Записки научных
семинаров ПОМИ
Том 378, 2010 г.

А. Л. Чистов

АЛГОРИТМЫ ПОЛИНОМИАЛЬНОЙ СЛОЖНОСТИ ДЛЯ НОВОЙ МОДЕЛИ ПРЕДСТАВЛЕНИЯ АЛГЕБРАИЧЕСКИХ МНОГООБРАЗИЙ (В НУЛЕВОЙ ХАРАКТЕРИСТИКЕ)

Введение

Настоящая работа завершает цикл статей [13, 14, 3, 4, 5, 6, 7, 8] (исправление леммы 2 из работы [8] см. в [9]), [9, 10, 11, 12], где предлагаются полиномиальные алгоритмы для алгебраических многообразий в нулевой характеристике (мы не используем результатов из [12] в данной статье; однако частный случай этих результатов, содержащийся в [7], здесь необходим). Прежде чем формулировать наши результаты, мы опишем, как задать квазипроективное алгебраическое многообразие, используя системы представителей точек его неприводимых компонент. Модель представления алгебраических многообразий, предлагаемая здесь, слегка обобщает модель из [6], см. замечания ниже. В [6] описание алгоритмов для этого представления было отложено. Оно стало возможным только с использованием результатов ещё шести статей [4, 7, 8, 9, 10, 11]. Формулировки результатов данной статьи без доказательств были опубликованы как тезисы доклада на конференции, см. [15].

Пусть k – поле нулевой характеристики с алгебраическим замыканием $\overline{k}$. Пусть $X_0, X_1, \dots$ – независимые переменные над k. Обозначим через $\mathbb{P}^n(\overline{k})$, $n \geq 0$, 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 (структура определённого над k алгебраического многообразия на $\mathbb{P}^n(\overline{k})$ задаётся здесь, например, однородным кольцом $k[X_0, \dots, X_n]$, определённым 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

Ключевые слова: алгебраические многообразия, эффективные алгоритмы, гладкая стратификация, индексы пересечения.

нулей идеалов и многочленов с другими полями коэффициентов в аффинных и проективных пространствах (это будет видно из контекста).

Пусть W – квазипроективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$ и W определено над k. Тогда мы представляем его в виде

$$W = \bigcup_{1\le i\le b} W^{(i)} \setminus \bigcup_{b+1\le i\le a} W^{(i)}, \tag{1}$$

где $1 \le b \le a$ – целые числа и все $W^{(i)}$, $1 \le i \le a$, являются проективными алгебраическими многообразими в $\mathbb{P}^n(\overline{k})$, определёнными над k. Каждое алгебраическое многообразие $W^{(i)}$, $1 \le i \le a$, есть объединение некоторых неприводимых компонент многообразия $V^{(i)} = \mathcal{Z}(f_1^{(i)}, \dots, f_{m(i)}^{(i)}) \subset \mathbb{P}^n(\overline{k})$, где однородные многочлены $f_1^{(i)}, \dots, f_{m(i)}^{(i)} \in k[X_0, \dots, X_n]$ заданы, $m(i) \ge 1$. Для всякого $0 \le s \le n$ обозначим через $V^{(i,s)}$ (соответственно $W^{(i,s)}$) объединение всех неприводимых компонент размерности $n-s$ многообразия $\mathcal{Z}(f_1^{(i)}, \dots, f_{m(i)}^{(i)})$ (соответственно $W^{(i)}$). Тогда $W^{(i,s)}$ есть объединение некоторых неприводимых компонент многообразия $V^{(i,s)}$. Для всякого $0 \le s \le n$ задано такое семейство линейных форм $L_{s+1}^{(i,s)}, \dots, L_n^{(i,s)} \in k[X_0, \dots, X_n]$, что

$$\#V^{(i,s)} \cap \mathcal{Z}(L_{s+1}^{(i,s)}, \dots, L_n^{(i,s)}) < +\infty, \tag{2}$$

всякая точка $\xi \in V^{(i,s)} \cap \mathcal{Z}(L_{s+1}^{(i,s)}, \dots, L_n^{(i,s)})$ является гладкой точкой алгебраического многообразия $\mathcal{Z}(f_1^{(i)}, \dots, f_{m(i)}^{(i)})$ и пересечение касательных пространств в точке ξ многообразий $V_s^{(i)}$ и $\mathcal{Z}(L_{s+1}^{(i,s)}, \dots, L_n^{(i,s)})$ трансверсально, т.е.

$$T_{\xi, V_s^{(i)}} \cap \mathcal{Z}(L_{s+1}^{(i,s)}, \dots, L_n^{(i,s)}) = \{\xi\} \tag{3}$$

(мы рассматриваем касательное пространство $T_{\xi, V_s^{(i)}}$ как подпространство в $\mathbb{P}^n(\overline{k})$). Задано множество точек

$$\Xi^{(i,s)} = W^{(i,s)} \cap \mathcal{Z}(L_{s+1}^{(i,s)}, \dots, L_n^{(i,s)}).$$

Каждая точка из $\Xi^{(i,s)}$ представлена в виде (11), см. ниже. Следовательно, справедливо следующее свойство. Пусть $\xi \in V^{(i,s)} \cap$

$\mathcal{Z}(L_{s+1}^{(i,s)}, \dots, L_n^{(i,s)})$ и E – однозначно определённая неприводимая над k компонента алгебраического многообразия $V^{(i,s)}$, такая, что $\xi \in E$. Тогда $\xi \in \Xi^{(i,s)}$ в том и только в том случае, если E является компонентой многообразия $W^{(i)}$. В дальнейшем, если не оговорено противное, мы предполагаем, что $\deg_{X_0,\dots,X_n} f_j^{(i)} < d$ для всех i, j.

Таким образом, формально предлагаемое в этой статье представление многообразия W является четвёркой

$$(f, L, \Xi, b), \tag{4}$$

где f – семейство многочленов

$$f_j^{(i)}, \quad 1 \le j \le m(i),\ 1 \le i \le a, \tag{5}$$

L – семейство линейных форм

$$L_w^{(i,s)}, \quad s+1 \le w \le n,\ 0 \le s \le n,\ 1 \le i \le a, \tag{6}$$

и Ξ – семейство конечных множество точек

$$\Xi^{(i,s)}, \quad 0 \le s \le n,\ 1 \le i \le a. \tag{7}$$

Обозначим также

$$\Xi^{(i)} = \bigcup_{0 \le s \le n} \Xi^{(i,s)}. \tag{8}$$

В [6] рассматривается только случай $b = 1$. В настоящей статье по сравнению с [6] мы заменяем нижний индекс s на верхний для того, чтобы избежать двусмысленности в обозначениях, когда рассматривается более одного алгебраического многообразия, см. ниже.

Заметим, что условия (2) и (3) всегда могут быть проверены при помощи алгоритмов из [3]; более подробное обсуждение см. во введении статьи [6]. Заметим также, что для заданной точки $y \in \mathbb{P}^n(\overline{k})$ можно выяснить, верно ли, что $y \in W^{(i,s)}$, используя алгоритмы из [3] и [2], см. введение из [6]. Таким образом, для заданной точки $y \in \mathbb{P}^n(\overline{k})$ можно выяснить, также за полиномиальное время, верно ли, что $y \in W^{(i)}$, $1 \le i \le a$, а также $y \in W$.

Пусть $W = \bigcup_{i \in I} W_i$ – разложение многообразия W в объединение определённых над k и неприводимых над k (соответственно неприводимых над $\overline{k}$) компонент и даны представления (4). Тогда, применяя

теорему 1 из [7] (или более сильную теорему 2 из [9]) и теорему 2 из [7], можно построить для всякого $i \in I$ представление $(f, L_i, \Xi_i, 1)$ неприводимой компоненты W_i (в случае, когда W_i неприводима над $\overline{k}$, мы строим минимальное поле определения k_i многообразия W_i, содержащее k, и заменяем основное поле k на k_i в представлении компоненты W_i, подробности см. в [7]). Время работы этого алгоритма полиномиально от d^n и длины записи входных данных, см. [7] (а также доказательство теоремы 1 ниже в частном случае $\nu = 1$).

Далее (см. теорему 3 ниже), пусть W_1, W_2 – два квазипроективных алгебраических многообразия, которые аналогичны W и заданы аналогичным образом (с той же самой оценкой d на степени многочленов). Тогда можно выяснить, верно ли, что $W_1 = W_2$, за полиномиальное время от d^n и длины записи входных данных. В [6] это доказано, только когда W_1 и W_2 – проективные алгебраические многообразия. Общий случай квазипроективных многообразий является трудным. Теорема 3 является следствием теоремы 2, в которой рассматривается более общая ситуация: многообразия W_1 и W_2 заменяются пересечениями конечного числа квазипроективных алгебраических многообразий.

Для доказательства теоремы 2 (и, следовательно, теоремы 3) нам требуется сначала описать алгоритм для построения пересечения ν квазипроективных многообразий, заданных в рассматриваемой модели, за время, полиномиальное от $d^{n\nu}$ и длины записи входных данных, см. теорему 1 ниже. Этот алгоритм использует редукцию к диагонали. Здесь следует применить теорему 1 из [9]. Последняя теорема имеет длинное доказательство. Она основывается на [8, 7, 4] и других наших статьях, см. [9]. Кроме того, в теореме 1 вычисляются индексы пересечения алгебраических многообразий, когда они определены. Заметим здесь, что на выходе алгоритма из теоремы 1 пересечение квазипроективных алгебраических многообразий не задано в рассматриваемой модели. Неприводимые компоненты пересечения не всегда могут быть заданы при помощи систем представителей точек неприводимых компонент некоторого многообразия $\mathcal{V}$ с хорошими оценками на степени задающих $\mathcal{V}$ полиномов. Всё же мы получаем на выходе алгоритма из теоремы 1 всю информацию о пересечении. Можно рассматривать представление пересечения алгебраических многообразий из утверждения (а) теоремы 1 как обобщение представления (4) на случай пересечения алгебраических многообразий, заданных в виде (4).

Обозначим $m = m(1)$ и $f_i = f_i^{(1)}$, $1 \le i \le m$. Пусть $V = \mathcal{Z}(f_1, \dots, f_m) \subset \mathbb{P}^n(\overline{k})$ – алгебраическое многообразие. Напомним определение из [6].

Определение 1. *Гладкое покрытие алгебраического многообразия V есть конечное семейство*

$$V_\alpha, \quad \alpha \in A, \tag{9}$$

гладких квазипроективных алгебраических многообразий $V_\alpha \subset \mathbb{P}^n(\overline{k})$, $\alpha \in A$, такое, что V представляется как объединение $V = \cup_{\alpha \in A} V_\alpha$. Далее мы требуем, чтобы все неприводимые компоненты V_α имели одну и ту же размерность (которая зависит только от α). Гладкая стратификация алгебраического многообразия V – это гладкое покрытие V_α, $\alpha \in A$, многообразия V, такое, что дополнительно для всяких двух индексов $\alpha_1, \alpha_2 \in A$ выполняется следующее условие: если $\alpha_1 \ne \alpha_2$, то $V_{\alpha_1} \cap V_{\alpha_2} = \varnothing$.

В этой статье мы предполагаем, что степень произвольного алгебраического многообразия равна сумме всех степеней его неприводимых компонент (различных размерностей). Степень квазипроективного алгебраического многообразия $\mathcal{V}$ по определению равна степени его замыкания в проективном пространстве.

В [6], используя конструкцию локальных параметров из [4], мы доказываем существование гладкого покрытия (соответственно гладкой стратификации) (9) алгебраического многообразия V с оценкой на степени стратов $2^{2^{n^C}} d^n$ и числом стратов $2^{2^{n^C}} d^n$ (соответственно числом стратов $2^{2^{n^C}} d^{n(n+1)/2}$) для некоторой абсолютной константы $0 < C \in \mathbb{R}$, см. теорему 2 из [6]. Конструкции из [6] являются вполне явными. Оказывается, что достаточно дополнительно использовать только теорему 1 и теорему 2 (последнюю лишь в случае $(\nu, \nu_1) = (3, 2)$) для того, чтобы получить алгоритмы для построения гладкого покрытия и гладкой стратификации из теоремы 2 статьи [6] со временем работы полиномиальным от $2^{2^{n^C}} d^{n^2}$ и длины записи входных данных, см. теорему 4 ниже.

Теперь мы переходим к точным формулировкам. Пусть целые числа a, b, $m(i)$, $1 \le i \le b$, однородные многочлены $f_j^{(i)} \in k[X_0, \dots, X_n]$, $1 \le j \le m(i)$, $1 \le i \le a$, алгебраические многообразия $V^{(i)}$, $W^{(i)}$, и W – такие же, как и выше.

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

$$\begin{gathered} \deg_{X_0,\dots,X_n}(f_j^{(i)}) < d,\ \deg_{t_\gamma}(f_j^{(i)}) < d_2,\ \mathrm{l}(f_j^{(i)}) < M, \\ \deg_Z(F) < d_1,\ \deg_{t_\gamma}(F) < d_1,\ \mathrm{l}(F) < M_1, \end{gathered} \tag{10}$$

для всех $1 \le j \le m(i)$, $1 \le i \le a$, $1 \le \gamma \le l$. Размер (или длина записи) $\mathrm{L}(f)$ многочлена f определяется как произведение $\mathrm{l}(f)$ на число всех целых коэффициентов многочлена f в плотном представлении. Имеем

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

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

Замечание 1. В дальнейшем, если не оговорено противное, мы будем считать, что l фиксировано. Время работы алгоритмов из теорем 1 и 2 (см. ниже) является по существу тем же самым, что и при решении систем полиномиальных уравнений с конечным множеством корней в проективном пространстве. Также и алгоритмы для теоремы 4 сводятся к решению таких систем. Поэтому все эти теоремы могут быть сформулированы и в случае, когда l не является фиксированным, см. [2]. Заметим, что константы $O(\dots)$ (см. теоремы 1, 2 и

4 ниже) 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 $0 \leq i_0 \leq n$, такой, что $X_{i_0}(z) \neq 0$, и задан изоморфизм полей

$$k(z) = k((X_1/X_{i_0})(z), \ldots, (X_n/X_{i_0})(z)) \simeq k[\eta] = k[Z]/(\Phi), \qquad (11)$$

причём $\sum\limits_{0 \leq i \leq n} c_i (X_i/X_{i_0})(z) \mapsto \eta$ под действием изоморфизма (11), коэффициенты $c_i \in \mathbb{Z}$ заданы, и $\Phi \in k[Z]$ – минимальный многочлен элемента η над k со старшим коэффициентом $\mathrm{lc}_Z\, \Phi = 1$. Таким образом, точка z определена с точностью до сопряжения над k. Более точно, представление (11) 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 $\deg_{t_\alpha} g$, $1 \leq \alpha \leq l$, 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 как $\mathrm{L}(\Phi) + \sum\limits_{0 \leq i \leq n} \mathrm{L}(X_i/X_{i_0})$. Пусть теперь Ξ – произвольное конечное множество точек, определённое над k, и всякая точка из Ξ задана в виде (11). Тогда Ξ задает нульмерное алгебраическое многообразие, определённое над k. Положим длину записи $\mathrm{L}(\Xi)$ множества Ξ равной сумме длин записи его неприводимых над k компонент.

Напомним, что в [10] мы даём определение трансверсальности пересечения алгебраических многообразий. Теперь мы дадим аналогичное естественное определение, относящееся к собственным пересечениям. Пусть $W_1, \ldots, W_\nu \subset \mathbb{P}^n(\overline{k})$, $\nu \geq 1$, суть ν квазипроективных алгебраических многообразий, определённых над k. Пусть E – произвольная определённая над k и неприводимая над k компонента многообразия $W_1 \cap \ldots \cap W_\nu$. Мы будем говорить, что пересечение $W_1 \cap \ldots \cap W_\nu$ собственно в E (в объемлющем пространстве $\mathbb{P}^n(\overline{k})$), в том и только в том случае, если для всяких определённых над k и неприводимых над k компонент E_i, $1 \leq i \leq \nu$, многообразий W_i, таких, что $E_i \supset W$, справедливо равенство $\sum\limits_{1 \leq i \leq \nu} (n - \dim E_i) = n - \dim E$ (и, следовательно,

$\dim E_i$ зависит только от i). Пересечение многообразий $W_1, \dots, W_\nu$ собственно (в объемлющем пространстве $\mathbb{P}^n(\overline{k})$) тогда и только тогда, когда оно собственно во всякой его определённой над k и неприводимой над k компоненте.

Если $\nu = 2$, то $i(W_1, W_2; E) = i(W_1, W_2; E')$, где E' – произвольная неприводимая над $\overline{k}$ компонента многообразия E и индекс пересечения $i(W_1, W_2; E')$ определяется обычным образом (см., например, [1]).

Для произвольного $\nu > 2$ мы определяем индекс пересечения $i(W_1, \dots, W_\nu; E)$ алгебраических многообразий $W_1, \dots, W_\nu$ в E рекурсивно формулой

$$i(W_1, \dots, W_\nu; E) = \sum_{E''} i(W_1, \dots, W_{\nu-1}; E'') i(E'', W_\nu; E),$$

где E'' пробегает все неприводимые над k компоненты многообразия $W_1 \cap \dots \cap W_{\nu-1}$, такие, что $E'' \supset E$. Для $\nu = 1$ естественно положить $i(W_1; E) = 1$.

