqslant j \leqslant r$, $1 \leqslant \gamma \leqslant l$. Размер (или длина записи) $\mathrm{L}(f)$ многочлена $f$ определяется как произведение $\mathrm{l}(f)$ и числа всех целых коэффициентов многочлена $f$ в плотном представлении. Имеем

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

Аналогично $\mathrm{L}(F) < d_1^{l+1} M_1$.

**Замечание 3.** В дальнейшем, если не оговорено противное, мы будем считать, что $l$ фиксировано. Время работы алгоритмов из теоремы 1 и теоремы 1 работы [10] является по существу тем же самым, что и при решении систем полиномиальных уравнений с конечным множеством решений в проективном пространстве. Так что эти теоремы могут быть сформулированы также в случае, когда $l$ не является фиксированным, см. [3]. Заметим, что константы $O(\dots)$, (см. [10, теорема 1] и леммы ниже и в работе [10]) в оценках длин записи целых коэффициентов линейных форм $L_j'$, $L_j$ являются абсолютными; они не зависят от $l$.

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

$$k(z) = k((X_1/X_{i_0})(z), \dots , (X_n/X_{i_0})(z)) \simeq k[\eta] = k[Z]/(\Phi), \qquad (21)$$

причём $\sum_{0\leqslant i\leqslant n} c_i(X_i/X_{i_0})(z) \ \mapsto \ \eta$ под действием изоморфизма (21), коэффициенты $c_i \in \mathbb{Z}$ заданы и $\Phi \in k[Z]$ – минимальный многочлен элемента $\eta$ над $k$ со старшим коэффициентом $\mathrm{lc}_Z \Phi = 1$. Таким образом, точка $z$ определена с точностью до сопряжения над $k$. Более точно, представление (21) задаёт определённое над $k$ и неприводимое над $k$ алгебраическое многообразие размерности 0.

Пусть $g \in k[\eta]$ – произвольный элемент. Тогда $g = G(\eta)$ для однозначно определённого многочлена $G \in k[Z]$, такого, что $\deg_Z G < \deg_Z \Phi$. Длина записи целых коэффициентов $\mathrm{l}(g)$, длины записи $\mathrm{L}(g)$ и степени $\deg_{t_\alpha} g$, $1 \leqslant \alpha \leqslant l$, элемента $g$ определены формулами

$$\mathrm{l}(g) = \mathrm{l}(G), \quad \mathrm{L}(g) = \mathrm{L}(G), \quad \deg_{t_\alpha} g = \deg_{t_\alpha} G.$$

Определим длину записи $\mathrm{L}(z)$ точки $z$ равной $\mathrm{L}(\Phi) + \sum\limits_{0\leqslant i\leqslant n} \mathrm{L}(X_i/X_{i_0})$.

Пусть $W_1, W_2 \subset \mathbb{P}^n(\overline{k})$ – два квазипроективных алгебраических многообразия, определённых над $k$. Пусть $W_3$ – произвольная определённая над $k$ и неприводимая над $k$ компонента пересечения $W_1 \cap W_2$. Мы будем говорить, что пересечение $W_1 \cap W_2$ трансверсально в $W_3$ тогда и только тогда, когда существует точка $x \in W_3$, такая, что $x$ – гладкая точка каждого $W_i$, $i = 1, 2$, и пересечение касательных пространств $T_{x,W_1} \cap T_{x,W_2}$ многообразий $W_1$ и $W_2$ в точке $x$ трансверсально, то есть $\dim(T_{x,W_1} \cap T_{x,W_2}) = n - \dim(T_{x,W_1}) - \dim(T_{x,W_2})$. Мы будем говорить, что пересечение $W_1 \cap W_2$ трансверсально тогда и только тогда, когда оно трансверсально в каждой своей определённой над $k$ и неприводимой над $k$ компоненте. Аналогичным образом определяется трансверсальность для пересечения конечного числа алгебраических многообразий.

Согласно лемме 17 из [10], если пересечение $W_1 \cap W_2$ трансверсально и $y$ – произвольная гладкая точка многообразия $W_1 \cap W_2$, то $y$ является гладкой точкой каждого $W_i$, $i = 1, 2$, и пересечение касательных пространств $T_{y,W_1} \cap T_{y,W_2}$ многообразий $W_1$ и $W_2$ в точке $y$ трансверсально.

**Теорема 1.** *Пусть поле $k$, алгебраические многообразия $V$, $W$, $W'$, многочлены $F$, $f_1, \dots, f_m$, $e_0, \dots, e_r$ и точка $x^{(0)} \in W$ заданы как выше. Можно вычислить размерности $\dim W = n - s$, $\dim W' = n - \sigma$ (следовательно, $n \geqslant \sigma \geqslant s \geqslant 0$). Пусть дано $L' = (L'_0, L'_{\sigma+1}, \dots, L'_n) \in \mathcal{U}'_0$. Предположим, что все линейные формы $L'_j$, $j \in \{0, \sigma+1, \dots, n\}$, имеют коэффициенты из конечнопорождённого расширения $k'$ поля $k$, которое задано минимальным многочленом примитивного элемента поля $k'$ над чисто трансцендентным расширением поля $k$ фиксированной степени трансцендентности. В формулировке теоремы мы предполагаем, что все точки $y', y'', x$ (см. ниже) заданы аналогично (21), но с полем $k'$ вместо $k$. Положим $L'_{n+1} = L'_0$, $e'_j = L'_j(e_0, \dots, e_r)$ для всех $j$. Положим $\widetilde{V}_i = (V \cup \mathcal{Z}(e'_{i+1})) \cap \mathcal{Z}(e'_{\sigma+1}, \dots, e'_i)$ и $\iota = i - \sigma + s$ для всех $\sigma \leqslant i \leqslant n$. Тогда можно построить элемент $\overline{\lambda} = (L_0, L_1, \dots, L_{n+1})$, где $L_0, L_1, \dots, L_{n+1}$ – линейные формы от $X_0, \dots, X_n$ с целыми коэффициентами с длиной записи $O(n \log d + (n-\sigma) \log d')$, такие, что справедливы следующие утверждения* (a) *и* (b).

(a) *Для всякого $\sigma \leqslant i \leqslant n$ пересечение алгебраических многообразий $\widetilde{V}_i$ и $\mathcal{Z}(L_{\iota+1}, \dots, L_n)$ трансверсально, $W_i(L') \cap \mathcal{Z}(L_0, L_{\iota+1}, \dots, L_n) = \emptyset$, и $\#(L_{n+1}/L_0)(W_i(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)) = D_i(L')$ в $\mathbb{P}^n(\overline{k})$. Далее, для всякого $\sigma \leqslant i \leqslant n$ утверждение теоремы 2 (см. раздел 1) выполняется для $\widetilde{V}_i$ вместо $V$. В частности, можно вычислить все точки из $W_i(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$ для всякого $\sigma \leqslant i \leqslant n$.*

(b) *Для всякого $\sigma + 1 \leqslant i \leqslant n + 1$ пересечение алгебраических многообразий $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ и $\mathcal{Z}(L_{\iota+1}, \dots, L_n)$ трансверсально, $W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_0, L_{\iota+1}, \dots, L_n) = \emptyset$, и $\#(L_{n+1}/L_0)(W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)) = D_i(L') + D_i^{(1)}(L') + D_i^{(2)}(L') + D_i^{(3)}(L')$ в $\mathbb{P}^n(\overline{k})$. Для всякого $\sigma + 1 \leqslant i \leqslant n + 1$ утверждение теоремы 2 (см. раздел 1) выполняется для $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ вместо $V$ (заметим, что здесь $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ не задано явно системой полиномиальных уравнений). В частности, можно построить конечное множество $W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$, и для всякой неприводимой над $\overline{k}$ компоненты $E$ многообразия $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ пересечение $E \cap \mathcal{Z}(L_{\iota+1}, \dots, L_{n-1})$ неприводимо над $\overline{k}$. Далее, для любых двух точек $y', y'' \in W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$ можно выяснить, верно ли, что $y'$ и $y''$ принадлежат одной и той же определённой над $k'$ и не-*

*приводимой над $k'$ (соответственно определённой над $\overline{k}$ и неприводимой над $\overline{k}$) компоненте многообразия $W_{i-1}(L')\cap\mathcal{Z}(e'_i)$ (в случае неприводимых над $\overline{k}$ компонент мы предполагаем, что явно задан композит $k'(y',y'')$ полей $k'(y')$ и $k'(y'')$ над $k'$ аналогично теореме 2 из* [8] *и выполняется оценка на длину записи композита, которая полиномиальна от длины записи входных данных, ср.* [8]*). Наконец, для всякой точки $y'\in W_{i-1}(L')\cap\mathcal{Z}(e'_i)\cap\mathcal{Z}(L_{\iota+1},\dots,L_n)$ можно вычислить число точек $y''\in W_{i-1}(L')\cap\mathcal{Z}(e'_i)\cap\mathcal{Z}(L_{\iota+1},\dots,L_n)$, таких, что $y'$ и $y''$ принадлежат одной и той же определённой над $k'$ и неприводимой над $k'$ (соответственно определённой над $\overline{k}$ и неприводимой над $\overline{k}$) компоненте многообразия $W_{i-1}(L')\cap\mathcal{Z}(e'_i)$.*

*Пусть $\overline{\lambda}$ – произвольный элемент, удовлетворяющий условиям* (a) *и* (b) *(не обязательно построенный алгоритмом), и $\sigma+1\leqslant i\leqslant n+1$ – целое число. Тогда справедливы следующие утверждения.*

(c) *Пусть дана точка $y'\in W_{i-1}(L')\cap\mathcal{Z}(e'_i)\cap\mathcal{Z}(L_{\iota+1},\dots,L_n)$. Обозначим через $E$ единственную определённую над $k'$ и неприводимую над $k'$ (соответственно определённую над $\overline{k}$ и неприводимую над $\overline{k}$) компоненту многообразия $W_{i-1}(L')\cap\mathcal{Z}(e'_i)$, такую, что $y'\in W_{i-1}(L')\cap\mathcal{Z}(e'_i)$. Тогда для произвольной точки $x\in\mathbb{P}^n(\overline{k})$ можно выяснить, верно ли, что $x\in E$, и, более общим образом, можно вычислить кратность $\mu(x,E)$ точки $x$ на $E$ (снова, если $E$ неприводимо над $\overline{k}$, мы предполагаем, что явно задан композит $k'(x,y')$ полей $k'(x)$ и $k'(y')$ над $k'$, как в* (b)*).*

(d) *Для заданной точки $y'\in W_{i-1}(L')\cap\mathcal{Z}(e'_i)\cap\mathcal{Z}(L_{\iota+1},\dots,L_n)$ можно выяснить, верно ли, что $y'$ является элементом $W_i(L')$ (соответственно $W_i^{(1)}(L')$, $W_i^{(2)}(L')$, $W_i^{(3)}(L')$). Следовательно, согласно (b) и (c), можно вычислить степени $\deg W_i(L')$, $\deg W_i^{(1)}(L')$, $\deg W_i^{(2)}(L')$, $\deg W_i^{(3)}(L')$. Кроме того, для всякой неприводимой над $\overline{k}$ компоненты $E$ многообразия $W_{i-1}(L')\cap\mathcal{Z}(e'_i)$ условие $E\subset\mathcal{Z}(e_0,\dots,e_r)$ выполняется в том и только в том случае, если $E\cap\mathcal{Z}(L_{\iota+1},\dots,L_n)\subset\mathcal{Z}(e_0,\dots,e_r)$.*

(e) *Согласно утверждениям* (b), (c), (d)*, для произвольной точки $x\in\mathbb{P}^n(\overline{k})$ можно вычислить кратности $\mu(x,W_i(L'))$ (соответственно $\mu(x,W_i^{(1)}(L'))$, $\mu(x,W_i^{(2)}(L'))$, $\mu(x,W_i^{(3)}(L'))$) точки $x$ на $W_i(L')$ (соответственно $W_i^{(1)}(L')$, $W_i^{(2)}(L')$, $W_i^{(3)}(L')$).*

(f) *В условиях пункта* (c) *предположим, что* $E$ *является определённой над* $\overline{k'}$ *и неприводимой над* $\overline{k'}$ *компонентой. Тогда можно вычислить индекс пересечения* $i(W_{i-1}(L'), \mathcal{Z}(e'_i); E)$ *алгебраических многообразий* $W_{i-1}(L')$ *и* $\mathcal{Z}(e'_i)$ *в компоненте* $E$ *в проективном пространстве* $\mathbb{P}^n(\overline{k})$.

(g) *Отождествим множество всех наборов, каждый из которых состоит из* $(n+2)$ *линейных форм, принадлежащих* $\overline{k}[X_0, \dots, X_n]$, *с аффинным пространством* $\mathbb{A}^{(n+1)(n+2)}(\overline{k})$. *Пусть* $\mathfrak{l} \in \mathbb{A}^{(n+1)(n+2)}(\overline{k})$ *– прямая, определённая над* $k'$, *такая, что* $\overline{\lambda} \in \mathfrak{l}$. *Тогда для всех* $\lambda^* \in \mathfrak{l}(k')$ *(здесь* $\mathfrak{l}(k')$ *– множество* $k'$*-точек прямой* $\mathfrak{l}$*; мы предполагаем, что* $\lambda^* = (L_0^*, \dots, L_{n+1}^*)$, *где все* $L_j^* \in \overline{k}[X_0, \dots, X_n]$ *– линейные формы), за исключением не более чем полиномиального от* $d^n(d')^{n-\sigma}$ *числа, справедливы утверждения* (a) *и* (b) *с* $\lambda^*$ *вместо* $\overline{\lambda}$. *Для всякого элемента* $\lambda^* \in \mathfrak{l}(k')$ *можно выяснить, верно ли, что справедливы утверждения* (a) *и* (b) *с* $\lambda^*$ *вместо* $\overline{\lambda}$.

