Эффективная гладкая стратификация алгебраического многообразия в нулевой характеристике и её приложения

А. Л. Чистов

Санкт-Петербургский институт информатики
и автоматизации Российской академии наук,
199178 Санкт-Петербург, В.О. 14-ая линия, 39
e-mail: sliss@iias.spb.su

1999

Аннотация

Рассмотрим проективное алгебраическое многообразие V, заданное как множество всех общих нулей семейства однородных многочленов степеней меньше, чем d относительно $n+1$ переменных с коэффициентами из поля k нулевой характеристики. Мы доказываем, что V может быть представлено как объединение самое большее $C(n)d^n$ (соответственно $C(n)d^{n(n+1)/2}$) гладких квазипроективных многообразий (соответственно попарно не пересекающихся гладких квазипроективных многообразий) со степенями (степень квазипроективного алгебраического многообразия равна степени его замыкания в топологии Зарисского), ограниченными сверху $C(n)d^n$, где $C(n) < 2^{2^{n^C}}$ для абсолютной константы $C > 0$. Далее, в случае нулевой характеристики предлагаются алгоритмы для построения регулярных последовательностей и последовательностей локальных параметров для неприводимых компонент многообразия V. Сложность этих алгоритмов полиномиальна от длины записи входных данных и $C(n)d^n$. Наконец в случае, когда k является подполем $\mathbb{R}$, предлагается алгоритм для вычисления размерности множества $V(\mathbb{R})$ всех $\mathbb{R}$-точек V со сложностью полиномиальной от длины записи входных данных и $C(n)d^n$.

Введение

Пусть k – поле нулевой характеристики, и $\mathbb{P}^n(\overline{k})$ – n-мерное проективное пространство над алгебраическим замыканием $\overline{k}$ поля k, имеющее однородные координаты $X_0, \dots, X_n$. Рассмотрим проективное алгебраическое многообразие V, заданное как множество всех общих нулей семейства однородных многочленов степени меньше, чем d относительно $n+1$ переменных $X_0, \dots, X_n$ с коэффициентами из поля k.

ОПРЕДЕЛЕНИЕ 1 Гладкое покрытие *алгебраического многообразия V есть конечное семейство*

$$V_\alpha, \quad \alpha \in A, \tag{1}$$

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 $\alpha_1, \alpha_2 \in A$, если $\alpha_1 \neq \alpha_2$, то $V_{\alpha_1} \cap V_{\alpha_1} = \emptyset$.*

ЗАМЕЧАНИЕ 1 Пусть l_1 и l_2 – две различные прямые в $\mathbb{P}^2$. Тогда семейство квазипроективных алгебраических многообразий l_1 и $l_2 \setminus l_1$ определяет гладкую стратификацию многообразия $l_1 \cup l_2$. Этот пример показывает, что некоторые многообразия V_α могут содержать гладкие точки и особые точки V одновременно.

В этой статье мы введём новое представление квазипроективных алгебраических многообразий удобное с алгоритмической точки зрения. Используя это представление, мы доказываем существование гладкого покрытия и гладкой стратификации (1), таких что для всякого $\alpha \in A$ степень замыкания в топологии Зарисского $\deg \overline{V}_\alpha$ ограничена сверху величиной $2^{2^{n^C}} d^n$, где $C > 0$ – абсолютная константа. Кроме того, число элементов $\#A$ ограничено сверху величиной $2^{2^{n^C}} d^n$ для случая гладкого покрытия и $2^{2^{n^C}} d^{n(n+1)/2}$ для случая гладкой стратификации. Подробные формулировки см. в Теореме 2 и Теореме 4 из Раздела 2. Константа C (а также другие константы ниже) может быть вычислена явно при помощи доказательств из статьи и из [5].

Используя результаты настоящей статьи, [4], [6], можно предложить в случае нулевой характеристики алгоритмы для построения гладкого покрытия (соответственно гладкой стратификации) V за полиномиальное время от длины записи входных данных и $2^{2^{n^C}} d^n$ (соответственно $2^{2^{n^C}} d^{n(n+1)/2}$) для абсолютной константы $C > 0$, см. Замечание 3 ниже. В дальнейшем, если будет интерес к этой тематике, мы надеемся описать эти алгоритмы в одной из следующих статей. Здесь следует использовать результаты [4]. Метод [4] является по-существу классическим. Алгоритм из [4] имеет полиномиальную сложность и содержит поучительные (с точки зрения теории вычислений) идеи из алгебры и анализа.

В алгоритмической части статьи в случае нулевой характеристики и, когда поле k является конечнопорождённым расширением $\mathbb{Q}$, мы описываем алгоритм для построения последовательностей локальных параметров для компонент алгебраических многообразий за полиномиальное время от длины записи входных данных и $2^{2^{n^C}} d^n$, где $C > 0$ является абсолютной константой, см. Теорему 1. В случае, когда k является подполем $\mathbb{R}$, существование гладкого покрытия, доказанное в Теореме 2, позволяет построить алгоритм для вычисления размерности вещественного алгебраического многообразия $V(\mathbb{R})$ за полиномиальное время от длины записи входных данных и $2^{2^{n^C}} d^n$, см. Теорему 3.

В настоящей статье доказательства основываются на [5], [7]. В [5] описана эффективная конструкция (в математическом смысле, без алгоритмов) регулярных последовательностей и последовательностей локальных параметров в локальных кольцах компонент алгебраических многообразий. Используя эффективные оценки для степеней локальных параметров из [5] и результаты из [7], мы предлагаем алгоритм для построения регулярных последовательностей и последовательностей локальных параметров в локальном кольце компоненты размерности $n - s$ алгебраического многообразия V за полиномиальное время от длины записи входных данных и $n^{2^{s^C}} d^n$.

Перейдём к точным формулировкам. Пусть даны однородные многочлены $f_1, \ldots, f_m \in k[X_0, \ldots, X_n]$ Рассмотрим замкнутое алгебраическое множество или алгебраическое многообразие (в этой статье мы не различаем эти понятия)

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

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

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

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

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

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

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

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

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

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

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

ЗАМЕЧАНИЕ 2 *В дальнейшем мы будем предполагать без ограничения общности, что многочлены $f_1, \ldots, f_m$ являются линейно независимыми над k. Следовательно, $\dim V \le n-1$.*

Пусть W – определённое над k и неприводимое над k проективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$, и размерность $\dim W = n - s$. Пусть $\mathfrak{P} = \mathcal{I}(W) \subset k[X_0, \ldots, X_n]$ – однородный простой идеал, соответствующий W. Напомним, что в [5] введены $\mathfrak{P}$-последовательности. Именно, рассмотрим последовательность однородных многочленов $g_1, \ldots, g_j \in \mathfrak{P}$, $1 \le j \le s$. Пусть $0 \le u < j$ – целое число. Обозначим через $\mathcal{W} = \mathcal{W}(\mathfrak{P}, u)$ множество всех определённых над k и неприводимых над k компонент W' алгебраического многообразия $\mathcal{Z}(g_1, \ldots, g_u)$, таких что $W' \supset V$. Предположим, что для всякого целого числа $0 \le u < j$, многочлен $g_{u+1} \in \mathfrak{P}$ является многочленом g наименьшей степени, таким что для всякой неприводимой компоненты $W' \in \mathcal{W}$ выполнено $W' \not\subset \mathcal{Z}(g)$. Тогда всякая такая последовательность $g_1, \ldots, g_j$ называется $\mathfrak{P}$*–последовательностью (длины j)*.

Отметим, что если $g_1, \ldots, g_j$ является $\mathfrak{P}$-последовательностью, то для всякого $0 \le u \le j$ всякая неприводимая компонента алгебраического многообразия $\mathcal{Z}(g_1, \ldots, g_u)$ содержащая V имеет размерность $n - u$. В частности, когда $j = s$, алгебраическое многообразие V является неприводимой компонентой $\mathcal{Z}(g_1, \ldots, g_s)$.

Напомним, что $g_1, \ldots, g_s$ – является системой локальных параметров алгебраического многообразия W в гладкой точке $x_0 \in W$ в том и только в том случае, если $g_1, \ldots, g_s$ порождают идеал многообразия W в локальном кольце $\mathcal{O}_{x_0, \mathbb{P}^n(\overline{k})}$ точки x_0 в $\mathbb{P}^n(\overline{k})$. Далее, $g_1, \ldots, g_s$ является последовательностью локальных параметров алгебраического многообразия W тогда и только тогда, когда существует гладкая точка $x_0 \in W$, такая что $g_1, \ldots, g_s$ – система локальных параметров алгебраического многообразия W в точке x_0.

ТЕОРЕМА 1 *Пусть дана гладкая точка $x_0 \in V$ (то, что x_0 – гладкая точка V может быть проверено при помощи алгоритма из [7]). Это означает, что известен индекс $0 \le i_0 \le n$, такой что $X_{i_0}(x_0) \ne 0$, и задан изоморфизм полей*

$$k(x_0) = k((X_1/X_{i_0})(x_0), \ldots, (X_n/X_{i_0})(x_0)) = k[\eta] \simeq k[Z]/(\Phi), \qquad (2)$$

где $\eta = \sum_{0 \le i \le n} c_i (X_i/X_{i_0})(x_0)$, коэффициенты $c_i \in \mathbb{Z}$ заданы, и $\Phi \in k[Z]$ – минимальный многочлен элемента η над k со старшим коэффициентом $\mathrm{lc}_Z \Phi = 1$ (так что точка x_0 определена с точностью до сопряжения над k). Пусть W – однозначно определённая неприводимая над k компонента *многообразия V, такая что $x_0 \in W$. Пусть $\mathfrak{P} = \mathcal{I}(W) \subset k[X_0, \ldots, X_n]$ – однородный простой идеал, соответствующий W. Пусть $\dim W = n - s$, где $1 \le s \le n$. Тогда справедливы следующие утверждения.*

(i) *Можно вычислить s и построить $\mathfrak{P}$-последовательность $g_1, \ldots, g_s \in k[X_0, \ldots, X_n]$. Следовательно, $\deg g_i \le d$ для всех $1 \le i \le s$ и согласно [5]*

$$\deg g_1 \cdot \ldots \cdot \deg g_s \le n^{2^{s^C}} \deg W,$$

где $0 < C \in \mathbb{R}$ – абсолютная константа. Время работы алгоритма для построения $\mathfrak{P}$-последовательности полиномиально от d^n, d_1, d_2, M, M_1, m и длины записи точки x_0.

(ii) *Можно построить однородные многочлены $h_1, \ldots, h_s \in k[X_0, \ldots, X_n]$ и точку $x \in W$, такие что x является гладкой точкой V, координата $X_{i_0}(x) \ne 0$, и $h_1/X_{i_0}^{\deg h_1}, \ldots, h_s/X_{i_0}^{\deg h_s}$ является системой локальных параметров W в точке x, степени*

$$\deg_{X_0,\ldots,X_n} h_i \le n^{2^{s^C}} \deg g_i \le n^{2^{s^C}} d, \quad 1 \le i \le s,$$

для абсолютной константы $0 < C \in \mathbb{R}$. Время работы алгоритма для построения многочленов $h_1, \ldots, h_s$ полиномиально от $n^{2^{s^C}} d^n$, d_1, d_2, M, M_1, m и длины записи точки x_0, где $0 < C \in \mathbb{R}$ – абсолютная константа.

Отметим здесь, что используя алгоритмы из [7], можно построить множество S, содержащее систему представителей семейства множеств гладких точек всех неприводимых компонент V, такое что длина записи всякой точки из S ограничена сверху полиномом от d^n, d_1, d_2, M, M_1, m, и число точек $\#S \le d^n$.

Перед тем, как формулировать наш следующий результат, нам потребуется описать, как мы будем представлять квазипроективные алгебраические многообразия в этой статье. Пусть W – квазипроективное алгебраическое многообразие в $\mathbb{P}^n(\overline{k})$, и W определено над k. Тогда представим

$$W = W^{(1)} \setminus \cup_{2 \le i \le a} W^{(i)}, \tag{3}$$

где все $W^{(i)}$, $1 \le i \le a$ – являются проективными алгебраическими многообразиями в $\mathbb{P}^n(\overline{k})$, определёнными над k. Всякое алгебраическое многообразие $W^{(i)}$, $1 \le i \le a$, задано как объединение некоторых неприводимых компонент алгебраического многообразия $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)}) \subset \mathbb{P}^n(\overline{k})$, где однородные многочлены $f_1^{(i)}, \ldots, f_{m(i)}^{(i)} \in k[X_0, \ldots, X_n]$ заданы (здесь не следует путать верхний индекс (i) с производной). Для всякого $1 \le s \le n$ обозначим через $V_s^{(i)}$ (соответственно $W_s^{(i)}$) объединение всех неприводимых компонент размерности $n - s$ многообразия $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)})$ (соответственно $W^{(i)}$). Следовательно, $W_s^{(i)}$ является объединением некоторых неприводимых компонент $V_s^{(i)}$. Для всякого $1 \le s \le n$ задано семейство линейных форм $L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)} \in k[X_0, \ldots, X_n]$ с целыми коэффициентами, такое что число точек

$$\# V_s^{(i)} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)}) < +\infty \tag{4}$$

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

$$T_{\xi, V_s^{(i)}} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)}) = \{\xi\}. \tag{5}$$

Задано множество точек

$$\Xi_s^{(i)} = W_s^{(i)} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)}).$$

Следовательно, выполнено следующее свойство. Пусть $\xi \in V_s^{(i)} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)})$, и V' – является однозначно определённой неприводимой над k компонентой алгебраического многообразия $V_s^{(i)}$, такой что $\xi \in V'$. Тогда $\xi \in \Xi_s^{(i)}$ в том и только в том случае, если V' является компонентой многообразия $W^{(i)}$.

Таким образом, формально принятое в этой статье представление W является тройкой

$$(f, L, \Xi), \tag{6}$$

где f – семейство многочленов

$$f_j^{(i)}, \quad 1 \le j \le m(i),\, 1 \le i \le a, \tag{7}$$

L – семейство линейных форм

$$L_{s,j}^{(i)}, \quad s+1 \le j \le n,\, 1 \le s \le n,\, 1 \le i \le a, \tag{8}$$

и Ξ – семейство конечных множеств точек

$$\Xi_s^{(i)}, \quad 1 \le s \le n,\, 1 \le i \le a. \tag{9}$$

Обозначим также

$$\Xi^{(i)} = \bigcup_{1 \le s \le n} \Xi_s^{(i)}. \tag{10}$$

Отметим, что (4) и (5) могут быть всегда проверены, используя алгоритмы из [7]. Заметим также, что для заданной точки $y \in \mathbb{P}^n(\overline{k})$ можно решить, верно ли, что $y \in W_s^{(i)}$, при помощи алгоритмов из [7] и [3]. Именно, построим линейно независимые линейные формы $M_{s+2}, \ldots, M_n$, которые являются линейными комбинациями $L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)}$, такими что $M_j(y) = 0$, $s+2 \le j \le n$. Построим систему полиномиальных уравнений, задающих все кривые V'', которые являются неприводимыми компонентами пересечения

$$\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)}) \cap \mathcal{Z}(M_{s+2}, \ldots, M_n),$$

такими что $V'' \cap \Xi_s^{(i)} \neq \emptyset$. Тогда $y \in W_s^{(i)}$ тогда и только тогда, когда $y \in V''$ для некоторой кривой V''.

Таким образом, для заданной точки $y \in \mathbb{P}^n(\overline{k})$ можно выяснить за полиномиальное время, верно ли, что $y \in W^{(i)}$, $1 \le i \le a$, и $y \in W$.

Кроме того, для алгебраического многообразия W', которое аналогично W и задано подобным же образом, можно выяснить верно ли, что $W' = W$

за полиномиальное время. Докажем этот факт, когда W и W' являются проективными алгебраическими многообразиями. В этом случае достаточно проверить, что $W \setminus W' = \emptyset$ и $W' \setminus W = \emptyset$. Чтобы проверить, что, например, $W \setminus W' = \emptyset$ достаточно доказать это равенство в окрестности каждой точки $\xi \in \Xi^{(1)}$. Сначала выясним, как и выше, верно ли, что $\xi \in W'$ и, если $\xi \in W'$, построим точку $\xi_1 \in W' \cap W$, которая является бесконечно близкой к ξ, и ξ_1 является гладкой точкой многообразия W', см. выше. Теперь, если $W \setminus W' = \emptyset$ в бесконечно малой (относительно поля определения точки ξ_1) окрестности точки ξ_1, то $W \setminus W' = \emptyset$ в бесконечно малой окрестности точки ξ. Равенство $W \setminus W' = \emptyset$ в бесконечно малой окрестности точки ξ_1 может быть проверено при помощи решения системы полиномиальных уравнений и неравенств с абсолютными величинами, см. [10], [11].

ЗАМЕЧАНИЕ 3 Основываясь на [4], можно предложить полиномиальный алгоритм, для того чтобы выяснить, принадлежат ли две заданные точки из W одной и той же неприводимой компоненте W, определённой над k или $\overline{k}$. В частности можно выяснить, верно ли, что W является неприводимым алгебраическим многообразием. Используя результаты [4], [6], можно построить алгоритмы для выяснения того, верно ли, что $W_1 \subset W_2$ для двух квазипроективных алгебраических многообразий W_1 и W_2, заданных в описанной здесь форме. Мы не будем описывать эти алгоритмы в этой статье. Анализируя доказательство Теоремы 2, см. ниже, можно увидеть, что эти алгоритмы позволяют построить гладкое покрытие (соответственно гладкую стратификацию) V за полиномиальное время от длины записи входных данных и $2^{2^{n^C}} d^n$ (соответственно $2^{2^{n^C}} d^{n(n+1)/2}$) для абсолютной константы $C > 0$. Отметим, что если гладкое покрытие V построено, то Теорема 3, см. ниже, является тривиальной.

ТЕОРЕМА 2 *Существует гладкое покрытие (соответственно гладкая стратификация) V_α, $\alpha \in A$, алгебраического многообразия V, такое что (соответственно такая 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 $1 \le s \le n$, и $s = s(\alpha)$ зависит от α. Пусть (6) – построенное представление V_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. (7). Тогда построенное представление 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) $m(1) = s$ и, если $a \ge 2$, то $m(2) = 1$. Следовательно, если $a \ge 2$, 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 Зарисского подмножеством последнего алгебраического многообразия в случае гладкой стратификации).

(iii) Существуют линейно независимые линейные формы $Y_0, \ldots, Y_n \in k[X_0, \ldots, X_n]$, такие что $X_i = \sum_{0 \le j \le n} x_{i,j} Y_j$, все коэффициенты $x_{i,j} \in k$,

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

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

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 $0,\dots,n$.

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

(vi) Для всех $\alpha\in A$, $1\le j\le s(\alpha)$ длины записи коэффициентов многочленов $h_{\alpha,j}$ ограничены сверху полиномом от $n^{2^{s(\alpha)^C}} d^n$, 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 $2^{2^{n^C}} d^n$, 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 $0<C\in\mathbb{R}$.