Здесь все индексы пересечения рассматриваются в $\mathbb{P}^n(\overline{k})$. Чтобы уточнить это, мы обозначаем

$$i_{\mathbb{P}^n(\overline{k})}(W_1, \dots, W_\nu; E) = i(W_1, \dots, W_\nu; E).$$

Предположим, что все W_j, $1 \le j \le \nu$, являются подмногообразиями аффинного пространства $\mathbb{A}^n(\overline{k})$. Можно отождествить $\mathbb{A}^n(\overline{k})$ с $\mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(X_0)$. В этом случае мы будем обозначать также $i_{\mathbb{A}^n(\overline{k})}(W_1, \dots, W_\nu; E) = i(W_1, \dots, W_\nu; E)$, когда последний индекс пересечения определён.

Мы используем редукцию к диагонали для индексов пересечения. Именно, пусть $\nu \ge 1$ – целое число. Отождествим аффинное пространство $\mathbb{A}^{n\nu}(\overline{k})$ с $(\mathbb{A}^n(\overline{k}))^\nu$. Положим $\Delta = \{(x, x, \dots, x) \in \mathbb{A}^{n\nu}(\overline{k}) : x \in \mathbb{A}^n(\overline{k})\}$ равным диагональному подмногообразию. Теперь мы используем отождествление

$$\mathbb{A}^n(\overline{k}) = (\mathbb{A}^n(\overline{k}))^\nu \cap \Delta. \tag{12}$$

Пусть $W_1, \dots, W_\nu$ – аффинные алгебраические многообразия в $\mathbb{A}^n(\overline{k})$ и E – определённая над k и неприводимая над k компонента многообразия $W_1 \cap \dots \cap W_\nu$, такая, что последнее пересечение собственно в E. Тогда согласно отождествению (12) многообразие E является

определённой над k и неприводимой над k компонентой многообразия $(W_1 \times \ldots \times W_\nu) \cap \Delta$. Очевидно, что последнее пересечение собственно в E. Мы имеем

$$i_{\mathbb{A}^n(\overline{k})}(W_1, \ldots, W_\nu; E) = i_{\mathbb{A}^{n\nu}(\overline{k})}(W_1 \times \ldots \times W_\nu, \Delta; E). \qquad (13)$$

Эта формула редукции к диагонали хорошо известна для $\nu = 2$ (см., например, [1]). Для произвольного ν она доказывается индукцией по ν с использованием общих свойств индексов пересечения (эти общие свойства также могут быть найдены в [1]; мы оставляем подробности читателю).

Пусть $\nu \geq 1$ – целое число. Для всякого целого числа $1 \leq \alpha \leq \nu$ пусть $m_\alpha(i), a_\alpha, b_\alpha, f^{(i)}_{\alpha,j}, W_\alpha, W^{(i)}_\alpha, V^{(i)}_\alpha, W^{(i)}_\alpha, V^{(i,s)}_\alpha, W^{(i,s)}_\alpha, L^{(i,s)}_{\alpha,\beta}, \Xi^{(i,s)}_\alpha$, $(f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha) = \rho_\alpha$ аналогичны введённым выше объектам $m(i)$, a, b, $f^{(i)}_j$, W, $W^{(i)}$, $V^{(i)}$, $W^{(i)}$, $V^{(i,s)}$, $W^{(i,s)}$, $L^{(i,s)}_\beta$, $\Xi^{(i,s)}$, $(f, L, \Xi, b) = \rho$ соответственно. В дальнейшем в этой статье мы предполагаем, что выполняются неравенства (10) с $f^{(i)}_{\alpha,j}$ вместо $f^{(i)}_j$ для всякого $1 \leq \alpha \leq \nu$.

Теорема 1. *Предположим, что для всякого $1 \leq \alpha \leq \nu$ дано представление $(f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha)$ квазипроективного алгебраического многообразия W_α. Тогда можно построить линейные формы $L_0, \ldots, L_{n+1} \in k[X_0, \ldots, X_n]$ с целыми коэффициентами с длиной записи $O(n\nu \log d + \sum_{1 \leq i \leq \nu} \log b_i + \log(\sum_{1 \leq i \leq \nu} a_i))$, конечное множество индексов J и для всякого $j \in J$ конечное множество Ξ_j точек из $W_1 \cap \ldots \cap W_\nu$ (каждая точка представляется в виде (11)), такие, что справедливы следующие утверждения.*

(a) *Для всякого $j \in J$ существует единственная определённая над k и неприводимая над k компонента многообразия $W_1 \cap \ldots \cap W_\nu$ (обозначим её через E_j), такая, что $\dim E_j = n - s(j)$ и $\Xi_j = E_j \cap \mathcal{Z}(L_{s(j)+1}, \ldots, L_n)$ в $\mathbb{P}^n(\overline{k})$. Обратно, для всякого определённой над k и и неприводимой над k компоненты E' многообразия $W_1 \cap \ldots \cap W_\nu$ существует такое $j' \in J$, что $E' = E_{j'}$. Следовательно, $W_1 \cap \ldots \cap W_\nu = \bigcup_{j \in J} E_j$ – разложение многообразия $W_1 \cap \ldots \cap W_\nu$ на неприводимые над k компоненты. Пусть $\overline{E}_j$ – замыкание многообразия E_j относительно топологии Зариского в $\mathbb{P}^n(\overline{k})$. Тогда для всякого $j \in J$ имеем*

$$\Xi_j \cap \mathcal{Z}(L_0) = \varnothing, \quad \#\Xi_j = \#(L_{n+1}/L_0)(\Xi_j) = \deg \overline{E}_j \qquad (14)$$

(*здесь и ниже* $\#(.)$ *обозначает число элементов множества*), *и все точки из* Ξ_j *являются гладкими точками многообразия* $W_1 \cap \ldots \cap W_\nu$. *Кроме того,*

$$E_j = \overline{E}_j \setminus \Big(\bigcup_{1 \le \alpha \le \nu} \bigcup_{b_\alpha + 1 \le i \le a_\alpha} W_\alpha^{(i)} \Big).$$

(b) *Если пересечение многообразий* $W_1, \ldots, W_\nu$ *собственно в* E_j, *то можно вычислить индекс пересечения* $i_{\mathbb{P}^n(\overline{k})}(W_1, \ldots, W_\nu; E_j)$ *и для всякой точки* $\xi \in \Xi_j$ *справедливо равенство* $i_{\mathbb{P}^n(\overline{k})}(W_1, \ldots, W_\nu; E_j) = i_{\mathbb{P}^n(\overline{k})}(W_1, \ldots, W_\nu, \mathcal{Z}(L_{s(j)+1}, \ldots, L_n); \xi)$.

(c) *Для произвольной точки* $z \in \mathbb{P}^n(\overline{k})$ (*заданной в виде* (11)) *можно выяснить, верно ли, что* $z \in E_j$, *и, более того, вычислить кратность* $\mu(z, E_j)$ *точки* z *на* E_j.

(d) *Отождествим множество всех наборов, каждый из которых состоит из* $(n+2)$ *линейных форм, принадлежащих* $\overline{k}[X_0, \ldots, X_n]$, *с* $\mathbb{A}^{(n+1)(n+2)}(\overline{k})$. *Для всякого* $j \in J$ *и произвольного* $\lambda^* = (L_0^*, \ldots, L_{n+1}^*)$, *где все* $L_j^* \in \overline{k}[X_0, \ldots, X_n]$ *– линейные формы, положим* $\Xi_j^* = E_j \cap \mathcal{Z}(L_{s(j)+1}, \ldots, L_n) \subset \mathbb{P}^n(\overline{k})$. *Пусть* $\mathfrak{l} \in \mathbb{A}^{(n+1)(n+2)}(\overline{k})$ *– прямая, определённая над* k', *такая, что* $\overline{\lambda} = (L_0, \ldots, L_{n+1}) \in \mathfrak{l}$. *Тогда для всех* $\lambda^* \in \mathfrak{l}(k')$ *(здесь* $\mathfrak{l}(k')$ *– множество всех* k'*-точек прямой* $\mathfrak{l}$*) за исключением не более чем полиномиального от* $d^{n\nu}(\sum_{1 \le i \le \nu} a_i) \prod_{1 \le \alpha \le \nu} b_\alpha$ *числа утверждение* (a) *выполняется с* λ^*, Ξ_j^*, $j \in J$, *вместо* $\overline{\lambda}, \Xi_j$, $j \in J$. *Для всякого элемента* $\lambda^* \in \mathfrak{l}(k')$ *можно выяснить, справедливо ли утверждение* (a) *с* λ^*, Ξ_j^*, $j \in J$, *вместо* $\overline{\lambda}, \Xi_j$, $j \in J$.

Время работы алгоритма для построения линейных форм $L_0, \ldots, L_n$ *и семейства конечных множеств* Ξ_j, $j \in J$, *удовлетворяющих условию* (a), *а также алгоритма из утверждения* (b) *полиномиально от* $d^{n\nu}$, $\prod_{1 \le \alpha \le \nu} b_\alpha$ *и суммы длин записи* $\sum_{1 \le \alpha \le \nu} \mathrm{L}((f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha))$. *Более точно, это время работы полиномиально от* $d^{n\nu}$, $\prod_{1 \le \alpha \le \nu} b_\alpha$, $\sum_{1 \le \alpha \le \nu} a_\alpha$, M, M_1, d_1, d_2, $\sum_{1 \le \alpha \le \nu,\ 1 \le i \le a_\alpha} m(\alpha, i)$ *и*

$$\sum_{0 \le s \le n,\ 1 \le \alpha \le \nu,\ 1 \le i \le a_\alpha} \mathrm{L}(\Xi_\alpha^{(i,s)}), \qquad \sum_{0 \le s \le n,\ s+1 \le w \le n,\ 1 \le \alpha \le \nu,\ 1 \le i \le a_\alpha} \mathrm{L}(L_{\alpha,w}^{(i,s)}).$$

Время работы алгоритма из п. (c) *(соответственно* (d)*) полиномиально от тех же самых величин и длины записи* $\mathrm{L}(z)$ *точки* z *(соответственно длины записи* $\mathrm{L}(\lambda^*)$ *элемента* λ^**).*

Теорема 2. *Предположим, что выполняются условия теоремы* 1, *т.е. для всякого* $1 \le \alpha \le \nu$ *задано представление* $(f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha)$ *квазипроективного алгебраического многообразия* W_α. *Пусть* ν_1 – *целое число, такое, что* $1 \le \nu_1 \le \nu$. *Тогда можно построить линейные формы* $L_0, \dots, L_{n+1} \in k[X_0, \dots, X_n]$ *с целыми коэффициентами с длиной записи* $O(n\nu \log d + \sum_{1\le i\le \nu} \log b_i + \log(\sum_{1\le i\le \nu} a_i))$, *конечное множество индексов* $J^{(1)}$ *(соответственно* $J^{(2)}$*) и для всякого* $j \in J^{(1)}$ *(соответственно* $j \in J^{(2)}$*) конечное множество* Ξ_j *точек из* $W_1 \cap \dots \cap W_{\nu_1}$ *(соответственно* $W_{\nu_1+1} \cap \dots \cap W_\nu$*), такие, что справедливы следующие утверждения.*

(a) *Для всякого* $j \in J^{(1)}$ *(соответственно* $j \in J^{(2)}$*) существует единственная определённая над* k *и неприводимая над* k *компонента* E *многообразия* $W_1 \cap \dots \cap W_{\nu_1}$ *(соответственно* $W_{\nu_1+1} \cap \dots \cap W_\nu$*), такая, что* $\dim E = n - s(j)$ *и* $\Xi_j = E \cap \mathcal{Z}(L_{s(j)+1}, \dots, L_n)$ *в* $\mathbb{P}^n(\overline{k})$. *Обозначим* $E = E_j$. *Обратно, для всякой определённой над* k *и неприводимой над* k *компоненты* E' *многообразия* $W_1 \cap \dots \cap W_{\nu_1}$ *(соответственно* $W_{\nu_1+1} \cap \dots \cap W_\nu$*) существует такой индекс* $j' \in J^{(1)}$ *(соответственно* $j' \in J^{(2)}$*), что* $E' = E_{j'}$. *Следовательно,*

$$W_1 \cap \dots \cap W_{\nu_1} = \bigcup_{j\in J^{(1)}} E_j, \quad W_{\nu_1+1} \cap \dots \cap W_\nu = \bigcup_{j\in J^{(2)}} E_j$$

являются разложениями многообразий $W_1 \cap \dots \cap W_{\nu_1}$ *и* $W_{\nu_1+1} \cap \dots \cap W_\nu$ *в объединение неприводимых над* k *компонент. Пусть* $\overline{E}_j$ – *замыкание многообразия* E_j *относительно топологии Зариского в* $\mathbb{P}^n(\overline{k})$. *Тогда для всякого* $j \in J^{(1)}$ *(соответственно* $j \in J^{(2)}$*) имеем*

$$\Xi_j \cap \mathcal{Z}(L_0) = \varnothing, \quad \#\Xi_j = \#(L_{n+1}/L_0)(\Xi_j) = \deg \overline{E}_j, \tag{15}$$

и все точки множества Ξ_j *являются гладкими точками многообразия* $W_1 \cap \dots \cap W_{\nu_1}$ *(соответственно* $W_{\nu_1+1} \cap \dots \cap W_\nu$*). Положим* $A^{(1)} = \{1, \dots, \nu_1\}$, $A^{(2)} = \{\nu_1 + 1, \dots, \nu\}$. *Тогда для всякого* $j \in J^{(i)}$, $i = 1, 2$, *имеем*

$$E_j = \overline{E}_j \setminus \Big(\bigcup_{\alpha\in A^{(i)}} \bigcup_{b_\alpha+1\le i\le a_\alpha} W_\alpha^{(i)} \Big).$$

(b) *Для всяких* $j_1 \in J^{(1)}$ *и* $j_2 \in J^{(2)}$ *можно выяснить, верно ли, что* $E_{j_1} \subset \overline{E}_{j_2}$. *Более точно, для построенных линейных форм*

$L_0, \dots, L_{n+1}$ включение $E_{j_1} \subset \overline{E}_{j_2}$ справедливо в том и только в том случае, если $\Xi_{j_1} \subset \overline{E}_{j_2}$.

(c) *Для всяких $j_1 \in J^{(1)}$ и $j_2 \in J^{(2)}$ можно выяснить, верно ли, что $E_{j_1} \subset E_{j_2}$.*

Время работы каждого из алгоритмов из этой теоремы полиномиально от $d^{n\nu}$, $\prod_{1\le\alpha\le\nu} b_\alpha$ и суммы длин записи $\sum\limits_{1\le\alpha\le\nu} \mathrm{L}((f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha))$. Более точно, рассматриваемое время работы полиномиально от $d^{n\nu}$, $\prod_{1\le\alpha\le\nu} b_\alpha$, $\sum\limits_{1\le\alpha\le\nu} a_\alpha$, M, M_1, d_1, d_2, $\sum\limits_{1\le\alpha\le\nu,\ 1\le i\le a_\alpha} m(\alpha, i)$ и

$$\sum_{0\le s\le n,\ 1\le\alpha\le\nu,\ 1\le i\le a_\alpha} \mathrm{L}(\Xi_\alpha^{(i,s)}), \qquad \sum_{0\le s\le n,\ s+1\le w\le n,\ 1\le\alpha\le\nu,\ 1\le i\le a_\alpha} \mathrm{L}(L_{\alpha,w}^{(i,s)}).$$

Как немедленное следствие теоремы 2, мы получаем следующий результат.