*Время работы алгоритма для вычисления* $s$, $\sigma$ *и построения* $\overline{\lambda}$ *(соответственно алгоритма из* (a), (b), (d), (f)) *полиномиально от* $d^n$, $(d')^n$, $d_1$, $d_2$, $d'_2$, $M$, $M'$, $M_1$, $m$, $r$, *длины записи* $\mathrm{L}(x^{(0)})$ *точки* $x^{(0)}$, *и длины записи* $\mathrm{L}(L')$ *элемента* $L'$ *(включая длину записи примитивного элемента минимального элемента поля* $k'$, *см. выше). Время работы алгоритмов из* (c) *и* (e) *(соответственно* (g)) *полиномиально от тех же самых величин и длины записи* $\mathrm{L}(x)$ *точки* $x$ *(соответственно длины записи* $\mathrm{L}(\lambda^*)$ *элемента* $\lambda^*$*).*

Заметим здесь, что трудность в доказательстве утверждения (b) теоремы 1 в сравнении с её утверждением (a) (и теоремой 2) состоит в том, что некоторые компоненты $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ могут содержаться в $\overline{V \setminus W}$.

**Замечание 4.** В дальнейшем во многих случаях, когда мы говорим, что $a_1, \dots, a_\mu$ (здесь может быть любое другое семейство переменных или коэффициентов некоторых многочленов, может быть только одна переменная) являются бесконечно малыми величинами, удобно понимать под этим, допуская вольность речи, что каждое $a_1, \dots, a_\mu$ является бесконечно малой величиной или нулём. Обычно мы оговариваем явно, что $a_1, \dots, a_\mu$ могут быть равны нулю. Но даже если где-нибудь мы забыли оговорить равенство нулю явно, читатель легко увидит это из контекста. Это не приведёт к двусмысленности. Например, допуская вольность речи, удобнее сказать, что все коэффициенты линейной формы $\widetilde{L}_0$ являются бесконечно малыми величинами, но всё же мы говорим в этом случае, что все ненулевые коэффициенты линейной формы $\widetilde{L}_0$ являются бесконечно малыми величинами.

## 1. Построение линейных сечений в общем положении алгебраического многообразия

Напомним некоторые обозначения из [8]. Пусть $V \subset \mathbb{P}^n(\overline{k})$ – произвольное проективное алгебраическое многообразие (не обязательно то же самое, что во введении). Для всякого $0 \leqslant j \leqslant n$ обозначим через $V_j$ объединение всех неприводимых компонент многообразия $V$ размерности $j$. Пусть $L_0, L_1, \dots, L_{n+1} \in k[X_0, \dots, X_n]$ – линейные формы, $L_w = \sum_{0 \leqslant i \leqslant n} l_{w,i} X_i$, где $l_{w,i} \in k$, $0 \leqslant w \leqslant n+1$, $0 \leqslant i \leqslant n$. Положим $\overline{\lambda} = (L_0, L_1, \dots, L_{n+1})$. Обозначим через $\widetilde{\lambda}$ семейство коэффициентов $l_{w,i}$, $0 \leqslant w \leqslant n+1$, $0 \leqslant i \leqslant n$. Рассмотрим следующее условие.

(B) Для всякого $0 \leqslant j \leqslant n$ множество $A_j = V_j \cap \mathcal{Z}(L_{j+1}, \dots, L_n)$ является конечным (или пустым, если $V_j = \emptyset$) в $\mathbb{P}^n(\overline{k})$, состоит из гладких точек многообразия $V$, и пересечение касательных пространств многообразий $V_j$ и $\mathcal{Z}(L_{j+1}, \dots, L_n)$ во всех этих точках трансверсально. Линейная форма $L_0$ не обращается в нуль тождественно ни в какой точке из $A_j$ (т.е. $A_j \cap \mathcal{Z}(L_0) = \emptyset$), и $\#(L_{n+1}/L_0)(A_j) = \#A_j = \deg V_j$.

Если $V$ – из введения, то, применяя алгоритмы из [4] и [3], для заданных линейных форм $L_0, \dots, L_n$ (или, что то же самое, для заданного $\overline{\lambda}$) можно выяснить, верно ли, что выполняется условие (B), за полиномиальное время от $d^n$, $d_1$, $d_2$, $M$, $M_1$, $m$ и суммы длин записей $\sum_{0 \leqslant j \leqslant n+1} \mathrm{L}(L_j)$ линейных форм $L_j$.

В дальнейшем мы будем рассматривать также свойство (B) линейных форм с коэффициентами из расширения поля $k$, заменяя $k$ на его расширение. В частности, целые числа $a_j(\overline{\lambda})$, $b_j(\overline{\lambda})$ (см. ниже) определены также, если коэффициенты линейных форм $L'_j$ принадлежат расширению поля $k$ и свойство (B) выполняется над алгебраическим замыканием этого расширения.

Предположим, что $\overline{\lambda}$ удовлетворяет условию (B). Пусть $Z_0, \dots, Z_{n+1}$ – независимые переменные. Для всякого $0 \leqslant j \leqslant n$

обозначим через $\Phi_j \in k[Z_0, Z_{j+1}, Z_{j+2}, \dots, Z_{n+1}] = B_j$ ненулевой сепарабельный многочлен минимальной степени, такой, что $\Phi_j(L_0, L_{j+1}, L_{j+2}, \dots, L_{n+1})$ обращается в нуль тождественно на $V_j$. Тогда $\deg_{Z_{n+1}} \Phi_j = \deg \Phi_j = \deg V_j$. Если не оговорено противное, мы выбираем и фиксируем $\Phi_j$ так, что старший коэффициент $\Phi_j$ относительно $Z_{n+1}$ равен 1. Обозначим через $R_j \in k[Z_0, Z_{j+1}, Z_{j+2}, \dots, Z_n]$ дискриминант $\Phi_j$ относительно $Z_{n+1}$ и через $R_{j,0}$ бесквадратную часть $R_j$ (т.е. $R_{j,0}$ – сепарабельный многочлен наибольшей степени, делящий $R_j$). Положим $\Phi_{j,*} = \Phi_j(Z_0, 0, \dots, 0, Z_n, Z_{n+1}) \in k[Z_0, Z_n, Z_{n+1}]$, $R_{j,*} = R_j(Z_0, 0, \dots, 0, Z_n) \in k[Z_0, Z_n]$, $R_{j,0,*} = R_{j,0}(Z_0, 0, \dots, 0, Z_n) \in k[Z_0, Z_n]$. Если $V_j = \emptyset$, то $\Phi_j = R_j = 1$. Если $j = n$, то $\Phi_j$, $R_j$, $\Phi_{j,*}$, $R_{j,*}$ не зависят от $Z_n$. Обозначим через $R_{j,*,0}$ бесквадратную часть $R_{j,*}$. Если зависимость от $\overline{\lambda}$ является существенной,то мы будем обозначать введённые объекты через $\Phi_{\overline{\lambda},j}$, $R_{\overline{\lambda},j}$, $R_{\overline{\lambda},j,0}$, $\Phi_{\overline{\lambda},j,*}$, $R_{\overline{\lambda},j,*}$, $R_{\overline{\lambda},j,0,*}$ и $R_{\overline{\lambda},j,*,0}$. В частности, расширяя поле $k$ до $k_{\overline{v}}$ (см. введение), мы получаем $\Phi_{\overline{v},j}$, $R_{\overline{v},j}$, $R_{\overline{v},j,0}$, $\Phi_{\overline{v},j,*}$, $R_{\overline{v},j,*}$, $R_{\overline{v},j,0,*}$ и $R_{\overline{v},j,*,0}$. Кроме того, мы выбираем последние элементы сепарабельными многочленами из кольца $k[\widetilde{v}, Z_0, \dots, Z_{n+1}]$.

**Лемма 1.** *При предыдущих обозначениях для всякого* $0 \leqslant j \leqslant n$ *многочлен* $\Phi_{\overline{v},j}(\widetilde{\lambda}, Z_0, Z_{j+1}, Z_{j+2}, \dots, Z_{n+1})$ *– ненулевой и совпадает с* $\Phi_{\lambda,j}$ *с точностью до ненулевого множителя из* $k$.

**Доказательство.** Пусть $\nu \in k$. Тогда $v_0, v_{s+1}, \dots, v_n, v_{n+1} + \nu v_0$ – общие линейные формы относительно $X_0, \dots, X_n$ над $k$. Более общим образом, всякий линейный автоморфизм $\gamma$ кольца $k[v_0, v_{j+1}, \dots, v_{n+1}]$ над $k$ индуцирует однозначно определённый линейный автоморфизм $\gamma' : k[\widetilde{v}] \to k[\widetilde{v}]$, такой, что (обозначим через $\gamma'(\widetilde{v})$ семейство элементов, полученных под действием $\gamma'$ на элементы из $\widetilde{v}$) $\Phi_{\overline{v},j}(\gamma'(\widetilde{v}), \gamma(v_0), \gamma(v_{j+1}), \dots, \gamma(v_{n+1})) = \Phi_{\overline{v},j}$.

Следовательно, достаточно доказать лемму для $L_0, L_{j+1}, \dots, L_n, L_{n+1} + \nu L_0$ вместо $L_0, L_{j+1}, \dots, L_n, L_{n+1}$. Выберем $\nu \in k$ так, что $V_j \cap \mathcal{Z}(L_{j+1}, \dots, L_n, L_{n+1} + \nu L_0) = \emptyset$. Тогда выполняются условия леммы 13 из работы [6] для $j$, $V_j$ и линейных форм $L_0, L_{j+1}, \dots, L_n, L_{n+1} + \nu L_0$ вместо $s$, $\mathcal{Z}(\mathfrak{P})$ и $L_0, L_s, \dots, L_n$. Требуемое утверждение немедленно следует из леммы 13 работы [6], поскольку $\deg \Phi_{\overline{\lambda},j} = \deg \Phi_{\overline{v},j}$. □

**Замечание 5.** Аналогичным образом можно усилить лемму 13 из [6], заменяя там условия (63), (64) на одно условие $\mathcal{Z}(\mathfrak{P}) \cap$

$\mathcal{Z}(L_0, L_s, \dots, L_n) = \emptyset$.

Теперь положим $b_j(\overline{\lambda}) = b_j(\overline{\lambda}, V) = \deg_{Z_0, Z_{j+1}, \dots, Z_n} R_{j,0}$; $a_j(\overline{\lambda}) = a_j(\overline{\lambda}, V) = \deg_{Z_0, Z_n} R_{j,*,0}$. Если условие (B) справедливо для $\overline{\lambda}$ и $V$ является многообразием из введения, то (см. [8]), используя [3], можно построить все $\Phi_{j,*}$, $R_{j,*}$, $0 \leqslant j \leqslant n$, за полиномиальное время от $d^n$ и длины записи входных данных. После этого можно вычислить $R_{j,*,0}$ и $a_j(\overline{\lambda}, V)$ за то же самое время. Пусть $\lambda^* = (L_0^*, \dots, L_{n+1}^*)$, где все $L_j^*$ – линейные формы с коэффициентами из расширения $k^*$ поля $k$. Если условие (B) выполняется для $\lambda^*$, то, расширяя основное поле, можно аналогичным образом вычислить $a_j(\lambda^*, V)$.

Заметим, что $b_j(\overline{\lambda}) = \deg_{Z_0, Z_n} R_{j,0,*}$. Мы имеем $a_j(\overline{\lambda}) \leqslant b_j(\overline{\lambda}) \leqslant \deg V_j(-1 + \deg V_j)$ для всех $j$, см. [8]. Очевидно, $a_{n-1}(L') = b_{n-1}$. Далее (см. [8, теоремы 1 и 3]), если $a_j(\overline{\lambda}) = b_j(\overline{\lambda})$ (или, что то же самое, $\deg_{Z_0, Z_n} R_{j,*,0} = \deg_{Z_0, Z_n} R_{j,0,*}$) для всех $1 \leqslant j \leqslant n-2$, то выполняются утверждения (a), (b), (c) теоремы 1 из [8]. Для заданного $\overline{\lambda}$, удовлетворяющего утверждениям (a), (b), (c) теоремы 1 из [8], можно построить, согласно [8], все объекты из утверждений (d) и (e) этой теоремы и доказать (d) и (e) (при условии, что все $L_w$ имеют целые коэффициенты с длиной записи $O(n \log d)$).

Положим $b_j = b_j(\overline{v}) = b_j(V) = b_j(\overline{v}, V) = \deg_{Z_0, Z_{j+1}, \dots, Z_n} R_{\overline{v}, j, 0}$; $a_j = a_j(\overline{v}) = a_j(V) = a_j(\overline{v}, V) = \deg_{Z_0, Z_n} R_{\overline{v}, j, *, 0}$. Тогда $b_j = a_j$ (см. [8]) для всех $0 \leqslant j \leqslant n-1$. Мы будем отождествлять множество всех $(n+2)$-наборов линейных форм из $k[X_0, \dots, X_n]$ с $\mathbb{A}^{(n+2)(n+1)}(\overline{k})$. Следующая лемма получается непосредственно, ср. [4].