ЗАМЕЧАНИЕ 4 *Отметим, что если получены оценки (в настоящее время они не получены) для локальных параметров над совершенными полями ненулевой характеристики, аналогичные оценкам из [5], то все утверждения Теоремы 2 (за исключением утверждений о длинах записи целых коэффициентов) также справедливы над совершенными бесконечными полями ненулевой характеристики. Доказательство остаётся без изменений для таких бесконечных полей. Соответственно для конечных полей требуются только незначительные изменения в формулировке и доказательстве Теоремы 2.*

Отметим, что существование требуемых линейных форм из представления (6) в Теореме 2 следует, см. [7], автоматически из существования всех других объектов из формулировки этой теоремы.

Ключом к доказательству Теоремы 2 для случая гладкого покрытия является Теорема 4, которая формулируется в Разделе 2. Случай гладкой стратификации требует упорядочивания алгебраических многообразий. Это упорядочивание описано в Разделе 4. Теорема 2 для случая гладкой стратификации доказана в Разделе 5. Отметим также, что вопрос о том, возможно ли построить гладкую стратификацию с $\#A \le 2^{2^{n^C}} d^n$ (в обозначениях Теоремы 2) является не исследованным.

Теперь предположим, что k – вещественное упорядоченное поле. Пусть k удовлетворяет следующему условию.

(A) *Пусть конечное расширение $K \supset k$ вещественных упорядоченных полей задано примитивным элементом и его многочленом. Тогда для элемента $a \in K$ можно проверить, верно ли, что $a > 0$ за полиномиальное время.*

Заметим, что, если $k = \mathbb{Q}$, то k удовлетворяет этому свойству. Если поле k удовлетворяет этому свойству, то всякое конечное расширение k_1, являющееся вещественным упорядоченным полем, также удовлетворяет этому свойству. Если $\varepsilon > 0$ является бесконечно малой величиной относительно поля k, то вещественное упорядоченное поле $k(\varepsilon)$ удовлетворяет этому свойству.

Обозначим через R вещественно замкнутое поле, являющееся расширением k. Для алгебраического многообразия V, определённого над k, обозначим через $V(R)$ вещественное алгебраическое многообразие над полем R, соответствующее V (т.е. множество точек $V(R)$ является множеством точек V с координатами из R). Всякое вещественное алгебраическое многообразие может быть получено таким образом. Определение вещественных алгебраических многообразий см. в [8]. Размерность $\dim V(R)$ вещественного алгебраического многообразия $V(R)$ определяется естественным образом как максимум размерностей его гладких точек, см. [8].

ТЕОРЕМА 3 *Пусть k – вещественное упорядоченное поле, удовлетворяющее условию (A), и R – вещественно замкнутое поле, содержащее k. Тогда размерность $\dim V(R)$ множества R-точек алгебраического многообразия V можно вычислить за полиномиальное время от $2^{2^{n^C}} d^n$, d_1, d_2, M, M_1, m, где $0 < C \in \mathbb{R}$ – абсолютная константа. Более того, если на выходе алгоритма $\dim V(R) = n - s$, то фактически время работы алгоритма полиномиально от $n^{2^{s^C}} d^n$, d_1, d_2, M, M_1, m.*

1 Алгоритм для построения регулярных последовательностей и последовательностей локальных параметров

Используя алгоритм из [7], раздел 3, построим линейные формы Y_0, Y_{s+1}, $Y_{s+2}, \ldots, Y_n \in k(x_0)[X_0, \ldots, X_n]$, такие что $Y_0(x_0) \ne 0$, точка x_0 является изолированной в пересечении $W \cap \mathcal{Z}(Y_{s+1}, \ldots, Y_n)$, и пересечение касательного пространства W в точке x_0 и $\mathcal{Z}(Y_{s+1}, \ldots, Y_n)$ трансверсально, т.е. $T_{x_0,W} \cap \mathcal{Z}(Y_{s+1}, \ldots, Y_n) = \{x_0\}$.

Пусть V' – произвольное проективное алгебраическое многообразие, определённое над k, и $V' = \cup_{j\in J} V'_j$ – разложение V в объединение неприводимых компонент над k. Пусть $x \in V'$. Тогда определена кратность $\mu(x, V'_j) \ge 0$ точки x алгебраического многообразия V'_j, ср. [7]. Удобно теперь определить кратность $\mu(x, V) = \sum_{j\in J} \mu(x, V'_j)$.

ЛЕММА 1 *Пусть выполнены условия Теоремы 1, пусть* $1 \le j \le s$ *и* $\psi_1, \ldots, \psi_j \in k[X_0, \ldots, X_n]$ *– однородные многочлены, такие что* $\mathcal{Z}(\psi_1, \ldots, \psi_j) \supset W$*, размерность всякой неприводимой компоненты* $\mathcal{Z}(\psi_1, \ldots, \psi_j)$*, содержащей* W*, равна* $n - j$*, и* $\deg \psi_i \le D$ *для всех* $1 \le i \le j$*. Пусть* $\psi \in k[X_0, \ldots, X_n]$ *– однородный многочлен, и* $\deg \psi \le D$*. Тогда можно выяснить, обращается ли в нуль тождественно* ψ *на* W*. Если* ψ *не обращается в нуль тождественно на* W*, то можно построить точку* $x' \in W$ *и линейные формы* $L'_{s+1}, \ldots, L'_n \in k(x_0)[X_0, \ldots, X_n]$*, удовлетворяющие следующим условиям.*

(i) x' *– гладкая точка многообразия* V *(и, следовательно, гладкая точка* W*).*

(ii) $Y_0(x') \ne 0$.

(iii) $L'_{s+1}, L'_{s+2}, \ldots, L'_n$ *– линейные формы относительно* $Y_0, Y_{s+1}, \ldots, Y_n$ *с целыми коэффициентами с длинами записи* $O(n \log(dD))$*.*

(iv) Точка x' *является изолированной в пересечении* $W \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n)$*.*

(v) Пересечение касательного пространства многообразия W *в точке* x' *и* $\mathcal{Z}(L'_{s+1}, \ldots, L'_n)$ *трансверсально, т.е.* $T_{x',W} \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n) = \{x'\}$*.*

(vi) $\psi(x') \ne 0$.

(vii) $\mu(x', \mathcal{Z}(\psi_1, \ldots, \psi_j)) = \min_{x \in W} \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_j))$.

Время работы алгоритма для построения точки x' *и линейных форм* $L'_{s+1}, \ldots, L'_n$ *полиномиально от длины записи входных данных и* $(dD)^n$*.*

ДОКАЗАТЕЛЬСТВО Построим вещественную структуру на поле k, см. [10], [11]. Пусть $\varepsilon_1 > 0$ – бесконечно малая величина относительно поля k, и $\varepsilon_2 > 0$ – бесконечно малая величина относительно поля $k(\varepsilon_1)$. Положим $K = k(\varepsilon_1, \varepsilon_2)$. Так что K снабжено вещественной структурой, и можно рассматривать системы алгебраических уравнений и неравенств с квадратами абсолютных величин над K и решать их над $\overline{K}$, см. [10], [11]. То же самое справедливо, если заменить K на $k(\varepsilon_1)$. Пусть $x_0 = (x_{0,0} : \ldots : x_{0,n})$, где все $x_{0,j} \in k(x_0)$, $0 \le j \le n$. Рассмотрим систему уравнений и неравенств с коэффициентами из K относительно переменных $X_0, \ldots, X_n$, Z

$$\left\{ \begin{array}{ll} \sum_{0 \le i \le n} |X_i - x_{0,i}|^2 < \varepsilon_1, & \\ f_i = 0, & 1 \le i \le m, \\ \psi Z - 1 = 0. & \end{array} \right. \qquad (11)$$

Тогда, ср. [11], [7], система (11) не имеет решений в $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1)})$, тогда и только тогда, когда многочлен ψ обращается в нуль тождественно на W. В дальнейшем в доказательстве этой леммы мы будем предполагать, что система (11) имеет решение.

Предположим, что $x'' \in W$, и линейные формы $L''_{s+1}, \ldots, L''_n \in k(x_0)[X_0, \ldots, X_n]$ удовлетворяют условиям, которые получены из (i)–(v) заменой x' и $L'_{s+1}, \ldots, L'_n$ на x'' и $L''_{s+1}, \ldots, L''_n$. Следовательно,

$$\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j)) \ge \min_{x \in W} \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_j)). \qquad (12)$$

Заметим, что если мы знаем заранее, что $x'' \in W$, то мы можем проверить, удовлетворяют ли точка x'' и линейные формы $L''_{s+1}, \ldots, L''_n$ условиям (i)–(vi) (где x' и линейные формы L'_j заменены на x'' и линейные формы L''_j), используя алгоритмы из [7]. Мы можем вычислить также кратность $\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j))$.

Покажем, что мы можем выяснить, имеет ли место равенство в (12) и, если (12) является строгим неравенством, мы можем построить новую точку x''' и новые линейные формы $L'''_{s+1}, \ldots, L'''_n$ аналогичные x'' и $L''_{s+1}, \ldots, L''_n$ и, такие что $\psi(x''') \neq 0$, и

$$\mu(x''', \mathcal{Z}(\psi_1, \ldots, \psi_j)) < \mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j)).$$

В самом деле, пусть $x''_0, \ldots, x''_n \in \overline{k}$ являются, такими что $x'' = (x''_0 : \ldots : x''_n)$. Вычислим, используя алгоритм из [7], размерность $r = \dim_{x''} \mathcal{Z}(\psi_1, \ldots, \psi_j)$ в точке x'', т.е. максимум размерностей неприводимых компонент W_2 алгебраического многообразия $\mathcal{Z}(\psi_1, \ldots, \psi_j)$, таких что $x'' \in W_2$. Построим, используя алгоритм из [7], линейные формы $M_0, M_{r+1}, M_{r+2}, \ldots, M_n$ с целыми коэффициентами с длинами записи $O(n \log D)$, такие что

$$\mathcal{Z}(\psi_1, \ldots, \psi_j) \cap \mathcal{Z}(M_0, M_{r+1}, M_{r+2}, \ldots, M_n) = \emptyset$$

в окрестности точки x''.

Рассмотрим систему уравнений и неравенств с коэффициентами из поля K относительно переменных $X_0, \ldots, X_n$, $Z_0, \ldots, Z_n$, Z

$$\left\{ \begin{array}{ll} \sum_{0 \le i \le n} |X_i - x''_i|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |Z_i - x''_i|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |X_i - Z_i|^2 \ge \varepsilon_2, & \\ M_i(X_0 - Z_0, \ldots, X_n - Z_n) = 0, & i = 0, r+1, r+2, \ldots, n, \\ f_i = 0, & 1 \le i \le m, \\ \psi_i(Z_0, \ldots, Z_n) = 0, & 1 \le i \le j, \\ \psi Z - 1 = 0. & \end{array} \right. \qquad (13)$$

Тогда, ср. [11], [7], система (13) не имеет решений в $\mathbb{A}^{2n+3}(\overline{K})$ тогда и только тогда, когда (12) является равенством.

Предположим, что система (13) имеет решение. Тогда построим это решение $x^*_0, \ldots, x^*_n$, $z^*_0, \ldots, z^*_n$, z^*. Предположим, что система (13) не имеет решений, тогда построим решение $x^*_0, \ldots, x^*_n$, z^* системы (11).

Обозначим $x^* = (x^*_0 : \ldots : x^*_n) \in \mathbb{P}^n(\overline{K})$. Тогда $\psi(x^*) \neq 0$ и, ср. [7],

$$\mu(x^*, \mathcal{Z}(\psi_1, \ldots, \psi_j)) < \mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j))$$

в случае, когда система (13) имеет решение, и

$$\mu(x^*, \mathcal{Z}(\psi_1, \ldots, \psi_j)) = \min_{x \in W} \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_j))$$

в случае, когда система (13) не имеет решений. Положим $L^*_i = L''_i - (L''_i/Y_0)(x^*)Y_0$ для всех $s+1 \le i \le n$. Тогда точка x^* и линейные формы $L^*_{s+1}, \ldots, L^*_n$ удовлетворяют свойствам, которые требуются для точки x''' и $L'''_{s+1}, \ldots, L'''_n$, но $x^* \in \mathbb{P}^n(\overline{K})$ и соответствующие линейные формы имеют коэффициенты из поля $\overline{K}$.

Представим линейные формы L_i^*, $s+1 \le i \le n$ как линейные комбинации $Y_0, Y_{s+1}, \ldots, Y_n$ с коэффициентами $l_{i,j} \in \overline{\overline{K}}$, причём $l_{i,j}$ – коэффициент при Y_j линейной формы L_i^*. Далее, ср. [11], [7], мы можем заменить в линейных формах L_i^*, $s+1 \le i \le n$ один произвольный коэффициент $l_{i,j}$ на целый коэффициент с длиной записи $O(n \log(dD))$ и получить линейные формы $\widetilde{L}_{s+1}, \ldots, \widetilde{L}_n$ и точку $\widetilde{x}$, удовлетворяющие тем же самым свойствам, что и линейные формы $L_{s+1}^*, \ldots, L_n^*$ и точка x^*. Более точно, предположим, что мы хотим заменить коэффициент $l_{0,s+1}$ на целый коэффициент. Мы перебираем возможные целые значения этого заменяемого коэффициента и проверяем каждый раз выполняются ли требуемые свойства. Пересечение

$$V \cap \mathcal{Z}(L_{s+2}^*, \ldots, L_n^*)$$

имеет однозначно определённую неприводимую компоненту Q, такую что $x^* \in Q$, и Q является кривой, содержащейся в W. Эта кривая Q может быть построена при помощи алгоритма из [3]. Мы выберем $\widetilde{x} \in Q$. Таким образом, мы имеем критерий для проверки того, что $\widetilde{x} \in W$. Используя критерий для вычисления кратности точки из [7], мы видим также, что число точек $y \in Q$, таких что

$$\mu(x^*, \mathcal{Z}(\psi_1, \ldots, \psi_j)) < \mu(y, \mathcal{Z}(\psi_1, \ldots, \psi_j))$$

ограничено сверху полиномом от $(Dd)^n$. Аналогичным образом можно рассмотреть случаи, когда не удовлетворяется одно из свойств аналогичных (i)–(vi).

Следовательно, заменяя последовательно все коэффициенты в линейных формах $L_{s+1}^*, \ldots, L_n^*$ на целые коэффициенты с длинами записи $O(n \log(dD))$, мы получим в конечном счёте требуемые линейные формы $L_{s+1}''', \ldots, L_n'''$ и точку x'''. Заметим также, что в случае, когда система (13) не имеет решений, и $\psi(x') \neq 0$, мы можем взять просто $x''' = x'$ и $L_j''' = L_j'$ для всех j.

Теперь возьмём в качестве базы $x'' = x_0$ и применим описанную процедуру рекурсивно, т.е. будем заменять каждый раз, когда построена x''', точку x'' на x''' и возвращаться к началу. Таким образом, в конечном счёте мы придём к случаю, когда система (13) не имеет решений. В этом случае положим $x' = x'''$ и $L_i' = L_i'''$, $s+1 \le i \le n$. Оценка для времени работы описанного алгоритма следует немедленно из оценок для времени работы использованных алгоритмов. Лемма доказана.

ЗАМЕЧАНИЕ 5 *Предположим, что в условиях Леммы 1 целое число $1 \le j_1 \le j$, и x_0 – гладкая точка алгебраического многообразия $\mathcal{Z}(\psi_1, \ldots, \psi_{j_1})$. Тогда к свойствам (i)–(vii) в формулировке Леммы 1 можно добавить следующее.*

(viii) Точка x' является гладкой точкой многообразия $\mathcal{Z}(\psi_1, \ldots, \psi_{j_1})$.

Доказательство этого варианта леммы аналогично исходному, так как согласно [7] имеется критерий, чтобы выяснить, является ли точка гладкой.

Наша цель теперь – доказать Теорему 1. Сначала докажем утверждение (i). Положим $\delta^{(0)} = 1$, $j_0 = 0$. Далее рекурсивно на шаге $a \ge 1$ мы построим следующие объекты.

- Целые числа $j_a \geq 1$ и $\delta^{(a)} \geq 1$.
- $\mathfrak{P}$-последовательность $g_1, g_2, \ldots, g_{j_a}$, такую что степень $\deg g_{j_a} = \delta^{(a)}$.
- Точку $x_a \in W$ (которая задана аналогично точке x_0), такую что x_a является гладкой точкой V, $Y_0(x_a) \neq 0$, и

$$\mu(x_a, \mathcal{Z}(g_1, \ldots, g_{j_a})) = \min_{x \in W} \mu(x, \mathcal{Z}(g_1, \ldots, g_{j_a})). \tag{14}$$

- Линейные формы $L_{a,s+1}, L_{a,s+2}, \ldots, L_{a,n}$ относительно $Y_0, Y_{s+1}, \ldots, Y_n$ с целыми коэффициентами с длинами записи $O(n \log(d\delta^{(a)}))$, такие что $Y_0(x_a) \neq 0$, точка x_a является изолированной в пересечении $W \cap \mathcal{Z}(L_{a,s+1}, \ldots, L_{a,n})$, и пересечение касательного пространства W в точке x_a и $\mathcal{Z}(L_{a,s+1}, \ldots, L_{a,n})$ трансверсально, т.е. $T_{x_0,W} \cap \mathcal{Z}(L_{a,s+1}, \ldots, L_{a,n}) = \{x_a\}$.

Шаг a является последним тогда и только тогда, когда $j_a = s = n - \dim W$.

Предположим, что шаг $(a-1)$ не является последним, или $a = 1$. Опишем шаг a рекурсии. Пусть $x_{a-1,0}, \ldots, x_{a-1,n} \in \overline{k}$ являются, такими что $x_{a-1} = (x_{a-1,0} : \ldots : x_{a-1,n})$.

Обозначим для краткости $j_{a-1} = r$. Согласно (14), с a заменённым на $a-1$, для всякой неприводимой компоненты W_1 алгебраического многообразия $\mathcal{Z}(g_1, \ldots, g_r)$, такой что $x_{a-1} \in W_1$, выполнено $W_1 \supset W$, и размерность $\dim W_1 = n - r$. Построим, используя алгоритм из [7] Раздел 6 (здесь мы оставляем простое упражнение для читателя), линейные формы $M_0, M_{r+1}, M_{r+2}, \ldots, M_n$ с целыми коэффициентами с длинами записи $O(n \log(\delta + 1))$, такие что x_{a-1} является изолированной точкой пересечения

$$\mathcal{Z}(g_1, \ldots, g_r) \cap \mathcal{Z}(M_{r+1}, M_{r+2}, \ldots, M_n)$$

в $\mathbb{P}^n(\overline{k})$, линейная форма $M_0(x_{a-1}) \neq 0$, и пересечение

$$\mathcal{Z}(g_1, \ldots, g_r) \cap \mathcal{Z}(M_{r+1} - \varepsilon_1 M_0, M_{r+2}, M_{r+3} \ldots, M_n) = T$$

содержит $\mu(x_{a-1}, \mathcal{Z}(g_1, \ldots, g_r))$ различных точек в $\mathbb{P}^n(\overline{k(\varepsilon_1)})$, которые являются бесконечно близкими к x_{a-1}. Все точки из T являются гладкими точками алгебраического многообразия $\mathcal{Z}(g_1, \ldots, g_r)$, см. [7].

Будем перебирать $\delta = \delta^{(a-1)}, \delta^{(a-1)} + 1, \ldots$. Для рассматриваемого значения δ построим базис векторного пространства однородных многочленов $g \in k[X_0, \ldots, X_n]$ степени δ, таких что $g(x_i) = 0$ для всех $0 \leq i \leq a-1$. Это может быть сделано при помощи решения системы линейных уравнений над k, используя представления точек x_i, аналогичные (2), которые построены на предыдущих шагах рекурсии. Обозначим через S множество элементов построенного базиса.