Теорема 3. *Предположим, что даны представления $(f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha)$, $\alpha = 1, 2$, двух квазипроективных алгебраических многообразий W_α. Тогда можно выяснить, верно ли, что $W_1 \subset W_2$. Следовательно, можно выяснить также, верно ли, что $W_2 \subset W_1$, и верно ли, что $W_1 = W_2$. Время работы этого алгоритма полиномиально от d^n и длин записи $\mathrm{L}((f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha))$ данных представлений многообразий W_α, $\alpha = 1, 2$.*

Доказательство. Действительно, по теореме 2 можно узнать, выполняется ли включение $W_1 \subset W_2$ (соответственно $W_2 \subset W_1$). Теорема доказана (по модулю теоремы 2). □

Теорема 4. *Можно построить такое гладкое покрытие (соответственно гладкую стратификацию) V_α, $\alpha \in A$, алгебраического многообразия V, что всякое квазипроективное алгебраическое многообразие V_α определено над k, неприводимо над k и представлено в описанном выше виде. Пусть $\dim V_\alpha = n - s$, где $0 \le s \le n$, и $s = s(\alpha)$ зависит от α. Пусть (4) – построенное представление многообразия V_α (оно зависит от α). Обозначим $h_{\alpha,j} = f_j^{(1)}$, $1 \le j \le m(1)$, и $\Delta_\alpha = f_1^{(2)}$, если $a \ge 2$, см. (5). Тогда построенное представление многообразия V_α удовлетворяет следующим свойствам.*

(i) *В случае гладкого покрытия $a = 2$, если $s < n$, и $a = 1$, если $s = n$. В случае гладкой стратификации $a \le 2^{2^{n^C}} d^{n(n+1)/2}$, где $0 < C \in \mathbb{R}$ – абсолютная константа.*

(ii) *Имеем* $m(1) = s$, *а если* $a \geq 2$, *то* $m(2) = 1$. *Следовательно, если* $a \geq 2$, *то* V_α *является неприводимой компонентой алгебраического многообразия* $\mathcal{Z}(h_{\alpha,1}, \ldots, h_{\alpha,s}) \setminus \mathcal{Z}(\Delta_\alpha)$ *в случае гладкого покрытия (соответственно открытым в топологии Зариского подмножеством последнего алгебраического многообразия в случае гладкой стратификации).*

(iii) *Существуют такие линейно независимые линейные формы* $Y_0, \ldots, Y_n \in k[X_0, \ldots, X_n]$, *что* $X_i = \sum\limits_{0 \leq j \leq n} x_{i,j} Y_j$, *все коэффициенты* $x_{i,j}$ *лежат в* k, *все* $x_{i,j}$ *являются целыми числами с длинами записи* $O(2^{n^C} + n \log d)$, *где* $0 < C \in \mathbb{R}$ *– абсолютная константа, и*

$$\Delta_\alpha = \det(\partial h_{\alpha,i}/\partial Y_j)_{1 \leq i,j \leq s} = \det(\sum_{0 \leq v \leq n} x_{v,j} \partial h_{\alpha,i}/\partial X_v)_{1 \leq i,j \leq s}.$$

Следовательно, V_α *является гладким алгебраическим многообразием по теореме о неявной функции. Кроме того, в случае гладкого покрытия можно взять* $Y_i = X_{\sigma(i)}$ *для некоторой перестановки* σ *множества* $0, \ldots, n$.

(iv) *Длины записи целых коэффициентов линейных форм из семейства* L *равны* $O(2^{n^C} + n \log d)$, *где* $0 < C \in \mathbb{R}$ *– абсолютная константа.*

(v) *Для всех* $\alpha \in A$, $1 \leq j \leq s(\alpha)$, *степени* $\deg_{X_0,\ldots,X_n} h_{\alpha,j}$ *меньше* $n^{2^{s(\alpha)^C}} d$ *для абсолютной константы* $0 < C \in \mathbb{R}$. *В случае гладкой стратификации для всех* $i > 2$, j *степени* $\deg_{X_0,\ldots,X_n} f_j^{(i)}$ *меньше* $2^{2^{n^C}} d$.

(vi) *Для всех* $\alpha \in A$, $1 \leq j \leq s(\alpha)$, *длины записи коэффициентов многочленов* $h_{\alpha,j}$ *ограничены сверху полиномом от* $n^{2^{s(\alpha)^C}} d^{s(\alpha)n}$, d_1, d_2, M, M_1, m, *где* $0 < C \in \mathbb{R}$ *– абсолютная константа. В случае гладкой стратификации для всех* $i > 2$, j *длины записи коэффициентов многочленов* $f_j^{(i)}$ *ограничены сверху полиномом от* $2^{2^{n^C}} d^{n^2}$, d_1, d_2, M, M_1, m, *где* $0 < C \in \mathbb{R}$ *– абсолютная константа.*

(vii) *Число элементов* $\#A$ *множества* A *ограничено сверху величиной* $2^{2^{n^C}} d^n$ *в случае гладкого покрытия (соответственно* $2^{2^{n^C}} d^{n(n+1)/2}$ *в случае гладкой стратификации) для абсолютной константы* $0 < C \in \mathbb{R}$.

Время работы алгоритма для построения гладкого покрытия, а также гладкой стратификации полиномиально от $2^{2^{n^C}} d^{n^2}$, d_1, d_2, M, M_1, m, *где* $0 < C \in \mathbb{R}$ *– абсолютная константа.*

Доказательство. В теореме 2 работы [6] мы доказываем существование всех объектов из формулировки теоремы 2. При этом необходимо ещё одно исправление в формулировке этой теоремы: в оценках длин записи коэффициентов в пункте (vi) мы заменили d^n на $d^{s(\alpha)n}$ для гладкого покрытия (соответственно на d^{n^2} для гладкой стратификации), см. [16]. Теперь согласно разделам 2–5 из работ [6] и [16] достаточно использовать теоремы 1 и 2 настоящей статьи для того, чтобы получить алгоритмы для конструкций из доказательства теоремы 2 работы [6]. Более точно, используя теоремы 1 и 2, можно немедленно построить алгебраические многообразия, возникающие в доказательстве теоремы 2 из [6]. Мы оставляем читателю все подробности.

Требуемые оценки на время работы алгоритмов из теоремы 4 немедленно следуют из оценок на время работы использованных алгоритмов. Теорема доказана (по модулю теорем 1 и 2). □

1. Доказательство теоремы 1

Лемма 1. *Пусть V – проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$, такое, что все его неприводимые компоненты имеют одну и ту же размерность $n-s$, где $0 \le s \le n$. Пусть $L_0, \dots, L_{n+1} \in \overline{k}[X_0, \dots, X_n]$ – линейные формы. Обозначим $\Xi = V \cap \mathcal{Z}(L_{s+1}, \dots, L_n)$ в $\mathbb{P}^n(\overline{k})$. Предположим, что для $\overline{\lambda} = (L_0, \dots, L_{n+1})$ выполняется следующее условие:*

$$\mathcal{Z}(L_s) \cap \Xi = \varnothing. \tag{16}$$

Отождествим множество всех наборов, состоящих из $(n+2)$ линейных форм из $\overline{k}[X_0, \dots, X_n]$, с аффинным пространством $\mathbb{A}^{(n+1)(n+2)}(\overline{k})$. Пусть $\lambda^* = (L_0^*, \dots, L_{n+1}^*) \in \mathbb{A}^{(n+1)(n+2)}(\overline{k})$, где все $L_j^* \in \overline{k}[X_0, \dots, X_n]$ – линейные формы. Положим $\Xi^* = V \cap \mathcal{Z}(L_{s+1}, \dots, L_n) \subset \mathbb{P}^n(\overline{k})$. Пусть $\mathfrak{l} \in \mathbb{A}^{(n+1)(n+2)}(\overline{k})$ – такая прямая, что $\overline{\lambda} \in \mathfrak{l}$. Тогда для всех $\lambda^* \in \mathfrak{l}$ за исключением не более чем полиномиального от $2^{n-s+1} \deg V$ числа выполняется условие (16) *для λ^* вместо $\overline{\lambda}$, т.е. для L_s^*, Ξ^* вместо L_s, Ξ.*

Доказательство. Пусть $\overline{\lambda} \ne \lambda^{(1)} = (L_0^{(1)}, \dots, L_{n+1}^{(1)}) \in \mathfrak{l}$. Тогда из теоремы Безу следует, что для всех $t \in \overline{k}$ за исключением не более чем полиномиального от $2^{n-s+1} \deg V$ числа пересечение $V \cap \mathcal{Z}(L_j + tL_j^{(1)},\ s \le j \le n)$ непусто в $\mathbb{P}^n(\overline{k})$ (ср., например, доказательство леммы 16 в [10]). Лемма доказана. □

Далее, пусть $f_1, \dots, f_m$, V, W, s, σ, $x^{(0)}$, $e_0, \dots, e_r$, p, $\mathcal{U}_0'''$ – из формулировки теоремы 1 работы [9] и теоремы 1 работы [10], но сейчас мы не требуем, чтобы $\dim(W \cap \mathcal{Z}(e_0, \dots, e_r)) < \dim W$.

Заметим, что условие $\dim(W \cap \mathcal{Z}(e_0, \dots, e_r)) = \dim W$ эквивалентно тому, что $W \subset \mathcal{Z}(e_0, \dots, e_r)$. В этом случае $\sigma = n+1$ и $p : \varnothing \to \mathbb{P}^r(\overline{k})$ – тривиальный морфизм. Очевидно, можно выяснить (непосредственно или при помощи теорем 1 и 2 из [7]), верно ли, что $W \subset \mathcal{Z}(e_0, \dots, e_r)$.

Пусть $L'_w \in \overline{k}[X_0, \dots, X_r]$, $w \in \{0, \sigma+1, \dots, n\}$, – семейство линейных форм. Пусть $L'_{n+1} = L'_0$. Положим $L' = (L'_0, L'_{\sigma+1}, \dots, L'_n)$.

Напомним, что в [9] для V, W, p для всякого $\sigma \le i \le n+1$ определены алгебраические многообразия $W_i(L') = W(L'_{\sigma+1}, \dots, L'_i)$, $W_i^{(\beta)}(L') = W^{(\beta)}(L'_{\sigma+1}, \dots, L'_i)$, $\beta = 1, 2, 3$ (для $i = \sigma$ они не зависят от L').

Если $W \subset \mathcal{Z}(e_0, \dots, e_r)$, то по определению $\mathcal{U}'_0 = \mathcal{U}''_0 = \mathcal{U}'''_0$ является множеством, состоящим из одного элемента $L' = ()$, и $W_{n+1}(L') = \varnothing$, $W_{n+1}^{(1)}(L') = W$, $W_{n+1}^{(2)}(L') = \varnothing$, $W_{n+1}^{(3)}(L') = \varnothing$.

Положим $\widetilde{e}_i = e'_i = L'_i(e_0, \dots, e_r)$, $i \in \{\sigma+1, \dots, n+1\}$ (ср. введение из [9]). Для удобства обозначений положим $\widetilde{e}_\sigma = e'_\sigma = 0$, многообразие $W_{\sigma-1}(L') = W$. Следовательно, теперь $W = W_{\sigma-1}(L') \cap \mathcal{Z}(\widetilde{e}_\sigma)$. Поэтому

$$W_{i-1}(L') \cap \mathcal{Z}(\widetilde{e}_i) = W_i(L') \cup W_i^{(1)}(L') \cup W_i^{(2)}(L') \cup W_i^{(3)}(L'),\ \sigma \le i \le n+1. \tag{17}$$

Если $i \ge \sigma+1$ и $W \not\subset \mathcal{Z}(e_0, \dots, e_r)$, равенство (17) следует из введения статьи [9].

Утверждения (a) и (b) теоремы 1 из [9] упрощаются, когда $W \subset \mathcal{Z}(e_0, \dots, e_r)$. Именно, пусть $\overline{\lambda} = (L_0, \dots, L_{n+1})$, где все $L_w \in k[X_0, \dots, X_n]$ – линейные формы. *Если $W \subset \mathcal{Z}(e_0, \dots, e_r)$, то по определению мы будем говорить, что утверждения* (a) *и* (b) *теоремы 1 из* [9] *справедливы для (V, W и) $\overline{\lambda}$ в том и только в том случае, если $\overline{\lambda}$ удовлетворяет утверждению теоремы 2 из* [9] *для V*. Если $W \subset \mathcal{Z}(e_0, \dots, e_r)$, то можно построить $\overline{\lambda}$, удовлетворяющее утверждениям (a) и (b) теоремы 1 из [9], при помощи теоремы 2 из [9]. Очевидно, если $W \subset \mathcal{Z}(e_0, \dots, e_r)$, то утверждение (g) теоремы 1 из [9] остаётся верным (его доказательство только упрощается).

Пусть теперь $N > 0$ – целое число. Предположим, что $f_1^{(j)}, \dots, f_{m(j)}^{(j)} \in k[X_0, \dots, X_n]$, $V^{(j)}$, $W^{(j)}$, $s(j)$, $\sigma(j)$, $x^{(0,j)}$, $e_0^{(j)}, \dots, e_r^{(j)}$, $p^{(j)}$, $\mathcal{U}'''_{j,0}$ для всякого $1 \le j \le N$ аналогичны рассматриваемым $f_1, \dots, f_m$, V, W, s, σ, $x^{(0)}$, $e_0, \dots, e_r$, p, $\mathcal{U}'''_0$. Следовательно, мы не исключаем, что

$W^{(j)} \subset \mathcal{Z}(e_0^{(j)}, \dots, e_r^{(j)})$ для некоторых j.

Пусть $f_1^{(j)}, \dots, f_{m(j)}^{(j)}$, $0 \le j \le N$, удовлетворяют тем же самым оценкам на степени и длины записи коэффициентов, что и $f_1, \dots, f_m$ из теоремы 1 работы [9]. Предположим, что $e_\alpha^{(j)} = e_\alpha$, $0 \le \alpha \le r$, одни и те же для всех $1 \le j \le N$. Далее, предположим, что если $e_\alpha \ne 0$, то

$$\deg_{X_0,\dots,X_n}(e_\alpha) = d',\ \deg_{t_\gamma}(e_\alpha) < d_2',\ \mathrm{l}(e_\alpha) < M'$$

для всех $1 \le \gamma \le l$, $0 \le \alpha \le r$, т.е. $e_0, \dots, e_r$ удовлетворяют оценкам на степени и длины записи коэффициентов из формулировки теоремы 1 работы [9].

В определениях многообразий $W(L'_{\sigma+1}, \dots, L'_i)$, $W^{(\beta)}(L'_{\sigma+1}, \dots, L'_i)$, $\beta = 1,2,3$, $\sigma \le i \le n+1$, заменим тройку (V, W, p) на $(V^{(j)}, W^{(j)}, p^{(j)})$ (следовательно, σ заменяется на $\sigma(j)$; и $L'_{\sigma(j)+1}, \dots, L'_{n+1} \in \overline{k}[X_0, \dots, X_r]$ являются линейными формами, $L'_{n+1} = L'_0$). Обозначим полученные многообразия через $W^{(j)}(L'_{\sigma(j)+1}, \dots, L'_i)$, $W^{(j,\beta)}(L'_{\sigma(j)+1}, \dots, L'_i)$, $\beta = 1,2,3$, $\sigma(j) \le i \le n+1$, соответственно (поскольку в дальнейшем мы не будем использовать V, W, p, первое обозначение $W^{(j)}(L'_{\sigma(j)+1}, \dots, L'_i)$ не приведёт к двусмысленности для $j \le 3$).

Положим $e'_{j,i} = \widetilde{e}_i = L'_i(e_0, \dots, e_r)$ для всех $i \in \{\sigma(j)+1, \dots, n+1\}$, $1 \le j \le N$. Для удобства обозначений положим $e'_{j,\sigma(j)} = 0$ для всякого $1 \le j \le N$. Следовательно, теперь условие (17) выполняется для $V^{(j)}, W^{(j)}, p^{(j)}$ вместо V, W, p. (заметим, что здесь $e'_{j,i}$ соответствует $\widetilde{e}_i$). Определим $\iota = \iota(j,i) = i - \sigma(j) + s(j)$.

Положим $\sigma = \min\{\sigma(j) : 1 \le j \le N\}$ (в дальнейшем мы не будем использовать старое σ, определённое для V, W, p, L', и, следовательно, это новое определение числа σ не приведёт к двусмысленности). Положим $L' = (L'_0, L'_{\sigma+1}, \dots, L'_n)$. Далее, обозначим для краткости $W_i^{(j)}(L') = W^{(j)}(L'_{\sigma(j)+1}, \dots, L'_i)$ и $W_i^{(j,\beta)}(L') = W^{(j,\beta)}(L'_{\sigma(j)+1}, \dots, L'_i)$ для всех $\beta = 1,2,3$, $\sigma(j) \le i \le n+1$.

Лемма 2. *При рассматриваемых предположениях на $V^{(j)}$, $W^{(j)}$, $p^{(j)}$, $1 \le j \le N$, можно вычислить элемент $L' = (L'_0, L'_{\sigma+1}, \dots, L'_n)$, такой, что $(L'_0, L'_{\sigma(j)+1}, \dots, L'_n) \in \mathcal{U}'''_{j,0}$ для всякого $1 \le j \le N$ и все линейные формы L'_w, $w \in \{0, \sigma+1, \dots, n\}$, имеют целые коэффициенты с длиной записи $O(n \log d + (n-\sigma)\log d' + \log N)$. Далее, для этого L' можно построить линейные формы $L_0, \dots, L_{n+1}$ с целыми коэффициентами с*

длиной записи $O(n\log d+(n-\sigma)\log d'+\log N)$, *такие, что выполняются утверждения теоремы 1 работы* [9] *для* $V^{(j)}$ *и* $(L'_0, L'_{\sigma(j)+1}, \dots, L'_n)$ *вместо* V *и* $(L'_0, L'_{\sigma+1}, \dots, L'_n)$ *для всех* $0 \le j \le N$ *(т.е. линейные формы* $L'_0, L'_{\sigma(j)+1}, \dots, L'_n$ *и* $L_0, \dots, L_{n+1}$ *не зависят от* j*; другие объекты из формулировки этой теоремы для* $V^{(j)}$ *зависят от* j*). Далее, линейные формы* $L_0, \dots, L_{n+1}$ *удовлетворяют дополнительно следующим условиям. Для всех* $x \in W^{(j)}_{i-1}(L') \cap \mathcal{Z}(e'_{j,i}) \cap \mathcal{Z}(L_{\iota(j,i)+1}, \dots, L_n)$ *для всех* $1 \le j, \beta \le N$ *для всех* $\sigma(j) \le i \le n+1$, $\sigma(\beta) \le \alpha \le n+1$ *имеем*

$$\begin{aligned}&\mu(x, W^{(\beta)}_{\alpha-1}(L') \cap \mathcal{Z}(e'_{\beta,\alpha}))\\ &= \min\{\mu(x', W^{(\beta)}_{\alpha-1}(L') \cap \mathcal{Z}(e'_{\beta,\alpha})) \,:\, x' \in W^{(j)}_{i-1}(L') \cap \mathcal{Z}(e'_{j,i})\}.\end{aligned} \tag{18}$$

В частности, если E_1 *(соответственно* E_2*) – определённая над* k *и неприводимая над* k *компонента многообразия* $W^{(j)}_{i-1}(L') \cap \mathcal{Z}(e'_{j,i})$ *(соответственно* $W^{(\beta)}_{\alpha-1}(L') \cap \mathcal{Z}(e'_{\beta,\alpha})$*), такая, что* $E_1 \not\subset E_2$*, то* $x \notin E_2$*. Время работы этого алгоритма полиномиально от* $d^n(d')^{n-\sigma}$, d_1, d_2, M, M_1, m, N *и суммы длин записи* $\sum\limits_{0\le i\le N} \mathrm{L}(x^{(0,i)})$ *точек* $x^{(0,i)}$.