**Лемма 2.** *Существует определённое над $k$ открытое в топологии Зариского подмножество $\mathcal{V}' \subset \mathbb{A}^{(n+2)(n+1)}(\overline{k})$, такое, что для всякого $\overline{\lambda} \in \mathcal{V}'$ выполняется свойство* (B) *и $b_j(\overline{\lambda}) = a_j(\overline{\lambda}) = b_j$ для всех $0 \leqslant j \leqslant n$.*

**Лемма 3.** *Пусть $K$ – произвольное расширение поля $k$. Предположим, что $L_w \in \overline{K}[X_0, \dots, X_n]$, $0 \leqslant w \leqslant n+1$. Пусть $\overline{\lambda}$ удовлетворяет свойству* (B) *(над $\overline{K}$). Пусть $\mathfrak{l} \subset \mathbb{A}^{(n+2)(n+1)}(\overline{K})$ – прямая, содержащая $\overline{\lambda}$. Тогда для всех $\lambda^* \in \mathfrak{l}$, за исключением не более чем полиномиального от $2^n \sum_{0 \leqslant j \leqslant n} \deg V_j$ числа, элемент $\lambda^*$ удовлетворяет свойству* (B) *и справедливы неравенства $b_j(\overline{\lambda}) \leqslant b_j(\lambda^*)$,*

$a_j(\overline{\lambda}) \leqslant a_j(\lambda^*)$ *для всех* $0 \leqslant j \leqslant n$.

**Доказательство.** Доказательство получается непосредственно согласно теореме Безу, ср. [4]. $\square$

**Теорема 2.** *Пусть $V$ – многообразие из введения. В условиях теоремы 1 из [8] можно построить все объекты из формулировки этой теоремы так, что дополнительно выполнены условия $b_j = b_j(\overline{\lambda}) = a_j(\overline{\lambda})$ для всех $0 \leqslant j \leqslant n$ (и, следовательно, все $L_w$, $0 \leqslant w \leqslant n+1$, являются линейными формами с целыми коэффициентами с длиной записи $O(n \log d)$ и вычисляются целые числа $b_j = b_j(\overline{\lambda}) = a_j(\overline{\lambda}) = a_j$).*

**Доказательство.** Мы будем считать без ограничения общности, что $\dim V < n$ и, следовательно, достаточно доказать утверждения теоремы для всех $1 \leqslant j \leqslant n-1$. Согласно предыдущим замечаниям, достаточно построить $\overline{\lambda}$, такое, что все $L_w$, $0 \leqslant w \leqslant n+1$, – линейные формы с целыми коэффициентами с длиной записи $O(n \log d)$ и $b_j = b_j(\overline{\lambda})$. Конструкция требуемого $\overline{\lambda}$ рекурсивна. Возьмём в качестве базы рекурсии произвольный элемент $\overline{\lambda}$, удовлетворяющий свойству (B), т.е. всем требуемым условиям, но не обязательно условию $b_j = b_j(\overline{\lambda})$ (например, можно взять в качестве $\overline{\lambda}$ элемент, построенный в теореме 1 из [8]).

Опишем общий шаг рекурсии. Пусть $1 \leqslant j \leqslant n-2$ – максимальное число, такое, что для всех $1 \leqslant w < j$ целые числа $b_w$ вычислены, $b_w = a_w(\overline{\lambda})$ и $V_j \neq \emptyset$ (последнее условие мы проверяем при помощи алгоритма из [4]). Вычислим, используя алгоритмы из [4] и [3], многочлены $\Phi_{\overline{\lambda},j,*}$, $R_{\overline{\lambda},j,*}$ и $R_{\overline{\lambda},j,*,0}$. Мы будем предполагать без ограничения общности, что $Z_0$ не делит $R_{\overline{\lambda},j,*,0}$, заменяя при необходимости $Z_0$ на $Z_0 - \mu Z_n$ для подходящего целого числа $\mu$, ограниченного сверху числом $d^{2n}$.

Пусть $1 \leqslant \tau \leqslant 4$ является целым числом. Пусть $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$ – целые числа. Предположим, что поле $k$ снабжено вещественной структурой (см. [12]). Пусть $k_j = k(\varepsilon_1, \ldots, \varepsilon_j)$, $0 \leqslant j \in \mathbb{Z}$, где $\varepsilon_j > 0$ для $j \geqslant 1$ является бесконечно малой величиной относительно поля $k_{j-1}$. Пусть $X_{w,i}$, $1 \leqslant w \leqslant 4$, $0 \leqslant i \leqslant n$; $Z_{w,i}$, $i \in \{0, j+1, \ldots, n+1\} = I_j$, $1 \leqslant w \leqslant \tau$, – переменные. Обозначим для краткости $L'_i = L_i + \sum_{1 \leqslant w \leqslant \tau} Z_{w,i} X_{j_w}$, $i \in I_j$ (так что все $L'_i$ зависят от выбора $j_1, \ldots, j_\tau$). Обозначим $X^{(i)} = (X_{i,0}, \ldots, X_{i,n})$ и для произвольного многочлена $c$ от $n+1$ переменных положим $c(X^{(i)}) = c(X_{i,0}, \ldots, X_{i,n})$, $1 \leqslant i \leqslant 4$. Предположим, что $j \leqslant n-2$.

Рассмотрим следующую систему полиномиальных уравнений и неравенств с квадратами абсолютных величин с коэффициентами из $k_3$ относительно переменных $X_{w,i}$, $1 \leqslant w \leqslant 4$, $0 \leqslant i \leqslant n$, и $Z_{w,i}$, $i \in \{0, j+1, \dots, n+1\} = I_j$, $1 \leqslant w \leqslant \tau$:

$$\begin{cases} \sum_{i \in I_j} \sum_{1 \leqslant w \leqslant \tau} |Z_{i,w}|^2 \leqslant \varepsilon_1, & \\ \varepsilon_2 \leqslant |L'_n(X^{(1)}) - L'_n(X^{(3)})|^2 \leqslant \varepsilon_1, & \\ |L'_{n+1}(X^{(i)}) - L'_{n+1}(X^{(i+1)})|^2 = \varepsilon_3, & i = 1, 3, \\ L'_\nu(X^{(i_1)}) = L'_\nu(X^{(i_2)}) = 0, & 1 \leqslant i_1 < i_2 \leqslant 4, j+1 \leqslant \nu \leqslant n-1, \\ L'_n(X^{(i)}) - L'_n(X^{(i+1)}) = 0, & i = 1, 3, \\ L'_0(X^{(i)}) - 1 = 0, & 1 \leqslant i \leqslant 4. \end{cases} \tag{22}$$

**Лемма 4.** *Пусть $1 \leqslant j \leqslant n-2$ – целое число. Неравенство $a_j(\overline{\lambda}) < b_j$ выполняется в том и только в том случае, если существуют $1 \leqslant \tau \leqslant 4$ и $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$, удовлетворяющие следующему свойству. Система* (22) *имеет решение $X_{w,i} = x^*_{w,i} \in \overline{k_3}$, $1 \leqslant w \leqslant 4$, $0 \leqslant i \leqslant n$; $Z_{w,i} = z^*_{w,i} \in \overline{k_3}$, $i \in \{0, j+1, \dots, n+1\}$, $1 \leqslant w \leqslant \tau$, такое, что*

$$(x^*_{w,0} : \ldots : x^*_{w,n}) \in V_j(\overline{k_3}), \quad 1 \leqslant w \leqslant 4. \tag{23}$$

**Доказательство.** Существует $\varepsilon' > 0$, такое, что $\varepsilon'$ – бесконечно малая величина относительно поля $k_1$ и $\varepsilon_2$ – бесконечно малая величина относительно поля $k_1(\varepsilon')$.

Предположим, что $a_j(\overline{\lambda}) < b_j$. Согласно лемме 2, существуют линейные формы $L''_w \in \overline{k(\varepsilon')}[X_0, \ldots, X_n]$, $0 \leqslant w \leqslant n+1$, такие, что все ненулевые коэффициенты $L''_w - L_w$, $0 \leqslant w \leqslant n+1$, – бесконечно малые величины относительно поля $k$ и $a_j(\lambda') = b_j$, где $\lambda' = (L''_0, \ldots, L''_{n+1})$. Заменим в системе (22) все $L'_i$ на $L''_i$ и удалим первое неравенство. Обозначим полученную систему через (**).

Согласно лемме 1, все ненулевые коэффициенты многочлена $R_{\lambda',j,0,*}$ являются бесконечно близкими к соответствующим коэффициентам $R_{\overline{\lambda},j,0,*}$, и $R_{\lambda',j,0,*}(1, Z_n)$ имеет больше различных корней, чем $R_{\overline{\lambda},j,0,*}(1, Z_n)$. Следовательно, по принципу переноса (см. [11]) существуют корни $Z_n = z_{\alpha,n} \in k(\varepsilon')$, $\alpha = 1, 3$, многочлена $R_{\lambda',j,0,*}(1, Z_n)$, такие, что $z_{1,n} - z_{3,n}$ является бесконечно малой величиной из $\overline{k(\varepsilon')}$. Напомним, что $\mathrm{lc}_{Z_{n+1}} \Phi_{\lambda',j} = 1$. Следовательно, для $\alpha = 1,3$ по принципу переноса, применённому к многочлену $\Phi_{\lambda',j,*}(1, z_{\alpha,n}, Z)$, существуют $\widetilde{z}_{\alpha,n} \in \overline{k(\varepsilon')}$, $\widetilde{z}_{\beta,n+1} \in \overline{k(\varepsilon',\varepsilon_3)}$, $\beta = \alpha, \alpha+1$, такие, что $\widetilde{z}_{\alpha,n} - z_{\alpha,n} \in \overline{k(\varepsilon',\varepsilon_3)}$ – бесконечно малая величина относительно поля $k_2(\varepsilon')$, $|\widetilde{z}_{\alpha,n+1} - \widetilde{z}_{\alpha+1,n+1}|^2 = \varepsilon_3$ и $\Phi_{\lambda',j,*}(1, \widetilde{z}_{\alpha,n}, \widetilde{z}_{\beta,n+1}) = 0$ для $\beta = \alpha, \alpha+1$. Положим $\widetilde{z}_{\beta,n} = \widetilde{z}_{\alpha,n}$ для $\alpha = 1,3$, $\beta = \alpha, \alpha+1$. Морфизм $V_j \to \mathcal{Z}(\Phi_{\lambda',j})$, $(X_0 : \ldots : X_n) \mapsto (L''_0 : L''_{j+1} : \ldots : L''_n)$, – конечный доминантный. Следовательно, существует решение системы $(**)$, задающее точку из $V_j(\overline{k(\varepsilon',\varepsilon_3)})^4$ и удовлетворяющее дополнительным уравнениям $L''_\nu(X^{(\beta)}) = 0$, $j+1 \leqslant \nu \leqslant n-1$, $L''_j(X^{(\beta)}) = \widetilde{z}_{\beta,j}$, $j = n, n+1$, $\beta = 1,2,3,4$. Пусть это решение будет $X_{w,i} = \widetilde{x}_{w,i}$, $1 \leqslant w \leqslant 4$, $0 \leqslant i \leqslant n$.

Теперь мы хотим заменить все $L''_i$ на $L_i + \sum_{1\leqslant w\leqslant\tau} \widetilde{z}_{w,i} X_{j_w}$, $i \in \{0, j+1, \ldots, n\}$, для подходящих $1 \leqslant \tau \leqslant 4$, $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$ и $\widetilde{z}_{w,i} \in \overline{k(\varepsilon',\varepsilon_3)}$, которые являются бесконечно малыми величинами относительно поля $k$ (если они отличны от нуля). Пусть $\tau \geqslant 1$ равно рангу матрицы $(\widetilde{x}_{w,i})$. Выберем $(\tau\times\tau)$-минор $\Delta_0 \neq 0$ рассматриваемой матрицы, такой, что для любого другого $(\tau\times\tau)$-минора $\Delta_1$ этой матрицы $\Delta_1/\Delta_0$ не является бесконечно большим относительно поля $k$. Пусть $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$ – номера столбцов минора $\Delta_0$. Тогда по правилу Крамера можно записать

$$\widetilde{x}_{w,q} = \sum_{1\leqslant\nu\leqslant\tau} \mu_{w,q,\nu} \widetilde{x}_{w,j_\nu}, \tag{24}$$

$1 \leqslant w \leqslant 4$, где каждое $\mu_{w,q,\nu} \in \overline{k(\varepsilon',\varepsilon_3)}$ не является бесконечно большим относительно поля $k$. Согласно (24), можно найти $\widetilde{z}_{w,i}$ для всех $1 \leqslant w \leqslant \tau$, $i \in I_j$, такие, что $X_{w,i} = \widetilde{x}_{w,i}$, $1 \leqslant w \leqslant 4$, $0 \leqslant i \leqslant n$, и $Z_{w,i} = \widetilde{z}_{w,i}$, $1 \leqslant w \leqslant \tau$, $i \in I_j$, – решение системы (22), задающее точку из $V_j^4(\overline{k(\varepsilon',\varepsilon_3)})$. Таким образом, мы построили требуемое решение для некоторых $1 \leqslant \tau \leqslant 4$ и $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$, но над полем $\overline{k(\varepsilon',\varepsilon_3)}$. Теперь по принципу переноса (см. [11]) или непосредственно получаем, что существует также требуемое решение над полем $\overline{k_3}$ для рассматриваемых $1 \leqslant \tau \leqslant 4$ и $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$.

Обратно, предположим, что система (22) имеет решение для некоторых $1 \leqslant \tau \leqslant 4$ и $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$. Тогда, как это следует из описания алгоритма ниже, $a_j(\overline{\lambda}) < b_j$. □

Вернёмся к описанию алгоритма для теоремы 2. Будем перебирать целые числа $\tau$ и $j_1, \ldots, j_\tau$, такие, что $1 \leqslant \tau \leqslant 4$ и

$0 \leqslant j_1 < \ldots < j_\tau \leqslant n$. Применяя теорему 2 из [9] к алгебраическому многообразию $\mathrm{con}(V) \subset \mathbb{A}^{n+1}(\overline{k})$ (которое является множеством нулей однородного идеала многообразия $V$ в $\mathbb{A}^{n+1}(\overline{k})$) и используя [4], мы выясняем, верно ли, что (22) имеет решение, удовлетворяющее (23). Если это верно, строим такое решение. Если система (22) не имеет решения, удовлетворяющего (23), то мы переходим к следующим $\tau$ и $j_1, \ldots, j_\tau$.