Если S пусто, то мы переходим к следующему значению δ, т.е. к $\delta + 1$. Предположим, что множество S непусто. Тогда мы перебираем элементы $g \in S$. Для $g \in S$ применим Лемму 1 с $j = j_{a-1}$, $\psi_i = g_i$, $1 \leq i \leq j$, $\psi = g$ и выясним, обращается ли g в нуль тождественно на W.

Предположим, что g не обращается в нуль тождественно на W. Тогда, используя Лемму 1, построим точку x' и линейные формы $L'_{s+1}, \ldots, L'_n$. Положим $x_a = x'$ и $L_{a,j} = L'_j$, $s + 1 \leq j \leq n$. Используя алгоритм из

[3], построим представление аналогичное (2) для точки x_a. В этом случае положим $j_a = j_{a-1}$, $\delta^{(a)} = \delta^{(a-1)}$.

Предположим, что g обращается в нуль тождественно на W. Пусть $z \in T$. Пусть $z_0, \ldots, z_n \in \overline{k(\varepsilon_1)}$, и $z = (z_0 : \ldots : z_n)$. Рассмотрим систему уравнений и неравенств с коэффициентами из поля K относительно переменных $X_0, \ldots, X_n$, Z

$$\left\{ \begin{array}{ll} \sum_{0 \le i \le n} |X_i - z_i|^2 < \varepsilon_2, & \\ g_i = 0, & 1 \le i \le r, \\ gZ - 1 = 0. & \end{array} \right. \qquad (15)$$

Система (15) не имеет решений в $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1, \varepsilon_2)})$ тогда и только тогда, когда g обращается в нуль тождественно на неприводимой компоненте W_1 многообразия $\mathcal{Z}(g_1, \ldots, g_r)$, такой что $z \in W_1$, ср. [10], [11]. Выясним для всякого $z \in T$, имеет ли система (15) решение в $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1, \varepsilon_2)})$ и построим подмножество $T(g) \subset T$, состоящее из всех точек $z \in T$, таких что система (15) имеет решение в $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1, \varepsilon_2)})$.

Затем мы переходим к следующему элементу $g \in S$. Если все элементы из S перебраны, то построим подмножество $S_1 \subset S$, состоящее из всех многочленов g, обращающихся в нуль тождественно на W, и выясним, верно ли, что $\cup_{g \in S_1} T(g) = T$. Если $\cup_{g \in S_1} T(g) \ne T$, то существует неприводимая компонента W_1 многообразия $\mathcal{Z}(g_1, \ldots, g_r)$, и $z \in T$, такие что $z \in W_1$, и все многочлены из S обращаются в нуль тождественно на W_1. Напомним, что $W_1 \supset W$. Следовательно, не существует $\mathfrak{P}$-последовательности $g_1, \ldots, g_{j_{a-1}}, \widetilde{g}$, такой что $\widetilde{g}$ принадлежит линейному пространству с базисом S. Так что мы переходим в этом случае к следующему значению δ, т.е. к $\delta + 1$.

Предположим, что $\cup_{g \in S_1} T(g) = T$. Тогда построим, ср. [11], [7], рассматривая системы аналогичные (15), линейную комбинацию

$$q = \sum_{g \in S_1} c_g g,$$

где c_g являются целыми числами с длинами записи $O(r \log(\delta + 1))$, такую что q не обращается в нуль тождественно на всякой неприводимой компоненте W_1 многообразия $\mathcal{Z}(g_1, \ldots, g_r)$, для которой $x_{a-1} \in W_1$. Положим $j_a = j_{a-1} + 1$, $\delta^{(a)} = \delta$ и $g_{j_a} = q$. Применяя Лемму 1 (с $\psi = 1$), построим требуемые точку x_a и линейные формы $L_{a,s+1}, \ldots, L_{a,n}$. Используя алгоритм из [3], построим представление аналогичное (2) для точки x_a. Этим заканчивается описание шага a и всего алгоритма.

Заметим, что $a \le \delta^{(a)} \binom{\delta^{(a)} + n}{n}$. Теперь оценка для времени работы описанного алгоритма следует немедленно из [5] и оценок для времени работы применённых алгоритмов. Утверждение (i) Теоремы 1 доказано.

Теперь наша цель – доказать утверждение (ii) Теоремы 1. Используя (i), построим $\mathfrak{P}$-последовательность $g_1, \ldots, g_s$. Пусть $0 \le r < s$ – целое число. Предположим, что мы уже построили, используя рекурсию по r, точку $x \in W$, которая является гладкой точкой $\mathcal{Z}(g_1, \ldots, g_s)$, и однородные многочлены

$$h_1, \ldots, h_r, g_{r,r+1}, \ldots, g_{r,s} \in k[X_0, \ldots, X_n],$$

такие что

(a) x является гладкой точкой $\mathcal{Z}(h_1, \ldots, h_r)$,

(b) W является неприводимой компонентой $\mathcal{Z}(h_1, \ldots, h_r, g_{r,r+1}, \ldots, g_{r,s})$,

(c) x является гладкой точкой $\mathcal{Z}(h_1, \ldots, h_r, g_{r,r+1}, \ldots, g_{r,s})$,

(d) $g_{r,j} = \sum_{1 \le v \le j} q_{r,j,v} g_v$, где $q_{r,j,v} \in k[X_0, \ldots, X_n]$ являются однородными многочленами, и $\deg q_{r,j,v} = \deg g_j - \deg g_v$ для всех $1 \le v \le j$.

(так что в случае базы рекурсии $r = 0$ дана гладкая точка $x = x_0 \in W$, и мы положим $g_{0,j} = g_j$ для всякого $1 \le j \le s$). Наша цель – построить многочлен h_{r+1} и однородные многочлены $g_{r+1,r+2}, \ldots, g_{r+1,s}$, такие что свойства (a)–(d) будут удовлетворяться, если заменить r на $r+1$ (может быть с другой точкой x).

Пусть $X_{i_0}(x) \ne 0$. Сделав при необходимости перестановку координат многообразия $\mathbb{P}^n(\overline{k})$, мы будем предполагать без ограничения общности, что $i_0 = 0$.

Обозначим $\psi_i = h_i / X_0^{\deg h_i}$, $1 \le i \le r$, и $\rho_j = g_{r,j}/X_0^{\deg g_{r,j}}$, $r+1 \le j \le s$.

Обозначим через $Z_i = X_i/X_0 - (X_i/X_0)(x)$, $1 \le i \le n$, координатные функции аффинного пространства $\mathbb{A}^n(\overline{k}) = \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(X_0)$. Следовательно, $\psi_j, \rho_w \in \overline{k}[Z_1, \ldots, Z_n]$ для всех j, w.

Построим, используя алгоритм из [7], касательное пространство $T_{x,W}$ алгебраического многообразия W в точке x. Более точно, построим линейные формы $Y_1, \ldots, Y_s \in k(x)[Z_1, \ldots, Z_n]$ (напомним, что $k(x)$ – поле, порождённое над k аффинными координатами $(X_i/X_0)(x)$, $1 \le i \le n$, точки x), такие что $T_{x,W} = \mathcal{Z}(Y_1, \ldots, Y_s)$, и $d_x \psi_i = Y_i$ для всякого $1 \le i \le r$. Рассмотрим произвольные многочлены $\varphi_j \in \overline{k}[Z_1, \ldots, Z_n]$, $r+1 \le j \le s$, и индексы $1 \le i_{s+1} < \ldots < i_n \le n$, такие что

$$\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s$$

является системой локальных параметров алгебраического многообразия W в точке x, дифференциалы $d_x \varphi_i = Y_i$ для всякого $r+1 \le i \le s$, и

$$\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{i_{s+1}}, \ldots, Z_{i_n}$$

является системой локальных параметров алгебраического многообразия $\{x\}$, состоящего из одной точки x. Мы будем предполагать без ограничения общности, что $i_j = j$ для всех $s+1 \le j \le n$.

Сделав при необходимости перестановку координат $Z_1, \ldots, Z_s$, мы будем предполагать без ограничения общности, что минор матрицы Якоби в точке x

$$\det\left(\left(\partial \psi_i / \partial Z_j\right)(x)\right)_{1 \le i,j \le r} \ne 0. \tag{16}$$

Рассмотрим кольцо формальных степенных рядов

$$\Omega = \overline{k}[[\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n]]. \tag{17}$$

Это кольцо совпадает с кольцом формальных степенных рядов от $Z_1, \ldots, Z_n$ над $\overline{k}$. Следовательно, оно содержит кольцо $k[X_1/X_0, \ldots, X_n/X_0]$. Всякий элемент F кольца Ω может быть представлен в виде

$$F = \sum_{i_1, \ldots, i_n \ge 0} F_{i_1, \ldots, i_n} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n}, \tag{18}$$

где все $F_{i_1,\ldots,i_n} \in \overline{k}$. Обозначим через

$$\widetilde{\mathfrak{P}} = (\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s)$$

идеал кольца Ω, порождённый элементами $\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s$. Пусть $F \in k[X_1/X_0, \ldots, X_n/X_0]$. Тогда

$$F \in \widetilde{\mathfrak{P}} \quad \text{тогда и только тогда, когда} \quad \mathcal{Z}(F) \supset V \setminus \mathcal{Z}(X_0). \tag{19}$$

Для произвольного формального степенного ряда F обозначим

$$\operatorname{ord} F = \min\{i_{r+1} + \ldots + i_s \ : \ F_{0,\ldots,0,i_{r+1},\ldots,i_n} \neq 0\}.$$

Следовательно, $\operatorname{ord} F$ – неотрицательное целое число или $+\infty$.

Пусть для формального степенного ряда F выполнено (18). Положим

$$\nu_0 = \nu_0(x, F) = \min\{i_{r+1} + \ldots + i_n \ : \ F_{0,\ldots,0,i_{r+1},\ldots,i_n} \neq 0\},$$
$$\operatorname{lf}(x, F) = \sum_{i_{r+1}+\ldots+i_n=\nu_0} F_{0,\ldots,0,i_{r+1},\ldots,i_n} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n}.$$

Следовательно, $\operatorname{lf}(x, F) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n]$. Обозначим через

$$\operatorname{Lf}(x, F) \in \overline{k}[Y_{r+1}, \ldots, Y_s, Z_{s+1}, \ldots, Z_n]$$

многочлен, такой что $\operatorname{Lf}(x, F)(\varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n) = \operatorname{lf}(x, F)$.

Введём операторы дифференцирования $\mathcal{D}_j$, $r + 1 \leq j \leq s$ на кольце Ω формулами

$$\mathcal{D}_j(F) = \det \begin{pmatrix} \partial\psi_1/\partial Z_1 & \ldots & \partial\psi_1/\partial Z_r & \partial\psi_1/\partial Z_j \\ \vdots & \vdots & \vdots & \vdots \\ \partial\psi_r/\partial Z_1 & \ldots & \partial\psi_r/\partial Z_r & \partial\psi_r/\partial Z_j \\ \partial F/\partial Z_1 & \ldots & \partial F/\partial Z_r & \partial F/\partial Z_j \end{pmatrix}.$$

Следовательно, если $F \in \overline{k}[Z_1, \ldots, Z_n]$, то степени относительно $Z_1, \ldots, Z_n$

$$\deg \mathcal{D}_i(F) \leq \deg F + \deg h_1 + \ldots + \deg h_r - r - 1. \tag{20}$$

Если $F \in k[X_1/X_0, \ldots, X_n/X_0]$, то $\mathcal{D}_i(F) \in k[X_1/X_0, \ldots, X_n/X_0]$ для всякого $r + 1 \leq i \leq s$. По Теоремам 1, 2 и Лемме 18 из [5] мы имеем

$$\operatorname{ord} \rho_{r+1} \leq 1 + \frac{\deg h_1 \cdot \ldots \cdot \deg h_r \deg g_{r+1} \cdot \ldots \cdot \deg g_s}{\deg W} \leq n^{2^{s^{C_0}}}$$

для некоторой абсолютный константы $C_0 > 0$.

Пусть $\mu_0 = \min\{\mu(z, \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) \ : \ z \in W\}$. Построим, используя Лемму 1, точку x' аналогичную x и, такую что

$$\mu(x', \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) = \mu_0.$$

Заменяя точку x на x', мы будем предполагать без ограничения общности, что $x = x'$.

ЛЕММА 2 *Пусть* $\nu = \operatorname{ord} \rho_{r+1}$. *Представим* ρ_{r+1} *как элемент кольца* Ω

$$\rho_{r+1} = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n},$$

где все $a_{i_1,\ldots,i_n} \in \overline{k}$. *Тогда* $\nu = \nu_0(x, \rho_{r+1})$ *или, что эквивалентно,* $\mathrm{lf}(x, \rho_{r+1}) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$.

ДОКАЗАТЕЛЬСТВО Обозначим через R локальное кольцо алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_r) \setminus \mathcal{Z}(X_0) = \mathcal{Z}(\psi_1, \ldots, \psi_r)$ в точке x. Так что R является регулярным локальным кольцом и, следовательно, факториальным кольцом. Имеется естественное вложение

$$R \longrightarrow \overline{k}[[\varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n]] = \Omega_1,$$

где Ω_1 – кольцо формальных степенных рядов от $\varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n$ над $\overline{k}$. Существует естественный эпиморфизм $p : \Omega \to \Omega_1$. Пусть $z \in R$, и $\widetilde{z}$ – элемент кольца Ω, такой что $p(\widetilde{z}) = z$. Положим $\nu_0(x, z) = \nu_0(x, \widetilde{z})$ и $\mathrm{lf}(x, z) = p(\mathrm{lf}(x, \widetilde{z}))$. Тогда $\nu_0(x, z)$ и $\mathrm{lf}(x, z)$ не зависят от выбора $\widetilde{z}$. Пусть $\overline{\rho}_{r+1} \in R$ – образ ρ_{r+1}. Нам необходимо доказать, что $\mathrm{lf}(x, \overline{\rho}_{r+1}) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$. Представим

$$\overline{\rho}_{r+1} = \lambda \prod_{i \in I} \eta_i^{e_i},$$

где η_i – неприводимые элементы R, и λ является обратимым элементом R. Выберем элементы $\widetilde{\eta}_i \in \overline{k}(Z_1, \ldots, Z_n) \cap \Omega$, такие что $p(\widetilde{\eta}_i) = \eta_i$ для всякого $i \in I$. Тогда $\mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})$ совпадает с $\cup_{i \in I} \mathcal{Z}(\widetilde{\eta}_i, \psi_1, \ldots, \psi_r)$ в окрестности относительно топологии Зарисского точки x. Далее, кратность

$$\mu(x, \mathcal{Z}(\widetilde{\eta}_i, \psi_1, \ldots, \psi_r)) = \nu_0(x, \eta_i),$$

как это следует из определения кратности, используя многочлен Гильберта-Самюэля, см. [2]. Следовательно,

$$\mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) = \sum_{i \in I} \nu_0(x, \eta_i). \tag{21}$$

Мы имеем $\mathrm{lf}(x, \overline{\rho}_{r+1}) = \mathrm{lf}(x, \lambda) \prod_{i \in I} \mathrm{lf}(x, \eta_i)^{e_i}$. Следовательно, достаточно доказать, что $\mathrm{lf}(x, \eta_i) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$ для всякого $i \in I$.

Предположим, что $\mathrm{lf}(x, \overline{\rho}_{r+1}) \notin \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$. Тогда существует $i_0 \in I$, такое что

$$\mathrm{lf}(x, \eta_{i_0}) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n] \setminus \overline{k}[\varphi_{r+1}, \ldots, \varphi_s].$$

Пусть ε_i – бесконечно малая величина относительно поля $\overline{k(\varepsilon_{s+1}, \ldots, \varepsilon_{i-1})}$ для всякого $s+1 \leq i \leq n$. Обозначим через $x'' \in W(\overline{k(\varepsilon_{s+1}, \ldots, \varepsilon_n)})$ точку, являющуюся бесконечно близкой к x, такую что $Z_j(x'') = \varepsilon_j$, $s+1 \leq j \leq n$. Обозначим через R'' локальное кольцо алгебраического многообразия W в точке x''. Следовательно, $\overline{\rho}_{r+1}, \eta_i \in R''$, $i \in I$, и λ – обратимый элемент кольца R''. Рассмотрим кольцо формальных степенных рядов

$$\Omega'' = \overline{k}[[\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{s+1} - Z_{s+1}(x''), \ldots, Z_n - Z_n(x'')]]. \tag{22}$$

Для элемента $F \in \Omega''$ определим $\nu_0(x'', F)$ и $\mathrm{lf}(x'', F)$, заменяя в определении $\nu_0(x, F)$ и $\mathrm{lf}(x, F)$ кольцо Ω на Ω'' и $Z_{s+1}, \ldots, Z_n$ на $Z_{s+1} - Z_{s+1}(x''), \ldots, Z_n - Z_n(x'')$.

Следовательно, $\nu_0(x'', \eta_i) \le \nu_0(x, \eta_i)$, $i \in I$, и $\nu_0(x'', \eta_{i_0}) < \nu_0(x, \eta_{i_0})$ согласно выбору i_0 и точки x''. С другой стороны, аналогично (21) мы имеем

$$\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) \le \sum_{i \in I} \nu_0(x'', \eta_i).$$

Таким образом, $\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) < \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1}))$. Полученное противоречие доказывает лемму.

ЛЕММА 3 *Пусть $F \in R$ – элемент, такой что $\mathrm{lf}(x, F) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$ и, следовательно, $\mathrm{Lf}(x, F) \in \overline{k}[Y_{r+1}, \ldots, Y_s]$. Тогда существует $r+1 \le j \le s$, такое что $\mathrm{ord}(\mathcal{D}_j(F)) = \mathrm{ord}(F) - 1$, и*

$$\mathrm{lf}(x, \mathcal{D}_j(F)) = \sum_{r+1 \le i \le s} \frac{\partial\, \mathrm{Lf}(x, F)}{\partial Y_i}(\varphi_{r+1}, \ldots, \varphi_s)\, \mathrm{lf}(x, \mathcal{D}_j(\varphi_i)).$$

Следовательно, $\mathrm{lf}(x, \mathcal{D}_j(F)) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$ для этого j.

ДОКАЗАТЕЛЬСТВО По определению операторов $\mathcal{D}_i$, условию (16) и, так как всякая линейная комбинация элементов $\psi_{r+1}, \ldots, \psi_s$ является локальным параметром в точке x, векторы

$$(\mathcal{D}_{r+1}(\psi_i)(x), \ldots, \mathcal{D}_s(\psi_i)(x)) \in (\overline{k})^{s-r}, \quad r+1 \le i \le s,$$

линейно независимы над $\overline{k}$. Отсюда утверждение леммы следует немедленно.