Доказательство. Применяя теорему 1(a) из работы [10], мы строим для всякого $1 \le j \le N$ элемент $L^{(j)} \in \mathcal{U}'''_{j,0}$. Далее, используя теорему 1(f) из работы [10] и алгоритм редукции к целым коэффициентам (см. предложение 2 работы [8]), мы строим элемент $L' = (L'_0, L'_{\sigma+1}, \dots, L'_n)$, такой, что все линейные формы L'_α, $\alpha \in \{0, \sigma+1, \dots, n\}$, имеют целые коэффициенты с длиной записи $O(n\log d+(n-\sigma)\log d'+\log N)$ и $(L'_0, L'_{\sigma(j)+1}, \dots, L'_n) \in \mathcal{U}'''_{j,0}$ для всякого $1 \le j \le N$.

Применяя теорему 1 из работы [9] (и замечания, приведённые выше, в случае, когда $W^{(j)} \subset \mathcal{Z}(e_0, \dots, e_r)$), мы строим для всякого $1 \le j \le N$ элемент $\overline{\lambda}^{(j)} = (L^{(j)}_0, \dots, L^{(j)}_{n+1})$ (аналогичный $\overline{\lambda}$), удовлетворяющий утверждениям (a) и (b) теоремы 1 из [9] для $(V^{(j)}, W^{(j)}, p^{(j)})$ вместо (V, W, p). Далее, применяя теорему 1(g) из работы [9] и алгоритм редукции к целым коэффициентам (см. предложение 2 работы [8]), мы строим такой элемент $\overline{\lambda} = (L_0, \dots, L_{n+1})$, что для этого $\overline{\lambda}$ выполняются утверждения теоремы 1 работы [9] для $(V^{(j)}, W^{(j)}, p^{(j)})$ вместо (V, W, p) для всех $0 \le j \le N$.

Теперь мы собираемся описать рекурсию по $(L_0, \dots, L_{n+1})$. Рекурсивное предположение состоит в том, что для всех $0 \le j \le N$ справедливы утверждения теоремы 1 работы [9] для $(\overline{\lambda}, V^{(j)}, W^{(j)}, p^{(j)})$ вместо $(\overline{\lambda}, V, W, p)$ и известно такое целое число $1 \le w \le n$ (база рекурсии есть $w = n$), что для всякого $1 \le j \le N$ для всякого $\sigma(j) \le i \le n+1$, если $\iota = \iota(i,j) \ge w+1$, то

$$W_{i-1}^{(j)}(L') \cap \mathcal{Z}(e'_{j,i}) \cap \mathcal{Z}(L_\iota, \dots, L_n) = \varnothing \tag{19}$$

в $\mathbb{P}^n(\overline{k})$. На следующем шаге рекурсии при помощи теоремы 1(g) работы [9], леммы 1 и алгоритма редукции к целым коэффициентам (см. предложение 2 работы [8]), мы строим минимально возможное целое число $t_w > 0$, такое, что сформулированное рекурсивное предположение выполняется для $w-1$ и $(L_0, \dots, L_w + t_w L_0, L_{w+1}, \dots, L_{n+1})$ вместо $(L_0, \dots, L_{n+1})$. Согласно оценкам из теоремы 1(g) работы [9] и леммы 1, целое число t_w имеет длину записи $O(n \log d + (n-\sigma)\log d' + \log N)$. После этого мы заменяем $L_0, \dots, L_{n+1}$ на $(L_0, \dots, L_w + t_w L_0, L_{w+1}, \dots, L_{n+1})$. Если $w - 1 \ge 1$, то мы переходим к следующему шагу рекурсии. Таким образом, в конце рекурсии рекурсивное предположение выполняется с $w = 0$. Очевидно, условие (19) удовлетворяется также, если $\iota(j,i) = 0$. Следовательно, в конце рекурсии оно справедливо для всякого $1 \le j \le N$ и для всякого $\sigma(j) \le i \le n+1$.

Далее, для всякого $\sigma \le i \le n+1$ мы определяем линейную проекцию $\varphi^{(i)} : \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(L_0, L_{\iota+1}, \dots, L_n) \to \mathbb{P}^{n-\iota}(\overline{k})$, $(X_0, \dots, X_n) \mapsto (L_0 : L_{\iota+1} : \dots : L_n)$. Для всякого $\sigma(j) \le i \le n+1$ для всякого $1 \le j \le N$ положим $\varphi_i^{(j)}$ равным ограничению проекции $\varphi^{(i)}$ на $W_{i-1}^{(j)}(L') \cap \mathcal{Z}(e'_{j,i})$. Тогда, $\varphi_i^{(j)}$ – конечный доминантный морфизм согласно утверждениям (a) и (b) теоремы 1 работы [9] для $V^{(j)}, W^{(j)}, p^{(j)}$ вместо V, W, p. Пусть $z = (1 : z_1 : \dots : z_n) \in \mathbb{P}^n(\overline{k})$ – точка. Обозначим для краткости $P_i^{(j)}(z) = (\varphi_i^{(j)})^{-1}((1 : z_{\iota+1} : \dots : z_n))$.

Заметим, что $W_{i-1}^{(j)}(L')$ является объединением некоторых неприводимых компонент многообразия

$$V_{i-1}^{(j)}(L') = \mathcal{Z}(f_1^{(j)}, \dots, f_{m(j)}^{(j)}, L'_{\sigma(j)+1}, \dots, L'_{i-1}).$$

Следовательно, применяя теорему 2 работы [8] к множеству $U'' = \mathcal{Z}(e'_{j,i}, L_{\iota+1} - z_{\iota+1}L_0, \dots, L_n - z_n L_0)$ и после этого теорему 2 работы [7],

можно построить $P_i^{(j)}(z)$ (ср. также [9, §2], где описан алгоритм для вычисления $\varphi_i^{-1}((1:\nu_{\iota+1}:\ldots:\nu_n))$). Положим

$$\mu(z)=\sum_{1\le j,\beta\le N}\ \sum_{\sigma(j)\le i\le n+1}\ \sum_{\sigma(\beta)\le\alpha\le n+1}\ \sum_{x\in P_i^{(j)}(z)}\mu(x,W_{\alpha-1}^{(\beta)}(L')\cap\mathcal{Z}(e'_{\beta,\alpha})).$$

Следовательно, согласно теореме 1(e) работы [9] можно вычислить $\mu(z)$ для заданного z. Наша цель – построить точку z с минимально возможным $\mu(z)$.

Опишем новую рекурсию относительно $\overline{\lambda}$ и $z=(1:z_1:\ldots:z_n)$. Мы берём построенные $\overline{\lambda}=(L_0,\ldots,L_{n+1})$ и $z=(1:0:\ldots:0)$ как базу рекурсии. Рекурсивное предположение состоит в том, что линейные формы $L_0, L_1-z_1L_0,\ldots,L_n-z_nL_0, L_{n+1}$ (вместо $L_0,\ldots,L_{n+1}$) удовлетворяют утверждениям (a) и (b) теоремы 1 из [9] для $(V^{(j)},W^{(j)},p^{(j)})$ вместо (V,W,p) для всех $0\le j\le N$ и, кроме того (положим $z_0=0$), для всякого $1\le j\le N$ для всякого $\sigma(j)\le i\le n+1$

$$W_{i-1}^{(j)}(L')\cap\mathcal{Z}(e'_{j,i})\cap\mathcal{Z}(L_{\iota(j,i)}-z_{\iota(j,i)}L_0,\ldots,L_n-z_nL_0)=\varnothing \qquad (20)$$

в $\mathbb{P}^n(\overline{k})$. Заметим, что утверждение (20) для базы рекурсии следует из (19). Далее, из условия (20) следует, что для всякого (i,j,β,α,x), такого, что $1\le j,\beta\le N$, $\sigma(j)\le i\le n+1$, $\sigma(\beta)\le\alpha\le n+1$, $x\in P_i^{(j)}(z)$ и $\dim W_{i-1}^{(j)}(L')\cap\mathcal{Z}(e'_{j,i})>\dim W_{\alpha-1}^{(\beta)}(L')\cap\mathcal{Z}(e'_{\beta,\alpha})$, для всякой неприводимой компоненты E_1 многообразия $W_{i-1}^{(j)}(L')\cap\mathcal{Z}(e'_{j,i})$ для всякой неприводимой компоненты E_2 многообразия $W_{\alpha-1}^{(\beta)}(L')\cap\mathcal{Z}(e'_{\beta,\alpha})$ имеем

$$(E_1\cap\mathcal{Z}(L_{\iota(j,i)+1}-z_{\iota(j,i)}L_0,\ldots,L_n-z_nL_0))\cap E_2=\varnothing.$$

Опишем общий шаг этой рекурсии. Мы перебираем наборы (i,j,β,α,x), состоящие каждый из пяти элементов, таких, что $1\le j,\beta\le N$, $\sigma(j)\le i\le n+1$, $\sigma(\beta)\le\alpha\le n+1$, $x\in P_i^{(j)}(z)$ и $\dim W_{i-1}^{(j)}(L')\cap\mathcal{Z}(e'_{j,i})\le\dim W_{\alpha-1}^{(\beta)}(L')\cap\mathcal{Z}(e'_{\beta,\alpha})$ (последнее условие эквивалентно неравенству $\iota(j,i)\ge\iota(\beta,\alpha)$).

Для рассматриваемого набора (i,j,β,α,x) мы вычисляем множество $P_i^{(j)}(z)$ (см. выше) и затем целое число $\mu(z)$. Напомним, что для произвольного проективного алгебраического многообразия $E\subset$

$\mathbb{P}^n(\overline{k})$ мы обозначаем через $\mathrm{con}(E) \subset \mathbb{A}^{n+1}(\overline{k})$ аффинное алгебраическое многообразие, которое является множеством всех нулей однородного идеала многообразия E в $\mathbb{A}^{n+1}(\overline{k})$.

Мы строим вещественную структуру на поле k, см. [13, 14]. Пусть $\varepsilon_1 > 0$ является бесконечно малой величиной относительно поля k и $\varepsilon_2 > 0$ является бесконечно малой величиной относительно поля $k(\varepsilon_1)$. Положим $k_2 = k(\varepsilon_1, \varepsilon_2)$. Применяя теорему 2 работы [8] к аффинному многообразию $(\mathrm{con}(V_{i-1}^{(j)}(L')) \times \mathrm{con}(V_{\alpha-1}^{(\beta)}(L')))(\overline{k_2})$, мы выясняем, существует ли такая пара $(x'', x''') \in (W_{i-1}^{(j)}(L') \times W_{\alpha-1}^{(\beta)}(L'))(\overline{k_2})$, что

$$\begin{cases} \sum\limits_{0 \le w \le n} |(X_w/L_0)(x'') - (X_w/L_0)(x)|^2 \le \varepsilon_1, \\ \varepsilon_2 \le \sum\limits_{0 \le w \le n} |(X_w/L_0)(x'') - (X_w/L_0)(x''')|^2 \le \varepsilon_1, \\ \varphi^{(\alpha)}(x'') = \varphi^{(\alpha)}(x'''), \\ e'_{j,i}(x'') = e'_{\beta,\alpha}(x''') = 0 \end{cases} \tag{21}$$

(ср. с системой (2) из [3]). Если не существует такой пары (x'', x''') и не все наборы (i, j, β, α, x) перебраны, то мы переходим к следующему набору (i, j, β, α, x). Предположим, что существует пара $(x'', x''') \in (W_{i-1}^{(j)}(L') \times W_{\alpha-1}^{(\beta)}(L'))(\overline{k_2})$, удовлетворяющая условиям (21). Тогда мы вычисляем $\varphi_i^{(j)}(x'') = (1 : z''_{\iota+1} : \ldots : z''_n)$, где $z''_w \in \overline{k_2}$ для всех w. Положим $z''_w = z'_w$ для $1 \le \alpha \le \iota$ и $z'' = (1 : z''_1 : \ldots : z''_n)$. Тогда $\mu(z'') < \mu(z')$.

Нетрудно видеть (согласно, например, [3]), что для всякого β для всякого α для произвольной прямой $\mathfrak{l} \subset \mathbb{P}^n(\overline{k_2})$ и любой точки $x^* \in \mathfrak{l}$ число элементов $x^{**} \in \mathfrak{l}$ с $\mu(x^{**}, W_{\alpha-1}^{(\beta)}(L') \cap \mathcal{Z}(e'_{\beta,\alpha})) > \mu(x^*, W_{\alpha-1}^{(\beta)}(L') \cap \mathcal{Z}(e'_{\beta,\alpha}))$ ограничено сверху полиномом от $d^n(d')^{n-\sigma}$ (ср. также доказательство леммы 1 из [6]). Следовательно, применяя теорему 1(g) работы [9], лемму 1 и алгоритм редукции к целым коэффициентам (см. предложение 2 работы [8]) к точкам z'' и $(1 : 0 : \ldots : 0)$, можно построить точку $\widetilde{z} = (1 : \widetilde{z}_1 : \ldots : \widetilde{z}_n) \in \mathbb{P}^n(\overline{k})$ с целыми $\widetilde{z}_w$ с длиной записи $O(n \log d + (n - \sigma) \log d' + \log N)$, такую, что для $\overline{\lambda}$ и $\widetilde{z}$ (вместо $\overline{\lambda}$ и z) выполняется рекурсивное предположение. Тогда мы заменяем $(\overline{\lambda}, z)$ на $(\overline{\lambda}, \widetilde{z})$ и переходим к следующему шагу рекурсии.

В конце концов мы придём к случаю, когда для всех перебранных 5-наборов (i, j, β, α, x) не существует пары (x'', x'''), удовлетворяющей всем рассматриваемым условиям. Тогда $\mu(x, W_{\alpha-1}^{(\beta)}(L') \cap \mathcal{Z}(e'_{\beta,\alpha})) =$

$\min\{\mu(x', W_{\alpha-1}^{(\beta)}(L') \cap \mathcal{Z}(e'_{\beta,\alpha})) : x' \in W_{i-1}^{(j)}(L') \cap \mathcal{Z}(e'_{j,i})\}$ для всех $x \in P_i^{(j)}(z)$ для всех $1 \le j$, $\beta \le N$, $\sigma(j) \le i \le n+1$, $\sigma(\beta) \le \alpha \le n+1$. Этот шаг является заключительным. Мы заменяем $L_0, \dots, L_{n+1}$ на $L_0, L_1 - z_1 L_0, \dots, L_n - z_n L_0, L_{n+1}$ соответственно. Теперь новые $L_0, \dots, L_{n+1}$ удовлетворяют всем требуемым условиям.

Требуемая оценка на время работы описанного алгоритма немедленно следует из оценок на время работы использованных алгоритмов. Лемма доказана. □

Перейдём к доказательству теоремы 1. Покажем, что случай $\nu = 1$ сводится к случаю $\nu = 2$. Действительно, достаточно положить $m_\alpha(i)$, a_α, b_α, $f_{\alpha,j}^{(i)}$, W_α, V_α, $W_\alpha^{(i)}$, $V_\alpha^{(i)}$, $W_\alpha^{(i)}$, $V_\alpha^{(i,s)}$, $W_\alpha^{(i,s)}$, $L_{\alpha,\beta}^{(i,s)}$, $\Xi_\alpha^{(i,s)}$, $(f_\alpha, L_\alpha, \Xi_\alpha, b_\alpha) = \rho_\alpha$ для $\alpha = 2$ равными соответствующим объектам с $\alpha = 1$ и применить теорему 1 для $\nu = 2$. Таким образом, мы будем в дальнейшем предполагать без ограничения общности, что $\nu \ge 2$. Кроме того, мы будем считать, что $n \ge 1$.