Предположим, что система (22) не имеет решения, удовлетворяющего (23), для всех $1 \leqslant \tau \leqslant 4$ и $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$. Тогда $b_j = a_j(\overline{\lambda})$ согласно лемме 4. Если $j+1 = n-1$, то элемент $\overline{\lambda}$, удовлетворяющий утверждению теоремы 2, построен. Предположим, что $j+1 \leqslant n-2$. Тогда мы заменяем $j$ на $j+1$ и переходим к следующему шагу описываемой рекурсии.

Предположим, что (22) имеет решение, удовлетворяющее (23), для некоторых $1 \leqslant \tau \leqslant 4$ и $0 \leqslant j_1 < \ldots < j_\tau \leqslant n$. Вычислим (см. [12]) $z_{w,i} = \mathrm{st}_{\varepsilon_3}(z^*_{w,i})$, $1 \leqslant w \leqslant \tau$, $i \in I_j$, где все $z^*_{w,i}$ – из формулировки леммы 4. Положим $L^*_i = L_i$ для $i \in \{1, \ldots, j\}$ и $L^*_i = L_i + \sum_{1 \leqslant w \leqslant \tau} z_{w,i} X_{j_w}$ для $i \in I_j$. Тогда $L^*_i$ – линейные формы с коэффициентами из $\overline{k_3}$. Положим $\lambda^* = (L^*_0, \ldots, L^*_n)$. По лемме 2 элемент $\lambda^*$ удовлетворяет свойству (B). Из системы (22) получаем, что многочлен $R_{\lambda^*,j,*}(1, Z_n)$ имеет больше различных корней, чем $R_{\overline{\lambda},j,*}(1, Z_n)$. Следовательно, $a_j(\overline{\lambda}) < a_j(\lambda^*)$ и $a_w(\overline{\lambda}) = a_w(\lambda^*)$ для $1 \leqslant w < j$. Применяя лемму 3 и алгоритм редукции к целым коэффициентам (см. [9, предложение 2]), мы последовательно заменяем коэффициенты линейных форм $L^*_i$ на целые числа с длиной записи $O(n \log d)$ и получаем новые линейные формы $L^{**}_i$, $0 \leqslant i \leqslant n+1$, с целыми коэффициентами с длиной записи $O(n \log d)$, удовлетворяющие условию (B) и такие, что (обозначим $\lambda^{**} = (L^{**}_0, \ldots, L^{**}_{n+1})$) $a_w(\lambda^{**}) \geqslant a_w(\lambda^*)$ для всех $1 \leqslant w \leqslant j$. В частности, $a_j(\lambda^{**}) > a_j(\overline{\lambda})$. Теперь мы заменяем $\overline{\lambda}$ на $\lambda^{**}$ и переходим к следующему шагу описываемой рекурсии.

Таким образом, в заключение мы построим элемент $\overline{\lambda}$, удовлетворяющий утверждению теоремы 2. Отметим, что по теореме Безу общее число шагов описываемой рекурсии ограничено сверху полиномом от $d^n$. Оценка на время работы алгоритма для теоремы 2 немедленно следует из оценок на время работы использованных алгоритмов. Теорема доказана. $\square$

## 2. Доказательство теоремы 1

Цель этого раздела – доказать теорему 1.

**Лемма 5.** *Пусть $\nu \geqslant 0$ и $m_i \geqslant 1$, $1 \leqslant i \leqslant \nu$, – целые числа. Предположим, что $f_1^{(i)}, \ldots, f_{m_i}^{(i)} \in k[X_0, \ldots, X_n]$ – однородные многочлены, аналогичные $f_1, \ldots, f_m$, т.е. $f_1^{(i)}, \ldots, f_{m_i}^{(i)}$ удовлетворяют тем же оценкам для степеней и длин записи коэффициентов, что и $f_1, \ldots, f_m$. Пусть $V^{(i)} = \mathcal{Z}(f_1^{(i)}, \ldots, f_{m_i}^{(i)})$ в $\mathbb{P}^n(\overline{k})$. Тогда можно построить линейные формы $L_0, \ldots, L_{n+1}$ с целыми коэффициентами с длиной записи $O(n \log d + \log \nu)$, такие, что выполняются утверждения теоремы 2 для $V^{(i)}$ вместо $V$ для всех $0 \leqslant i \leqslant \nu$ (т.е. линейные формы $L_0, \ldots, L_{n+1}$ не зависят от $i$; другие объекты из утверждения этой теоремы для $V^{(i)}$ зависят от $i$). Время работы этого алгоритма полиномиально от $d^n$, $d_1$, $d_2$, $M$, $M_1$, $m$, $\nu$.*

**Доказательство.** Следует из леммы 3 и алгоритма редукции к целым коэффициентам, см. [9, предложение 2] (мы оставляем подробности читателю). $\square$

Пусть $V$ и $W$ – многообразия из введения. Перейдём к описанию алгоритма. Напомним, что дана точка $x^{(0)} \in W$. Мы можем предполагать без ограничения общности, что $x^{(0)} \notin \mathcal{Z}(e_0, \ldots, e_r)$, ср. алгоритм из [9]. Осуществляя перестановки $X_0, \ldots, X_n$ и $e_0, \ldots, e_r$, мы будем предполагать, не умаляя общности, что $(e_0 X_0)(x^{(0)}) \neq 0$. Применяя теорему 5 из [4], мы строим индексы $1 \leqslant i_\sigma < \ldots < i_n \leqslant r$ и $1 \leqslant j_{s+1} < \ldots < j_\sigma \leqslant n$, такие, что семейство $X_{j_{s+1}}/X_0, \ldots, X_{j_\sigma}/X_0$, $e_{i_\sigma}/e_0, \ldots, e_{i_n}/e_0 \in k(W)$ алгебраически независимо и $\sigma$ является минимально возможным. Для удобства обозначений мы будем предполагать без ограничения общности, что $i_w = w$ для $\sigma \leqslant w \leqslant n$ и $j_w = w$ для $s+1 \leqslant w \leqslant \sigma$. Теперь $\dim W = n - s$ и $\dim W' = n - \sigma$.

В дальнейшем $\sigma + 1 \leqslant i \leqslant n+1$ – произвольное, но фиксированное (мы осуществляем конструкцию для всех $\sigma + 1 \leqslant i \leqslant n+1$). Применим лемму 5 к $n - \sigma + 1$ алгебраическим многообразиям $\widetilde{V}_j$, $\sigma \leqslant j \leqslant n$, и построим линейные формы $L_0, \ldots, L_{n+1}$ с целыми коэффициентами с длиной записи $O(n \log(dd'))$. Фактически по теореме Безу, применяя алгоритм редукции к целым коэффициентам (см. [9, предложение 2]), можно получить новые линейные формы $L_0, \ldots, L_{n+1}$, удовлетворяющие тем же самым свойствам, но с целыми коэффициентами с длиной записи $O(n \log d + (n - \sigma) \log d')$.

Так что мы будем предполагать в дальнейшем, что справедлива последняя оценка. Теперь утверждение (a) выполняется для $L_0, \dots, L_{n+1}$. В дальнейшем линейные формы $L_0, \dots, L_{n+1}$ будут изменяться рекурсивно в алгоритме.

Далее целью будет построить линейные формы $L_0, \dots, L_{n+1}$, удовлетворяющие (a) и (b). Согласно теореме 2 из [8], можно выяснить, верно ли, что $x \in W_i(L')$. Следовательно (заменяя $i$ на $i-1$), можно выяснить, верно ли, что $x \in W_{i-1}(L') \cap \mathcal{Z}(e'_i) = W_i(L') \cup W_i^{(1)}(L') \cup W_i^{(2)}(L') \cup W_i^{(3)}(L')$, см. введение.

Покажем, что многочлен $e'_i$ не обращается в нуль тождественно ни на какой неприводимой компоненте многообразия $W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$. В самом деле, по теореме 1 из [8] для $\widetilde{V}_{i-1}$ все точки многообразия $W_{i-1}(L') \cap \mathcal{Z}(L_\iota, \dots, L_n)$ являются гладкими точками $\widetilde{V}_{i-1}$. Имеем $\dim W_{i-1}(L') \cap \mathcal{Z}(e'_i) = n - \iota$, см. введение. Следовательно, всякая неприводимая компонента многообразия $W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$ содержит точку из $W_{i-1}(L') \cap \mathcal{Z}(L_\iota, \dots, L_n) \setminus \mathcal{Z}(e'_i)$. Требуемое утверждение доказано. Таким образом, $\dim W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n) \cap \mathcal{Z}(e'_i) = 0$.

Используя алгоритм из [3], мы строим все определённые над $k'$ неприводимые над $k'$ компоненты размерности один алгебраического многообразия $\widetilde{V}_{i-1} \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$ и затем, применяя теорему 2 из [8], выбираем среди них компоненты многообразия $W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$. После этого мы строим все точки из множества $S_i = W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n) \cap \mathcal{Z}(e'_i)$. Мы будем предполагать без ограничения общности, что $S_i \cap \mathcal{Z}(L_0) = \emptyset$ и $L_0(x) \neq 0$, так как иначе, используя алгоритм редукции к целым коэффициентам, можно заменить линейную форму $L_0$ на новую и удовлетворить эти условия и все условия из (a).

Обозначим через $\varphi^{(i)}$ морфизм линейной проекции $\mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(L_0, L_{\iota+1}, \dots, L_n) \to \mathbb{P}^{n-\iota}(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (L_0 : L_{\iota+1} : \ldots : L_n)$, и через $\varphi_i$ ограничение $\varphi^{(i)}$ на $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$. Тогда $\varphi_i$ – конечная доминантная линейная проекция. Пусть $x' \in \mathbb{P}^n(\overline{k'})$. Положим $\mu_j(x') = \mu(x', W_{j-1}(L') \cap \mathcal{Z}(e'_j))$, $\sigma + 1 \leqslant j \leqslant n+1$. Для всякого $\sigma + 1 \leqslant i \leqslant n$ положим

$$\mu^{(i)}(z') = \\ \Big(\#\varphi_i^{-1}(z'),\ \#(\varphi_i^{-1}(z') \setminus \mathcal{Z}(e_0, \dots, e_r)),\ \sum_{x' \in \varphi_i^{-1}(z')} \ \sum_{\sigma+1 \leqslant j \leqslant i-1} \mu_j(x')\Big).$$

Тогда $\mu^{(i)}(z') \in \mathbb{Z}^3$. Пусть $(a_1, b_1, c_1), (a_2, b_2, c_2) \in \mathbb{Z}^3$. Положим $(a_1, b_1, c_1) > (a_2, b_2, c_2)$ тогда и только тогда, когда $(a_1 > a_2) \vee ((a_1 = a_2) \& (b_1 > b_2)) \vee ((a_1 = a_2) \& (b_1 = b_2) \& (c_1 < c_2))$. Мы будем использовать это определение также с другими основными полями, содержащими $k'$. Эта формула определяет линейный порядок на $\mathbb{Z}^3$. В дальнейшем в доказательстве мы будем рассматривать этот линейный порядок на $\mathbb{Z}^3$. Пусть $\mathfrak{l} \subset \mathbb{P}^{n-\iota}(\overline{k'})$ – прямая, такая, что $z' \in \mathfrak{l}$. Из теоремы Безу следует, что для всех $z'' \in \mathfrak{l}$, за исключением не более чем полиномиального от $d^n(d')^{n-\sigma}$ числа, справедливо неравенство $\mu^{(i)}(z'') \geqslant \mu^{(i)}(z')$ (здесь мы оставляем детали читателю). То же самое утверждение выполняется для любого другого основного поля $k^*$, содержащего $k'$.

Пусть даны $\nu_{\iota+1}, \ldots, \nu_n \in \overline{k'}$ (или, более общим образом, $\nu_{\iota+1}, \ldots, \nu_n$ из расширения поля $\overline{k'}$). Тогда можно построить множество $\varphi_i^{-1}((1 : \nu_{\iota+1} : \ldots : \nu_n))$ следующим образом. Обозначим через $\mathcal{L}_0$ (соответственно $\mathcal{L}_\nu$) подпространство линейных форм, порождённое $L_{\iota+1}, \ldots, L_n$ (соответственно $L_{\iota+1} - \nu_{\iota+1} L_0, \ldots, L_n - \nu_n L_0$) и вычислим пересечение $\mathcal{L}' = \mathcal{L}_0 \cap \mathcal{L}_\nu$. Построим, используя теоремы 1 и 2 из [8], множество $S''_{i-1} = W_{i-1}(L') \cap \mathcal{Z}(L_\iota, \ldots, L_n)$. Если все $\nu_j$ равны нулю, то $\varphi_i^{-1}((1 : 0 : \ldots : 0)) = S_i$. Так что мы будем предполагать без ограничения общности, что не все $\nu_j$ равны нулю, скажем, $\nu_{\iota+1} \neq 0$. Построим при помощи алгоритма из [3] семейство $E_a$, $a \in A$, всех неприводимых компонент размерности 2 алгебраического многообразия $\widetilde{V}_{i-1} \cap \mathcal{Z}(\mathcal{L}')$, таких, что $E_a \cap S''_{i-1} \neq \emptyset$. Тогда, снова применяя алгоритм из [3], мы строим пересечение $E_a \cap \mathcal{Z}(L_{\iota+1} - \nu_{\iota+1} L_0) \cap \mathcal{Z}(e'_i)$. Множество $\varphi_i^{-1}((1 : \nu_{\iota+1} : \ldots : \nu_n))$ является объединением последних пересечений по всем $a \in A$.