Конструируя первые члены разложения ρ_{r+1} в кольце формальных степенных рядов $k(x)[[Y_1, \ldots, Y_s, Z_{s+1}, \ldots, Z_n]]$, вычислим $\mathrm{Lf}(x, \rho_{r+1})$ и $\nu_0(x, \rho_{r+1})$. Предположим, что для некоторого $0 \le \alpha \le \nu_0(x, \rho_{r+1}) - 2$ мы уже построили индексы $r+1 \le j_1, \ldots, j_\alpha \le s$, такие что

$$\begin{gathered}\mathrm{ord}\, \mathcal{D}_{j_\alpha} \ldots \mathcal{D}_{j_1} \rho_{r+1} = \nu_0(x, \rho_{r+1}) - \alpha, \\ \mathrm{Lf}(x, \mathcal{D}_{j_\alpha} \ldots \mathcal{D}_{j_1} \rho_{r+1}) \in k(x)[Y_{r+1}, \ldots, Y_s]\end{gathered}$$

(база рекурсии есть $\alpha = 0$). На следующем шаге рекурсии применим Лемму 3 к $F = \mathcal{D}_{j_\alpha} \ldots \mathcal{D}_{j_1} \rho_{r+1}$ и вычислим индекс $j_{\alpha+1}$, такой что сформулированные свойства будут удовлетворяться для $\alpha + 1$. В конечном счёте мы получим индексы $r+1 \le j_1, \ldots, j_\beta \le s$, $\beta = \nu_0(x, \rho_{r+1}) - 1$. Затем положим

$$\begin{gathered}\psi_{r+1} = \mathcal{D}_{j_\beta} \ldots \mathcal{D}_{j_1} \rho_{r+1} \in k(x)[Z_1, \ldots, Z_n], \\ h_{r+1} = \psi_{r+1} X_0^{\deg_{Z_1, \ldots, Z_n} \psi_{r+1}} \in k[X_0, \ldots, X_n].\end{gathered}$$

Таким образом, h_{r+1} обращается в нуль тождественно на W, и x является гладкой точкой алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_{r+1})$.

Покажем, как построить все многочлены $g_{r+1,j}$ и $q_{r+1,j,v}$, такие что условия (b) и (d) удовлетворяются с r, заменённым $r+1$. Предположим, что мы уже построили однородные многочлены $g_{r+1,j}$, $q_{r+1,j,v}$ для всех

$\alpha \le j \le s$, $1 \le v \le j$ для некоторого $r+3 \le \alpha \le s+1$, и размерность каждой неприводимой компоненты, содержащей точку x, алгебраического многообразия

$$\mathcal{Z}(h_1, \ldots, h_{r+1}, g_{r+1,\alpha}, \ldots, g_{r+1,s}) = S_\alpha$$

есть $n-r-s+\alpha-2$. Алгебраическое многообразие W является неприводимой компонентой

$$\begin{aligned}&\mathcal{Z}(h_1, \ldots, h_{r+1}, g_{r,r+1}, \ldots, g_{r,s}) = \\ &\mathcal{Z}(h_1, \ldots, h_{r+1}, g_{r,r+1}, \ldots, g_{r,\alpha-1}, g_{r+1,\alpha}, \ldots, g_{r+1,s}) = \\ &S_\alpha \cap \mathcal{Z}(g_{r,r+1}, \ldots, g_{r,\alpha-1}).\end{aligned}$$

Согласно [7] мы можем вычислить размерность алгебраического многообразия (которое задано системой полиномиальных уравнений) в точке x, т.е. максимум размерностей неприводимых компонент рассматриваемого алгебраического многообразия, содержащих точку x. Следовательно, ср. [10], [11], мы можем построить однородные многочлены $g_{r+1,\alpha-1}$, $q_{r+1,\alpha-1,v}$, $1 \le v \le \alpha-1$, такие что $\deg q_{r+1,\alpha-1,v} = \deg g_{\alpha-1} - \deg g_v$, и многочлен $g_{r+1,\alpha-1}$, не обращается в нуль тождественно на каждой неприводимой компоненте, содержащей точку x, алгебраического многообразия S_α.

Следовательно, размерность всякой неприводимой компоненты, содержащей точку x, алгебраического многообразия $S_{\alpha-1}$ есть $n-r-s+\alpha-3$.

Таким образом, используя рекурсию по α, мы построим все многочлены $g_{r+1,v}$ и $q_{r+1,j,v}$, такие что условия (b) и (d) удовлетворяются с r, заменённым на $r+1$. Наконец, применяя Лемму 1 и Замечание 5, в случае, когда $\psi = 1$, последовательность $\psi_1, \ldots, \psi_j$ есть $h_1, \ldots, h_{r+1}$, $g_{r+1,r+2}, \ldots, g_{r+1,s}$ (так что $j = s$) и $j_1 = r+1$, построим x' и заменим x на x'. Теперь условия (a)–(d) удовлетворяются с r, заменённым на $r+1$.

Таким образом, мы построим в конечном счёте требуемые в утверждении (ii) Теоремы 1 однородные многочлены $h_1, \ldots, h_s$. То, что $\mathrm{Lf}(x, \rho_{r+1}) \in \overline{k}[Y_{r+1}, \ldots, Y_s]$, и неравенство $\operatorname{ord} \rho_{r+1} \le n^{2^{s^{C_0}}}$ важно для оценок времени работы описанного алгоритма. Неравенства $\deg h_i < n^{2^{s^C}} \deg g_i$, $1 \le i \le s$, следуют из оценки для $\operatorname{ord} \rho_{r+1}$ и (20), ср. Лемма 19 [5]. Оценка для времени работы описанного алгоритма теперь следует немедленно из оценок для времени работы использованных алгоритмов. Теорема 1 полностью доказана.

2 Измельчение покрытия

Для доказательства Теоремы 2 в случае гладкого покрытия мы сформулируем более точный результат. Пусть V_α, $\alpha \in A_1$ – семейство определённых над k и неприводимых над k квазипроективных алгебраических многообразий $\mathbb{P}^n(\overline{k})$. Пусть $\dim V_\alpha = n - s$ где $1 \le s = s(\alpha) \le n$. Для всякого $\alpha \in A_1$ пусть даны однородные многочлены $h_1, \ldots, h_s \in k[X_0, \ldots, X_n]$ и индексы $0 \le i_1 < \ldots < i_s \le n$ (эти однородные многочлены и индексы зависят от α). Обозначим

$$\Delta_\alpha = \det(\partial h_v / \partial X_{i_w})_{1 \le v, w \le s}.$$

Пусть V_α является определённой над k и неприводимой над k компонентой алгебраического многообразия

$$\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(\Delta_\alpha)$$

для всякого $\alpha \in A_1$.

ТЕОРЕМА 4 *Пусть V – алгебраическое многообразие из Введения. Пусть W_β, $\beta \in B$ – семейство определённых над k и неприводимых над k проективных алгебраических многообразий. Пусть $\dim W_\beta = n - s(\beta)$, где $1 \le s(\beta) \le n$. Пусть однородные многочлены $g_{\beta,1}, \ldots, g_{\beta,m(\beta)} \in k[X_0, \ldots, X_n]$. Обозначим $\mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}) = S_\beta$. Пусть*

$$W_\beta \subset \mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}) = S_\beta \subset V$$

для всякого $\beta \in B$. Предположим, что

$$V \setminus \bigcup_{\beta \in B} W_\beta \subset \bigcup_{\alpha \in A_1} V_\alpha. \tag{23}$$

Тогда для всякого $\beta \in B$ существует конечное семейство определённых над k и неприводимых над k проективных алгебраических многообразий $W_{\beta,\gamma}$, $\gamma \in \Gamma_\beta$, с $\dim W_{\beta,\gamma} = n - s(\gamma)$, $1 \le s(\gamma) \le n$, удовлетворяющих следующим свойствам.

(a) Для всяких $\beta \in B$, $\gamma \in \Gamma_\beta$ имеет место включение

$$W_{\beta,\gamma} \subset W_\beta.$$

(b) Имеет место вложение

$$V \setminus \bigcup_{\beta \in B} \bigcup_{\gamma \in \Gamma_\beta} W_{\beta,\gamma} \subset \bigcup_{\alpha \in A_1} V_\alpha.$$

(c) Для всяких $\beta \in B$, $\gamma \in \Gamma_\beta$ существуют индексы $\alpha_1, \ldots, \alpha_r \in A_1$ (здесь эти индексы и r зависят от γ), такие что $\dim W_{\beta,\gamma} < \dim V_{\alpha_i}$ для всех $1 \le i \le r$, и $W_{\beta,\gamma}$ является неприводимой компонентой алгебраического многообразия

$$\mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}, \Delta_{\alpha_1}, \ldots, \Delta_{\alpha_r}).$$

(d) Справедливо неравенство

$$(\max_{1 \le i \le r} \deg \Delta_{\alpha_i})^{n-s(\beta)} \deg W_\beta \ge \sum_{\gamma \in \Gamma_\beta} (\max_{1 \le i \le r} \deg \Delta_{\alpha_i})^{n-s(\gamma)} \deg W_{\beta,\gamma}.$$

(e) Для всяких $\beta_1, \beta_2 \in B$, $\gamma_1 \in \Gamma_{\beta_1}$, $\gamma_2 \in \Gamma_{\beta_2}$, если $(\beta_1, \gamma_1) \ne (\beta_2, \gamma_2)$, то $W_{\beta_1,\gamma_1} \not\subset W_{\beta_2,\gamma_2}$.

(f) Для всякого $\alpha \in A_1$, для всяких $\beta \in B$, $\gamma \in \Gamma_\beta$ справедливо неравенство $\dim V_\alpha \cap W_{\beta,\gamma} < \dim W_{\beta,\gamma}$.

ДОКАЗАТЕЛЬСТВО Мы можем положить при необходимости $\Gamma_\beta = \emptyset$ для некоторого β. Следовательно, мы можем предполагать без ограничения общности, что $W_{\beta_1} \not\subset W_{\beta_2}$, если $\beta_1 \neq \beta_2$, и $W_{\beta_1} \not\subset \cup_{\alpha\in A_1} V_\alpha$ для всех $\beta_1, \beta_2 \in B$. Обозначим через $\mathcal{F}$ семейство вложений $W_\beta \subset S_\beta$, $\beta \in B$.

Теперь мы опишем общий план доказательства. Построение требуемого семейства $W_{\beta,\gamma}$, $\gamma \in \Gamma_\beta$, $\beta \in B$, осуществляется рекурсивно за конечное число (это будет доказано) шагов, начиная с первого шага. На i-ом шаге мы построим дерево $\mathcal{T}_i$ и семейство $\mathcal{F}_i$ вложений $W_\beta \subset S_\beta$, $\beta \in B_i$, причём $\mathcal{F}_i$ и B_i аналогичны $\mathcal{F}$ и B. Дерево $\mathcal{T}_{i-1}$ является поддеревом $\mathcal{T}_i$ для всякого $i \geq 1$ (дерево $\mathcal{T}_0$ будет определено). Мы построим также подмножество $E_i \subset B_i$, такое что для любых двух $\beta_1, \beta_2 \in B_i \setminus E_i$ мы имеем $W_{\beta_1} \not\subset W_{\beta_2}$, если $\beta_1 \neq \beta_2$, и $W_{\beta_1} \not\subset \cup_{\alpha\in A_1} V_\alpha$. Множество листьев дерева $\mathcal{T}_i$ равно B_i. Для всякого $\beta \in B_i$ вложение $W_\beta \subset S_\beta$ соответствует листу β. Обозначим $\dim W_\beta = n - s(\beta)$, $\beta \in B_i$.

Будет доказано включение

$$V \setminus \bigcup_{\beta\in B_i\setminus E_i} W_\beta \subset \bigcup_{\alpha\in A_1} V_\alpha. \tag{24}$$

Для всякого $\beta \in B$ обозначим через $\Gamma_{i,\beta}$ множество всех $\gamma \in B_i \setminus E_i$, являющихся потомками β или совпадающих с β. Для всякого $\beta \in B$, для всякого $\gamma \in \Gamma_{i,\beta}$ будет установлено включение

$$W_\gamma \subset W_\beta. \tag{25}$$

Мы докажем, что для всякого $\gamma \in \Gamma_{i,\beta}$ существуют индексы $\alpha_1, \ldots, \alpha_r \in A_1$ (здесь эти индексы и r зависят от γ), такие что $\dim W_\gamma < \dim V_{\alpha_i}$ для всех $1 \leq i \leq r$, и

$$S_\gamma = \mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}, \Delta_{\alpha_1}, \ldots, \Delta_{\alpha_r}). \tag{26}$$

Будет установлено также неравенство

$$(\max_{1\leq i\leq r} \deg \Delta_{\alpha_i})^{n-s(\beta)} \deg W_\beta \geq \sum_{\gamma\in\Gamma_{i,\beta}} (\max_{1\leq i\leq r} \deg \Delta_{\alpha_i})^{n-s(\gamma)} \deg W_{\beta,\gamma}. \tag{27}$$

Положим $\mathcal{F}_0 = \mathcal{F}$, $B_0 = B$ и $E_0 = \emptyset$. Дерево $\mathcal{T}_0$ имеет корень v^* (здесь мы вводим новый элемент). Все листья $\beta \in B$ этого дерева являются сыновьями v^*. Положим $\Gamma_{0,\beta} = \{\beta\}$ для всякого $\beta \in B$. Для $i = 0$ включение (24) следует из (23). Включение (25) тривиально. Неравенство (26) справедливо в этом случае. Неравенство (27) также выполнено с $r = 0$.

Пусть $i \geq 0$. Шаг i является заключительным (или, если $i = 0$, не требуется никакой конструкции) тогда и только тогда, когда для всякого $u \in B_i \setminus E_i$ алгебраическое многообразие W_u является неприводимой компонентой S_u, и для всякого $\alpha \in A_1$ справедливо неравенство $\dim V_\alpha \cap W_u < \dim W_u$. Пусть N – номер последнего шага рассматриваемой конструкции. По определению положим $\Gamma_\beta = \Gamma_{N,\beta}$ для всякого $\beta \in B$ и $W_{\beta,\gamma} = W_\gamma$ для всяких $\beta \in B$, $\gamma \in \Gamma_\beta$. Тогда требуемые утверждения (a)–(d) следуют из (25), (24), (26) и (27) для $i = N$. Утверждение (e) теоремы выполнено, поскольку для любых двух различных $\beta_1, \beta_2 \in B_N \setminus E_N$ мы имеем $W_{\beta_1} \not\subset W_{\beta_2}$. Последнее утверждение (f) справедливо, так как для всяких $\alpha \in A_1$, $\beta \in B_N \setminus E_N$ справедливо неравенство $\dim V_\alpha \cap W_\beta < \dim W_\beta$.

Мы будем предполагать без ограничения общности, что наша конструкция содержит по крайней мере один шаг.

Перейдём к подробностям. Предположим, что $(i-1)$-ый шаг не является последним, или $i=1$. Опишем, как выполнить i-ый шаг. Мы предполагаем, что $\mathcal{T}_{i-1}$, $\mathcal{F}_{i-1}$ и E_{i-1} уже построены, и (24), (25), (26), (27) доказаны для $i-1$, если $i>1$. В случае, когда $i-1=0$ (24), (25), (26), (27) также выполняются, как мы видели выше.

Поскольку $(i-1)$-ый шаг не является последним или $i=1$, то выполнено по крайней мере одно из следующих условий:

(a) существуют $u \in B_{i-1} \setminus E_{i-1}$ и определённая над k и неприводимая над k компонента W многообразия S_u, такие что $W_u \subset W$ и $W_u \neq W$.

(b) существует $\alpha \in A_1$, такое что $\dim V_\alpha \cap W_u = \dim W_u$.

Если выполнено (a), то $W \not\subset \bigcup_{\beta \in B_{i-1} \setminus E_{i-1}} W_\beta$. Следовательно, по (24) (для $i-1$) существует $\alpha \in A_1$, такое что $V_\alpha \cap W$ содержит непустое открытое в топологии Зарисского подмножество W. Следовательно, замыкание в топологии Зарисского $\overline{V}_\alpha \supset W$ и

$$\overline{V}_\alpha \supset W_u. \tag{28}$$

Второе условие $\dim V_\alpha \cap W_u = \dim W_u$ также влечёт (28). Выберем индекс α, такой что справедливо (28), и, если выполнено (a), то $\overline{V}_\alpha \supset W$.

Предположим, что $\mathcal{Z}(\Delta_\alpha) \supset W_u$ (следовательно, выполнено условие (a)). Тогда вершина u дерева $\mathcal{T}_i$ по определению имеет единственного сына u_1 (мы будем предполагать без ограничения общности, что этот новый индекс u_1 не является целым числом и не принадлежит никакому множеству индексов B_ι, введённому ранее). Этому сыну u_1 мы приписываем вложение $W_u \subset S_u \cap \mathcal{Z}(\Delta_\alpha)$. Так что $W_{u_1} = W_u$ и $S_{u_1} = S_u \cap \mathcal{Z}(\Delta_\alpha)$. Множество листьев дерева $\mathcal{T}_i$ по определению $B_{i-1} \cup \{u_1\} \setminus \{u\}$ и $E_i = E_{i-1}$. Следовательно, для любых двух различных $\beta_1, \beta_2 \in B_i \setminus E_i$ мы имеем $W_{\beta_1} \not\subset W_{\beta_2}$. Таким образом, дерево $\mathcal{T}_i$ построено в этом случае. Требуемые (24), (25), (26), (27) для i следуют из тех же самых утверждений для $i-1$ в этом случае. Отметим здесь, что $W \not\subset S_{u_1}$ в рассматриваемом случае.

Предположим, что $\mathcal{Z}(\Delta_\alpha) \not\supset W_u$. Представим

$$\mathcal{Z}(\Delta_\alpha) \cap W_u = \bigcup_{\beta \in B_u} W_\beta,$$

где W_β, $\beta \in B_u$, является семейством всех определённых над k и неприводимых над k компонент алгебраического многообразия $\mathcal{Z}(\Delta_\alpha) \cap W_u$ (мы будем предполагать без ограничения общности, что все индексы B_u не являются целыми числами и не принадлежат никакому множеству индексов B_ι, введённому ранее).

Обозначим через E_u подмножество всех $\beta \in B_u$, таких что существует $\beta_1 \in B_{i-1} \setminus (E_{i-1} \cup \{u\})$ с $W_\beta \subset W_{\beta_1}$ или $W_\beta \subset \cup_{\alpha \in A_1} V_\alpha$.

По определению множество сыновей u в дереве $\mathcal{T}_i$ есть B_u. Каждому $\beta \in B_u$ сопоставим вложение $W_\beta \subset S_u \cap \mathcal{Z}(\Delta_\alpha) = S_\beta$. По определению множество листьев дерева $\mathcal{T}_i$ есть

$$B_i = (B_{i-1} \cup B_u) \setminus \{u\}.$$

Положим по определению

$$E_i = (E_{i-1} \cup E_u) \setminus \{u\}.$$

Следовательно, для любых двух различных $\beta_1, \beta_2 \in B_i \setminus E_i$ мы имеем $W_{\beta_1} \not\subset W_{\beta_2}$. Таким образом, дерево $\mathcal{T}_i$ построено в этом случае.

Заметим, что $B_i \setminus E_i = (B_{i-1} \setminus (E_{i-1} \cup \{u\})) \cup (B_u \setminus E_u)$. Следовательно,

$$W_u \setminus \left(\bigcup_{\beta \in B_u \setminus E_u} W_\beta \cup \bigcup_{\beta \in B_{i-1} \setminus (E_{i-1} \cup \{u\})} W_\beta \right) \subset W_u \setminus \mathcal{Z}(\Delta_\alpha) \subset V_\alpha$$

в рассматриваемом случае. Следовательно, (24) для i следует из того же самого включения для $i-1$. Требуемые (25), (26), (27) для i следуют из тех же самых утверждений для $i-1$ и теоремы Безу в этом случае.