Пусть $\rho = (f, L, \Xi, b)$ – представление (4). Мы будем использовать следующие обозначения. Положим $n(\rho) = n$, $a(\rho) = a$, $b(\rho) = b$, $q_1(i, \rho) = V^{(i)}$ и $q_2(i, \rho) = W^{(i)}$ для всякого $1 \le i \le a = a(\rho)$. Эти функториальные обозначения $n(.)$, $a(.)$, $b(.)$, $q_1(.,.)$ и $q_2(.,.)$ используются также для других представлений, аналогичных (4). Положим

$$B_1 = \{(i_1, \dots, i_\nu) : 1 \le i_\alpha \le b_\alpha \ \&\ i_\alpha \in \mathbb{Z} \ \&\ 1 \le \alpha \le \nu \ \&\ \alpha \in \mathbb{Z}\}.$$

Заметим, что

$$\bigcap_{1\le\alpha\le\nu} W_\alpha = \Big(\bigcup_{(i_1,\dots,i_\nu)\in B_1} \bigcap_{1\le\alpha\le\nu} W_\alpha^{(i_\alpha)} \Big) \setminus \Big(\bigcup_{1\le\alpha\le\nu} \bigcup_{b_\alpha+1\le i\le a_\alpha} W_\alpha^{(i)} \Big). \tag{22}$$

Перебирая $c = 1, 2, \dots$, построим такое множество целых чисел $\mathcal{C}$, что для всякого $c \in \mathcal{C}$

$$\Big(\bigcup_{1\le\alpha\le\nu} \bigcup_{1\le j\le a_\alpha} \Xi_\alpha^{(j)} \Big) \cap \mathcal{Z}\Big(\sum_{0\le i\le n} c^i X_i \Big) = \varnothing \tag{23}$$

в $\mathbb{P}^n(\overline{k})$,

$$\#\mathcal{C} = n \Big(d^{n\nu} \prod_{1\le\alpha\le\nu} b_\alpha + d^n \sum_{1\le\alpha\le\nu} a_\alpha \Big) + n + 1 \tag{24}$$

и все элементы из $\mathcal{C}$ являются минимально возможными, т.е. сумма $\sum\limits_{c\in\mathcal{C}} c$ – минимально возможная. Согласно теореме Безу, максимальный элемент $\max\mathcal{C}$ множества $\mathcal{C}$ ограничен сверху полиномом от $d^{n\nu}(\sum\limits_{1\le\alpha\le\nu} a_\alpha)\prod\limits_{1\le\alpha\le\nu} b_\alpha$. Положим

$$\mathcal{H} = \Big\{ \sum_{0\le i\le n} c^i X_i \,:\, c\in\mathcal{C} \Big\}.$$

Тогда $\mathcal{H}$ – множество линейных форм с целыми коэффициентами.

Для всякого $H\in\mathcal{H}$ мы осуществляем следующую конструкцию. Определяемые ниже объекты зависят от H, хотя мы и не указываем это явно в обозначениях. Отождествим $\mathbb{P}^n(\overline{k})\setminus\mathcal{Z}(H)$ с $\mathbb{A}^n(\overline{k})$, где $\mathbb{A}^n(\overline{k})$ имеет координатные функции $Y_i = X_i/H$, $1\le i\le n$. Для всякого квазипроективного многообразия $E\subset\mathbb{P}^n(\overline{k})$ положим $\widetilde{E} = E\setminus\mathcal{Z}(H)\subset\mathbb{A}^n(\overline{k})$. Ниже для удобства мы обозначаем $\widetilde{W_\alpha} = \widetilde{\widetilde{W_\alpha}}$ и т.д., т.е. используем волну, не учитывая нижние и верхние индексы. Это не приведёт к двусмысленности. Теперь из равенства (22) следует, что

$$\bigcap_{1\le\alpha\le\nu}\widetilde{W_\alpha} = \Big(\bigcup_{(i_1,\dots,i_\nu)\in B_1}\ \bigcap_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)}\Big)\setminus\Big(\bigcup_{1\le\alpha\le\nu}\ \bigcup_{b_\alpha+1\le i\le a_\alpha}\widetilde{W}_\alpha^{(i)}\Big). \tag{25}$$

Отождествим $\mathbb{A}^{n\nu}(\overline{k})$ с $(\mathbb{A}^n(\overline{k}))^\nu$, где для всякого $1\le i\le\nu$ прямой множитель $\mathbb{A}^n(\overline{k})$ с номером i многообразия $\mathbb{A}^{n\nu}(\overline{k})$ в левой части последнего равенства имеет координатные функции $Y_{i,j}$, $1\le j\le n$. Следовательно, $\mathbb{A}^{n\nu}(\overline{k})$ имеет координатные функции $Y_{i,j}$, $1\le i\le\nu$, $1\le j\le n$. Положим $\Delta = \{(x,x,\dots,x)\in\mathbb{A}^{n\nu}(\overline{k}) \,:\, x\in\mathbb{A}^n(\overline{k})\}$ равным диагональному подмногообразию (ср. введение).

Отождествим $\mathbb{A}^{n\nu}(\overline{k})$ с подмногообразием в $\mathbb{P}^{n\nu}(\overline{k})$, где $\mathbb{P}^{n\nu}(\overline{k})$ имеет однородные координатные функции $X_{0,0}$, $X_{i,j}$, $1\le i\le\nu$, $1\le j\le n$, и $Y_{i,j} = X_{i,j}/X_{0,0}$. Положим $\overline{\Delta}$ равным замыканию Δ в $\mathbb{P}^{n\nu}(\overline{k})$ относительно топологии Зариского.

Далее мы предполагаем, что справедливо отождествление (12). Из него вытекает, что $\bigcap_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)} = (\prod\limits_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)})\cap\Delta$ для всякого $(i_1,\dots,i_\nu)\in B_1$ и $\widetilde{W}_\alpha^{(i)} = (\widetilde{W}_\alpha^{(i)})^\nu\cap\Delta$ для всех $b_\alpha+1\le i\le a_\alpha$, $1\le\alpha\le\nu$. Заметим, что пересечение $\bigcap_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)}$

трансверсально тогда и только тогда, когда трансверсально пересечение $(\prod_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)})\cap\Delta$, и в этом случае $\deg\bigcap_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)} = \deg\prod_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)} = \prod_{1\le\alpha\le\nu}\deg\widetilde{W}_\alpha^{(i_\alpha)}$. В общем случае выполняется неравенство $\deg\bigcap_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)} \le \deg\prod\limits_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)}$.

Для всякого $(i_1,\dots,i_\nu)\in B_1$ обозначим

$$V_{i_1,\dots,i_\nu} = \prod_{1\le\alpha\le\nu}\widetilde{V}_\alpha^{(i_\alpha)} \subset \mathbb{A}^{n\nu}(\overline{k}),$$
$$W_{i_1,\dots,i_\nu} = \prod_{1\le\alpha\le\nu}\widetilde{W}_\alpha^{(i_\alpha)} \subset V_{i_1,\dots,i_\nu}.$$

Тогда $V_{i_1,\dots,i_\nu}$ – аффинное алгебраическое многообразие, заданное системой полиномиальных уравнений относительно $Y_{i,j}$, $1\le i\le\nu$, $1\le j\le n$, и $W_{i_1,\dots,i_\nu}$ является объединением некоторых неприводимых компонент многообразия $V_{i_1,\dots,i_\nu}$. Обозначим через $\overline{V}_{i_1,\dots,i_\nu}$ (соответственно $\overline{W}_{i_1,\dots,i_\nu}$) замыкание многообразия $V_{i_1,\dots,i_\nu}$ (соответственно $W_{i_1,\dots,i_\nu}$) относительно топологии Зарискогo в $\mathbb{P}^{n\nu}(\overline{k})$. Тогда $\overline{V}_{i_1,\dots,i_\nu}$ – проективное алгебраическое многообразие, заданное системой полиномиальных уравнений относительно $X_{0,0}$, $X_{i,j}$, $1\le i\le\nu$, $1\le j\le n$, и $\overline{W}_{i_1,\dots,i_\nu}$ является объединением некоторых неприводимых компонент многообразия $V_{i_1,\dots,i_\nu}$.

Пусть $\overline{V}_{i_1,\dots,i_\nu}\cup\mathcal{Z}(X_{0,0}) = \bigcup\limits_{j\in J'_{i_1,\dots,i_\nu}} E_j$ – разложение в объединение определённых над k и неприводимых над k компонент E_j, $j\in J'_{i_1,\dots,i_\nu}$.

Для всякого $(i_1,\dots,i_\nu)\in B_1$ мы применяем теорему 1 работы [7] к алгебраическому многообразию $\overline{V}_{i_1,\dots,i_\nu}\cup\mathcal{Z}(X_{0,0})$ (вместо V) и строим для всякого $j\in J'_{i_1,\dots,i_\nu}$ представление ρ_j, аналогичное (4), неприводимой компоненты E_j, такое, что $n(\rho_j)=n\nu$, $a(\rho_j)=b(\rho_j)=1$, $q_1(1,\rho_j) = \overline{V}_{i_1,\dots,i_\nu}\cup\mathcal{Z}(X_{0,0})$ и $q_2(1,\rho_j) = E_j$. Положим $\Xi_{i_1,\dots,i_\nu} = \prod\limits_{1\le\alpha\le\nu}\Xi_\alpha^{(i_\alpha)} \subset \mathbb{A}^{n\nu}(\overline{k}) \subset \mathbb{P}^{n\nu}(\overline{k})$. Ввиду условия (23), для всякой неприводимой компоненты E многообразия $\overline{V}_{i_1,\dots,i_\nu}\cup\mathcal{Z}(X_{0,0})$ пересечение $E\cap\Xi_{i_1,\dots,i_\nu}$ непусто тогда и только тогда, когда E является неприводимой компонентой многообразия $\overline{W}_{i_1,\dots,i_\nu}$, т.е. конечное множество $\Xi_{i_1,\dots,i_\nu}$ задаёт $\overline{W}_{i_1,\dots,i_\nu}$ как объединение некоторых неприводимых компонент многообразия $\overline{V}_{i_1,\dots,i_\nu}\cup\mathcal{Z}(X_{0,0})$. Теперь, применяя теорему 2 работы [7], мы строим такое подмножество $J_{i_1,\dots,i_\nu}\subset J'_{i_1,\dots,i_\nu}$,

что

$$\overline{W}_{i_1,\dots,i_\nu} = \bigcup_{j\in J_{i_1,\dots,i_\nu}} E_j.$$

Заметим, что $E_j \not\subset \mathcal{Z}(X_{0,0})$ для всякого $j \in J_{i_1,\dots,i_\nu}$ и для всякого $(i_1,\dots,i_\nu) \in B_1$.

Положим $a_1' = a_1 + \#\mathcal{C}$. Пусть H_j, $a_1+1 \le j \le a_1'$, – семейство линейных форм, такое, что $\{H_j : a_1+1 \le j \le a_1'\} = \mathcal{H}$. Положим $V_1^{(j)} = W_1^{(j)} = \mathcal{Z}(H_j)$ для всякого $a_1+1 \le j \le a_1'$.

Положим

$$B_2 = \{(\alpha,i) : 1 \le \alpha \le \nu \,\&\, \alpha \in \mathbb{Z} \,\&\, b_\alpha + 1 \le i \le a_\alpha \,\&\, i \in \mathbb{Z}\}$$

и $B_2' = B_2 \cup \{(1,i) : a_1+1 \le i \le a_1'\}$. Тогда $B_2 \subset B_2'$. Для всякого $(\alpha,i) \in B_2'$ положим

$$V_{\alpha;i} = (\widetilde{V}_\alpha^{(i)})^\nu \subset \mathbb{A}^{n\nu}(\overline{k}),$$
$$W_{\alpha;i} = (\widetilde{W}_\alpha^{(i)})^\nu \subset V_{\alpha;i}.$$

Тогда $V_{\alpha;i}$ – аффинное алгебраическое многообразие, заданное системой полиномиальных уравнений относительно $Y_{i,j}$, $1 \le i \le \nu$, $1 \le j \le n$, и $W_{\alpha;i}$ является объединением некоторых неприводимых компонент многообразия $V_{\alpha;i}$. Обозначим через $\overline{V}_{\alpha;i}$ (соответственно $\overline{W}_{\alpha;i}$) замыкание многообразия $V_{\alpha;i}$ (соответственно $W_{\alpha;i}$) относительно топологии Зариского в $\mathbb{P}^{n\nu}(\overline{k})$. Тогда $\overline{V}_{\alpha;i}$ является проективным алгебраическим многообразием, заданным системой полиномиальных уравнений относительно $X_{0,0}$, $X_{i,j}$, $1 \le i \le \nu$, $1 \le j \le n$, и $\overline{W}_{\alpha;i}$ – объединение некоторых неприводимых компонент многообразия $\overline{V}_{\alpha;i}$.

Пусть $\overline{V}_{\alpha;i} \cup \mathcal{Z}(X_{0,0}) = \bigcup_{j\in J'_{\alpha;i}} E_j$ – разложение в объединение определённых над k и неприводимых над k компонент E_j, $j \in J'_{\alpha;i}$.

Для всякого $(\alpha,i) \in B_2'$ мы применяем теорему 1 работы [7] к алгебраическому многообразию $\overline{V}_{\alpha;i} \cup \mathcal{Z}(X_{0,0})$ (вместо V) и строим для всякого $j \in J'_{\alpha;i}$ представление ρ_j, аналогичное (4), неприводимой компоненты E_j, такое, что $n(\rho_j) = n\nu$, $a(\rho_j) = b(\rho_j) = 1$, $q_1(1,\rho_j) = \overline{V}_{\alpha;i} \cup \mathcal{Z}(X_{0,0})$ и $q_2(1,\rho_j) = E_j$. Поскольку $\Xi_\alpha^{(j)}$ для всех $1 \le \alpha \le \nu$, $1 \le j \le a_\alpha$ известны, мы можем построить множество $\Xi_{\alpha;i}$ гладких точек многообразия $\overline{V}_{\alpha;i} \cup \mathcal{Z}(X_{0,0})$, удовлетворяющих

следующему свойству. Для всякой неприводимой компоненты E многообразия $\overline{V}_{\alpha;i} \cup \mathcal{Z}(X_{0,0})$ пересечение $\Xi_{\alpha;i} \cap E$ непусто в том и только в том случае, если E является неприводимой компонентой многообразия $\overline{W}_{\alpha;i}$. После этого, применяя теорему 2 работы [7], мы строим такое подмножество $J_{\alpha;i} \subset J'_{\alpha;i}$, что

$$\overline{W}_{\alpha;i} = \bigcup_{j \in J_{\alpha;i}} E_j.$$

Заметим, что $E_j \not\subset \mathcal{Z}(X_{0,0})$ для всякого $j \in J_{\alpha;i}$ и для всякого $(\alpha, i) \in B'_2$.

Построим также представление $\rho_{j_{0,0}}$, такое, что $n(\rho_{j_{0,0}}) = n\nu$, $a(\rho_{j_{0,0}}) = b(\rho_{j_{0,0}}) = 1$, $q_1(\rho_{j_{0,0}}) = q_2(\rho_{j_{0,0}}) = \mathcal{Z}(X_{0,0})$.

Чтобы упростить обозначения, мы будем предполагать без ограничения общности, что

- для всех $(i_1, \ldots, i_\nu) \in B_1$, $(i'_1, \ldots, i'_\nu) \in B_1$, если $(i_1, \ldots, i_\nu) \neq (i'_1, \ldots, i'_\nu)$, то $J_{i_1,\ldots,i_\nu} \cap J_{i'_1,\ldots,i'_\nu} = \varnothing$,
- для всех $(i_1, \ldots, i_\nu) \in B_1$, $(\alpha, i) \in B'_2$ имеем $J_{i_1,\ldots,i_\nu} \cap J_{\alpha;i} = \varnothing$,
- для всех $(\alpha, i) \in B'_2$, $(\alpha', i') \in B'_2$, если $(\alpha, i) \neq (\alpha', i')$, то $J_{\alpha;i} \cap J_{\alpha';i'} = \varnothing$,

заменяя при необходимости рассматриваемые множества индексов на новые. Положим

$$J_1 = \bigcup_{(i,\ldots,i_\nu) \in B_1} J_{i_1,\ldots,i_\nu}, \quad J'_2 = \bigcup_{(\alpha,i) \in B'_2} J_{\alpha;i}, \quad J'_0 = \{j_{0,0}\} \cup J_1 \cup J'_2,$$

$$J_2 = \bigcup_{(\alpha,i) \in B_2} J_{\alpha;i}, \quad J_0 = J_1 \cup J_2.$$

Кроме того, в дальнейшем мы будем считать, не умаляя общности, что $J'_0 \cap \mathbb{Z} = \varnothing$, т.е. всякий элемент из J'_0 не является целым числом. Обозначим $V^{(j)} = q_1(1, \rho_j)$, $W^{(j)} = q_2(1, \rho_j)$ для всех $j \in J'_0$.

Положим $r = n(\nu - 1) - 1$ и возьмем $e_0, \ldots, e_r$ равным семейству многочленов $X_{1,i} - X_{w,i}$, $2 \leq w \leq \nu$, $1 \leq i \leq n$ (мы выбираем произвольный линейный порядок на элементах последнего семейства, чтобы получить $e_0, \ldots, e_r$). Отметим, что $\overline{\Delta} = \mathcal{Z}(e_0, \ldots, e_r)$. Более того, $e_0, \ldots, e_r$ порождают однородный идеал многообразия $\overline{\Delta} \subset \mathbb{P}^{n\nu}(\overline{k})$, и $\dim \overline{\Delta} = n\nu - r - 1$. Обозначим через $\delta : \mathbb{P}^{n\nu}(\overline{k}) \setminus \mathcal{Z}(e_0, \ldots, e_r) \to \mathbb{P}^r(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (e_0 : \ldots : e_r)$, морфизм линейной проекции. Обозначим через $p^{(j)} : W^{(j)} \setminus \mathcal{Z}(e_0, \ldots, e_r) \to \mathbb{P}^r(\overline{k})$

ограничение морфизма δ на $W^{(j)} \setminus \mathcal{Z}(e_0, \dots, e_r)$ для всякого $j \in J'_0$. Отметим, что если $W^{(j)} \subset \overline{\Delta}$, то $\dim W^{(j)} = 0$ (но, конечно, обратное неверно).