Пусть $\mu^{(i)}(z') = (a(z'), b(z'), c(z'))$. Наша цель – построить точку $z' \in \mathbb{P}^{n-\iota}(\overline{k'})$ с максимально возможным $\mu^{(i)}(z')$. Сначала мы получим $z'$, такую, что $a(z') = \deg W_{i-1}(L') \cap \mathcal{Z}(e'_i)$. Опишем рекурсию относительно $z'$. Возьмём $z' = (1 : 0 : \ldots : 0)$ как базу рекурсии. Мы действуем аналогично алгоритму для вычисления степени из [4]. На общем шаге рекурсии мы ищем точку $z''$ бесконечно близкую к $z'$ и такую, что $a(z'') > a(z')$ (если $z''$ существует). Именно, построим все точки $x' \in \varphi_i^{-1}(z')$. *Пусть $i = j$.* Для всякой $x'$, применяя теорему 2 из [9] к алгебраическому многообразию $(\mathrm{con}(\widetilde{V}_{i-1}) \times \mathrm{con}(\widetilde{V}_{i-1}))(\overline{k'_2})$, мы выясняем, существует ли пара $(x'', x''') \in (W_{i-1}(L') \times W_{i-1}(L'))(\overline{k'_2})$, такая, что

$$\begin{cases} \sum\limits_{0 \leqslant w \leqslant n} |(X_w/L_0)(x'') - (X_w/L_0)(x')|^2 \leqslant \varepsilon_1, \\ \varepsilon_2 \leqslant \sum\limits_{0 \leqslant w \leqslant n} |(X_w/L_0)(x'') - (X_w/L_0)(x''')|^2 \leqslant \varepsilon_1, \\ e'_i(x'') = e'_j(x''') = 0, \\ \varphi^{(j)}(x'') = \varphi^{(j)}(x'''); \end{cases} \tag{25}$$

ср. с системой (2) из [4]. Равенство $a(z') = \deg W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ не выполняется тогда и только тогда, когда существуют $x'', x'''$ для некоторого $x'$. В этом случае мы выбираем такое $x'$, полагаем $z'' = \varphi_i(x'')$, применяем алгоритм редукции к целым коэффициентам к $z'' \in \mathbb{P}^{n-\iota}(\overline{k'}) \setminus \mathcal{Z}(X_0)$ (см. [9, предложение 2]) и получаем точку $\widetilde{z}$ с целыми координатами, такую, что $a(\widetilde{z}) > a(z')$. Следовательно, $\mu^{(i)}(\widetilde{z}) > \mu^{(i)}(z')$. Затем мы заменяем $z'$ на $\widetilde{z}$ и переходим к следующему шагу рекурсии.

В заключение мы придём к случаю, когда для всех $x'$ не существует $(x'', x''')$. Тогда $a = \deg W_{i-1}(L') \cap \mathcal{Z}(e'_i)$. Следовательно, в частности, дифференциал $d_{x'}\varphi_i$ – изоморфизм для всякой точки $x' \in \varphi_i^{-1}(z')$, ср. [4] (мы оставляем подробности читателю). Согласно теореме Безу и алгоритму редукции к целым коэффициентам, $z' = (1 : z'_{i,i-\sigma+s+1} : \ldots : z'_{i,n})$, где все $z'_{i,j}$ – целые числа с длиной записи $O(n \log d + (n-\sigma)\log d')$.

Теперь мы собираемся максимизировать $\#(\varphi_i^{-1}(z') \setminus \mathcal{Z}(e_0, \ldots, e_r))$. Мы перебираем точки $x \in \varphi_i^{-1}(z') \cap \mathcal{Z}(e_0, \ldots, e_r)$. Рассмотрим следующую систему полиномиальных уравнений и неравенств с коэффициентами из $\overline{k'_2}$:

$$\begin{cases} \sum\limits_{0 \leqslant j \leqslant r} |e_j|^2 = \varepsilon_2, \\ \sum\limits_{0 \leqslant i \leqslant n} |X_i - (X_i/L_0)(x)|^2 \leqslant \varepsilon_1, \\ e'_i = 0, \\ L_0 = 1. \end{cases} \tag{26}$$

Применим теорему 2 из [9] к этой системе и многообразию $\mathrm{con}(V \cap \mathcal{Z}(e'_{\sigma+1}, \ldots, e'_{i-1}))$ и построим множество $S'' \subset \mathbb{A}^{n+1}(\overline{k'_2})$ из формулировки этой теоремы. Обозначим через $S''' \subset \mathbb{P}^n(\overline{k_2'})$ множество, соответствующее $S''$ при естественной проекции $\mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$. Далее, применяя теорему 2 из [8], мы выясняем, существует ли точка $x^* \in S''' \cap W_{i-1}(L')(\overline{k_2'})$. Очевидно такая точка существует в том и только в том случае, если $x \in W_i(L') \cap W_i^{(3)}(L')$. Предположим, что такая точка существует. Тогда положим $z^* = \varphi_i(x^*)$. Следовательно, $x^* \in \varphi_i^{-1}(z^*) \setminus \mathcal{Z}(e_0, \dots, e_r)$, и для всякого $x_1 \in \varphi_i^{-1}(z') \setminus \mathcal{Z}(e_0, \dots, e_r)$ существует точка $x_1^* \in \varphi_i^{-1}(z^*) \setminus \mathcal{Z}(e_0, \dots, e_r)$, которая бесконечно близка к $z_1$ (согласно, например, предложению 6 из [12]). Поэтому $\#(\varphi_i^{-1}(z^*) \setminus \mathcal{Z}(e_0, \dots, e_r)) > \#(\varphi_i^{-1}(z') \setminus \mathcal{Z}(e_0, \dots, e_r))$ и, следовательно, $\mu^{(i)}(z^*) > \mu^{(i)}(z')$. Применяя алгоритм редукции к целым коэффициентам (см. [9, предложение 2], можно последовательно заменить координаты $z^*$ на целые числа (мы находим их при помощи перебора) с длиной записи $O(n \log d + (n-\sigma)\log(d'))$ и получить точку $z''$, такую, что $a(z'') = a(z^*)$, $b(z'') \geqslant b(z^*) > b(z')$. Поэтому $\mu^{(i)}(z'') \geqslant \mu^{(i)}(z^*)$. Теперь мы заменяем $z'$ на $z''$ и переходим к следующему шагу рекурсии.

Если не существует точки $x^* \in W_{i-1}(L')(\overline{k_2'})$, задающей решение системы (26), и не все точки из $\varphi_i^{-1}(z') \setminus \mathcal{Z}(e_0, \dots, e_r)$ перебраны, то мы переходим к следующей точке $x \in \varphi_i^{-1}(z') \setminus \mathcal{Z}(e_0, \dots, e_r)$. Если все точки из $\varphi_i^{-1}(z') \setminus \mathcal{Z}(e_0, \dots, e_r)$ перебраны, то мы получили требуемую точку $z'$, такую, что $a(z') = \deg W_{i-1}(L') \cap \mathcal{Z}(e_i')$ и $b(z')$ максимально возможное.

Применяя алгоритм редукции к целым коэффициентам (см. [9, предложение 2]), можно предполагать дополнительно, что $z'_{i,j} = z'_{i_1,j}$ для всех $\sigma + 1 \leqslant i_1 < i \leqslant n$, $i - \sigma + s + 1 \leqslant j \leqslant n$, т.е. $z'_{i,j} = z'_j$, $s + 2 \leqslant j \leqslant n$, не зависит от $i$. Тогда для всех $\sigma + 1 \leqslant i \leqslant n + 1$

$$W_{i-1}(L') \cap \mathcal{Z}(e_i') \cap \mathcal{Z}(L_0, L_{\iota+1}, \dots, L_n) = \emptyset, \tag{27}$$

$$\begin{aligned} &\#(W_{i-1}(L') \cap \mathcal{Z}(e_i') \cap \mathcal{Z}(L_{\iota+1} - z'_{\iota+1}L_0, \dots, L_n - z'_n L_0)) = \\ &= \deg(W_{i-1}(L') \cap \mathcal{Z}(e_i')). \end{aligned} \tag{28}$$

Далее, применяя лемму 3 и алгоритм редукции к целым коэффициентам, мы будем предполагать без ограничения общности, что линейные формы $L_0, \dots, L_{s+1}, L_{s+2} - z'_{s+2}L_0, \dots, L_n - z'_n L_0, L_{n+1}$ удовлетворяют дополнительно утверждению (a) вместо $L_0, \dots, L_{n+1}$ (мы оставляем детали читателю). Теперь, заменяя $L_j$ на $L_j - z'_j L_0$, $s+2 \leqslant j \leqslant n$, мы будем считать в дальнейшем, что $z'_j = 0$ для всех $s+2 \leqslant j \leqslant n$. Положим $\overline{\lambda} = (L_0, \dots, L_{n+1})$. Тогда $\overline{\lambda}$ удовлетворяет условию (B) из начала раздела 1 для алгебраического многообразия $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ (вместо $V$) для всякого $\sigma+1 \leqslant i \leqslant n+1$. Кроме того, $a((1:0:\ldots:0))$ и $b((1:0:\ldots:0))$ являются максимально возможными для всякого $\sigma+1 \leqslant i \leqslant n+1$.

Напомним, что определены целые числа $a_\iota(\overline{\lambda}, W_{i-1}(L') \cap \mathcal{Z}(e'_i))$ и $b_\iota(W_{i-1}(L') \cap \mathcal{Z}(e'_i))$ (см. раздел 1). До конца доказательства мы будем обозначать для краткости $a_\iota(\overline{\lambda}) = a_\iota(\overline{\lambda}, W_{i-1}(L') \cap \mathcal{Z}(e'_i))$, $b_\iota = b_\iota(W_{i-1}(L') \cap \mathcal{Z}(e'_i))$ и использовать аналогичные обозначения для других элементов, скажем, писать $\lambda^*$ вместо $\overline{\lambda}$. Теперь можно вычислить целое число $a_\iota(\overline{\lambda})$ следующим образом. Используя алгоритм из [3], для всякого $\sigma+1 \leqslant i \leqslant n+1$ мы строим все неприводимые над $k'$ компоненты размерности 2 пересечения $\widetilde{V}_{i-1} \cap \mathcal{Z}(L_{\iota+1}, \dots, L_{n-1})$. Согласно теореме 1 из [8] (можно также применить вместо нее теорему 2) и теореме 2 из [8], выберем среди них все неприводимые над $k'$ компоненты $E$ многообразия $W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_{n-1})$. Снова, используя алгоритм из [3], мы строим все неприводимые над $k'$ компоненты $E \cap \mathcal{Z}(e'_i)$ для всех $E$. Это есть все неприводимые над $k'$ компоненты многообразия $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$. Согласно [3], мы строим также сепарабельные многочлены $\Phi_{\iota,*} \in k'[Z_0, Z_n, Z_{n+1}]$ (см. раздел 1), соответствующие алгебраическому многообразию $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ вместо $V$ из раздела 1 (заметим здесь, что все неприводимые компоненты $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ имеют размерность $n-\iota$ и, следовательно, мы сопоставляем только один многочлен $\Phi_{\iota,*}$ многообразию $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$). После этого мы вычисляем дискриминант $R_{\iota,*}$ многочлена $\Phi_{\iota,*}$ относительно $Z_{n+1}$, его бесквадратную часть $R_{\iota,*,0}$ и целое число $a_\iota(\overline{\lambda}) = \deg R_{\iota,*,0}$ для всякого $\sigma+1 \leqslant i \leqslant n+1$. Мы будем обозначать также $\Phi_{\iota,*} = \Phi_{\overline{\lambda},\iota,*}$ и $R_{\iota,*} = R_{\overline{\lambda},\iota,*}$, если важна зависимость от $\overline{\lambda}$ (см. раздел 1).