Чтобы доказать, что наша конструкция состоит только из конечного числа шагов мы введём инвариант $a(\mathcal{F})$, соответствующий семейству $\mathcal{F}$ (или аналогичному) вложений $W_\beta \subset S_\beta$, $\beta \in B$ из формулировки теоремы (причём B не является фиксированным для этого инварианта).

Обозначим через $\mathbb{Z}_+ = \{z \in \mathbb{Z} \; : \; z \geq 0\}$ множество всех неотрицательных целых чисел. Положим $Z(j) = \mathbb{Z}_+^{j+2}$ для $j \in \mathbb{Z}_+$. Рассмотрим лексикографический порядок на $Z(j)$. Именно, пусть $x = (x_1, \ldots, x_{j+2})$, $y = (y_1, \ldots, y_{j+2})$ – два элемента из $Z(j)$. Тогда $x > y$, в том и только в том случае, если существует i, такое что $1 \leq i \leq j+2$ и

$$x_1 = y_1, \; \ldots, \; x_{i-1} = y_{i-1} \quad \text{и} \quad x_i > y_i \, .$$

По определению положим $Z^* = Z(1) \times Z(2) \times \ldots \times Z(n)$. Рассмотрим лексикографический порядок на множестве Z^*. Именно, пусть $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ – два элемента из Z^*. Тогда $x > y$ в том и только в том случае, если существует i, такое что $1 \leq i \leq n$ и

$$x_1 = y_1, \; \ldots, \; x_{i-1} = y_{i-1} \quad \text{и} \quad x_i > y_i \, .$$

Заметим, что всякая строго убывающая последовательность элементов множества Z^* является конечной, т.е. Z^* удовлетворяет условию обрыва убывающих цепей.

Обозначим через $S_{\beta,i}$ объединение всех неприводимых компонент W многообразия S_β, таких что размерность $\dim W = n - i$, и $W \supset W_\beta$. Так что, если $S_{\beta,i} \neq \emptyset$, то $0 \leq i \leq s(\beta)$. Положим $\deg S_{\beta,i} = s_{\beta,i}$ и $\deg W_\beta = w_\beta$ для всех i, β.

В дальнейшем мы будем предполагать без ограничения общности, что $B \cap \mathbb{Z} = \emptyset$, вводя при необходимости новые индексы. Обозначим через $B^{(j)}$, $1 \leq j \leq n$, множество всех $\beta \in B$, таких что $s(\beta) = j$. По определению положим

$$\begin{aligned}
&w_j = \sum_{\beta \in B^{(j)}} w_\beta, \quad 1 \leq j \leq n, \\
&s_{j,i} = \sum_{\beta \in B^{(j)}} s_{\beta,i}, \quad 0 \leq i \leq j, \; 1 \leq j \leq n, \\
&a_j = (w_j, s_{j,0}, s_{j,1}, \ldots, s_{j,j}) \in Z(j), \quad 1 \leq j \leq n, \\
&a(\mathcal{F}) = (a_1, \ldots, a_n) \in Z^*.
\end{aligned}$$

Заметим, что для всякого $i \geq 1$, если описанная конструкция семейства $W_{\beta,\gamma}$, $\gamma \in \Gamma_\beta$, $\beta \in B$, состоит по крайней мере из i шагов, то $a(\mathcal{F}_{i-1}) > a(\mathcal{F}_i)$. Следовательно, по условию обрыва убывающих цепей существует только конечное число N шагов. Теорема доказана.

ЗАМЕЧАНИЕ 6 *Отметим, что если в условиях Теоремы 4 дополнительно для всех $\alpha \in A_1$, $\beta \in B$ мы имеем $W_\beta \not\supset V_\alpha$, то для всех $\alpha \in A_1$, $\beta \in B$, $\gamma \in \Gamma_\beta$ справедливо неравенство* $\dim V_\alpha \cap W_{\beta,\gamma} < \dim V_\alpha$.

3 Доказательство Теоремы 2 для случая гладкого покрытия

В условиях Теоремы 4 мы будем предполагать без ограничения общности, что для всяких различных $\beta_1, \beta_2 \in B$ пересечение $\Gamma_{\beta_1} \cap \Gamma_{\beta_2} = \emptyset$. Обозначим $W_\gamma = W_{\beta,\gamma}$ для всяких $\beta \in B$, $\gamma \in \Gamma_\beta$.

В дальнейшем мы будем использовать новые обозначения, отличные от обозначений из доказательства Теорема 4. Пусть $i \geq 1$ – целое число. Обозначим через A_i, B_i и Γ_i соответственно множества A_1, B и $\cup_{\beta \in B} \Gamma_\beta$ в старых обозначениях Теоремы 4. Тогда в конструкции Теоремы 4 на входе имеется пара семейств

$$V_\alpha,\ \alpha \in A_i, \quad W_\beta \subset S_\beta,\ \beta \in B_i, \tag{29}$$

а на выходе пара семейств

$$V_\alpha,\ \alpha \in A_i, \quad W_\gamma \subset S_\gamma,\ \gamma \in \Gamma_i. \tag{30}$$

Конструкция требуемого гладкого покрытия V_α, $\alpha \in A$ осуществляется рекурсивно за конечное число шагов, начиная с первого шага. Обозначим через W_γ, $\gamma \in \Gamma_0$ семейство всех определённых над k и неприводимых над k компонент V и положим $S_\gamma = \mathcal{Z}(f_1, \ldots, f_m)$ для всякого $\gamma \in \Gamma_0$. Положим $A_0 = \emptyset$. Мы можем предполагать без ограничения общности, что $\Gamma_0 \neq \emptyset$.

Опишем i-ый шаг, $i \geq 1$. В начале этого шага построена пара семейств (30) с i, заменённым на $i-1$, и $\Gamma_{i-1} \neq \emptyset$. Положим

$$B_i = \Gamma_{i-1}, \quad A_i = A_{i-1} \cup \Gamma_{i-1}$$

(мы можем здесь предполагать без ограничения общности, что $A_{i-1} \cap \Gamma_{i-1} = \emptyset$, вводя при необходимости новые индексы). Пусть $\dim W_\beta = n - s(\beta)$, где $1 \leq s(\beta) \leq n$ для всякого $\beta \in B_i$. Применяя Теорему 1, для всякого $\beta \in B_i$ построим семейство однородных многочленов $h_1, \ldots, h_s \in k[X_0, \ldots, X_n]$, индексы $0 \leq i_1 < \ldots < i_s \leq n$ (эти однородные многочлены и индексы зависят от β, $s = s(\beta)$) и многочлен

$$\Delta_\beta = \det(\partial h_v / \partial X_{i_w})_{1 \leq v, w \leq s},$$

такие что $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ является неприводимой компонентой алгебраического многообразия

$$\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(\Delta_\beta).$$

Следовательно, $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ является гладким квазипроективным алгебраическим многообразием. Положим $V_\beta = W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ для всякого $\beta \in B_i$.

Тогда применяя Теорему 4 к (29), мы получаем пару семейств (30). Если $\Gamma_i = \emptyset$, то V_α, $\alpha \in A_i$ является требуемым гладким покрытием. Если $\Gamma_i \neq \emptyset$, то мы переходим к $(i+1)$-ому шагу.

Согласно утверждению (f) Теоремы 4 в рассматриваемой конструкции может быть самое большее n шагов. Требуемые в Теореме 2 оценки для степеней и длин записи следуют немедленно из Теоремы 1 и Теоремы 4, см. также замечания о представлении (6) во Введении. Теорема 2 для случая гладкого покрытия доказана.

4 Конструкция частичного порядка на множестве неприводимых алгебраических многообразий

Пусть W_β, $\beta \in B$, – семейство определённых над k и неприводимых над k алгебраических многообразий, каждое из которых задано в виде (6) из Введения. Так что $\dim W_\beta = n - s(\beta)$, $1 \leq s(\beta) \leq n$. Пусть $W_{\beta_1} \neq W_{\beta_2}$ для всяких $\beta_1 \neq \beta_2$. В этом разделе мы построим частичный порядок и линейный порядок на множестве $\{W_\beta : \beta \in B\}$ или, что эквивалентно, на B.

Обозначим через B_s подмножество всех $\beta \in B$, таких что $\dim W_\beta = n-s$, $1 \leq s \leq n$. Для всяких $1 \leq s_1 < s_2 \leq n$, для всяких $\beta_1 \in B_{s_1}$, $\beta_2 \in B_{s_2}$ положим $\beta_1 < \beta_2$. Таким образом, мы получаем частичный порядок на B, который мы назовём предварительным. Теперь достаточно построить частичный порядок и линейный порядок на каждом множестве B_s, $1 \leq s \leq n$. Так что в дальнейшем мы будем предполагать без ограничения общности, что s фиксировано.

Для всякого $\beta \in B_s$ рассмотрим, см. Теорему 1, семейство однородных многочленов $h_1, \dots, h_s \in k[X_0, \dots, X_n]$, индексы $0 \leq i_1 < \dots < i_s \leq n$ (эти однородные многочлены и индексы зависят от β) и многочлен

$$\Delta_\beta = \det(\partial h_v / \partial X_{i_w})_{1 \leq v, w \leq s},$$

такие что $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ является неприводимой компонентой алгебраического многообразия

$$\mathcal{Z}(h_1, \dots, h_s) \setminus \mathcal{Z}(\Delta_\beta).$$

Следовательно, $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ является гладким квазипроективным алгебраическим многообразием. Мы будем обозначать также $h_i = h_{\beta,i}$, $1 \leq i \leq s$, когда зависимость от β будет существенна. Определим семейство

$$\mathcal{H} = \{h_{\beta,i}\}_{\beta \in B_s,\, 1 \leq i \leq s}.$$

Пусть $\delta_s = \max_{\beta \in B_s, 1 \leq i \leq s} \deg h_{\beta,i}$. В дальнейшем мы будем считать, не умаляя общности, что $\deg h_{\beta,i} = \delta_s$ для всех $\beta \in B_s$, $1 \leq i \leq s$, домножая при необходимости каждый $h_{\beta,i}$ на некоторый моном, не обращающийся в нуль тождественно на W_β.

Определим функцию

$$\sigma(\mathcal{H}) : B_s \times B_s \longrightarrow \{0, 1\}$$

следующим образом. Обозначим для краткости $\sigma = \sigma(\mathcal{H})$. Положим $\sigma(\beta, \beta') = 1$ (соответственно $\sigma(\beta, \beta') = 0$) тогда и только тогда, когда многочлены $h_{\beta,1}, \dots, h_{\beta,s}$ обращаются (соответственно по крайней мере один из многочленов $h_{\beta,1}, \dots, h_{\beta,s}$ не обращается) в нуль тождественно на алгебраическом многообразии $W_{\beta'}$. Для всякого $(\beta, \beta') \in B_s \times B_s$, такого что $\sigma(\beta, \beta') = 0$, определим также индекс $i_0 = i_0(\beta, \beta')$, для которого h_{β,i_0} не обращается в нуль тождественно на $W_{\beta'}$.

Для всякого $\tau \in B_s$ определим множества

$$\begin{aligned}
&B'_\tau = B'_\tau(\mathcal{H}) = \{(\beta', \beta) \in B_s \times B_s \,:\, \sigma(\beta', \tau) = 1 \,\&\\
&\sigma(\tau, \beta) = 1 \,\&\, \sigma(\beta', \beta) = 0\,\},\\
&B_\tau = B_\tau(\mathcal{H}) = \{\beta \,:\, \exists \beta'(\,(\beta', \beta) \in B'_\tau\,)\,\}.
\end{aligned}$$

Докажем, что мы можем построить семейство

$$\widetilde{\mathcal{H}} = \{\widetilde{h}_{\beta,i}\}_{\beta \in B_s,\, 1 \le i \le s}$$

аналогичное $\mathcal{H}$, такое что, заменяя $\mathcal{H}$ на $\widetilde{\mathcal{H}}$, мы получаем новое семейство $\mathcal{H}$, для которого дополнительно выполнено (35), см. ниже. Пусть $\tau \in B_s$. Сначала покажем, как построить новое семейство $\widetilde{\mathcal{H}}$ и функцию $\sigma(\widetilde{\mathcal{H}})$ аналогичные $\mathcal{H}$ и $\sigma(\mathcal{H})$, такие что для всякого $\tau \in B_s$, для всякого $\beta \in B_\tau(\mathcal{H})$

$$\sigma(\widetilde{\mathcal{H}})(\tau, \beta) = 0, \tag{31}$$

и для всяких $\tau, \beta \in B_s$

$$\sigma(\widetilde{\mathcal{H}})(\tau, \beta) \le \sigma(\mathcal{H})(\tau, \beta). \tag{32}$$

Положим

$$\widetilde{h}_{\tau,i} = h_{\tau,i} \quad \text{для всех} \quad \tau \in B_s,\ 1 \le i \le s-1. \tag{33}$$

Остаётся определить $\widetilde{h}_{\tau,s}$ для всех τ.

Построим функцию $\rho \,:\, B_\tau \to B_s$, удовлетворяющую условию, что

$$(\rho(\beta), \beta) \in B'_\tau$$

для всякого $\beta \in B_\tau$. Мы будем обозначать также $\rho = \rho(\tau, \mathcal{H})$.

Положим для всех $\tau \in B_s$

$$\widetilde{h}_{\tau,s} = h_{\tau,s} + \sum_{\beta \in B_\tau} c_\beta h_{\rho(\beta), i_0(\rho(\beta), \beta)}, \tag{34}$$

где c_β, $\beta \in B_\tau$, – некоторые элементы поля k (которые следует выбрать), такие что выполнены требуемые свойства (31), (32), и функция

$$\widetilde{\Delta}_\tau = \det(\partial \widetilde{h}_u / \partial X_{i_v})_{1 \le u,v \le s}$$

не обращается в нуль тождественно на W_τ (здесь индексы $0 \le i_1 < \ldots < i_s \le n$ – те же самые, которые были в определении Δ_τ). Кроме того, мы выберем $c_\beta \in \mathbb{Z}$ с длинами записи $\mathrm{l}(c_\beta) = O(\log(2 + \# B_s))$ для всех $\beta \in B_\tau$.

Для всякого $\tau \in B_s$ определим множества $B'_\tau(\widetilde{\mathcal{H}})$, $B_\tau(\widetilde{\mathcal{H}})$ и функцию $\rho(\tau, \widetilde{\mathcal{H}})$, заменяя в определениях $B'_\tau(\mathcal{H})$, $B_\tau(\mathcal{H})$ и $\rho(\mathcal{H})$ семейство $\mathcal{H}$ на $\widetilde{\mathcal{H}}$.

ЛЕММА 4 *Для всякого $\tau \in B_s$ множество $B_\tau(\widetilde{\mathcal{H}}) = \emptyset$.*

ДОКАЗАТЕЛЬСТВО Покажем, что если $\beta' \notin B_\tau(\mathcal{H})$, то $\sigma(\mathcal{H})(\tau, \beta') = \sigma(\widetilde{\mathcal{H}})(\tau, \beta')$. В самом деле, мы имеем $\sigma(\mathcal{H})(\tau, \beta') \geq \sigma(\widetilde{\mathcal{H}})(\tau, \beta')$ для всех τ, β'. Следовательно, достаточно рассмотреть случай, когда $\sigma(\mathcal{H})(\tau, \beta') = 1$. Условие $\beta' \notin B_\tau(\mathcal{H})$ влечёт, что для всякого $\beta \in B_\tau(\mathcal{H})$ многочлен $h_{\rho(\beta), i_0(\rho(\beta), \beta)}$ обращается в нуль тождественно на $W_{\beta'}$. Следовательно, согласно (33) и (34) $\sigma(\widetilde{\mathcal{H}})(\tau, \beta') = 1$, что доказывает наше утверждение.

Теперь предположим, что $\beta \in B_\tau(\widetilde{\mathcal{H}}) \neq \emptyset$ для некоторого τ. Положим $\beta_1 = \rho(\tau, \widetilde{\mathcal{H}})(\beta)$. Тогда $\sigma(\mathcal{H})(\beta_1, \beta) = 1$, поскольку, иначе, $\sigma(\widetilde{\mathcal{H}})(\tau, \beta) = 0$.

Если $\beta \notin B_{\beta_1}(\mathcal{H})$, то, как было доказано, $\sigma(\widetilde{\mathcal{H}})(\beta_1, \beta) = 1$. Это приводит к противоречию.

Следовательно, $\beta \in B_{\beta_1}(\mathcal{H})$. Положим $\beta_2 = \rho(\beta_1, \mathcal{H})(\beta)$. Так что $\sigma(\mathcal{H})(\beta_2, \beta) = 0$ и $\sigma(\mathcal{H})(\beta_2, \beta_1) = 1$. С другой стороны,

$$\sigma(\mathcal{H})(\beta_1, \tau) = \sigma(\widetilde{\mathcal{H}})(\beta_1, \tau) = 1.$$

Следовательно, $\sigma(\mathcal{H})(\beta_2, \tau) = 1$. Напомним, что

$$\sigma(\mathcal{H})(\tau, \beta) = \sigma(\widetilde{\mathcal{H}})(\tau, \beta) = 1.$$

Следовательно, $\sigma(\mathcal{H})(\beta_2, \beta) = 1$. Полученное противоречие доказывает лемму.

Теперь заменяя семейство $\mathcal{H}$ на $\widetilde{\mathcal{H}}$, мы будем предполагать в дальнейшем, что

$$B_\tau(\mathcal{H}) = \emptyset \quad \text{для всех} \quad \tau \in B_s. \tag{35}$$

Определим отношение эквивалентности на множестве B_s следующим образом. Два элемента $\beta, \tau \in B_s$ эквивалентны тогда и только тогда, когда $\sigma(\beta, \tau) = 1$ и $\sigma(\tau, \beta) = 1$ (транзитивность этого отношения следует из (35)). Построим фактормножество $\overline{B}_s$ множества B_s относительно этой эквивалентности. Обозначим через $\pi : B_s \longrightarrow \overline{B}_s$, $\pi(\beta) = \overline{\beta}$, естественную проекцию. Согласно (35) функция σ может быть представлена в виде $\sigma = \overline{\sigma} \circ (\pi \times \pi)$ для однозначно определённой функции $\overline{\sigma} : \overline{B}_s \times \overline{B}_s \longrightarrow \{0, 1\}$.

Введём частичный порядок на множестве $\overline{B}_s$ следующим образом. Пусть $u, v \in \overline{B}_s$. Тогда $u \geq v$ тогда и только тогда, когда $\overline{\sigma}(u, v) = 1$ (транзитивность этого частичного порядка следует из (35)).

Для всяких $u, v \in \overline{B}_s$, $\beta \in u$, $\tau \in v$, таких что $u > v$ положим по определению $\beta > \tau$. Таким образом, мы получаем частичный порядок на B_s. Требуемый частичный порядок на B по определению является минимальным частичным порядком (это подмножество $B \times B$), содержащим все построенные порядки на B_s, $1 \leq s \leq n$, и предварительный частичный порядок на B, описанный в начале раздела.

Известно, что всякий частичный порядок на конечном множестве может быть продолжен до линейного порядка. Так что мы продолжаем построенный частичный порядок на B до линейного порядка. Полученный линейный порядок является требуемым линейным порядком на B.