Пусть $j \in J'_0$ и $\sigma(j) \le i \le n\nu + 1$. Теперь $W_i^{(j)}(L'')$ (соответственно $W_i^{(j,\beta)}(L'')$, $\beta = 1, 2, 3$) – проективное алгебраическое многообразие в $\mathbb{P}^{n\nu}(\overline{k})$, и размерность всякой неприводимой компоненты $W_i^{(j)}(L'')$ (соответственно $W_i^{(j,\beta)}(L'')$) равна $n\nu - \iota(j,i) = n\nu - i + \sigma(j) - s(j)$, см. введение из [9] и начало этого раздела.

Заметим, что сейчас $W_i^{(j,3)}(L') = \varnothing$ для всех $j \in J'_0$ и $\sigma(j) \le i \le n\nu + 1$, поскольку $L'' \in \mathcal{U}''_{j,0}$, см. [9]. Далее, для всякого $j \in J'_0$ снова имеем

$$\bigcup_{\sigma(j) \le i \le n\nu+1} W_i^{(j,1)}(L'') = W^{(j)} \cap \overline{\Delta}, \tag{26}$$

так как $L'' \in \mathcal{U}''_{j,0}$ (напомним, что $\mathcal{U}'''_{j,0} \subset \mathcal{U}''_{j,0}$), см. введение из [9]. В этом случае мы обозначаем $W_i^{(j,1)}(L'') = W_i^{(j,1)}$.

Теперь мы собираемся применить лемму 2 с $N = \#J'_0$ и множеством индексов $j \in J'_0$ вместо $j \in \{1, \dots, N\}$. Мы заменяем также (n, σ) на $(n\nu, \sigma_1)$. В настоящее время все объекты из формулировки этой леммы определены естественным образом при помощи представлений ρ_j, $j \in J'_0$.

Таким образом, применяя лемму 2, мы получаем линейные формы $L''_0,\ L''_{\sigma_1+1}, \dots, L''_{n\nu} \in k[X_0, \dots,\ X_r]$ вместо $L'_0, L'_{\sigma+1}, \dots, L'_n$. Положим $L'' = (L''_0,\ L''_{\sigma_1+1}, \dots, L''_{n\nu})$, $e''_{j,w} = e''_w = L''_w(e_0, \dots, e_r)$ (напомним, что $L''_{n\nu+1} = L''_0$, см. введение из [9]) и $e''_{j,\sigma(j)} = 0$ для всех $w \in \{0, \sigma(j) + 1, \dots, n\nu + 1\}$ и $j \in J'_0$. Далее, мы строим линейные формы $L'''_0, \dots, L'''_{n\nu+1} \in k[X_{0,0}, X_{i,j},\ 1 \le j \le \nu,\ 1 \le i \le n]$ вместо $L_0, \dots, L_{n+1} \in k[X_0, \dots, X_n]$. Мы сменили обозначения L'_j на L''_j (соответственно L_w на L'''_w) для того, чтобы избежать двусмысленности в дальнейшем.

Применяя теорему 1 работы [9], построим для всякого $j \in J'_0$ для всякого $\sigma(j) - 1 \le i \le n\nu + 1$ конечные множества

$$A_i^{(j)} = W_{i-1}^{(j)}(L'') \cap \mathcal{Z}(e''_{j,i}) \cap \mathcal{Z}(L'''_{\iota(j,i)+1}, \dots, L'''_{n\nu}),$$
$$A_i^{(j,1)} = W_i^{(j,1)} \cap \mathcal{Z}(L'''_{\iota(j,i)+1}, \dots, L'''_{n\nu}).$$

Пусть E – определённая над k и неприводимая над k компонента многообразия $W_i^{(j,1)}$ с $j \in J'_0$ и $\sigma(j) \le i \le n\nu + 1$. Согласно лемме 2,

$E \subset \mathcal{Z}(X_{0,0})$ тогда и только тогда, когда $E \cap \mathcal{Z}(L'''_{\iota+1}, \dots, L'''_{n\nu}) \subset \mathcal{Z}(X_{0,0})$. Положим для всякого $j \in J_0$

$$\begin{aligned} D(H,j) &= \deg(W^{(j)} \cap \overline{\Delta} \setminus \mathcal{Z}(X_{0,0})) \\ &= \sum_{\sigma(j) \le i \le n\nu+1} \deg(W_i^{(j,1)} \setminus \mathcal{Z}(X_{0,0})) \\ &= \sum_{\sigma(j) \le i \le n\nu+1} \#(A_i^{(j,1)} \setminus \mathcal{Z}(X_{0,0})). \end{aligned}$$

Вычислим $D(H,j)$ по предыдущей формуле для всякого $j \in J_0$, а затем положим $D(H) = \sum\limits_{j \in J_0} D(H,j)$.

Мы строим такое подмножество $\mathcal{H}_0 \subset \mathcal{H}$, что $D(H') = \max\{D(H) : H \in \mathcal{H}\}$ для всякого $H' \in \mathcal{H}_0$. Мы утверждаем, что

(a) для всякого $H \in \mathcal{H}_0$ для всякого $(i_1, \dots, i_\nu) \in B_1$ для каждой определённой над k и неприводимой над k компоненты E_α многообразия $V_\alpha^{(i_\alpha)}$, $1 \le \alpha \le \nu$, включение $\bigcap_{1 \le \alpha \le \nu} \widetilde{E}_\alpha \subset \bigcap_{1 \le \alpha \le \nu} E_\alpha$ индуцирует взаимно однозначное соответствие между определёнными над k и неприводимыми над k компонентами алгебраических многообразий $\bigcap\limits_{1 \le \alpha \le \nu} \widetilde{E}_\alpha$ и $\bigcap\limits_{1 \le \alpha \le \nu} E_\alpha$,

(b) $\#\mathcal{H}_0 \ge n+1$.

Действительно, требуемые утверждения следуют из теоремы Безу и того, что для всякого непустого проективного алгебраического многообразия $\mathcal{V} \subset \mathbb{P}^n(\overline{k})$ существует не более n различных линейных форм $H \in \mathcal{H}$, таких, что $\mathcal{V} \subset \mathcal{Z}(H)$. Построим такое подмножество $\mathcal{H}_1 \subset \mathcal{H}_0$, что $\#\mathcal{H}_1 = n+1$.

Далее, для всякого $H \in \mathcal{H}_1$ мы осуществляем следующую конструкцию. Пусть E – определённая над k и и неприводимая над k компонента многообразия $W_i^{(j,1)}$ с $j \in J_0$ и $\sigma(j) \le i \le n\nu+1$. Пусть $\dim E = n\nu - \iota$. Тогда

$$E \cap \mathcal{Z}(L'''_{\iota+1}, \dots, L'''_{n\nu}) = \Xi_E \subset A_i^{(j,1)},$$

и $\iota = i - \sigma(j) + s(j)$. Заметим, что $E \not\subset \mathcal{Z}(X_{0,0})$ согласно свойству (a). Мы используем отождествление

$$E \setminus \mathcal{Z}(X_{0,0}) \subset \mathbb{A}^{n\nu}(\overline{k}) \cap \Delta = \mathbb{A}^n(\overline{k}) = \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(H) \subset \mathbb{P}^n(\overline{k}) \qquad (27)$$

при помощи изоморфизма (12). Для всех $j \in J_0$ построим все такие подмножества Ξ_E, применяя утверждения (a) и (b) теоремы 1 из работы [9]. Отметим, что при отождествлении (27) пересечение $\Xi_E \cap \big(\bigcup_{H\in\mathcal{H}_1} \mathcal{Z}(H)\big)$ пусто согласно выбору $(V_{1;i}, W_{1;i})$, $a_1+1 \le i \le a'_1$, и лемме 2.

Пусть $J' \subset J_0$ – подмножество. Мы будем говорить, что определённая над k и неприводимая над k компонента E многообразия $W^{(j)} \cap \overline{\Delta}$ с $j \in J'$ максимальна относительно J', тогда и только тогда, когда для всякого $j' \in J'$ для всякой определённой над k и неприводимой над k компоненты E' многообразия $W^{(j')} \cap \overline{\Delta}$ из включения $E \subset E'$ следует равенство $E = E'$.

Пусть E_γ, $\gamma = 1, 2,$ – определённая над k и неприводимая над k компонента многообразия $W^{(j_\gamma)} \cap \overline{\Delta}$ с $j_\gamma \in J_0$ и $E_\gamma \not\subset \mathcal{Z}(X_{0,0})$. Согласно лемме 2, включение $E_1 \subset E_2$ выполнено тогда и только тогда, когда $\Xi_{E_1} \subset E_2$.

Следовательно, применяя теорему 1 работы [9], можно построить множества Ξ_j, $j \in I_1$ (соответственно Ξ_j, $j \in I_2$), такие, что

- для всякого $j \in I_1$ (соответственно $j \in I_2$) имеем $\Xi_j = \Xi_E$ для некоторой определённой над k и неприводимой над k компоненты E многообразия $W^{(j')} \cap \overline{\Delta}$ с $j' \in J_1$ (соответственно $j' \in J_2$), такой, что E максимальна относительно J_0 (соответственно относительно J_2) и $E \not\subset \mathcal{Z}(X_{0,0})$.
- обратно, для всякого $j' \in J_1$ (соответственно $j' \in J_2$) для всякой определённой над k и неприводимой над k компоненты E многообразия $W^{(j')} \cap \overline{\Delta}$, такой, что E максимальна относительно J_0 (соответственно относительно J_2) и $E \not\subset \mathcal{Z}(X_{0,0})$, существует $j \in I_1$ (соответственно $j \in I_2$) с $\Xi_j = \Xi_E$,
- для всех $j_1, j_2 \in I_1$ (соответственно $j_1, j_2 \in I_2$), если $j_1 \ne j_2$, то $\Xi_{j_1} \ne \Xi_{j_2}$.

Для всякого $j \in I_1 \cup I_2$ положим $\overline{E}_j = \overline{E}$, где $\Xi_j = \Xi_E$ и $\overline{E}$ – замыкание многообразия $E \setminus \mathcal{Z}(X_{0,0})$ в $\mathbb{P}^n(\overline{k})$ относительно топологии Зарисского согласно вложению (27). Мы отождествляем Ξ_j с подмногообразием в $\mathbb{P}^n(\overline{k})$ согласно (27). Теперь $\overline{E}_j$, $j \in I_1$ (соответственно $\overline{E}_j$, $j \in I_2$), – семейство всех определённых над k и неприводимых над k компонент многообразия $\bigcup\limits_{(i_1,\dots,i_\nu)\in B_1} \bigcap_{1\le\alpha\le\nu} W_\alpha^{(i_\alpha)}$ (соответственно $\bigcup\limits_{1\le\alpha\le\nu} \bigcup\limits_{b_\alpha+1\le i\le a_\alpha} W_\alpha^{(i)}$) согласно лемме 2, свойству (a) и поскольку $H \in \mathcal{H}_1 \subset \mathcal{H}_0$.

Пусть $j_1 \in I_1$, $j_2 \in I_2$. Пусть $\mathbb{P}^{n\nu}(\overline{k}) \supset E_\gamma \setminus \mathcal{Z}(X_{0,0}) = E_{j_\gamma} \setminus \mathcal{Z}(H)$, $\gamma = 1, 2$, согласно вложению (27). Снова применяя теорему 1 работы [9], мы выясняем для всякого $j_1 \in I_1$ и для всякого $j_2 \in I_2$, верно ли, что $\Xi_{E_1} \subset E_2$. Это условие эквивалентно включению $\Xi_{j_1} \subset \overline{E}_{j_2}$, а также тому, что $\overline{E}_{j_1} \subset \overline{E}_{j_2}$, по лемме 2. Таким образом, мы строим подмножество

$$J = \{j \in I_1 \,:\, \Xi_j \not\subset \overline{E}_{j_2} \quad \text{для всех} \quad j_2 \in I_2\}.$$

Следовательно, согласно лемме 2, для всякого $j \in J$ и для всякого $j_2 \in J_2$ имеем $\Xi_j \not\subset W^{(j_2)} \cap \overline{\Delta}$. Для всякого $j \in J$ обозначим

$$E_j = \overline{E} \setminus \Big(\bigcup_{1 \le \alpha \le \nu} \; \bigcup_{b_\alpha + 1 \le i \le a_\alpha} W_\alpha^{(i)} \Big),$$

где E – определённая над k и и неприводимая над k компонента многообразия $W^{(j_1)} \cap \overline{\Delta}$ для некоторого $j_1 \in J_1$, такая, что $\Xi_j = \Xi_E$, и $\overline{E}$ определено выше. Теперь E_j, $j \in J$, – семейство всех определённых над k и и неприводимых над k компонент пересечения $W_1 \cap \ldots \cap W_\nu$, согласно свойству (а) и поскольку $H \in \mathcal{H}_1 \subset \mathcal{H}_0$.

Положим

$$(L'_0, L'_{\sigma+1}, \ldots, L'_n) = (L''_0, L''_{\sigma_1+1}, \ldots, L''_{n\nu})$$

и $L' = (L'_0, L'_{\sigma+1}, \ldots, L'_n)$ (следовательно, $\sigma = \sigma_1 - n(\nu-1)$). Мы строим L'. Рассмотрим гомоморфизм $\overline{k}$–алгебр $\tau : \overline{k}[X_{0,0}, X_{i,j},\ 1 \le i \le \nu,\ 1 \le j \le n] \to \overline{k}[X_0, \ldots, X_n]$, такой, что $\tau(X_{0,0}) = H$, $\tau(X_{i,j}) = X_j$ для всех $1 \le i \le \nu$, $1 \le j \le n$. Положим

$$(L_0, \ldots, L_{n+1}) = (\tau(L'''_0), \tau(L'''_{n(\nu-1)+1}), \tau(L'''_{n(\nu-1)+2}), \ldots, \tau(L'''_{n\nu+1}))$$

и построим линейные формы $L_0, \ldots, L_{n+1}$. В силу изоморфизма (12) мы имеем $\Xi_j \subset \mathbb{A}^n(\overline{k}) \subset \mathbb{P}^n(\overline{k})$ для всякого $j \in J$ (соответственно $j \in I_1$, $j \in I_2$). Согласно описанной конструкции, справедливо утверждение (а) теоремы 1 для полученных E_j, Ξ_j, $j \in J$, линейных форм $L'_0, L'_{\sigma+1}, \ldots, L'_n$ и $L_0, \ldots, L_{n+1}$ для всякого $H \in \mathcal{H}_1$. Напомним, что эти объекты зависят от H.

Теперь мы слегка изменим обозначения. *В дальнейшем в общем случае для того, чтобы учесть зависимость от H, мы будем писать*

$J(H)$ вместо J и $\Xi_j(H)$ вместо Ξ_j для всякого $j \in J(H)$. Выберем $H_0 \in \mathcal{H}_1$. Положим $J = J(H_0)$, $\Xi_j = \Xi_j(H_0)$ для всякого $j \in J(H_0)$ и возьмем $L'_0, L'_{\sigma+1}, \dots, L'_n$, $L_0, \dots, L_{n+1}$ равными построенным линейным формам, соответствующим H_0. Таким образом, утверждение (a) доказано.

Докажем (c). Будем перебирать линейные формы $H \in \mathcal{H}_1$. Предположим, что $z \notin \mathcal{Z}(H)$. Тогда мы перебираем $j \in J(H)$. Выберем определённую над k и неприводимую над k компоненту E многообразия $W^{(j_1)} \cap \overline{\Delta}$ для некоторого $j_1 \in J_1$, такую, что $\Xi_j(H) = \Xi_E$, см. выше. Используя изоморфизм (12) и применяя теорему 1 работы [9], мы выясняем, верно ли, что $z \in E$ (соответственно $z \in \bigcup\limits_{j_2 \in J_2} (W^{(j_2)} \cap \overline{\Delta})$). Теперь $z \in E_j$ тогда и только тогда, когда $z \in E$ и $z \notin \bigcup_{j_2 \in J_2} (W^{(j_2)} \cap \overline{\Delta})$. Если $z \in E_j$, то кратность $\mu(z, E_j) = \mu(z, E)$ вычисляется согласно теореме 1(c) работы [9], применённой к $V^{(j_1)}, W^{(j_1)}, p^{(j_1)}$ вместо V, W, p.