Пусть $1 \leqslant \tau \leqslant 4$ – целое число. Пусть $0 \leqslant i_1 < \ldots < i_\tau \leqslant n$ – целые числа. Предположим, что поле $k'$ снабжено вещественной структурой (см. [12]). Пусть $k'_j = k'(\varepsilon_1, \dots, \varepsilon_j)$, $0 \leqslant j \in \mathbb{Z}$, где $\varepsilon_j > 0$ для $j \geqslant 1$ является бесконечно малой величиной относительно поля $k'_{j-1}$. Пусть $X_{w,j}$, $1 \leqslant w \leqslant 4$, $0 \leqslant j \leqslant n$; $Z_{w,j}$, $j \in \{0, \iota+1, \dots, n+1\} = I_\iota$, $1 \leqslant w \leqslant \tau$, – переменные. Обозначим для краткости $\overline{L}_j = L_j + \sum_{1\leqslant w\leqslant\tau} Z_{w,j}X_{i_w}$, $j \in I_\iota$ (так что все $\overline{L}_j$ зависят от выбора $j_1, \dots, j_\tau$). Обозначим $X^{(j)} = (X_{j,0}, \dots, X_{j,n})$ и для произвольного многочлена $c$ от $n+1$ переменных положим $c(X^{(j)}) = c(X_{j,0}, \dots, X_{j,n})$, $1 \leqslant j \leqslant 4$. Предположим, что $\iota \leqslant n-2$. Рассмотрим следующую систему полиномиальных уравнений и неравенств с квадратами абсолютных величин с коэффициентами из $k_3'$ относительно переменных $X_{w,j}$, $1 \leqslant w \leqslant 4$, $0 \leqslant j \leqslant n$; и $Z_{w,j}$, $j \in \{0, \iota+1, \dots, n+1\} = I_\iota$, $1 \leqslant w \leqslant \tau$:

$$\left\{\begin{array}{ll}
\sum\limits_{j\in I_\iota}\sum\limits_{1\leqslant w\leqslant\tau} |Z_{j,w}|^2 \leqslant \varepsilon_1, & \\
\varepsilon_2 \leqslant |\overline{L}_n(X^{(1)}) - \overline{L}_n(X^{(3)})|^2 \leqslant \varepsilon_1, & \\
|\overline{L}_{n+1}(X^{(j)}) - \overline{L}_{n+1}(X^{(j+1)})|^2 = \varepsilon_3, & j = 1, 3, \\
\overline{L}_\nu(X^{(j_1)}) = \overline{L}_\nu(X^{(j_2)}) = 0, & 1 \leqslant j_1 < j_2 \leqslant 4, \\
\iota + 1 \leqslant \nu \leqslant n-1, & \\
\overline{L}_n(X^{(j)}) - \overline{L}_n(X^{(j+1)}) = 0, & j = 1, 3, \\
\overline{L}_0(X^{(j)}) - 1 = 0, & 1 \leqslant j \leqslant 4, \\
e_i'(X^{(j)}) = 0, & 1 \leqslant j \leqslant 4.
\end{array}\right. \tag{29}$$

**Лемма 6.** *Пусть $\iota \leqslant \min\{n-2, n+1-\sigma+s\}$. Неравенство $a_\iota(\overline{\lambda}) < b_\iota$ справедливо тогда и только тогда, когда существуют $1 \leqslant \tau \leqslant 4$ и $0 \leqslant i_1 < \ldots < i_\tau \leqslant n$, удовлетворяющие следующему свойству. Система* (29) *имеет решение $X_{w,i} = x^*_{w,i} \in \overline{k_3'}$, $1 \leqslant w \leqslant 4$, $0 \leqslant i \leqslant n$; $Z_{w,i} = z^*_{w,i} \in \overline{k_3'}$, $i \in \{0, \iota+1, \dots, n+1\}$, $1 \leqslant w \leqslant \tau$, такое, что*

$$(x^*_{w,0} : \ldots : x^*_{w,n}) \in W_{i-1}(L')(\overline{k_3'}), \quad 1 \leqslant w \leqslant 4. \tag{30}$$

**Доказательство.** Доказательство этой леммы аналогично доказательству леммы 4. $\square$

Вернёмся к алгоритму для утверждения (b). Мы опишем рекурсию относительно $\iota$. База рекурсии есть $\iota = s+1$. Опишем общий шаг этой рекурсии. Пусть $s+1 \leqslant \iota \leqslant n-2$ – максимальное число, такое, что для всех $s+1 \leqslant w < \iota$ целые числа $b_w(W_{i-1}(L') \cap \mathcal{Z}(e_i'))$ вычислены и $b_w(W_{i-1}(L') \cap \mathcal{Z}(e_i')) = a_w(\overline{\lambda}, W_{i-1}(L') \cap \mathcal{Z}(e_i'))$. Построим (см. выше) многочлены $\Phi_{\overline{\lambda},\iota,*}$, $R_{\overline{\lambda},\iota,*}$ и $R_{\overline{\lambda},\iota,*,0}$. Мы будем предполагать без ограничения общности, что $Z_0$ не делит $R_{\overline{\lambda},\iota,*,0}$, заменяя при необходимости $Z_0$ на

$Z_0 - \mu Z_n$ для подходящего целого числа $\mu$, ограниченого сверху полиномом от $d^n(d')^{n-\sigma}$. Линейная форма $L_0 - \mu L_n$ удовлетворяет тем же самым свойствам, что и $L_0$ (см. выше).

Будем перебирать целые числа $\tau$ и $i_1, \dots, i_\tau$, такие, что $1 \leqslant \tau \leqslant 4$ и $0 \leqslant i_1 < \dots < i_\tau \leqslant n$. Применяя теорему 2 из [9] к алгебраическому многообразию $\mathrm{con}(\widetilde{V}_{i-1}) \subset \mathbb{A}^{n+1}(\overline{k'})$ и [4], мы выясним, имеет ли система (29) решение, удовлетворяющее условию (30). Если имеет, то мы строим такое решение. Если не имеет, то мы переходим к следующим $\tau$ и $i_1, \dots, i_\tau$.

Предположим, что система (29) не имеет решения, удовлетворяющего условию (30), для всех $1 \leqslant \tau \leqslant 4$ и $0 \leqslant i_1 < \dots < i_\tau \leqslant n$. Тогда $a_\iota(\overline{\lambda}) = b_\iota$ согласно лемме 6.

Если $\iota = \min\{n-2, n+1-\sigma+s\}$, то элемент $\overline{\lambda}$, удовлетворяющий утверждению теоремы 2, построен. Предположим, что $\iota < \min\{n-2, n+1-\sigma+s\}$. Тогда мы заменяем $\iota$ на $\iota+1$ и переходим к следующему шагу рекурсии.

Предположим, что система (29) имеет решение, удовлетворяющее условию (30), для некоторых $1 \leqslant \tau \leqslant 4$ и $0 \leqslant i_1 < \dots < i_\tau \leqslant n$. Вычислим (см. [12]) $z_{w,j} = \mathrm{st}_{\varepsilon_3}(z^*_{w,j})$, $1 \leqslant w \leqslant \tau$, $j \in I_\iota$, где все $z^*_{w,j}$ – из формулировки леммы 6. Положим $L^*_j = L_j$ для $j \in \{1, \dots, \iota\}$ и $L^*_j = L_j + \sum_{1 \leqslant w \leqslant \tau} z_{w,j} X_{j_w}$ для $j \in I_\iota$. Тогда $L^*_j$ – линейные формы с коэффициентами из $\overline{k'_3}$. Положим $\lambda^* = (L^*_0, \dots, L^*_n)$. Согласно лемме 2, элемент $\lambda^*$ удовлетворяет свойству (B) для всех алгебраических многообразий $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$, $\sigma+1 \leqslant i \leqslant n+1$. Из системы (29) мы получаем, что многочлен $R_{\lambda^*,\iota,*}(1, Z_n)$ имеет больше различных корней, чем $R_{\overline{\lambda},\iota,*}(1, Z_n)$. Так что $a_\iota(\overline{\lambda}) < a_\iota(\lambda^*)$ и $a_w(\overline{\lambda}) = a_w(\lambda^*)$ для $1 \leqslant w < \iota$. Применяя лемму 3 и алгоритм редукции к целым коэффициентам (см. [9, предложение 2]), мы последовательно заменяем коэффициенты линейных форм $L^*_j$ на целые числа с длиной записи $O(n \log d + (n-\sigma)\log d')$ и получаем новые линейные формы $L^{**}_j$, $0 \leqslant j \leqslant n+1$, удовлетворяющие следующим свойствам. Все $L^{**}_j$, $0 \leqslant j \leqslant n+1$, имеют целые коэффициенты с длиной записи $O(n \log d + (n-\sigma)\log d')$ и удовлетворяют условию (B) для всех алгебраических многообразий $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$, $\sigma+1 \leqslant i \leqslant n+1$. Далее, $L^{**}_j$, $0 \leqslant j \leqslant n+1$, удовлетворяют утверждению (a) теоремы 1 с $L^*_j$ вместо $L_j$, $0 \leqslant j \leqslant n$, и (обозначим $\lambda^{**} = (L^{**}_0, \dots, L^{**}_{n+1})$) $a_w(\lambda^{**}) \geqslant a_w(\lambda^*)$ для всех $1 \leqslant w \leqslant \iota$. В частности, $a_\iota(\lambda^{**}) > a_\iota(\overline{\lambda})$.

Теперь мы заменяем $\overline{\lambda}$ на $\lambda^{**}$ и переходим к следующему шагу описываемой рекурсии.

Таким образом, в заключение мы построим элемент $\overline{\lambda}$, удовлетворяющий утверждениям (a) и (b) теоремы 1. Заметим, что, согласно теореме Безу, общее число шагов описанной рекурсии ограничено сверху полиномом от $d^n(d')^{n-\sigma}$.

Теперь любые две точки $y', y'' \in W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$ принадлежат одной и той же неприводимой над $k'$ (соответственно неприводимой над $\overline{k'}$) компоненте многообразия $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ в том и только в том случае, если они принадлежат одной и той же неприводимой над $k'$ (соответственно неприводимой над $\overline{k'}$) компоненте кривой $W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_{n-1})$. Мы построили все неприводимые компоненты последнего алгебраического многообразия (см. выше). Следовательно, можно выяснить, принадлежат ли $y'$ и $y''$ одной и той же неприводимой над $k'$ (соответственно неприводимой над $\overline{k'}$) компоненте кривой $W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_{n-1})$. Подробности аналогичны имеющимся в доказательстве теоремы 2 из [8]. Таким образом, можно вычислить число точек $y'' \in W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$, таких, что $y'$ и $y''$ принадлежат одной и той же определённой над $k'$ и неприводимой над $k'$ компоненте многообразия $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$.

Пусть $E$ – неприводимая над $\overline{k'}$ компонента $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$, такая, что $y' \in E$. Чтобы избежать построения композита $k'(y', y'')$, мы вычислим сначала, при помощи [3], минимальное поле определения $k''$ многообразия $E \cap \mathcal{Z}(L_{\iota+1}, \dots, L_{n-1})$, содержащее $k'$. Поле $k''$ совпадает с минимальным полем определения компоненты $E$, содержащим $k'$, ср. [8]. После этого мы осуществляем всю конструкцию над $k''$, т.е. предполагаем, что $L_j \in k''[X_0, \dots, X_n]$, $0 \leqslant j \leqslant n+1$. Это позволяет вычислить число точек $y'' \in W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$, таких, что $y'$ и $y''$ принадлежат $E$. Аналогичным образом в (c), расширяя основное поле $k'$ до $k''$, мы сводим случай неприводимой над $\overline{k'}$ компоненты $E$ к случаю определённой над $k''$ и неприводимой над $k''$ компоненты, т.е. для этой редукции в (c) достаточно рассмотреть только случай, когда $E$ является определённым над $k'$ и неприводимым над $k'$, и после этого заменить поле $k'$ на $k''$. Аналогичным образом в (f), расширяя основное поле $k'$ до $k''$, мы можем предполагать, что $E$ определена над основным полем. Так что в (f) мы будем считать без ограничения общности, что $E$ определена над $k'$ и неприводима над $\overline{k'}$. Алгоритмы для утверждений (a) и (b) описаны полностью.

**Лемма 7.** *Пусть $\sigma+1 \leqslant i \leqslant n+1$ – целое число. Пусть $k^*$ – конечнопорождённое расширение поля $k'$, заданное минимальным многочленом примитивного элемента поля $k^*$ над чисто трансцендентным расширением поля $k'$. Пусть $\lambda^* = (L_0^*, \dots, L_{n+1}^*)$, где все $L_j^* \in k'[X_0, \dots, X_n]$ – линейные формы. Тогда можно выяснить, верно ли, что пересечение $\widetilde{V}_{i-1}$ и $\mathcal{Z}(L_\iota^*, \dots, L_n^*)$ трансверсально. Предположим, что пересечение $\widetilde{V}_{i-1}$ и $\mathcal{Z}(L_\iota^*, \dots, L_n^*)$ трансверсально. Тогда $\#(W_{i-1}(L') \cap \mathcal{Z}(e_i') \cap \mathcal{Z}(L_\iota^*, \dots, L_n^*)) < +\infty$, и можно построить все точки из $W_{i-1}(L') \cap \mathcal{Z}(e_i') \cap \mathcal{Z}(L_\iota^*, \dots, L_n^*)$ в $\mathbb{P}^n(\overline{k^*})$. Далее, можно выяснить, верно ли, что пересечение $W_{i-1}(L') \cap \mathcal{Z}(e_i')$ и $\mathcal{Z}(L_{\iota+1}^*, \dots, L_n^*)$ трансверсально. Следовательно, можно узнать, выполняются ли утверждения* (a) *и* (b) *для $\lambda^*$ вместо $\overline{\lambda}$. Время работы алгоритма из этой леммы полиномиально от $d^n$, $(d')^n$, $d_1$, $d_2$, $d_2'$, $M$, $M'$, $M_1$, $m$, $r$, длины записи $\mathrm{L}(x^{(0)})$ точки $x^{(0)}$, длины записи $\mathrm{L}(L')$ элемента $L'$ и длины записи $\mathrm{L}(\lambda^*)$ элемента $\lambda^*$ (включая размеры минимальных многочленов примитивных элементов полей $k'$ и $k^*$).*

**Доказательство.** Согласно (a) и (b), мы знаем степени всех неприводимых компонент алгебраических многообразий $\widetilde{V}_{i-1}$ и $W_{i-1}(L') \cap \mathcal{Z}(e_i')$. Следовательно, применяя теорему 3 и теорему 2 из [8], можно выяснить, трансверсально ли пересечение $\widetilde{V}_{i-1}$ и $\mathcal{Z}(L_\iota^*, \dots, L_n^*)$ (мы оставляем детали читателю). Предположим, что последнее пересечение трансверсально. Тогда, заменяя в доказательстве утверждения (b) $L_j$ на $L_j^*$, $\iota+1 \leqslant j \leqslant n$, мы видим, что $W_{i-1}(L') \cap \mathcal{Z}(e_i') \cap \mathcal{Z}(L_{\iota+1}^*, \dots, L_n^*) = A^*$ – конечное множество в $\mathbb{P}^n(\overline{k'})$, и строим это множество аналогичным образом. Теперь пересечение $W_{i-1}(L') \cap \mathcal{Z}(e_i')$ и $\mathcal{Z}(L_{\iota+1}^*, \dots, L_n^*)$ трансверсально тогда и только тогда, когда $\#A^* = \deg W_{i-1}(L') \cap \mathcal{Z}(e_i')$. $\square$

Чтобы описать алгоритм для утверждения (c), достаточно рассмотреть случай, когда $E$ определено над $k'$ и неприводимо над $k'$, см. конец доказательства утверждения (b). Заменяя линейную форму $L_0$ на новую, мы будем предполагать, что

(i) $L_0(x) \neq 0$,

(ii) линейные формы $L_0, \dots, L_{n+1}$ удовлетворяют утверждениям (a), (b) теоремы 1,

(iii) $L_0, X_1, \dots, X_n$ линейно независимы над $k'$.