Рассмотрим семейство линейно независимых линейных форм

$$Y_i = \sum_{0 \leq j \leq n} y_{i,j} X_j, \quad 0 \leq i \leq n, \tag{36}$$

где $y_{i,j} \in k$ для всех i, j. Представим также

$$X_i = \sum_{0 \le j \le n} x_{i,j} Y_j, \quad 0 \le i \le n, \tag{37}$$

где $x_{i,j} \in k$ для всех i, j. Для всякого $u \in \overline{B}_s$ рассмотрим однородные многочлены

$$h_{u,i} = \sum_{\beta \in u} c_{\beta,i} h_{\beta,i}, \quad 1 \le i \le s, \tag{38}$$

где $c_{\beta,i} \in k$ для всех β, i. Положим

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

Мы немедленно получаем (рассматривая сначала все $x_{i,j}$ и $c_{\beta,i}$, как переменные), что существуют линейные формы (36) и однородные многочлены (38), такие что

- для всякого $\tau \in B_s$ алгебраическое многообразие $W_\tau \subset \mathcal{Z}(h_{u,1}, \ldots, h_{u,s})$ тогда и только тогда, когда $u \ge \overline{\tau}$ относительно построенного частичного порядка на $\overline{B}_s$.
- для всякого $\tau \in u$ многочлен Δ_u не обращается в нуль тождественно на W_τ (и, следовательно, $W_\tau \setminus \mathcal{Z}(\Delta_u)$ является неприводимой компонентой $\mathcal{Z}(h_{u,1}, \ldots, h_{u,s}) \setminus \mathcal{Z}(\Delta_u)$).

Кроме того, можно выбрать дополнительно все $x_{i,j}, c_{\beta,i} \in \mathbb{Z}$ с длинами записи $O(n + \log(1 + \#B_s))$.

5 Доказательство Теоремы 2 для случая гладкой стратификации

Мы докажем Теорему 2 в несколько более общей ситуации. Именно, пусть проективные алгебраические многообразия $V^{(i)}$, $1 \le i \le b$, аналогичны $W^{(i)}$, $1 \le i \le a$, из Введения. Пусть однородные многочлены $g_j^{(i)}$, $1 \le i \le b$, $1 \le j \le \mu(i)$, аналогичны многочленам $f_j^{(i)}$, $1 \le i \le a$, $1 \le j \le m(i)$ из Введения. Следовательно, $V^{(i)}$, $1 \le i \le b$, является объединением некоторых неприводимых компонент алгебраического многообразия $\mathcal{Z}(g_1^{(i)}, \ldots, g_{\mu(i)}^{(i)})$. Предположим, что $V^{(1)} = V$ и $g_j^{(1)} = f_j$, $1 \le j \le m = \mu(1)$. Положим

$$V' = V^{(1)} \setminus \bigcup_{2 \le i \le b} V^{(i)}.$$

Пусть степени и длины записи целых коэффициентов однородных многочленов $g_j^{(i)}$, $1 \le i \le b$, $1 \le j \le \mu(i)$, удовлетворяют тем же самым оценкам, что и степени и длины записи целых коэффициентов многочленов $f_1, \ldots, f_m$. Заменяя в Определении 1 V на V', мы получаем определение гладкого покрытия и гладкой стратификации квазипроективного алгебраического многообразия. Заменим в формулировке Теоремы 2 алгебраическое многообразие V на V'. Мы докажем Теорему 2 в случае гладкой стратификации в этой новой формулировке для квазипроективного алгебраического многообразия V'.

Конечно, новая формулировка Теоремы 2 является следствием исходной (для V), однако имеется некоторая разница. Именно, может случиться, что $\dim V' < \dim V$, и в этом случае новая формулировка Теоремы 2 является важной для применения индукционного предположения, см. ниже.

Мы будем обозначать в этом разделе требуемую гладкую стратификацию алгебраического многообразия V' через V'_α, $\alpha \in A$. Пусть $\dim V'_\alpha = n - s(\alpha)$, где $1 \le s(\alpha) \le n$ для всякого $\alpha \in A$. Мы докажем, что существует абсолютная константа $C_1 > 0$, такая что, если $\dim V' \le n-s$, где $1 \le s \le n$, то

$$\sum_{\alpha\in A} d^{n-s(\alpha)} \deg \overline{V'_\alpha} \le n^{2^{(n(n-s+1))^{C_1}}} d^{(n+s)(n-s+1)/2}, \tag{39}$$

где $\overline{V'_\alpha}$ является замыканием в топологии Зарисского многообразия V'_α.

В нашей конструкции мы используем индукцию по $\dim V'$. База $\dim V' = -1$, т.е. $V' = \emptyset$, тривиальна.

Конструкция гладкой стратификации V'_α, $\alpha \in A$, осуществляется рекурсивно за несколько шагов, начиная с первого (эта рекурсия не является индукцией по $\dim V'$).

Обозначим через W_γ, $\gamma \in \Gamma_0$, семейство всех определённых над k и неприводимых над k компонент V (чтобы избежать двусмысленности мы будем предполагать без ограничения общности, что все элементы Γ_0 не являются целыми числами). Заменим в Разделе 4 семейство W_β, $\beta \in B$, на W_γ, $\gamma \in \Gamma_0$, и построим линейный порядок на Γ_0, используя метод из этого раздела. Для всякого $\gamma \in \Gamma_0$ построим также однородные многочлены $h_j = h_{\overline{\gamma},j} \in k[X_0, \ldots, X_n]$, $1 \le j \le s$ и многочлен $\Delta_{\overline{\gamma}}$, где $\overline{\gamma} \in \overline{(\Gamma_0)}_s$, см. Раздел 4. Мы будем обозначать также $h_{\gamma,j} = h_{\overline{\gamma},j}$, $1 \le j \le s = s(\gamma)$, когда зависимость от γ будет существенна. Обозначим $\Delta_\gamma = \Delta_{\overline{\gamma}}$ для всякого $\gamma \in \Gamma_0$. Положим

$$W'_{0,\gamma} = W_\gamma \setminus \left(\bigcup_{\tau<\gamma,\, \tau\in\Gamma_0} W_\tau \cup \bigcup_{2\le j\le b} V^{(j)} \right)$$

для всякого $\gamma \in \Gamma_0$ (здесь и ниже в аналогичных ситуациях $\tau < \gamma$ означает по отношению к введённому линейному порядку на Γ_0). Положим $A_0 = \emptyset$. Мы можем предполагать без ограничения общности, что $\Gamma_0 \ne \emptyset$.

Опишем объекты известные в начале i-ого шага, $i \ge 1$.

- Построено семейство V_α, $\alpha \in A_{i-1}$, определённых над k и неприводимых k квазипроективных алгебраических многообразий в $\mathbb{P}^n(\overline{k})$. Пусть $\dim V_\alpha = n - s$, где $1 \le s = s(\alpha) \le n$. Для всякого $\alpha \in A_{i-1}$ даны однородные многочлены

  $$h_1, \ldots, h_s \in k[X_0, \ldots, X_n] \tag{40}$$

  и линейные формы $Y_0, \ldots, Y_n \in k[X_0, \ldots, X_n]$ (эти однородные многочлены зависят от α, $s = s(\alpha)$, и мы будем обозначать также $h_j = h_{\alpha,j}$, когда зависимость от α будет существенна). Справедливы неравенства

  $$\deg h_{\alpha,j} \le n^{2^{s(\alpha)^{C_2}}} d, \quad 1 \le j \le s(\alpha), \tag{41}$$

для всякого $\alpha \in A_{i-1}$, где $C_2 > 0$ – абсолютная константа. Мы будем предполагать, что выполнены (36) и (37), Раздел 4. Обозначим

$$\Delta_\alpha = \det(\partial h_v/\partial Y_w)_{1\le v,w\le s} = \det(\sum_{0\le u\le n} x_{u,w}\partial h_v/\partial X_u)_{1\le v,w\le s}.$$

Алгебраическое многообразие V_α является неприводимой компонентой алгебраического многообразия

$$\mathcal{Z}(h_{\alpha,1},\ldots,h_{\alpha,s}) \setminus \mathcal{Z}(\Delta_\alpha)$$

для всякого $\alpha \in A_{i-1}$. Для всякого $\alpha \in A_{i-1}$ обозначим $W_\alpha = \overline{V_\alpha}$, где $\overline{V_\alpha}$ является замыканием в топологии Зарисского многообразия V_α.

- Для всякого $\alpha \in A_{i-1}$ построено определённое над k и неприводимое над k квазипроективное алгебраическое многообразие

  $$V'_\alpha \subset V_\alpha \setminus \bigcup_{2\le j\le b} V^{(j)},$$

  такое что V'_α является непустым открытым в топологии Зарисского подмножеством V_α (следовательно, V'_α – гладкое и $V_\alpha \not\subset \bigcup_{2\le j\le b} V^{(j)}$).

- Построено подмножество $\Gamma_{i-1} \subset \Gamma_0$, такое что число элементов $\#\Gamma_{i-1} \le 1-i+\#\Gamma_0$, и для всякого $\gamma \in \Gamma_{i-1}$, для всякого $\gamma_1 \in \Gamma_0 \setminus \Gamma_{i-1}$ справедливо неравенство $\gamma > \gamma_1$, т.е. для всякого $j > 0$ множество Γ_j содержится в множестве, которое получено из Γ_{j-1} удалением минимального элемента.

- Для всякого $\gamma \in \Gamma_{i-1}$ построено определённое над k и неприводимое над k квазипроективное алгебраическое многообразие

  $$W'_{i-1,\gamma} \subset W_\gamma \setminus \bigcup_{2\le j\le b} V^{(j)},$$

  такое что $W'_{i-1,\gamma}$ является непустым открытым в топологии Зарисского подмножеством W_γ (в частности, $W'_{i-1,\gamma} \not\subset \bigcup_{2\le j\le b} V^{(j)}$).

Следующие свойства удовлетворяются в начале i-ого шага:

$$\bigcup_{\alpha\in A_{i-1}} V'_\alpha \cup \bigcup_{\gamma\in\Gamma_{i-1}} W'_{i-1,\gamma} = V', \tag{42}$$

$$W_\tau \setminus \bigcup_{2\le j\le b} V^{(j)} \subset \bigcup_{\alpha\in A_{i-1}} V'_\alpha \quad \text{для всякого} \quad \tau \in A_{i-1}, \tag{43}$$

$$V'_{\alpha_1} \cap V'_{\alpha_2} = \emptyset \quad \text{для всяких различных} \quad \alpha_1,\alpha_2 \in A_{i-1}, \tag{44}$$

$$W_\alpha \cap W'_{i-1,\gamma} = \emptyset \quad \text{для всяких} \quad \alpha \in A_{i-1},\ \gamma \in \Gamma_{i-1}, \tag{45}$$

$$W_\gamma \setminus \bigcup_{2\le j\le b} V^{(j)} \subset \bigcup_{\tau\le\gamma,\,\tau\in\Gamma_{i-1}} W'_{i-1,\tau} \cup \bigcup_{\alpha\in A_{i-1}} V'_\alpha \tag{46}$$

для всякого $\quad \gamma \in \Gamma_{i-1}$.

Очевидно, что эти свойства выполнены для $i-1=0$.

Опишем i-ый шаг, $i \geq 1$. В дальнейшем мы будем предполагать без ограничения общности, что все вводимые индексы (соответственно множества индексов) отличны от всех индексов (соответственно не пересекаются со всеми множествами индексов), рассматриваемых (соответственно рассматриваемыми) ранее.

Пусть γ_i – наименьший элемент множества Γ_{i-1}. Обозначим через W'_τ, $\tau \in D_i$, семейство всех определённых над k, и неприводимых над k компонент алгебраического многообразия $W'_{i-1,\gamma_i} \cap \mathcal{Z}(\Delta_{\gamma_i})$. Следовательно,

$$W'_{i-1,\gamma_i} \cap \mathcal{Z}(\Delta_{\gamma_i}) = \bigcup_{\tau \in D_i} W'_\tau.$$

Для всех $\tau \in D_i$ положим

$$W_\tau = \overline{W'_\tau},$$

где $\overline{W'_\tau}$ обозначает замыкание в топологии Зарисского многообразия W'_τ.

ЛЕММА 5 *Пусть $\tau \in D_i$. Тогда W'_τ является определённой над k и неприводимой над k компонентой алгебраического многообразия*

$$\mathcal{Z}(f_1, \ldots, f_m, h_{\gamma_i,1}, \ldots, h_{\gamma_i,s(\gamma_i)}, \Delta_{\gamma_i}) \setminus \left(\bigcup_{\alpha \in A_{i-1}} W_\alpha \cup \bigcup_{2 \leq j \leq b} V^{(j)} \right). \qquad (47)$$

Кроме того, размерность алгебраического многообразия (47) равна самое большее $-1 + \dim W_{\gamma_i}$.

ДОКАЗАТЕЛЬСТВО Согласно (45), (46) мы имеем

$$W'_{i-1,\gamma_i} = W_{\gamma_i} \setminus \left(\bigcup_{\alpha \in A_{i-1}} W_\alpha \cup \bigcup_{2 \leq j \leq b} V^{(j)} \right).$$

Следовательно,

$$W'_\tau = W_\tau \setminus \left(\bigcup_{\alpha \in A_{i-1}} W_\alpha \cup \bigcup_{2 \leq j \leq b} V^{(j)} \right).$$

Следовательно, достаточно доказать последнее утверждение леммы.

Достаточно доказать, что для всякой неприводимой компоненты W алгебраического многообразия (47) $\dim W < \dim W_{\gamma_i}$. Согласно (42), (44) для всякого $\gamma < \gamma_i$, $\gamma \in \Gamma_0$, существует $\alpha \in A_{i-1}$, такое что $W_\alpha = W_\gamma$. Следовательно, для всякой неприводимой компоненты W алгебраического многообразия (47) существует $\gamma \geq \gamma_i$, такое что $W \subset W_\gamma$. Если $\dim W_\gamma < \dim W_{\gamma_i}$, то лемма доказана. Предположим, что $\dim W_\gamma \geq \dim W_{\gamma_i}$. Тогда $\dim W_\gamma = \dim W_{\gamma_i}$, и

$$W_\gamma \not\subset \mathcal{Z}(h_{\gamma_i,1}, \ldots, h_{\gamma_i,s(\gamma_i)}, \Delta_{\gamma_i})$$

по построению линейного порядка на Γ_0. Следовательно, $W_\gamma \neq W$ и

$$\dim W_{\gamma_i} = \dim W_\gamma > \dim W.$$

Лемма доказана.

Обозначим через S_{γ_i} алгебраическое многообразие (47). Используя индукционное предположение, построим гладкую стратификацию V'_α, $\alpha \in A_{\gamma_i}$, квазипроективного алгебраического многообразия S_{γ_i} (мы можем предполагать без ограничения общности, что $(A_{i-1}\cup\Gamma_{i-1})\cap A_{\gamma_i}=\emptyset$). Мы также предположим, что построены соответствующие V_α, Δ_α и однородные многочлены (40) (зависящие от α) для всякого $\alpha \in A_{\gamma_i}$.

Для всякого $\gamma \in \Gamma_{i-1}\setminus\{\gamma_i\}$ положим

$$W'_{i,\gamma} = W'_{i-1,\gamma}\setminus \overline{S_{\gamma_i}},$$

где $\overline{S_{\gamma_i}}$ является замыканием в топологии Зарисского многообразия S_{γ_i}. Поскольку

$$W'_{i-1,\gamma}\cap\left(\bigcup_{\alpha\in A_{i-1}} W_\alpha \cup \bigcup_{2\le j\le b} V^{(j)}\right)=\emptyset,$$

мы имеем $W'_{i,\gamma} = W'_{i-1,\gamma}\setminus S_{\gamma_i}$ для всякого $\gamma\in\Gamma_{i-1}\setminus\{\gamma_i\}$.

Положим $V'_{\gamma_i} = W'_{i-1,\gamma_i}\setminus \mathcal{Z}(\Delta_{\gamma_i}) = W'_{i-1,\gamma_i}\setminus S_{\gamma_i}$ и $V_{\gamma_i} = W_{\gamma_i}\setminus\mathcal{Z}(\Delta_{\gamma_i})$. Напомним, что уже построены однородные многочлены $h_{\gamma_i,1},\ldots,h_{\gamma_i,s(\gamma_i)}$.

По определению положим

$$\Gamma_i = \{\gamma\in\Gamma_{i-1} \,:\, W'_{i,\gamma}\ne\emptyset \;\&\; \gamma\ne\gamma_i\},$$
$$A_i = A_{i-1}\cup A_{\gamma_i}\cup\{\gamma_i\}.$$

Докажем свойства (42)–(46) с $i-1$, заменённым на i. Действительно, эти новые свойства следуют немедленно из свойств (42)–(46) (для $i-1$) и определений.

Докажем неравенство (41) для всех $\alpha\in A_i$. Достаточно рассмотреть случай, когда $\alpha\in A_{\gamma_i}\cup\{\gamma_i\}$. Если $\alpha=\gamma_i$, то (41) следует из Теоремы 1 (ii), применённой к алгебраическому многообразию W_{γ_i}, которое является неприводимой компонентой V. Пусть $\alpha\in A_\gamma$. Тогда W_α является неприводимой компонентой алгебраического многообразия (47). Оценки для $\deg h_{\gamma_i,j}$, $\deg\Delta_{\gamma_i}$ следуют аналогичным образом из Теоремы 1 (ii), применённой к алгебраическому многообразию W_{γ_i}. Пусть C – константа из формулировки Теоремы 1 (ii). Пусть $C_2>C$. Тогда степени всех многочленов, которые определяют алгебраическое многообразие (47), ограничены сверху величиной

$$(s(\alpha)-1)n^{2^{(s(\alpha)-1)^{C_2}}}d. \tag{48}$$

Следовательно, для $\alpha\in A_{\gamma_i}$ неравенство (41) (с подходящим C_2, зависящим от C) следует из Теоремы 1 (ii).

Теперь, если $\Gamma_i\ne\emptyset$, мы переходим к следующему $(i+1)$-ому шагу. Если $\Gamma_i=\emptyset$ положим $A=A_i$. Тогда V'_α, $\alpha\in A$ является гладкой стратификацией V согласно (42), (44).

Остаётся доказать неравенство (39).

ЛЕММА 6 *Справедливо неравенство*

$$\sum_{\gamma\in\Gamma_0} d^{n-s(\gamma)}\deg W_\gamma \le d^n.$$

ДОКАЗАТЕЛЬСТВО В доказательстве этой леммы мы будем предполагать, что $\deg f_i = d$ для всякого $1 \le i \le m$, заменяя семейство f_i, $1 \le i \le m$ на

$$f_i X_j^{d-\deg f_i}, \quad 1 \le i \le m,\ 0 \le j \le n.$$

Далее, существуют линейные комбинации $h_j = c_{j,1}f_1 + \ldots + c_{j,m}f_m$, $1 \le j \le n$, со всеми коэффициентами $c_{j,i} \in k$, такими что для всякого $1 \le s \le n$, для всякого $\gamma \in \Gamma_0$, если $s(\gamma) \le s$, то W_γ является неприводимой компонентой алгебраического многообразия

$$\mathcal{Z}(h_1, \ldots, h_s). \tag{49}$$

Обозначим через W_γ, $\gamma \in H_s$, семейство всех определённых над k и неприводимых над k компонент алгебраического многообразия (49). Используя индукцию по s и теорему Безу, мы получим неравенство

$$\sum_{\gamma \in H_s} d^{s-s(\gamma)} \deg W_\gamma \le d^s.$$

Теперь утверждение леммы следует из последного неравенства для $s = n$. Лемма доказана.