Заметим, что согласно лемме 2 и нашей конструкции, для всякого $H \in \mathcal{H}_1$ для всякого $j \in J(H)$ пересечение $\Xi_j \cap (\bigcup_{H' \in \mathcal{H}_1} \mathcal{Z}(H'))$ пусто. Следовательно, используя рассмотренный случай $z \notin \mathcal{Z}(H_0)$ и применяя теорему 1 работы [9], можно выяснить для всякого $H \in \mathcal{H}_1$ для всякого $j \in J(H)$ для всякого $j_0 \in J$, верно ли, что $\Xi_j \subset E_{j_0}$. По лемме 2 включение $\Xi_j \subset E_{j_0}$ выполнено тогда и только тогда, когда $E_j = E_{j_0}$. Таким образом, мы можем построить такую биекцию $\gamma_H : J(H) \to J$, что $E_{\gamma_H(j)} = E_j$ для всякого $j \in J(H)$. В дальнейшем, заменяя $J(H)$ на J при помощи γ_H, мы будем предполагать без ограничения общности, что $J(H) = J$ и γ_H – тождественное отображение для всякого $H \in \mathcal{H}_1$.

Наконец, для всякой точки $z \in \mathbb{P}^n(\overline{k})$ существует линейная форма $H \in \mathcal{H}_1$, такая, что $H(z) \neq 0$, поскольку $\mathcal{H}_1 \subset \mathcal{H}$ и $\#\mathcal{H}_1 = n + 1$. Таким образом, можно выяснить, верно ли, что $z \in E_j$, и вычислить кратность $\mu(z, E_j)$ для всякого $j \in J$. Утверждение (c) доказано.

Докажем (b). Пусть E_j, $j \in J$, – определённая над k и неприводимая над k компонента многообразия $W_1 \cap \ldots \cap W_\nu$ и последнее пересечение собственно в E_j. Тогда $\widetilde{E}_j$ является неприводимой над k компонентой многообразия $\widetilde{W}_1 \cap \ldots \cap \widetilde{W}_\nu$ и $i_{\mathbb{P}^n(\overline{k})}(W_1, \dots, W_\nu; E_j) = i_{\mathbb{A}^n(\overline{k})}(\widetilde{W}_1, \dots, \widetilde{W}_\nu; \widetilde{E}_j)$. Как и выше, мы отождествляем $\widetilde{E}_j$ с определённой над k и неприводимой над k компонентой пересечения $(\widetilde{W}_1 \times \ldots \times \widetilde{W}_\nu) \cap \Delta$. Теперь при помощи редукции к диагонали,

см. введение работы [13], мы получаем, что $i_{\mathbb{A}^n(\overline{k})}(\widetilde{W}_1,\dots,\widetilde{W}_\nu;\widetilde{E}_j) = i_{\mathbb{A}^{n\nu}(\overline{k})}(\widetilde{W}_1\times\ldots\times\widetilde{W}_\nu,\Delta;\widetilde{E}_j)$. Пусть $\widetilde{E}$ (соответственно E) – замыкание многообразия $\widetilde{E}_j$ в $\mathbb{A}^{n\nu}(\overline{k})$ (соответственно $\mathbb{P}^{n\nu}(\overline{k})$) относительно топологии Зарискoго.

Положим $i(Q^{(1)},Q^{(2)};Q^{(3)})=0$ для любых проективных (соответственно аффинных) алгебраических многообразий $Q^{(1)},Q^{(2)},Q^{(3)}$, таких, что $Q^{(3)}$ определено над k и неприводимо над k и $Q^{(3)}$ не является неприводимой компонентой пересечения $Q^{(1)}\cap Q^{(2)}$.

Пусть $\gamma\in J_{i_1,\dots,i_\nu}$ для некоторого $(i_1,\dots,i_\nu)\in B_1$. Предположим, что E является неприводимой компонентой многообразия $\overline{W}_{i_1,\dots,i_\nu}\cap\overline{\Delta}$. Тогда пересечение $\overline{W}_{i_1,\dots,i_\nu}\cap\overline{\Delta}$ собственно в E. Напомним, что $e_0,\dots,e_r$ порождают идеал многообразия $\overline{\Delta}\subset\mathbb{P}^{n\nu}(\overline{k})$ и $\dim\overline{\Delta}=n\nu-r-1$. Следовательно, каждое e_w, $0\le w\le r$, является линейной комбинацией элементов $e''_0,e''_{\sigma_1+1},\dots,e''_{n\nu}$. Поэтому $n\nu-\sigma_1=r$, многообразие E является неприводимой компонентой пересечения $W^{(\gamma)}_{n\nu}(L'')\cap\mathcal{Z}(e''_{n\nu+1})$ и последнее пересечение собственно в E. Напомним, что $e''_0=e''_{n\nu+1}$, см. введение из [9]. Следовательно, по свойству индексов пересечения, соответствующему ассоциативности пересечения,

$$\begin{aligned} &i_{\mathbb{P}^{n\nu}(\overline{k})}(W^{(\gamma)},\overline{\Delta};E)=i_{\mathbb{P}^{n\nu}(\overline{k})}(W^{(\gamma)},\mathcal{Z}(e''_{\sigma_1+1}\dots,e''_{n\nu+1});E)\\ &=\sum_{E'}i_{\mathbb{P}^{n\nu}(\overline{k})}(W^{(\gamma)},\mathcal{Z}(e''_{\sigma_1+1},\dots,e''_{n\nu});E')i_{\mathbb{P}^{n\nu}(\overline{k})}(E',\mathcal{Z}(e''_{n\nu+1});E),\end{aligned}$$

где E' пробегает все определённые над k и неприводимые над k компоненты многообразия $W^{(\gamma)}_{n\nu}(L'')$. Но (см. введение из [9]) для всякого E' индекс пересечения $i(W^{(\gamma)},\mathcal{Z}(e''_{\sigma_1+1},\dots,e''_{n\nu});E')$ равен 1, поскольку $L''\in\mathcal{U}'_{j,0}$ (см. обозначения перед формулировкой леммы 2). Следовательно, $i(W^{(\gamma)},\overline{\Delta};E)=\sum\limits_{E'}i(E',\mathcal{Z}(e''_{n\nu+1});E)=i(W^{(\gamma)}_{n\nu}(L''),\mathcal{Z}(e''_{n\nu+1});E)$.

Теперь согласно общим свойствам индексов пересечения

$$i_{\mathbb{A}^{n\nu}(\overline{k})}(\widetilde{W}_1\times\ldots\times\widetilde{W}_\nu,\Delta;\widetilde{E}_j)=\sum_{(i,\dots,i_\nu)\in B_1}i_{\mathbb{A}^{n\nu}(\overline{k})}(W_{i_1,\dots,i_\nu},\Delta;\widetilde{E})$$

$$= \sum_{(i,\dots,i_\nu)\in B_1} i_{\mathbb{P}^{n\nu}(\overline{k})}(\overline{W}_{i_1,\dots,i_\nu}, \overline{\Delta}; E)$$
$$= \sum_{(i,\dots,i_\nu)\in B_1} \sum_{\gamma\in J_{i_1,\dots,i_\nu}} i_{\mathbb{P}^{n\nu}(\overline{k})}(E_\gamma, \overline{\Delta}; E)$$
$$= \sum_{(i,\dots,i_\nu)\in B_1} \sum_{\gamma\in J_{i_1,\dots,i_\nu}} i_{\mathbb{P}^{n\nu}(\overline{k})}(W_{n\nu}^{(\gamma)}(L''), \mathcal{Z}(e''_{n\nu+1}); E).$$

Мы вычисляем каждый индекс $i_{\mathbb{P}^{n\nu}(\overline{k})}(W_{n\nu}^{(\gamma)}(L''), \mathcal{Z}(e''_{n\nu+1}); E)$, применяя теорему 1(f) работы [9]. Затем можно сосчитать по данной формуле индекс $i_{\mathbb{A}^{n\nu}(\overline{k})}(\widetilde{W}_1 \times \ldots \times \widetilde{W}_\nu, \Delta; \widetilde{E}_j) = i_{\mathbb{P}^n(\overline{k})}(W_1, \dots, W_\nu; E_j)$. Равенство $i_{\mathbb{P}^n(\overline{k})}(W_1, \dots, W_\nu; E_j) = i_{\mathbb{P}^n(\overline{k})}(W_1, \dots, W_\nu, \mathcal{Z}(L_{s+1}, \dots, L_n); \xi)$ следует из свойства индексов пересечения, соответствующего ассоциативности пересечения. Утверждение (b) доказано.

При помощи изоморфизма (12) утверждение (d) немедленно следует из утверждения (g) теоремы 1 работы [9], применённой для всякого $j_0 \in J_0$ к $V^{(j_0)}, W^{(j_0)}, p^{(j_0)}$ вместо V, W, p.

Требуемые оценки на время работы алгоритмов из теоремы 1 немедленно следуют из оценок на время работы использованных алгоритмов. Теорема доказана.

2. Доказательство теоремы 2

Доказательство теоремы 2 аналогично доказательству теоремы 1. Более того, мы сведём теорему 2 к теореме 1. Если $\nu = \nu_1$, то все утверждения теоремы 2 немедленно следуют из теоремы 1. Таким образом, в дальнейшем мы будем считать без ограничения общности, что $\nu > \nu_1$ и поэтому $\nu \geq 2$. Кроме того, мы будем считать, что $n \geq 1$.

Положим $\mathcal{V}_\alpha^{(1)} = \mathcal{W}_\alpha^{(1)} = \mathbb{P}^n(\overline{k})$ и $\mathcal{V}_\alpha^{(j)} = V_\alpha^{(j-1)}$, $\mathcal{W}_\alpha^{(j)} = W_\alpha^{(j-1)}$ для всякого $1 \leq \alpha \leq \nu$, $2 \leq j \leq a_\alpha + 1$. Заменим для всякого $1 \leq \alpha \leq \nu$ пару (a_α, b_α) на $(a_\alpha + 1, b_\alpha + 1)$. Теперь естественным образом выполняются условия из формулировки теоремы 1 для $\mathcal{V}_\alpha^{(j)}$, $\mathcal{W}_\alpha^{(j)}$, $1 \leq j \leq a_\alpha + 1$, вместо $V_\alpha^{(j)}$, $W_\alpha^{(j)}$, $1 \leq j \leq a_\alpha$. Мы применяем конструкцию из доказательства теоремы 1 к $\mathcal{V}_\alpha^{(j)}$, $\mathcal{W}_\alpha^{(j)}$, $1 \leq j \leq a_\alpha + 1$, вместо $V_\alpha^{(j)}$, $W_\alpha^{(j)}$, $1 \leq j \leq a_\alpha$.

В дальнейшем $\mathcal{H}$, B_1 B_2, $J_{i_1,\dots,i_\nu}$ для $(i_1, \dots, i_\nu) \in B_1$, $J_{\alpha;i}$ для $(\alpha, i) \in B_2$, J_0, J_1, J_2, множества точек Ξ_E для всех определённых над k и неприводимых над k компонент E многообразий $W^{(j)} \cap \overline{\Delta}$ для всех $j \in J_0$, $\mathcal{H}_1$, линейные формы $L_0, \dots, L_{n+1}$, $L'_0, L'_{\sigma+1}, \dots, L'_n$ и другие

объекты, построенные в доказательстве теоремы 1, соответствуют $\mathcal{V}_\alpha^{(j)}$, $\mathcal{W}_\alpha^{(j)}$, $1 \le j \le a_\alpha + 1$. В настоящее время мы предполагаем, что Ξ_E и линейные формы $L_0, \dots, L_{n+1}$, $L'_0, L'_{\sigma+1}, \dots, L'_n$ соответствуют $H \in \mathcal{H}_1$ и, следовательно, зависят от H, см. раздел 1 (мы не фиксируем H_0 на этом этапе). Для всякого $H \in \mathcal{H}_1$ мы осуществляем следующую конструкцию. Некоторые объекты ниже зависят от H, хотя мы не указываем на это явно в обозначениях. Положим

$$
\begin{aligned}
B_{1,1} &= \{(i_1, \dots, i_{\nu_1}, 1, \dots, 1) \in B_1 \,:\, 2 \le i_\alpha \le b_\alpha + 1 \,\forall\, 1 \le \alpha \le \nu_1\},\\
\mathcal{B}_{1,1} &= \{(i_1, \dots, i_{\nu_1}) \,:\, (i_1, \dots, i_{\nu_1}, 1, \dots, 1) \in B_{1,1}\},\\
J_{1,1} &= \bigcup_{(i_1,\dots,i_\nu)\in B_{1,1}} J_{i_1,\dots,i_\nu},\\
B_{1,2} &= \{(1, \dots, 1, i_{\nu_1+1}, \dots, i_\nu) \in B_1 \,:\, 2 \le i_\alpha \le b_\alpha + 1 \,\forall\, \nu_1 + 1 \le \alpha \le \nu\},\\
\mathcal{B}_{1,2} &= \{(i_{\nu_1+1}, \dots, i_\nu) \,:\, (1, \dots, 1, i_{\nu_1+1}, \dots, i_\nu) \in B_{1,2}\},\\
J_{1,2}7 &= \bigcup_{(i_1,\dots,i_\nu)\in B_{1,2}} J_{i_1,\dots,i_\nu},\\
B_{2,1}7 &= \{(\alpha, i) \in B_2 \,:\, 1 \le \alpha \le \nu_1\},\\
J_{2,1}7 &= \bigcup_{(\alpha,i)\in B_{2,1}} J_{\alpha;i},\\
B_{2,2}7 &= \{(\alpha, i) \in B_2 \,:\, \nu_1 + 1 \le \alpha \le \nu\},\\
J_{2,2}7 &= \bigcup_{(\alpha,i)\in B_{2,2}} J_{\alpha;i}.
\end{aligned}
$$

Ниже мы используем определение компоненты, которая максимальна относительно множества индексов. Это определение дано в разделе 1. Применяя теорему 1 работы [9], мы строим семейство Ξ_j, $j \in I_{1,1}$ (соответственно $j \in I_{1,2}$, $j \in I_{2,1}$, $j \in I_{2,2}$), такое, что

- для всякого $j \in I_{1,1}$ (соответственно $j \in I_{1,2}$, $j \in I_{2,1}$, $j \in I_{2,2}$) множество Ξ_j есть Ξ_E для некоторой определённой над k и неприводимой над k компоненты E многообразия $W^{(j')} \cap \overline{\Delta}$ с $j' \in J_{1,1}$ (соответственно $j' \in J_{1,2}$, $j' \in J_{2,1}$, $j' \in J_{2,2}$), такой, что $E \not\subset \mathcal{Z}(X_{0,0})$ и E максимальна относительно $J_{1,1} \cup J_{1,2}$ (соответственно относительно $J_{1,2}$, $J_{2,1} \cup J_{2,2}$, $J_{2,2}$).
- обратно, для всякого $j' \in J_{1,1}$ (соответственно $j' \in J_{1,2}$, $j' \in J_{2,1}$, $j' \in J_{2,2}$) для всякой определённой над k и неприводимой над k компоненты E многообразия $W^{(j')} \cap \overline{\Delta}$, такой, что $E \not\subset \mathcal{Z}(X_{0,0})$ и

E максимально относительно $J_{1,1}\cup J_{1,2}$ (соответственно относительно $J_{1,2}$, $J_{2,1}\cup J_{2,2}$, $J_{2,2}$), существует $j\in I_{1,1}$ (соответственно $j\in I_{1,2}$, $j\in I_{2,1}$, $j\in I_{2,2}$) с $\Xi_j=\Xi_E$,

- для всех $j_1,j_2\in I_{1,1}$ (соответственно $j_1,j_2\in I_{1,2}$, $j_1,j_2\in I_{2,1}$, $j_1,j_2\in I_{2,2}$), если $j_1\neq j_2$, то $\Xi_{j_1}\neq\Xi_{j_2}$, и, следовательно, $E_{j_1}\neq E_{j_2}$ по лемме 2.

Для всякого $j\in I_{1,1}\cup I_{1,2}\cup I_{2,1}\cup I_{2,2}$ положим $\overline{E}_j=\overline{E}$, где $\Xi_j=\Xi_E$ и $\overline{E}$ – замыкание $E\setminus\mathcal{Z}(X_{0,0})$ в $\mathbb{P}^n(\overline{k})$ относительно топологии Зариского согласно включению (27). Теперь $\overline{E}_j$, $j\in I_{1,1}$ (соответственно $j\in I_{1,2}$, $j\in I_{2,1}$, $j\in I_{2,2}$) является семейством всех определённых над k и неприводимых над k компонент многообразия $\bigcup_{(i_1,\dots,i_{\nu_1})\in\mathcal{B}_{1,1}}\bigcap\limits_{1\le\alpha\le\nu_1}W_\alpha^{(i_\alpha)}$ (соответственно $\bigcup\limits_{1\le\alpha\le\nu_1}\bigcup\limits_{b_\alpha+1\le i\le a_\alpha}W_\alpha^{(i)}$, $\bigcup\limits_{(i_{\nu_1+1},\dots,i_\nu)\in\mathcal{B}_{1,2}}\bigcap\limits_{\nu_1+1\le\alpha\le\nu}W_\alpha^{(i_\alpha)}$, $\bigcup\limits_{\nu_1+1\le\alpha\le\nu}\bigcup\limits_{b_\alpha+1\le i\le a_\alpha}W_\alpha^{(i)}$) согласно лемме 2, свойству (а) из раздела 1 и поскольку $H\in\mathcal{H}_1\subset\mathcal{H}_0$.