Далее, применяя леммы 3 и 7, можно заменить линейные формы $L_1, \dots, L_{n+1}$ на новые, такие, что дополнительно

(iv) все $L_j$, $\iota + 1 \leqslant j \leqslant n$, являются линейными формами от $L_0, X_1, \dots, X_n$ с целыми коэффициентами с длиной записи $O(n \log d + (n-\sigma)\log(d'))$.

Пусть $\mathcal{L}$ – подпространство всех линейных форм из $k'(x)[X_0, \dots, X_n]$, обращающихся в нуль в точке $x$. Базис $\mathcal{L}$ есть $X_i - (X_i/L_0)(x)L_0$, $1 \leqslant i \leqslant n$. Положим $L''_j = L_j - (L_j/L_0)(x)L_0 \in \mathcal{L}$, $\iota + 1 \leqslant j \leqslant n$. Для всякого $1 \leqslant i \leqslant n+1$ положим $L_j = \widetilde{L}_j + \mu_j L_0$, где $\widetilde{L}_j \in k[X_1, \dots, X_n]$ и $\mu_j$ – целое число. Тогда, очевидно, $L''_j = \widetilde{L}_j(X_1 - (X_1/L_0)(x)L_0, \dots, X_n - (X_n/L_0)(x)L_0)$.

Чтобы вычислить кратности, мы опишем рекурсивный алгоритм относительно $L_0, ..., L_{n+1}$. Возьмём построенные $L_0, ..., L_{n+1}$, удовлетворяющие (i)–(iv), как базу рекурсии. В конце каждого шага, который не является заключительным, мы получаем новые линейные формы $L_0, \dots, L_{n+1}$, такие, что число элементов пересечения $W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L''_{\iota+1}, \dots, L''_n)$ больше, чем в начале шага (для старых $L_0, \dots, L_{n+1}$). В конце каждого шага (и, следовательно, если рассматриваемый шаг не является заключительным, в начале следующего шага) этой рекурсии выполняются условия (i)–(iv).

Для произвольного квазипроективного алгебраического многообразия $E$ и его точки $a$ обозначим через $\mathrm{con}(a, E)$ касательный конус многообразия $E$ в точке $x$ (см., например, [4]). Рассмотрим условие

$$\mathrm{con}(x, W_{i-1}(L') \cap \mathcal{Z}(e'_i)) \cap \mathcal{Z}(L''_{\iota+1}, \dots, L''_n) = \{x\}. \qquad (31)$$

В конце рекурсии будет выполнено условие (31).

Опишем общий шаг этой рекурсии. Мы следуем алгоритму для вычисления кратности из [4]. Единственное отличие здесь состоит в том, что алгебраическое многообразие $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ задано в несколько иной форме по сравнению с [4]. Но всё же, используя теорему 2 из [9], мы имеем сертификат для того, чтобы выяснить, верно ли, что $x \in W_{i-1}(L')$. Это позволяет описать аналог алгоритма из [4]. Напомним, что (см. начало раздела) для любых $\nu_{\iota+1}, \dots, \nu_n \in \overline{k'}$ можно вычислить $\varphi_i^{-1}((1 : \nu_{\iota+1} : \dots : \nu_n))$. Вычислим таким образом все точки из $W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L''_{\iota+1}, \dots, L''_n) = \varphi_i^{-1}(\varphi_i(x))$. Мы будем увеличивать рекурсивно число элементов в $W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L''_{\iota+1}, \dots, L''_n)$. Если это невозможно, то $L''_{\iota+1}, \dots, L''_n$ удовлетворяют условию (31).

Именно, пусть $\mathbb{A}^{2n+1}(\overline{k'})$ имеет координатные функции $X_0, \dots, X_n$, $Y_1, \dots, Y_n$. Построим однородный многочлен $\widetilde{e}_i \in k'(x)[X_0, \dots, X_n]$, такой, что $\widetilde{e}_i(L_0, X_1, \dots, X_n) = e'_i$. Теперь вместо системы (15) из [4] рассмотрим систему полиномиальных уравнений и неравенств с квадратами абсолютных величин от $2n+1$ переменных с коэффициентами из $\overline{k'_2}$

$$\begin{cases} \widetilde{e}_i(1, X_1 - (X_1/L_0)(x), \dots, X_n - (X_n/L_0)(x)) = 0, \\ \sum_{1 \leqslant i \leqslant n} |X_i - (X_i/L_0)(x)|^2 = \varepsilon_2^2, \\ \widetilde{L}_j(Y_1 - (X_1/L_0)(x), \dots, Y_n - (X_n/L_0)(x)) = 0, \\ \iota + 1 \leqslant j \leqslant n, \\ \sum_{1 \leqslant i \leqslant n} |X_i - Y_i|^2 \leqslant \varepsilon_1 \varepsilon_2^2, \\ L_0 - 1 = 0. \end{cases} \tag{32}$$

Тогда (ср. [4, лемма 8]) эта система имеет решение $(x_0^*, \dots, x_n^*, y_1^*, \dots, y_n^*) \in \mathbb{A}^{2n+1}(\overline{k'_2})$, такое, что

$$(x_0^* : x_1^* : \dots : x_n^*) \in W_{i-1}(L') \tag{33}$$

в том и только в том случае, если не выполняется условие (31). Можно применить теорему 2 из [9] и теорему 2 из [8] к алгебраическому многообразию $(\mathrm{con}(\widetilde{V}_{i-1}) \times \mathbb{A}^n)(\overline{k'_2}) \subset \mathbb{A}^{2n+1}(\overline{k'})$ и построить решение системы (32), удовлетворяющее условию (33), если оно существует.

Предположим, что решение системы (32), удовлетворяющее условию (33), построено. Тогда аналогично [4] можно построить линейные формы $L_j^* \in \overline{k'_2}[X_1, \dots, X_n]$, $\iota + 1 \leqslant j \leqslant n$, такие, что $L_j^*(X_1 - (X_1/L_0)(x), \dots, X_n - (X_n/L_0)(x)) = 0$, и коэффициенты линейных форм $L_j^*$ бесконечно близки относительно поля $k'$ к соответствующим коэффициентам $\widetilde{L}_j$ для всех $\iota + 1 \leqslant j \leqslant n$. Заметим, что $\#(W_{i-1}(L') \cap \mathcal{Z}(e'_i) \cap \mathcal{Z}(L^*_{\iota+1}, \dots, L^*_n) > \#\varphi_i^{-1}\varphi_i(x)$. Обозначим через $k^*$ поле, порождённое над $k'$ коэффициентами линейных форм $L_j^*$, $\iota+1 \leqslant j \leqslant n$. Положим $\lambda^* = (L_0, L_1 \dots, L_\iota, L^*_{\iota+1} +$

$\mu_{\iota+1}L_0,\dots,L_n^*+\mu_nL_0,L_{n+1})$. Тогда $\lambda^*$ бесконечно близко к $\overline{\lambda}$. Поэтому по лемме 2 утверждения (a) и (b) теоремы 1 справедливы для $\lambda^*$ и $k^*$ вместо $\overline{\lambda}$ и $k'$. Отсюда, согласно лемме 3, теореме Безу и лемме 7, применяя алгоритм редукции к целым коэффициентам, можно последовательно заменить коэффициенты линейных форм $L_j^*+\mu_jL_0$, $\iota+1\leqslant j\leqslant n+1$, в базисе $L_0,X_1,\dots,X_n$ и получить новые линейные формы $L_j^{**}$, $\iota+1\leqslant j\leqslant n+1$, удовлетворяющие следующим свойствам. Положим $L_j^{**}=L_j$ для всех $j\in\{1,\dots,\iota,n+1\}$ и $\lambda^{**}=(L_0^{**},\dots,L_{n+1}^{**})$. Тогда выполнены условия (i)–(iv) для $\lambda^{**}$ вместо $\overline{\lambda}$ и $\#W_{i-1}(L')\cap\mathcal{Z}(e_i')\cap\mathcal{Z}(L_{\iota+1}^{**},\dots,L_n^{**})\geqslant\#(W_{i-1}(L')\cap\mathcal{Z}(e_i')\cap\mathcal{Z}(L_{\iota+1}^{*},\dots,L_n^{*})>\#\varphi_i^{-1}\varphi_i(x)$. Теперь мы заменяем $\overline{\lambda}$ на $\lambda^{**}$ и переходим к следующему шагу рекурсии.

Таким образом, в заключение мы придём к случаю, когда система (32) не имеет решения, удовлетворяющего условию (33). Следовательно (см. выше), выполняется условие (31). Тогда (ср. [4, лемма 18]) кратность $\mu(x,E)$ равна числу точек $x^*\in S^*$, таких, что $x^*\in E$. Поэтому можно вычислить требуемую кратность согласно (b). Алгоритм для (c) описан полностью.

Утверждение (g) непосредственно следует из лемм 3 и 7.

Теперь мы можем вычислить $\mu^{(i)}(z')$ для заданной точки $z'\in\mathbb{P}^{n-\iota}(\overline{k})$ (и для любой другой точки с координатами из расширения поля $\overline{k}$, когда мы применяем алгоритм редукции к целым коэффициентам на шаге рекурсии, см. ниже). Вернёмся к конструкции точки $z'\in\mathbb{P}^{n-\iota}(\overline{k})$ с максимально возможным $\mu^{(i)}(z')$ (напомним, что мы осуществляем конструкцию для всех $\sigma+1\leqslant i\leqslant n+1$). Опишем рекурсию относительно $z'$. Возьмём $z'=(1:0:\ldots:0)$ как базу рекурсии. На общем шаге рекурсии мы ищем точку $z''$, которая бесконечно близка к $z'$ и удовлетворяет условию $\mu^{(i)}(z'')>\mu^{(i)}(z')$ (если $z''$ существует). Именно, построим все точки $x'\in\varphi_i^{-1}(z')$. Для всякой $x'$ для всякого $\sigma+1\leqslant j<i$, применяя теорему 2 из [9] к алгебраическому многообразию $(\mathrm{con}(\widetilde{V}_{i-1})\times\mathrm{con}(\widetilde{V}_{j-1}))(\overline{k_2'})$, мы выясняем, существует ли пара $(x'',x''')\in(W_{i-1}(L')\times W_{j-1}(L'))(\overline{k_2'})$, такая, что справедливо (25) (ср. с системой (2) из [4]). Элемент $\mu^{(i)}(z')$ не является максимально возможным тогда и только тогда, когда существуют $x'',x'''$ для некоторых $x'$ и $j$. В этом случае мы выбираем такие $x'$ и $j$ и полагаем $z''=\varphi_i(x'')$. Нетрудно видеть, используя, например, [4], что для любой прямой $\mathfrak{l}\subset\mathbb{P}^{n-\iota}(\overline{k})$ и для любой точ-

ки $z^* \in \mathfrak{l}$ существует только полиномиальное от $d^n(d')^{n-\sigma}$ число точек $z^{**} \in \mathfrak{l}$ с $\mu^{(i)}(z^{**}) < \mu^{(i)}(z^*)$, ср. также доказательство леммы 1 из [7]. Следовательно, мы применяем алгоритм редукции к целым коэффициентам к $z'' \in \mathbb{P}^{n-\iota}(\overline{k'}) \setminus \mathcal{Z}(X_0)$ (см. [9, предложение 2]) и получаем точку $\widetilde{z}$ с целыми координатами, такую, что $\mu^{(i)}(\widetilde{z}) > \mu^{(i)}(z')$. Затем мы заменяем $z'$ на $\widetilde{z}$ и переходим к следующему шагу рекурсии.

Наконец мы придём к случаю, когда для всех $x'$ и $j$ не существует $(x'', x''')$. Тогда $\mu^{(i)}(z')$ максимально возможное. Согласно теореме Безу и алгоритму редукции к целым коэффициентам, $z' = (1 : z'_{i,i-\sigma+s+1} : \ldots : z'_{i,n})$, где все $z'_{i,j}$ – целые числа с длинами записи $O(n \log d + (n-\sigma)\log d')$.

Применяя алгоритм редукции к целым коэффициентам (см. [9, предложение 2]), можно предполагать дополнительно, что $z'_{i,j} = z'_{i_1,j}$ для всех $\sigma + 1 \leqslant i_1 < i \leqslant n$, $i - \sigma + s + 1 \leqslant j \leqslant n$, т.е. $z'_{i,j} = z'_j$, $s+2 \leqslant j \leqslant n$, не зависит от $i$. Далее, применяя утверждение (g) (доказанное выше) и алгоритм редукции к целым коэффициентам, мы будем предполагать без ограничения общности, что линейные формы $L_0, \ldots, L_{s+1}, L_{s+2} - z'_{s+2}L_0, \ldots, L_n - z'_n L_0, L_{n+1}$ удовлетворяют дополнительно утверждениям из (a) и (b) (вместо $L_0, \ldots, L_{n+1}$; мы оставляем детали читателю). Заменяя $L_j$ на $L_j - z'_j L_0$, $s + 2 \leqslant j \leqslant n$, мы будем считать в дальнейшем, что $z'_j = 0$ для всех $s + 2 \leqslant j \leqslant n$. Положим $\overline{\lambda} = (L_0, \ldots, L_{n+1})$. Следовательно, теперь $\overline{\lambda}$ удовлетворяет утверждениям (a) и (b), и $\mu^{(i)}((1 : 0 : \ldots : 0))$ максимально возможное для всякого $\sigma + 1 \leqslant i \leqslant n + 1$.