Пусть N – число шагов описанной конструкции. Так что $N \le \#\Gamma_0$. Заметим, что для всякого $\alpha \in A$ мы имеем $W_\alpha = W_{\gamma_i}$, или $\alpha \in A_{\gamma_i}$ для некоторого $\gamma_i \in \Gamma_0$.

Обозначим для краткости $s(\gamma_i) = s_i$. По индукционному предположению, применённому к S_{γ_i}, и, поскольку степени всех многочленов, которые задают алгебраическое многообразие (47), ограничены сверху величиной (48), справедливо неравенство

$$\sum_{\alpha \in A_{\gamma_i}} (s_i n^{2^{s_i^{C_2}}} d)^{n-s(\alpha)} \deg W_\alpha \le n^{2^{(n(n-s_i))^{C_1}}} (s_i n^{2^{s_i^{C_2}}} d)^{(n+s_i+1)(n-s_i)/2}$$

для всякого $1 \le i \le N$. Следовательно, по Лемме 6 (и её доказательству)

$$\begin{aligned}
&\sum_{\alpha \in A} d^{n-s(\alpha)} \deg W_\alpha \le \\
&\sum_{1 \le i \le N} \left(d^{n-s_i} \deg W_{\gamma_i} + \sum_{\alpha \in A_{\gamma_i}} (s_i n^{2^{s_i^{C_2}}} d)^{n-s(\alpha)} \deg W_\alpha \right) \le \\
&\sum_{1 \le i \le N} \left(d^{n-s_i} \deg W_{\gamma_i} + n^{2^{(n(n-s_i))^{C_1}}} (s_i n^{2^{s_i^{C_2}}} d)^{(n+s_i+1)(n-s_i)/2} \right) \le \\
&d^n + \sum_{1 \le i \le N} n^{2^{(n(n-s_i))^{C_1}}} (s_i n^{2^{s_i^{C_2}}} d)^{(n+s_i+1)(n-s_i)/2} \le \\
&d^n + n^{2^{(n(n-s))^{C_1}}} \sum_{s \le j \le n} (n n^{2^{n^{C_2}}} d)^{(n+j+1)(n-j)/2} d^j \le \\
&n^{2^{(n(n-s+1))^{C_1}}} d^{(n+s)(n-s+1)/2}.
\end{aligned}$$

для абсолютной константы $C_1 > 0$. Таким образом, неравенство (39) доказано. Требуемые в Теореме 2 оценки для степеней и длин записи следуют немедленно из Теоремы 1, см. также замечания о представлении (6) во Введении. Теорема 2 для случая гладкой стратификации доказана.

6 Вычисление размерности вещественного алгебраического многообразия

Пусть k – вещественное упорядоченное поле с вещественным замыканием R, и V – алгебраическое многообразие из Введения. Следовательно, $V(R)$ является множеством точек вещественного алгебраического многообразия. Наша цель – вычислить размерность $V(R)$ и доказать Теорему 3. Достаточно найти размерность $(n+1)$-ого аффинного алгебраического многообразия $V(R) \setminus \mathcal{Z}(X_i)$, $0 \le i \le n$. Мы покажем, как вычислить $\dim V(R) \setminus \mathcal{Z}(X_0)$. Размерности других рассматриваемых аффинных многообразий вычисляются аналогичным образом. Для произвольного подмножества $S \subset \mathbb{P}^n(\overline{R})$ обозначим через $\overline{S}$ замыкание S в топологии Зарисского в $\mathbb{P}^n(\overline{R})$. Обозначим $V_0 = \overline{V(R) \setminus \mathcal{Z}(X_0)}$. Мы имеем $\dim V_0 = \dim V(R) \setminus \mathcal{Z}(X_0)$, и V_0 является проективным алгебраическим многообразием. Так что достаточно вычислить $\dim V_0$.

Пусть $\dim V_0(R) = n-r$, где $1 \le r \le n$. Тогда существует гладкая точка $\xi = (1 : \xi_1 : \ldots : \xi_n)$ вещественного многообразия $V_0(R)$ размерности $n-r$, см. [8].

Теперь рассмотрим гладкое покрытие V_α, $\alpha \in A$ многообразия V из Теоремы 2. Обозначим через A' подмножество всех $\alpha \in A$, таких что $V_\alpha(R) \setminus \mathcal{Z}(X_0) \ne \emptyset$. Мы имеем $\overline{V_\alpha} = \overline{V_\alpha(R)}$, так как V_α является гладким для всякого $\alpha \in A'$. Следовательно,

$$\bigcup_{\alpha \in A'} \overline{V_\alpha} = \bigcup_{\alpha \in A'} \overline{V_\alpha(R)} = \overline{(V \setminus \mathcal{Z}(X_0))(R)} = V_0.$$

Следовательно, V_0 определено над k, и существует единственная определённая над k и неприводимая над k компонента W' многообразия V_0, такая что ξ является гладкой точкой W'. Кроме того, $\dim W' = n - r$. Далее, существует $\alpha \in A'$, такое что $\overline{V_\alpha} = W'$. Следовательно, по Теореме 2 существуют однородные многочлены $h_1, \ldots, h_r \in k[X_0, \ldots, X_n]$ и индексы $1 \le i_1 < \ldots < i_r \le n$ (можно взять $i_1 \ge 1$, поскольку существуют гладкие точки в $W' \setminus \mathcal{Z}(X_0)$), удовлетворяющие следующему условию. Обозначим

$$\Delta = \det(\partial h_v / \partial X_{i_w})_{1 \le v, w \le r}. \tag{50}$$

Тогда $W' \setminus \mathcal{Z}(\Delta)$ является непустым и совпадает с неприводимой компонентой квазипроективного алгебраического многообразия

$$\mathcal{Z}(h_1, \ldots, h_r) \setminus \mathcal{Z}(\Delta)$$

Степень $\deg h_i < n^{2^{r^C}} d$, $1 \le i \le r$, где $C > 0$ – абсолютная константа.

Существует перестановка τ множества $\{1, \ldots, n\}$, такая что ξ является изолированной точкой вещественного алгебраического многообразия

$$V_0(R) \cap \mathcal{Z}(X_{\tau(r+1)} - \xi_{\tau(r+1)} X_0, \ldots, X_{\tau(n)} - \xi_{\tau(n)} X_0), \tag{51}$$

и пересечение касательных пространств в точке ξ

$$T_{\xi, V_0(R)} \cap \mathcal{Z}(X_{\tau(r+1)} - \xi_{\tau(r+1)} X_0, \ldots, X_{\tau(n)} - \xi_{\tau(n)} X_0) = \{\xi\} \tag{52}$$

трансверсально. В дальнейшем мы будем считать, не умаляя общности, как в доказательстве Леммы 6, что $\deg f_j = d$ для всех j. Пусть X_{n+1} – новая переменная. Положим

$$h = X_0^3 \sum_{1\le j\le m} f_j^2 - X_{n+1} \sum_{0\le i\le n} X_i^{2d+2}.$$

Пусть $1 \le s \le n$ – целое число, и σ – перестановка $\{1,\dots,n\}$. Рассмотрим систему полиномиальных уравнений относительно $X_0,\dots,X_n, X_{n+1}$

$$\left\{ \begin{array}{l} h = 0, \\ \partial h/\partial X_{\sigma(j)} = 0, \quad 2 \le j \le s, \end{array} \right. \tag{53}$$

которая определяет алгебраическое многообразие $S_{\sigma,s} \subset \mathbb{P}^{n+1}(\overline{k})$, причём $\mathbb{P}^{n+1}$ имеет координаты $(X_0 : \ldots : X_n : X_{n+1})$. Мы будем отождествлять $\mathcal{Z}(X_{n+1})$ с $\mathbb{P}^n$. Обозначим через $V_{\sigma,s}$ объединение всех неприводимых компонент $S_{\sigma,s}$, которые не содержатся ни в каком конечном объединении гиперплоскостей $\mathcal{Z}(X_{n+1} - vX_0)$, где $v \in \overline{k}$, и не содержатся в $\mathcal{Z}(X_0)$. Тогда размерность каждой неприводимой компоненты алгебраического многообразия $V_{\sigma,s}$ равна $n-s+1$, ср. [3]. Положим $W_{\sigma,s} = V_{\sigma,s} \cap \mathcal{Z}(X_{n+1})$.

Пусть $\xi^*_{s+1},\dots,\xi^*_n \in \overline{k}$. Обозначим через $C_{\sigma,s}(\xi^*_{s+1},\dots,\xi^*_n)$ объединение всех неприводимых компонент многообразия

$$S_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)}X_0, \dots, X_{\sigma(n)} - \xi^*_{\sigma(n)}X_0),$$

которые не содержатся ни в каком конечном объединении гиперплоскостей $\mathcal{Z}(X_{n+1} - vX_0)$, где $v \in \overline{k}$ и не содержатся в $\mathcal{Z}(X_0)$. Тогда, ср. [3], по тем же соображениям, что и выше для $V_{\sigma,s}$, размерность всякой неприводимой компоненты многообразия $C_{\sigma,s}(\xi^*_{s+1},\dots,\xi^*_n)$ равна 1, т.е. $C_{\sigma,s}(\xi^*_{s+1},\dots,\xi^*_n)$ является кривой. Следовательно, эта кривая является объединением некоторых компонент пересечения

$$V_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)}X_0, \dots, X_{\sigma(n)} - \xi^*_{\sigma(n)}X_0). \tag{54}$$

Но $V_{\sigma,s} \cap \mathcal{Z}(X_0) = \mathcal{Z}(X_0, X_{\sigma(2)}, \dots, X_{\sigma(s)}, \sum_{0\le i\le n} X_i^{2d+2})$. Следовательно,

$$V_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)}X_0, \dots, X_{\sigma(n)} - \xi^*_{\sigma(n)}X_0) \cap \mathcal{Z}(X_0) = \{(0 : \ldots : 0 : 1)\}.$$

Следовательно, пересечение (54) является кривой, и всякая неприводимая компонента (54) не содержится ни в каком конечном объединении гиперплоскостей $\mathcal{Z}(X_{n+1} - vX_0)$, где $v \in \overline{k}$, и не содержится в $\mathcal{Z}(X_0)$. Таким образом,

$$C_{\sigma,s}(\xi^*_{s+1},\dots,\xi^*_n) = V_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)}X_0, \dots, X_{\sigma(n)} - \xi^*_{\sigma(n)}X_0)$$

для всяких $\xi^*_{s+1},\dots,\xi^*_n \in \overline{k}$.

Рассмотрим систему полиномиальных уравнений

$$\left\{ \begin{array}{l} h = 0, \\ \partial h/\partial X_{\tau(j)} = 0, \quad 2 \le j \le r, \\ X_{\tau(j)} - \xi_{\tau(j)}X_0 = 0, \quad r+1 \le j \le n, \\ X_0 - 1 = 0. \end{array} \right. \tag{55}$$

Напомним, что ξ является изолированной точкой пересечения (51). Следовательно, рассматривая систему (55), ср. [14], [10], мы получаем, что точка $\xi \in C_{\tau,r}(\xi_{r+1},\dots,\xi_n)$. Следовательно, $C_{\tau,r}(\xi_{r+1},\dots,\xi_n)\cap \mathcal{Z}(X_{n+1})$ совпадает с $\{\xi\}$ в некоторой окрестности ξ в топологии вещественного поля R. Согласно теореме о неявной функции и тем же самым соображениям $W_{\tau,r}$ совпадает с W' в некоторой окрестности точки ξ в топологии вещественного поля R. Следовательно, W' является неприводимой компонентой многообразия $W_{\tau,r}$, ср. [15].

Пусть $\varepsilon_i > 0$ – является бесконечно малой величиной относительно поля $k(\varepsilon_1,\dots,\varepsilon_{i-1})$ для всякого $1 \le i \le 3$. Обозначим через $\widetilde{W}_{\sigma,s}$ алгебраическое многообразие

$$V_{\sigma,s}\cap \mathcal{Z}(X_{n+1}-\varepsilon_3 X_0),$$

рассматриваемое как подмногообразие в $\mathbb{P}^{n+1}(\overline{k(\varepsilon_3)})$.

Покажем, как построить линейные формы $Y_{s+1},\dots,Y_n \in k[X_0,\dots,X_n]$ с целыми коэффициентами с длинами записи $O(n \log d)$, такие что

$$W_{\sigma,s}\cap \mathcal{Z}(Y_{s+1},\dots,Y_n)\setminus \mathcal{Z}(X_0) \tag{56}$$

состоит из $\deg W_{\sigma,s}$ точек. Следовательно, ср., например, [7], все точки пересечения (56) являются гладкими точками многообразия $W_{\sigma,s}$ и пересечение (56) трансверсально в этих точках.

Умножим все уравнения системы (53) на X_0X_{n+1} и, используя алгоритм из [11], построим для всех $s+1 \le i \le n+1$ линейные формы $L_i \in k[X_0,\dots,X_n]$ с целыми коэффициентами с длинами записи $O(n \log d)$ и целые числа λ_i с длинами записи $O(n \log d)$, такие что число элементов пересечения

$$V_{\sigma,s}\cap \mathcal{Z}(L_{s+1}-\lambda_{s+1}X_{n+1},\dots,L_{n+1}-\lambda_{n+1}X_{n+1})$$

конечно и

$$V_{\sigma,s}\cap \mathcal{Z}(L_{s+1}-\lambda_{s+1}X_{n+1},\dots,L_{n+1}-\lambda_{n+1}X_{n+1})\cap \mathcal{Z}(X_0X_{n+1})=\emptyset. \tag{57}$$

Если всякое $\lambda_i = 0$, $s+1 \le i \le n$, то положим $D_i = L_i$, $s+1 \le i \le n$. Предположим, что существует $s+1 \le i_0 \le n$, такое что $\lambda_{i_0} \ne 0$. Скажем, например, $\lambda_{n+1} \ne 0$. Тогда положим $D_i = \lambda_{n+1}L_i - \lambda_i L_{n+1}$ для всех $s+1 \le i \le n$.

Всякая неприводимая компонента пересечения

$$V_{\sigma,s}\cap \mathcal{Z}(D_{s+1},\dots,D_n)$$

является кривой, которая не содержится $\mathcal{Z}(X_0X_{n+1})$ по (57). Следовательно, пересечение

$$W_{\sigma,s}\cap \mathcal{Z}(D_{s+1},\dots,D_n) \tag{58}$$

состоит из конечного числа точек.

Используя алгоритм из [3], построим все точки

$$\xi^{(i)} = (\xi_0^{(i)} : \dots : \xi_n^{(i)} : \varepsilon_3), \quad 1 \le i \le N_1,$$

пересечения

$$\widetilde{W}_{\sigma,s}\cap \mathcal{Z}(D_{s+1},\dots,D_n).$$

Тогда, см. [11] Предложение 2, или [7] Предложение 1, всякая точка пересечения (58) имеет вид $\mathrm{st}_{\varepsilon_3}(\xi^{(i)})$ для некоторого $1 \le i \le N_1$, где стандартная часть $\mathrm{st}_{\varepsilon_3}$ имеет тот же самый смысл, что и в [11], [7] (стандартная часть элемента $z \in \mathbb{P}^{n+1}(\overline{k(\varepsilon_3)})$ есть элемент $z' \in \mathbb{P}^{n+1}(\overline{k})$, который бесконечно близок к z). Так что мы строим, используя разложения Ньютона-Пюизе, см. [10], [11], [12], все элементы $\eta^{(i)}$, $1 \le i \le N_2$, пересечения (58). Пусть $\eta^{(i)} = (\eta_0^{(i)} : \ldots : \eta_n^{(i)})$, где $\eta_j^{(i)} \in \overline{k}$ и, если $\eta_0^{(i)} \ne 0$, то $\eta_0^{(i)} = 1$ для всякого $1 \le i \le N_2$.

Покажем, что мы можем предполагать без ограничения общности, что

$$\eta^{(i)} \notin \mathcal{Z}(X_0) \quad \text{для всех} \quad 1 \le i \le N_2, \tag{59}$$

заменяя при необходимости линейные формы $D_{s+1}, \ldots, D_n$ на новые. В самом деле, обозначим через N_3 число точек пересечения (58), которые не лежат в $\mathcal{Z}(X_0)$. Предположим, что $N_3 < N_2$ и, например, $\eta^{(1)} = (0 : \eta_1^{(1)} : \ldots : \eta_n^{(1)}) \in \mathcal{Z}(X_0)$ и $\eta^{(1)} = \mathrm{st}_{\varepsilon_3}(\xi^{(1)})$, где $\xi^{(1)} = (\xi_0^{(1)} : \ldots : \xi_n^{(1)} : \varepsilon_3\xi_0^{(1)})$, всякое $\xi_j^{(1)}$, $1 \le j \le n$ не является бесконечно большим относительно поля k, и существует $1 \le j_0 \le n$, такое что $\xi_{j_0}^{(1)}$ не является бесконечно малой величиной относительно поля k. Решая систему полиномиальных уравнений и неравенств с квадратами абсолютных величин, построим точку $x^* \in \widetilde{W}_{\sigma,s}$, такую что $x^* = (x_0^* : \ldots : x_n^* : \varepsilon_3 x_0^*)$, все $x_j^* \in \overline{k(\varepsilon_1, \varepsilon_2, \varepsilon_3)}$, $0 \le j \le n$, и

$$\begin{aligned} &|x_0^*|^2 + \sum_{1 \le j \le n} |x_j^* - \xi_j^{(1)}|^2 < \varepsilon_1, \\ &|x_0^*|^2 > \varepsilon_2. \end{aligned}$$

Затем построим $x_i' = \mathrm{st}_{\varepsilon_3}(x_i^*)$ для всех $0 \le i \le n$. Положим

$$\begin{aligned} &x' = (x_0' : x_1' : \ldots : x_n') \in \mathbb{P}^n(\overline{k(\varepsilon_1, \varepsilon_2)}), \\ &\widetilde{D}_j = D_j - (D_j/X_0)(x')X_0, \quad s+1 \le j \le n. \end{aligned}$$

Тогда, ср. [10], [11], число элементов

$$\# W_{\sigma,s} \cap \mathcal{Z}(\widetilde{D}_{s+1}, \ldots, \widetilde{D}_n) \setminus \mathcal{Z}(X_0) > N_3,$$

причём все эти элементы принадлежат $\mathbb{P}^n(\overline{k(\varepsilon_1, \varepsilon_2)})$. Следовательно, ср. [10], [11], [7] и также Раздел 1, заменяя последовательно все коэффициенты линейных форм $\widetilde{D}_{s+1}, \ldots, \widetilde{D}_n$ на целые коэффициенты с длинами записи $O(n \log d)$, мы получаем новые линейные формы $D'_{s+1}, \ldots, D'_n$, аналогичные $D_{s+1}, \ldots, D_n$, такие что

$$\# W_{\sigma,s} \cap \mathcal{Z}(D'_{s+1}, \ldots, D'_n) \setminus \mathcal{Z}(X_0) > N_3.$$

Теперь заменим линейные формы $D_{s+1}, \ldots, D_n$ на $D'_{s+1}, \ldots, D'_n$ и проитерируем описанную конструкцию до тех пор, пока не выполняется (59). Число итераций ограничено сверху степенью $\deg W_{\sigma,s}$ по теореме Безу. Требуемое утверждение доказано.