Пусть $j_1\in I_{i,1}$, $j_2\in I_{i,2}$ для некоторых $i=1,2$. Пусть $\mathbb{P}^{n\nu}(\overline{k})\supset E_\gamma\setminus\mathcal{Z}(X_{0,0})=E_{j_\gamma}\setminus\mathcal{Z}(H)$, $\gamma=1,2$, согласно отождествлению (27). Снова применяя теорему 1 работы [9], мы выясняем для всякого $i=1,2$ для всякого $j_1\in I_{i,1}$ для всякого $j_2\in I_{i,2}$, верно ли, что $\Xi_{E_1}\subset E_2$. Это включение эквивалентно включению $\Xi_{j_1}\subset\overline{E}_{j_2}$, а также тому, что $\overline{E}_{j_1}\subset\overline{E}_{j_2}$, по лемме 2. Таким образом, мы строим для $i=1,2$ множество

$$J^{(i)}=\{j\in I_{i,1}:\Xi_j\not\subset\overline{E}_{j_2}\quad\text{для всех}\quad j_2\in I_{i,2}\}.$$

Следовательно, по лемме 2 для всякого $j\in J^{(i)}$ и для всякого $j_2\in J_{i,2}$ имеем $\Xi_j\not\subset W^{(j_2)}\cap\overline{\Delta}$ для $i=1,2$. Напомним, что $A^{(1)}=\{1,\dots,\nu_1\}$, $A^{(2)}=\{\nu_1+1,\dots,\nu\}$, см. формулировку теоремы 2. Для всякого $j\in J^{(i)}$ обозначим

$$E_j=\overline{E}\setminus\Big(\bigcup_{\alpha\in A^{(i)}}\bigcup_{b_\alpha+1\le i\le a_\alpha}W_\alpha^{(i)}\Big),$$

где E – определённая над k и неприводимая над k компонента многообразия $W^{(j_1)}\cap\overline{\Delta}$ для некоторого $j_1\in J_{i,1}$, такого, что $\Xi_j=\Xi_E$, и $\overline{E}$ определено выше. Следовательно, E_j, $j\in J^{(i)}$, – семейство всех определённых над k и неприводимых над k компонент многообразия $\bigcap\limits_{\alpha\in A^{(i)}}W_\alpha$ согласно свойству (а) из раздела 1 и так как $H\in\mathcal{H}_1\subset\mathcal{H}_0$.

Теперь мы слегка изменим обозначения. *В дальнейшем в общем случае, чтобы учесть зависимость от H для всякого $i=1,2$, мы пишем $J^{(i)}(H)$ вместо $J^{(i)}$ и $\Xi_j(H)$ вместо Ξ_j для всякого $j\in J^{(i)}(H)$.*

Выберем $H_0 \in \mathcal{H}_1$, *ср. конструкцию из доказательства теоремы 1. Положим* $J^{(i)} = J^{(i)}(H_0)$, $\Xi_j = \Xi_j(H_0)$ *для всякого* $j \in J^{(i)}(H_0)$ *и возьмем* $L'_0, L'_{\sigma+1}, \ldots, L'_n$, $L_0, \ldots, L_{n+1}$ *равными построенным линейным формам, соответствующим* H_0. Теперь выполняется утверждение (a) теоремы 2. Утверждение (a) доказано.

Для всякого $i = 1, 2$ для всякого $H \in \mathcal{H}_1$ для всякого $j \in J^{(i)}(H)$ для всякого $j_0 \in J^{(i)}$, применяя утверждение (c) теоремы 1, можно выяснить, верно ли, что $\Xi_j \subset E_{j_0}$. Согласно лемме 2, включение $\Xi_j \subset E_{j_0}$ выполнено тогда и только тогда, когда $E_j = E_{j_0}$. Таким образом, мы можем построить биекцию $\gamma_{i,H} : J^{(i)}(H) \to J^{(i)}$, такую, что для всякого $j \in J^{(i)}(H)$ неприводимая компонента $E_{\gamma_{i,H}(j)}$ есть E_j. В дальнейшем, заменяя $J^{(i)}(H)$ на $J^{(i)}$ при помощи $\gamma_{i,H}$, мы будем предполагать без ограничения общности, что $J^{(i)}(H) = J^{(i)}$ и $\gamma_{i,H}$ – тождественное отображение для всякого $H \in \mathcal{H}_1$ и для всякого $i = 1, 2$.

Докажем утверждение (b). Пусть $j_1 \in J^{(1)}$, $j_2 \in J^{(2)}$ – произвольные индексы. Пусть $H \in \mathcal{H}_1$ – произвольная линейная форма. Напомним, что существуют $j'_i \in J_{1,i}$, $i = 1, 2$, и определённая над k и неприводимая над k компонента E_i многообразия $W^{(j'_i)} \cap \overline{\Delta}$, такие, что $\Xi_{j_i} = \Xi_{E_i}$. Мы выбираем такие j'_i и E_i для всякого $H \in \mathcal{H}_1$ и всякого $i = 1, 2$. Тогда по лемме 2 и описанной конструкции включение $E_{j_1} \subset \overline{E}_{j_2}$ выполняется в том и только в том случае, если $\Xi_{E_1} \subset E_2$ для $H = H_0$ (или любого другого фиксированного $H \in \mathcal{H}_1$). Мы выясняем, верно ли, что $\Xi_{E_1} \subset E_2$, используя утверждение (c) теоремы 1. Утверждение (b) доказано.

Докажем утверждение (c). Пусть $j_1 \in J^{(1)}$, $j_2 \in J^{(2)}$ – произвольные индексы. Напомним, что в настоящее время $\mathcal{H}_1$ – множество из конструкции из доказательства теоремы 1 с $\mathcal{V}_\alpha$, $\mathcal{W}_\alpha$ вместо V_α, W_α (см. выше) и $\bigcap_{H \in \mathcal{H}_1} \mathcal{Z}(H) = \varnothing$ в $\mathbb{P}^n(\overline{k})$ согласно свойству (b) из раздела 1. Теперь $E_{j_1} \subset E_{j_2}$ тогда и только тогда, когда $E_{j_1} \subset \overline{E}_{j_2}$ и для всякого $H \in \mathcal{H}_1$

$$(E_{j_1} \setminus \mathcal{Z}(H)) \cap \Big(\bigcup_{\nu_1+1 \le \alpha \le \nu} \bigcup_{b_\alpha+1 \le j \le a_\alpha} W_\alpha^{(j)} \Big) \subset \bigcup_{1 \le \alpha \le \nu_1} \bigcup_{b_\alpha+1 \le j \le a_\alpha} W_\alpha^{(j)}. \tag{28}$$

Таким образом, остаётся выяснить, для всякого ли $H \in \mathcal{H}_1$ выполняется условие (28).

Мы перебираем $H \in \mathcal{H}_1$. Пусть $j'_i \in J_{1,i}$, $i = 1, 2$, и неприводимые компоненты E_i многообразий $W^{(j'_i)} \cap \overline{\Delta}$ – такие же, как и выше. На-

помним, что $j_1' \in J_{i_1,\dots,i_\nu}$, где $i_1,\dots,i_\nu$ известны согласно нашей конструкции (и $i_1,\dots,i_{\nu_1} \geq 2$, $i_{\nu_1+1} = \dots = i_\nu = 1$). Мы отождествляем $E_{j_1} \setminus \mathcal{Z}(H)$ с $E_1 \setminus \mathcal{Z}(X_{0,0})$. Напомним, что в доказательстве теоремы 1 определены алгебраические многообразия $V_{i_1,\dots,i_\nu}$, $\overline{V}_{i_1,\dots,i_\nu}$. Теперь $V_{i_1,\dots,i_\nu}$, $\overline{V}_{i_1,\dots,i_\nu}$ соответствуют $\mathcal{V}_\alpha$, $\mathcal{W}_\alpha$ вместо V_α, W_α, см. выше. Аналогично для всякого $1 \leq \alpha \leq \nu$ и для всякого $b_\alpha + 2 \leq j \leq a_\alpha + 1$ определены алгебраические многообразия $V_{\alpha;j}$, $W_{\alpha;j}$, $\overline{V}_{\alpha;j}$, $\overline{W}_{\alpha;j}$. Они также соответствуют $\mathcal{V}_\alpha$, $\mathcal{W}_\alpha$ вместо V_α, W_α.

Далее, мы отождествляем $E_1 \setminus \mathcal{Z}(X_{0,0})$ с неприводимой компонентой многообразия $V_{i_1,\dots,i_\nu} \cap \Delta$ и E_1 с неприводимой компонентой многообразия $\overline{V}_{i_1,\dots,i_\nu} \cap \overline{\Delta}$. Следовательно, для всякого $\nu_1 + 1 \leq \alpha \leq \nu$ и для всякого $b_\alpha + 2 \leq j \leq a_\alpha + 1$ алгебраическое многообразие $(E_{j_1} \setminus \mathcal{Z}(H)) \cap W_\alpha^{(j)}$ отождествляется с $(E_1 \setminus \mathcal{Z}(X_{0,0})) \cap W_{\alpha;j} = E_1 \cap \overline{W}_{\alpha;j} \setminus \mathcal{Z}(X_{0,0})$. Теперь условие (28) эквивалентно включению

$$E_1 \cap \Big(\bigcup_{\nu_1+1 \leq \alpha \leq \nu} \bigcup_{b_\alpha+2 \leq j \leq a_\alpha+1} \overline{W}_{\alpha,j} \Big) \subset \bigcup_{1 \leq \alpha \leq \nu_1} \bigcup_{b_\alpha+2 \leq j \leq a_\alpha+1} (\overline{W}_{\alpha,j} \cup \mathcal{Z}(X_{0,0})). \tag{29}$$

Алгебраическое многообразие $\overline{V}_{i_1,\dots,i_\nu} \cap \overline{\Delta}$ задано явно системой однородных полиномиальных уравнений относительно $X_{0,0}$, $X_{i,j}$, $1 \leq i \leq \nu$, $1 \leq j \leq n$. Согласно описанной конструкции, можно найти представление ρ_1 многообразия E_1, такое, что $n(\rho_1) = n\nu$, $a(\rho_1) = b(\rho_1) = 1$, $q_1(1,\rho_1) = (\overline{V}_{i_1,\dots,i_\nu} \cap \overline{\Delta})$, $\mathcal{Z}(X_{0,0})$, $q_2(1,\rho_1) = E_1$.

Построим некоторые биекции

$$\tau_1 : \Big\{1,\dots, \sum_{1 \leq \alpha \leq \nu_1} (a_\alpha - b_\alpha)\Big\} \to \{(\alpha,j) : 1 \leq \alpha \leq \nu_1 \;\; b_\alpha + 2 \leq j \leq a_\alpha + 1\},$$

$$\tau_2 : \Big\{1,\dots, \sum_{\nu_1+1 \leq \alpha \leq \nu} (a_\alpha - b_\alpha)\Big\} \to \{(\alpha,j) : \nu_1 + 1 \leq \alpha \leq \nu \;\; b_\alpha + 2 \leq j \leq a_\alpha + 1\}.$$

Алгебраическое многообразие $\overline{V}_{\alpha;j}$ задано явно системой однородных полиномиальных уравнений относительно $X_{0,0}$, $X_{i,w}$, $1 \leq i \leq \nu$, $1 \leq w \leq n$. Согласно описанной конструкции, можно найти представление ρ' (соответственно ρ'') многообразия $\bigcup_{1 \leq \alpha \leq \nu_1} \bigcup_{b_\alpha+2 \leq j \leq a_\alpha+1} (\overline{W}_{\alpha,j} \cup$

$\mathcal{Z}(X_{0,0})$) (соответственно $\bigcup\limits_{\nu_1+1\le\alpha\le\nu}\ \bigcup\limits_{b_\alpha+2\le j\le a_\alpha+1}\overline{W}_{\alpha,j}$), такое, что $n(\rho')=n\nu$, $a(\rho')=b(\rho')=\sum_{1\le\alpha\le\nu_1}(a_\alpha-b_\alpha)$, $q_1(i,\rho')=\overline{V}_{\alpha;j}\cup\mathcal{Z}(X_{0,0})$, $q_2(i,\rho')=\overline{W}_{\alpha;j}\cup\mathcal{Z}(X_{0,0})$ (соответственно $n(\rho'')=n\nu$, $a(\rho'')=b(\rho'')=\sum\limits_{\nu_1+1\le\alpha\le\nu}(a_\alpha-b_\alpha)$, $q_1(i,\rho'')=\overline{V}_{\alpha;j}\cup\mathcal{Z}(X_{0,0})$, $q_2(i,\rho'')=\overline{W}_{\alpha;j}$), где $(\alpha,j)=\tau_1(i)$ (соответственно $(\alpha,j)=\tau_2(i)$).

Наконец, применяя утверждение (b) теоремы 2 с $(3,2,n\nu)$ вместо (ν,ν_1,n) и с

$$E_1,\ \bigcup_{\nu_1+1\le\alpha\le\nu}\ \bigcup_{b_\alpha+2\le j\le a_\alpha+1}\overline{W}_{\alpha,j},\ \bigcup_{1\le\alpha\le\nu_1}\ \bigcup_{b_\alpha+2\le j\le a_\alpha+1}(\overline{W}_{\alpha,j}\cup\mathcal{Z}(X_{0,0})),$$

заданными ρ_1, ρ'', ρ' (вместо $W_1,\dots,W_\nu$, заданных $\rho_1,\dots,\rho_\nu$, см. обозначения перед формулировкой теоремы 1), мы выясняем, справедливо ли условие (29). Как мы видели, $E_{j_1}\subset E_{j_2}$ в том и только в том случае, если $E_{j_1}\subset\overline{E}_{j_2}$ и (29) выполняется для всякого $H\in\mathcal{H}$. Таким образом, утверждение (c) доказано.

Требуемые оценки на время работы алгоритмов из теоремы 2 немедленно следуют из оценок на время работы использованных алгоритмов. Теорема доказана.

Литература

1. Р. Хартсхорн, *Алгебраическая геометрия*. Мир, М. (1981).
2. А. Л. Чистов, *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время*. — Зап. научн. семин. ЛОМИ **137** (1984), 124–188.
3. А. Л. Чистов, *Вычисление степеней алгебраических многообразий над полем нулевой характеристики за полиномиальное время и его приложения*. — Зап. научн. семинаров ПОМИ **258** (1999), 7–59.
4. А. Л. Чистов, *Сильная версия основного разрешающего алгоритма для экзистенциональной теории первого порядка вещественно замкнутых полей*. — Зап. научн. семин. ПОМИ **256** (1999), 168–211.
5. А. Л. Чистов, *Эффективная конструкция локальных параметров неприводимых компонент алгебраического многообразия*. — Труды С.-Петербургского мат. общества **7** (1999), 230–266.
6. А. Л. Чистов, *Эффективная гладкая стратификация алгебраического многообразия в нулевой характеристике и её приложения*. — Зап. научн. семин. ПОМИ **266** (2000), 254–311.
7. А. Л. Чистов, *Монодромия и критерии неприводимости с алгоритмическими приложениями в нулевой характеристическе*. — Зап. научн. семин. ПОМИ **292** (2002), 130–152.

8. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время.* I. — Зап. научн. семин. ПОМИ **307** (2004), 189–235.
9. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время.* II. — Зап. научн. семин. ПОМИ **325** (2005), 181–224.
10. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время.* III. — Зап. научн. семин. ПОМИ **344** (2007), 203–239.
11. А. Л. Чистов, *Вычисление степени доминантного морфизма в нулевой характеристике за полиномиальное время.* IV. — Зап. научн. семин. ПОМИ **360** (2008), 260–294.
12. A. L. Chistov, *A deterministic polynomial-time algorithm for the first Bertini theorem.* Preprint of the St. Petersburg Mathematical Society 2004-09 (2004).
13. A. L. Chistov, *Polynomial–time computation of the dimension of algebraic varieties in zero–characteristic.* — J. Symbolic Comput. **22**, No. 1 (1996), 1–25.
14. A. L. Chistov, *Polynomial–time computation of the dimensions of components of algebraic varieties in zero–characteristic.* — J. Pure Appl. Algebra **117/118** (1997), 145–175.
15. A. L. Chistov, *Efficient algorithms in zero-characteristic for a new model of representation of algebraic varieties.* — In: Computer Science – Theory and Applications, Lecture Notes Comput. Sci. **3967** (2006), pp. 137–146.
16. A. L. Chistov, *A correction in the statement of my theorem on the efficient smooth cover and smooth stratification of an algebraic variety.* — Preprint of the St. Petersburg Math. Soc., #13 (2004).

Chistov A. L. Polynomial-time algorithms for a new model of representation of algebraic varieties (in characteristic zero).

We suggest a model of representation of algebraic varieties based on representative systems of points of their irreducible components. Deterministic polynomial-time algorithms that substantiate this model are described in characteristic zero. The main result here is a construction of the intersection of algebraic varieties. As applications, we obtain efficient algorithms for constructing the smooth stratification and smooth cover of an algebraic variety suggested by the author earlier.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
наб. р. Фонтанки, д. 27,
191023 Санкт-Петербург, Россия

E-mail: alch@pdmi.ras.ru

Поступило 9 сентября 2010 г.