Теперь мы собираемся доказать (d). Предположим, что дана точка $x \in \mathbb{P}^n(\overline{k'})$. Напомним, что сейчас $z' = (1 : 0 : \ldots : 0) \in \mathbb{P}^{n-\iota}(\overline{k'})$. Построим прямую $\mathfrak{l}_x \subset \mathbb{P}^{n-\iota}(\overline{k'})$, такую, что $z', \varphi_i(x) \in \mathfrak{l}_x$. Построим точку $z^* \in \mathfrak{l}_x(\overline{k'(\varepsilon_1)})$ (здесь $\varepsilon_1$ – бесконечно малая величина относительно поля $k'$), которая бесконечно близка к $\varphi_i(x)$. Далее построим при помощи алгоритмов из [8, 9] подмножество $S^* \subset \varphi_i^{-1}(z^*)$ всех точек, которые бесконечно близки к $x$.

Число $\mu^{(i)}(z^*) = \mu^{(i)}(z')$ максимально возможное. Отсюда немедленно вытекают следующие утверждения. Справедливо равенство $\varphi_i^{-1}(z^*) \setminus \mathcal{Z}(e_0, \ldots, e_r) = \varphi_i^{-1}(z^*) \cap (W_i(L') \cup W_i^{(3)}(L'))$. Для произвольной неприводимой компоненты $E$ многообразия $W_{i-1} \cap \mathcal{Z}(e'_i)$ имеем $x \in E$ тогда и только тогда, когда существует точка $x^* \in S^*$, такая, что $x^* \in E$. Кроме того, если $E \not\subset \mathcal{Z}(e_0, \dots, e_r)$, то $x^* \in E \setminus \mathcal{Z}(e_0, \dots, e_r)$. Далее, всякая точка $x^* \in S^*$ принадлежит только одной неприводимой компоненте $E$ многообразия $W_{i-1} \cap \mathcal{Z}(e'_i)$. Если $x^* \in E$ и $x^* \in E_1$ для некоторой неприводимой компоненты многообразия $W_{j-1} \cap \mathcal{Z}(e'_j)$ с $\sigma \leqslant j < i$, то $E \subset E_1$.

Теперь, очевидно,

- $x^* \in W_i^{(3)}(L')$ в том и только в том случае, если $x^* \notin W_i(L')$ и $x^* \notin \mathcal{Z}(e_0, \dots, e_r)$.

Следовательно, можно выяснить, верно ли, что $x \in W_i^{(3)}(L')$. Далее,

- $x^* \in W_i^{(1)}(L') \cup W_i^{(2)}(L')$ в том и только в том случае, если $x^* \in \mathcal{Z}(e_0, \dots, e_r)$.

Поэтому можно выяснить, верно ли, что $x \in W_i^{(1)}(L') \cup W_i^{(2)}(L')$. Поскольку $i$ – произвольное, то можно также выяснить для всякого $\sigma \leqslant j < i$, верно ли, что $x \in W_j^{(1)}(L') \cup W_j^{(2)}(L')$. Расширяя основное поле и заменяя $x$ на $x^*$, можно выяснить для всякого $x^* \in S^*$ и для всякого $\sigma \leqslant j < i$, верно ли, что $x^* \in W_j^{(1)}(L') \cup W_j^{(2)}(L')$. Заметим, что

- $x^* \in W_i^{(2)}(L')$ тогда и только тогда, когда $x^* \in W_i^{(1)}(L') \cup W_i^{(2)}(L')$ и $x^* \in W_j^{(1)}(L') \cup W_j^{(2)}(L')$ для некоторого $\sigma \leqslant j < i$,
- $x^* \in W_i^{(1)}(L')$ в том и только в том случае, если $x^* \in W_i^{(1)}(L') \cup W_i^{(2)}(L')$ и $x^* \notin W_j^{(1)}(L') \cup W_j^{(2)}(L')$ для всякого $\sigma \leqslant j < i$.

Таким образом, можно выяснить, верно ли, что $x$ является элементом $W_i(L')$, $W_i^{(1)}(L')$, $W_i^{(2)}(L')$, $W_i^{(3)}(L')$, $\sigma \leqslant i \leqslant n+1$.

**Замечание 6.** Пусть $E$ – произвольная неприводимая компонента многообразия $W_i^{(3)}(L')$, такая, что $x^* \in E$. Фактически описанная конструкция позволяет также выяснить, существует ли неприводимая компонента $E_1$ многообразия $W_j^{(3)}(L')$ с $\sigma + 1 \leqslant j < i$, такая что $E \subset E_1$.

Применяя описанный алгоритм к точкам из $\varphi_i^{-1}(z')$, мы вычислим $\deg W_i(L') = \#(\varphi_i^{-1}(z') \cap W_i(L'))$ и $\deg W_i^{(j)}(L') = \#(\varphi_i^{-1}(z') \cap W_i^{(j)}(L'))$ для $j = 1, 2, 3$. Алгоритм для утверждения (d) описан.

Утверждение (e) немедленно следует из (b), (c) и (d).

Докажем (f). Достаточно рассмотреть только случай, когда $E$ определена над $k'$ и неприводима над $\overline{k'}$, см. конец доказательства утверждения (b). Так что мы будем предполагать, что $E$ определена над $k'$. Пусть $\overline{\lambda}$ – элемент, построенный в утверждении (b). Построим однородные многочлены $e_i'', e_0'' \in k[X_0, \dots, X_n]$, такие, что $\deg e_i'' = \deg e_0'' = d'$ и

$$\#(W_{i-1}(L') \cap \mathcal{Z}(e_i'') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n) \setminus (\mathcal{Z}(e_{i+1}' \cup \overline{V \setminus W}) = \\ = \#(e_i''/e_0'')(W_{i-1}(L') \cap \mathcal{Z}(e_i'') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)) = D_{i-1}(L')d'.$$

Это может быть сделано непосредственно, но мы используем теорему 1 из [9]. Именно, пусть $m_0, \dots, m_\nu$, $\nu = \binom{n+d'}{n} - 1$, – все мономы от $X_0, \dots, X_n$ степени $d'$. Рассмотрим морфизм $\omega : W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n) \to \mathbb{P}^\nu(\overline{k})$, $(X_0, \dots, X_n) \to (m_0 : \dots : m_\nu)$, т.е. ограничение морфизма Веронезе степени $d'$ на $W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$. Мы строим $e_i'', e_0''$, применяя теорему 1 из [9] к $\widetilde{V}_{i-1} \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$, $W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n)$ и $\omega$ вместо $V$, $W$ и $p$ соответственно.

Положим $\widetilde{e}_i = e_i' + \varepsilon e_i''$, где $\varepsilon > 0$ является бесконечно малой величиной относительно поля $k'$. Расширим основное поле $k'$ до $k'(\varepsilon)$. Теперь определено отображение стандартной части $\mathrm{st}_\varepsilon : \mathbb{P}^n(\overline{k(\varepsilon)}) \to \mathbb{P}^n(\overline{k})$. По лемме 3 из [10] (её доказательство не зависит от результатов настоящей статьи) или непосредственно получаем, что множество $W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n) \cap \mathcal{Z}(\widetilde{e}_i)$ конечно в $\mathbb{P}^n(\overline{k(\varepsilon)})$. Применяя утверждение (b) над основным полем $k'(\varepsilon)$, мы строим все точки (с точностью до сопряжения над $k'(\varepsilon)$; можно вычислить число элементов каждого класса сопряжённых над $k'(\varepsilon)$ точек согласно (b), подробности см. в [8]) конечного множества $\widetilde{I} = W_{i-1}(L') \cap \mathcal{Z}(L_{\iota+1}, \dots, L_n) \cap \mathcal{Z}(\widetilde{e}_i) \subset \mathbb{P}^n(\overline{k(\varepsilon)})$. Обозначим через $\widetilde{I}_{y'}$ подмножество всех точек $y \in \widetilde{I}$, таких, что $\mathrm{st}_\varepsilon(y) = y'$, т.е. всех точек $y$, которые бесконечно близки к $y'$ относительно поля $k'$. Вычисляя стандартные части точек из $\widetilde{I}$, мы строим множество $\widetilde{I}_{y'}$ (снова точки из $\widetilde{I}_{y'}$ заданы с точностью до сопряжения над $k'(\varepsilon)$; напомним также, что стандартные части вычисляются при помощи разложений Ньютона–Пюизе, см. [12]) и число элементов $\#\widetilde{I}_{y'}$. Теперь утверждение (f) следует из следующей леммы.

**Лемма 8.** *Индекс пересечения $i(W_{i-1}(L'), \mathcal{Z}(e_i'); E)$ равен $\#\widetilde{I}_{y'}$.*

**Доказательство.** Обозначим для краткости $\mathcal{L} = \mathcal{Z}(L_{\imath+1}, \dots, L_n) \subset \mathbb{P}^n(\overline{k})$. Пересечение $W_{i-1}(L') \cap \mathcal{Z}(e'_i)$ и $\mathcal{L}$ трансверсально. Точка $y' \in E \cap \mathcal{L}$ является гладкой точкой $W_{i-1}(L') \cap \mathcal{L}$. Следовательно, существует только одна неприводимая над $\overline{k'}$ компонента $E'$ многообразия $W_{i-1}(L') \cap \mathcal{L}$, такая, что $y' \in E'$. Теперь, согласно свойству индексов пересечения, соответствующих ассоциативности пересечения,

$$\begin{aligned}
&i(W_{i-1}(L'), \mathcal{Z}(e'_i); E) = i(W_{i-1}(L'), \mathcal{Z}(e'_i); E) i(E, \mathcal{L}; y') = \\
&= i(E', \mathcal{Z}(e'_i); y') i(W_{i-1}, \mathcal{L}; E') = i(E', \mathcal{Z}(e'_i); y') = \\
&= i(W_{i-1}(L') \cap \mathcal{L}, \mathcal{Z}(e'_i); y').
\end{aligned}$$

Но $\widetilde{e}_i$ бесконечно близок к $e'_i$, и $\#(W_{i-1}(L') \cap \mathcal{L} \cap \mathcal{Z}(\widetilde{e}_i)) = D_{i-1}(L')d'$. Известно (см. например, [1]), что в этом случае $i(W_{i-1}(L') \cap \mathcal{L}, \mathcal{Z}(e'_i); y') = \#\widetilde{I}_{y'}$. $\square$

Утверждение (f) доказано. Наконец, утверждение (g) непосредственно следует из леммы 3. Требуемые оценки на время работы алгоритмов, построенных в этом разделе, немедленно следуют из оценок на время работы использованных алгоритмов. Теорема 1 доказана полностью. $\square$

## Литература


1. Д. Мамфорд, *Алгебраическая геометрия I. Комплексные проективные многообразия.* Мир, М. (1979).
2. Р. Хартсхорн, *Алгебраическая геометрия.* Мир, М. (1981).
3. А. Л. Чистов, *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время.* — Зап. научн. семинаров ЛОМИ **137** (1984), 124–188.
4. А. Л. Чистов, *Вычисление степеней алгебраических многообразий над полем нулевой характеристики за полиномиальное время и его приложения.* — Зап. научн. семин. ПОМИ **258** (1999), 7–59.
5. А. Л. Чистов, *Сильная версия основного разрешающего алгоритма для экзистенциональной теории первого порядка вещественно замкнутых полей.* — Зап. научн. семин. ПОМИ **256** (1999), 168–211.
6. А. Л. Чистов, *Эффективная конструкция локальных параметров неприводимых компонент алгебраического многообразия.* — Труды Санкт-Петербургского математического общества **7** (1999), 230–266.
7. А. Л. Чистов, *Эффективная гладкая стратификация алгебраического многообразия в нулевой характеристике и её приложения.* — Зап. научн. семин. ПОМИ **266** (2000), 254–311.

8. А. Л. Чистов, *Монодромия и критерии неприводимости с алгоритмическими приложениями в нулевой характеристическе.* — Зап. научн. семин. ПОМИ **292** (2002), 130–152.
9. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время. I.* — Зап. научн. семин. ПОМИ **307** (2004), 189–235.
10. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время. III.* — подготовлено к публикации.
11. J. Bochnak, M. Coste, M.-F. Roy, *Géométrie Algébrique Réelle*. Springer-Verlag, Berlin–Heidelberg–New York (1987).
12. A. L. Chistov, *Polynomial-time computation of the dimensions of components of algebraic varieties in zero-characteristic.* — J. Pure Applied Algebra **117, 118** (1997), 145–175.

Chistov A. L. Polynomial-time computation of the degree of a dominant morphism in zero characteristic. II.

Consider a projective algebraic variety $W$ which is an irreducible component of the set of all common zeros of a family of homogeneous polynomials of degrees less than $d$ in $n+1$ variables in zero characteristic. Consider a dominant rational morphism from $W$ to $W'$ given by homogeneous polynomials of degree $d'$. We suggest algorithms for constructing objects in general position related to this morphism. They generalize some algorithms from the first part of the paper to the case $\dim W > \dim W'$. These algorithms are deterministic and polynomial in $(dd')^n$ and the size of the input.

С.-Петербургский институт
информатики и автоматизации РАН
*E-mail*: labta@iias.spb.su or sliss@iias.spb.su

Поступило 12 июля 2005 г.