Теперь для всякого $1 \le j \le N_2$ рассмотрим систему полиномиальных уравнений и неравенств относительно $X_0, \ldots, X_{n+1}$, $Z_0, \ldots, Z_{n+1}$ с квадратами абсолютных величин

$$\begin{cases} h=0, & \\ \partial h/\partial X_{\sigma(i)}=0, & 2\le i\le s,\\ h(Z_0,\ldots,Z_{n+1})=0, & \\ \partial h(Z_0,\ldots,Z_{n+1})/\partial Z_{\sigma(i)}=0, & 2\le i\le s,\\ X_{n+1}-\varepsilon_3=0, & \\ Z_{n+1}-\varepsilon_3=0, & \\ D_j(X_0-Z_0,\ldots,X_n-Z_n)=0, & j\in\{0,s+1,s+2,\ldots,n\},\\ \sum_{0\le i\le n}|X_i-\eta_i^{(j)}|^2\le\varepsilon_1, & \\ \sum_{0\le i\le n}|Z_i-\eta_i^{(j)}|^2\le\varepsilon_1, & \\ \sum_{0\le i\le n}|Z_i-X_i|^2\ge\varepsilon_2, & \\ X_0-1=0, & \\ Z_0-1=0. & \end{cases} \qquad (60)$$

Предположим, что для всякого $1\le j\le N_2$ система (60) не имеет решений. Тогда, ср. [7], пересечение (56) состоит из $\deg W_{\sigma,s}$ точек. В этом случае положим $Y_j=D_j$ для всякого $j\in\{0,s+1,s+2,\ldots,n\}$.

Предположим, что существует $1\le j\le N_2$, такое что система (60) имеет решение

$$(1,x_1^*,\ldots,x_n^*,\varepsilon_3,1,z_1^*,\ldots,z_n^*,\varepsilon_3)\in(\overline{k(\varepsilon_1,\varepsilon_2,\varepsilon_3)})^{2n+4}.$$

Тогда построим $x_i'=\mathrm{st}_{\varepsilon_3}(x_i^*)$ и $z_i'=\mathrm{st}_{\varepsilon_3}(z_i^*)$ для всех $1\le i\le n$. Положим

$$x'=(1:x_1':\ldots:x_n')\in\mathbb{P}^n(\overline{k(\varepsilon_1,\varepsilon_2)}),$$
$$\widetilde{D}_j=D_j-(D_j/X_0)(x')X_0,\quad s+1\le j\le n.$$

Тогда, ср. [7], число элементов множества

$$\#W_{\sigma,s}\cap\mathcal{Z}(\widetilde{D}_{s+1},\ldots,\widetilde{D}_n)\setminus\mathcal{Z}(X_0)>N_2,$$

причём последнее множество является подмножеством $\mathbb{P}^n(\overline{k(\varepsilon_1,\varepsilon_2)})$. Следовательно, ср. [10], [11], [7] и также Раздел 1, заменяя последовательно все коэффициенты линейных форм $\widetilde{D}_{s+1},\ldots,\widetilde{D}_n$ на целые коэффициенты с длинами записи $O(n\log d)$, мы получаем новые линейные формы $D'_{s+1},\ldots,D'_n$, аналогичные $D_{s+1},\ldots,D_n$, такие что

$$\#W_{\sigma,s}\cap\mathcal{Z}(D'_{s+1},\ldots,D'_n)\setminus\mathcal{Z}(X_0)>N_2.$$

Затем мы заменяем линейные формы $D_{s+1},\ldots,D_n$ на $D'_{s+1},\ldots,D'_n$ и итерируем описанную конструкцию до тех пор, пока существует $1\le j\le N_2$, такое что система (60) имеет решение. Число итераций ограничено сверху $\deg W_{\sigma,s}$ по теореме Безу. Таким образом, мы построим в конечном счёте требуемые линейные формы $Y_{s+1},\ldots,Y_n$.

Вернёмся к описанию алгоритма для вычисления $\dim V_0$. Будем перебирать $s=1,\ldots,n$ (здесь n является максимально возможным значением s, если только описываемый алгоритм не остановится для некоторого $s<n$). Мы будем предполагать (это индукционное предположение), что когда мы рассматриваем текущее значение s, то уже доказано, что

$$\dim V_0<n-s+1. \qquad (61)$$

Для рассматриваемого s мы будем перебирать σ, определённые выше. Для рассматриваемых s и σ построим линейные формы $Y_{s+1}, \dots, Y_n$ и все точки из (56) (аналогичным образом тому, как были построены точки из (58)). Мы будем перебирать точки пересечения (56). Обозначим через x_0, рассматриваемую точку пересечения (56). Обозначим через W однозначно определённую неприводимую над k компоненту многообразия $W_{\sigma,s}$, такую что $x_0 \in W$. Обозначим через $\mathfrak{P} \subset k[X_0, \dots, X_n]$ однородный простой идеал многообразия W. Мы увидим, что при рассмотрении s, σ и x_0 алгоритм приходит к одному из двух случаев. В первом случае $W' \neq W$, а во втором $\dim V_0 = n - s$.

Теперь мы хотим модифицировать алгоритм для построения регулярных последовательностей из Раздела 1. Именно, мы заменим там алгебраическое многообразие V на $W_{\sigma,s}$. Наша цель – выяснить, существует ли $\mathfrak{P}$-последовательность $g_1, \dots, g_s$ со степенями $\deg g_j \le n^{2^{s^C}} d$, $1 \le j \le s$, где $C > 0$ – константа из формулировки Теоремы 2. Далее, если такая $\mathfrak{P}$-последовательность существует, то мы построим её, а также другие соответствующие ей объекты, в частности, гладкую точку $x_a \in W$ и линейные формы $L_{a,s+1}, \dots, L_{a,n}$, где шаг a является последним, см. Раздел 1. Дополнительно мы увидим, что $x_a \notin \mathcal{Z}(X_0)$ (это будет следовать из модификации Леммы 1). Разница с Разделом 1 здесь состоит в том, что алгебраическое многообразие $W_{\sigma,s}$ не задано явно системой полиномиальных уравнений.

Эта модификация алгоритма из Раздела 1 будет описана позже. Сейчас предположим, что мы уже применили её и выяснили, что не существует требуемых $\mathfrak{P}$-последовательностей. Тогда, если не все точки пересечения (56) перебраны, мы переходим к следующей точке из (56). Если все точки из (56) перебраны, но не все σ перебраны, то мы переходим к следующему σ. Если все точки из (56) перебраны и все σ перебраны, и $s < n$, то мы переходим к следующему значению s, т.е. к $s + 1$. В этом случае $W' \neq W$ для всех σ и всех точек из (56) (мы увидим это в дальнейшем из описания алгоритма), и, следовательно, $\dim V_0 < n - s$. Следовательно, (61) доказано с s, заменённым на $s + 1$. Если все точки из (56), все σ перебраны, и $s = n$, то W' не является неприводимой компонентой многообразия $W_{\sigma,s}$ для всех σ и $1 \le s \le n$. Следовательно, как это вытекает из доказанного выше, $V_0 = \emptyset$, и $\dim V_0 = -1$ в этом случае.

Предположим, что мы уже применили модификацию алгоритма из Раздела 1 и построили $\mathfrak{P}$-последовательность $g_1, \dots, g_s$. Тогда W является неприводимой компонентой алгебраического многообразия $\mathcal{Z}(g_1, \dots, g_s)$. Положим $x = x_a$, где шаг a – последний в модификации алгоритма из Раздела 1. Тогда мы применим алгоритм из второй части Раздела 1 (на входе этого алгоритма требуются только многочлены $g_1, \dots, g_s$, точка x, и соответствующие линейные формы) и построим однородные многочлены $h_1, \dots, h_s \in k[X_0, \dots, X_n]$, индексы $1 \le i_1 < \dots < i_s \le n$, многочлен Δ определённый (50) с r, заменённым на s, и точку $z \in W \setminus \mathcal{Z}(X_0)$, такие что

- $z \in \mathcal{Z}(h_1, \dots, h_s) \setminus \mathcal{Z}(\Delta)$ и, следовательно, по теореме о неявной функции z является гладкой точкой этого квазипроективного алгебраического многообразия,
- $W \setminus \mathcal{Z}(\Delta)$ является неприводимой компонентой многообразия $\mathcal{Z}(h_1, \dots, h_s) \setminus \mathcal{Z}(\Delta)$.

Обозначим через V_1 алгебраическое многообразие $\mathcal{Z}(h_1,\dots,h_s)\setminus\mathcal{Z}(X_0\Delta)$. Все точки алгебраического многообразия V_1 являются гладкими. Следовательно, $W(R)\setminus\mathcal{Z}(X_0\Delta)$ является объединением (может быть пустым) некоторых связных компонент многообразия $V_1(R)$ (связные компоненты могут быть определены, используя, например, принцип переноса, подробности см. в [8]). Применим алгоритм из [14] и построим конечное подмножество S в $V_1(R)$, которое имеет непустое пересечение с каждой связной компонентой многообразия $V_1(R)$ с числом элементов $\#S$, ограниченным сверху полиномом от d^n. Построим подмножество S_1 множества S, состоящее из всех элементов S, которые принадлежат $W_{\sigma,s}$ (точка принадлежит $W_{\sigma,s}$ тогда и только тогда, когда существует бесконечно близкая к ней точка из $\widetilde{W}_{\sigma,s}$).

Далее, для всякой точки $z\in S_1$ мы выясним, существует ли бесконечно близкая к z точка

$$z'\in\mathcal{Z}(h_1,\dots,h_s)\setminus\mathcal{Z}(f_1,\dots,f_m).$$

В случае, когда для всякой точки $z\in S_1$ такая точка z' существует, $W\neq W'$ согласно предыдущим рассмотрениям, и мы переходим к следующей точке из (56), или следующему σ, или следующему s, или выясняем, что $\dim V_0=-1$, как это описано выше. В случае, когда не существует z' для некоторого z, существует бесконечно малая окрестность U точки z в алгебраическом многообразии V_1, такая что $U\subset V$, ср. [10], [11]. Следовательно, $\dim V_0\geq n-s$. С другой стороны, согласно (61) $\dim V_0<n-s+1$. Таким образом, $\dim V_0=n-s$.

Остаётся описать модификацию алгоритма из Раздела 1. Построим линейную форму $Y_0\in k[X_0,\dots,X_n]$ с целыми коэффициентами с длинами записи $O(n\log d)$, такую что

$$W_{\sigma,s}\cap\mathcal{Z}(Y_0,Y_{s+1},Y_{s+2},\dots,Y_n)=\emptyset$$

в $\mathbb{P}^n(\overline{k})$. Напомним, что мы заменили V на $W_{\sigma,s}$. Мы имеем также текущую точку $x_0\in W_{\sigma,s}\cap\mathcal{Z}(Y_{s+1},\dots,Y_n)$ и определённую над k и неприводимую над k компоненту W многообразия $W_{\sigma,s}$, такую что $x\in W$.

Прежде всего, напомним, что мы строим $\mathfrak{P}$-последовательность с $\deg g_i\leq n^{2^{s^C}}d$, $1\leq i\leq s$, если она существует, где C – константа из Теоремы 2. Так что, перебирая δ, см. Раздел 1, мы останавливаемся на значении $n^{2^{s^C}}d$.

В Лемме 1 свойство (v) заменяется на следующее.

(v) Множество $W_{\sigma,s}\cap\mathcal{Z}(L'_{s+1},\dots,L'_n)$ состоит из $\deg W_{\sigma,s}$ точек (следовательно, все эти точки являются гладкими точками $W_{\sigma,s}$). Далее, для всякой точки z из этого множество $X_0(z)\neq 0$, и пересечение касательных пространств $W_{\sigma,s}$ и $\mathcal{Z}(L'_{s+1},\dots,L'_n)$ в точке z трансверсально, т.е.

$$T_{z,W_{\sigma,s}}\cap\mathcal{Z}(L'_{s+1},\dots,L'_n)=\{z\}.$$

Система (11) заменяется на следующую.

$$\left\{\begin{array}{ll}\sum_{0\le i\le n}|X_i-x_{r,i}|^2<\varepsilon_1, & \\ h=0, & \\ \partial h/\partial X_{\sigma(j)}=0, & 2\le j\le s,\\ X_{n+1}-\varepsilon_3=0, & \\ X_0-1=0, & \\ |\psi|^2>\varepsilon_2. & \end{array}\right. \tag{62}$$

Тогда, ср. [11], [7], система (62) не имеет решений в $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1,\varepsilon_2,\varepsilon_3)})$ тогда и только тогда, когда многочлен ψ не обращается в нуль тождественно на W.

Система (13) заменяется на следующую.

$$\left\{\begin{array}{ll}\sum_{0\le i\le n}|X_i-x''_i|^2\le\varepsilon_1, & \\ \sum_{0\le i\le n}|Z_i-x''_i|^2\le\varepsilon_1, & \\ \sum_{0\le i\le n}|X_i-Z_i|^2\ge\varepsilon_2, & \\ M_i(X_0-Z_0,\ldots,X_n-Z_n)=0, & i=0,r+1,r+2,\ldots,n,\\ h=0, & 1\le i\le m,\\ \partial h/\partial X_{\sigma(j)}=0, & 2\le j\le s,\\ X_{n+1}-\varepsilon_3=0, & \\ X_0-1=0, & \\ \psi_i(Z_0,\ldots,Z_n)=0, & 1\le i\le j,\\ |\psi|^2>\varepsilon_2. & \end{array}\right. \tag{63}$$

Тогда, ср. [11], [7], система (63) не имеет решений в $\mathbb{A}^{2n+3}(\overline{k(\varepsilon_1,\varepsilon_2,\varepsilon_3)})$ тогда и только тогда, когда (12) является равенством.

Предположим, что система (63) имеет решение. Тогда построим решение $\xi^*_0,\ldots,\ \xi^*_n,\ z^*_0,\ldots,z^*_n,\ z^*$ системы (63). Предположим, что система (63) не имеет решений. Тогда построим решение $\xi^*_0,\ldots,\xi^*_n,\ z^*$ системы (62) (напомним, что мы предполагаем, что эта система имеет решение, см. Раздел 1).

Для всякого $0\le i\le n$ вычислим $\mathrm{st}_{\varepsilon_3}\,\xi^*_i=x^*_i$. Положим

$$x^*=(x^*_0:\ldots:x^*_n).$$

Тогда мы определим линейные формы L^*_j, $s+1\le j\le n$, теми же самыми формулами, что и в Разделе 1.

Последняя модификация относится к конструкции кривой Q. В нашем случае Q является неприводимой над $\overline{K}$ компонентой пересечения

$$W_{\sigma,s}\cap\mathcal{Z}(L^*_{s+2},\ldots,L^*_n),$$

такой что $x^*\in Q$. Следовательно, Q однозначно определена. Пусть $\varepsilon_4>0$ – бесконечно малая величина относительно поля $K=k(\varepsilon_1,\varepsilon_2)$, и ε_3 – бесконечно малая величина относительно поля $K(\varepsilon_4)$. Построим, решая систему полиномиальных уравнений и неравенств, точку

$$z'\in\widetilde{W}_{\sigma,s}\cap\mathcal{Z}(L^*_{s+2},\ldots,L^*_n),$$

такую что $|z'-x^*|^2=\varepsilon_4$. Вычислим

$$\mathrm{st}_{\varepsilon_3}(z')=z\in\mathbb{P}^n(\overline{K(\varepsilon_4)}).$$

Тогда z является общей точкой алгебраического многообразия Q. Так как Q определено над $\overline{K}$, мы можем построить, см. [3], систему полиномиальных уравнений с коэффициентами из $\overline{K}$, которая задаёт Q. Этим завершается описание всех модификаций алгоритма из Раздела 1 для построения регулярных последовательностей. Теорема 3 доказана.

Список литературы

[1] Нестеренко Ю. В., Оценки характеристической функции простого идеала. – Математический сборник, 1984, т. 123, с. 11–34.

[2] Хартсхорн Р., Алгебраическая геометрия. – М., Мир, 1981.

[3] Чистов А. Л., Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время. – Зап. научн. семинаров ЛОМИ АН, 1984, т. 137, с. 124–188.

[4] Чистов А. Л., Вычисление группы Галуа над функциональным полем характеристики нуль с алгебраически замкнутым полем констант за полиномиальное время. – в сборнике: Математические методы построения и анализа алгоритмов, Л., Наука, 1990, с 200–232.

[5] Чистов А. Л., Эффективная конструкция локальных параметров неприводимых компонент алгебраического многообразия. – Труды Санкт–Петербургского математического общества, 1999, т. 7 (принято к пуликации), см. также: St.Petersburg Mathematical Society Preprint # 1999-08,
http://www.pdmi.ras.ru/spbmo/preprint/1999/index.html#08

[6] Чистов А. Л., Сильная версия основного разрешающего алгоритма для экзистенциональной теории первого порядка вещественно замкнутых полей. – Зап. научн. семинаров ПОМИ, 1999, т. 256, с. 168–211. см. также: St.Petersburg Mathematical Society Preprint # 1999-10,
http://www.pdmi.ras.ru/spbmo/preprint/1999/index.html#10

[7] Чистов А. Л., Вычисление степеней алгебраических многообразий над полем нулевой характеристики за полиномиальное время и его приложения. – Зап. научн. семинаров ПОМИ, т. 258 (принято к пуликации), see also in English: St.Petersburg Mathematical Society Preprint # 1999-03,
http://www.pdmi.ras.ru/spbmo/preprint/1999/index.html#03

[8] Bochnak J., Coste M., Roy M.–F., Géométrie algébrique réelle. – Springer–Verlag, Berlin, Heidelberg, New York, 1987.

[9] Chardin M., Une majoration de la function de Hilbert et ses conséquences pour l'interpolation algébrique. – Bull. Soc. Math. France, 1989, vol. 117, p. 305–318.

[10] Chistov A. L., Polynomial–Time Computation of the Dimension of Algebraic Varieties in Zero–Characteristic. – Journal of Symbolic Computation, 1996, vol. 22, N 1, p. 1–25.

[11] Chistov A. L., Polynomial–time computation of the dimensions of components of algebraic varieties in zero–characteristic. – Journal of Pure and Applied Algebra, 1997, vol. 117 & 118, p. 145–175.

[12] Chistov A. L., Polynomial complexity of the Newton–Puiseux algorithm. – in: Lecture Notes in Computer Science, vol. 233, Springer, New York, Berlin, Heidelberg, 1986 p. 247–255.

[13] Lazard D., Résolution des systèmes d'équations algébrique. – Theoretical Computer Science, 1981, vol. 15, p. 77–110.

[14] Renegar J., A faster PSPACE algorithm for deciding the existential theory of reals. – in: Proc. 29th Annual Symp. on Foundations of Computer Sci., 1988, p. 291–295.

[15] Roy M.–F., Vorobjov N., Computing the Complexification of a Semi-algebraic Set. – in: Proc. of ISSAC'96 conference, 1996, p. 26–34.