Записки научных
семинаров ПОМИ
Том 258, 1999 г.

А. Л. Чистов

ВЫЧИСЛЕНИЕ СТЕПЕНЕЙ АЛГЕБРАИЧЕСКИХ МНОГООБРАЗИЙ НАД ПОЛЕМ НУЛЕВОЙ ХАРАКТЕРИСТИКИ ЗА ПОЛИНОМИАЛЬНОЕ ВРЕМЯ И ЕГО ПРИЛОЖЕНИЯ

Введение

В статье предлагаются полиномиальные алгоритмы для вычисления таких базисных численных характеристик алгебраических многообразий как степени, размерности компонент, содержащих заданную точку, кратностей точек. Кроме того, для заданного алгебраического многообразия V строится система представителей гладких точек с их касательными пространствами, такая что всякая неприводимая компонента V содержит по крайней мере одну точку из этого множества. Для заданной точки x алгебраического многообразия и семейства $\mathcal{Q}$ рациональных функций предлагается алгоритм для выяснения того, существует ли неприводимая компонента W этого алгебраического многообразия, содержащая точку x, и, такая что семейство $\mathcal{Q}$ является базисом трансцендентности поля рациональных функций W. Это дает алгоритм для того, чтобы выяснить, является ли заданный морфизм алгебраических многообразий доминантным. Рассматривается случай основного поля нулевой характеристики.

Настоящая статья продолжает [6] и [7]. Методы вещественной алгебраической геометрии [5] используются существенным образом как в данной статье, так и [6, 7]. Здесь являются важными результаты из [16] и [15]. Следует подчеркнуть, что настоящая статья не могла появиться, пока не были сделаны два принципиальных шага в [6] и [7]. В [6] решена проблема вычисления размерности в случае проективных алгебраических многообразий над полем нулевой характеристики. Алгоритм из [7] для вычисления размерности всех неприводимых компонент алгебраиче-

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

ского многообразия потребовал дополнительно четырех вложенных рекурсий. Отметим также, что в других терминах конструкция из [6, 7] является полиномиальным алгоритмом для выбора проекции в теореме Нетер о нормализации.

Вероятностные алгоритмы для проблем, рассмотренных в настоящей статье (и многих других, где требуется найти элемент в "общем положении") могут быть легко получены для любой характеристики поля коэффициентов.

Проблема вычисления размерности алгебраических многообразий является классической, и она рассматривалась, начиная с прошлого века [12]. В [13] сформулирована проблема вычисления размерности алгебраического многообразия с точки зрения близкой к теории сложности вычислений. В [10] построена вполне параллелизуемая арифметическая схема для вычисления размерности алгебраического многообразия за неравномерное последовательное полиномиальное время от длины записи входных данных и d^n. В общем случае из [10] можно получить только вероятностный алгоритм для этой задачи со сложностью полиномиальной от d^n. В [10] также поставлена проблема найти детерминированный алгоритм с битовой сложностью $d^{O(n)}$. Эта проблема решена в [6, 7] для случая нулевой характеристики. Здесь отражается ситуация в теории сложности, когда для многих проблем случайные объекты (или объекты в "общем положении") трудно построить детерминированно.

В этой статье мы строим детерминированные алгоритмы с битовой сложностью полиномиальной от d^n и длины записи входных данных, включая характеристику поля. Вопрос о том, существует ли такой алгоритм в случае ненулевой характеристики для какой–либо из проблем, рассматриваемых в этой статье и [6, 7] (т.е. для вычисления размерностей, степеней, кратностей и т. д.), является открытым. В [3] предлагается алгоритм для разложения алгебраического многообразия на неприводимые компоненты со сложностью полиномиальной от d^{n^2} и длины записи входных данных, включая характеристику поля. В случае произвольной характеристики, используя [3], можно получить для всех проблем, рассматриваемых в этой статье и [6, 7], алгоритмы с аналогичной оценкой сложности (т.е. полиномиальной от d^{n^2} и длины записи входных данных). Эта оценка сложности является наилучшей известной в случае произвольной характеристики.

Подчеркнем еще раз, что мы рассматриваем здесь детерминированные вычисления с битовой сложностью. Эта модель вычислений является наиболее важной с теоретической точки зрения.

Перейдем к точным формулировкам. Пусть поле $k = \mathbb{Q}(t_1, \dots, t_l, \theta)$, где $t_1, \dots, t_l$ алгебраически независимы над $\mathbb{Q}$, и θ – алгебраический над $\mathbb{Q}$ элемент с минимальным многочленом $F \in \mathbb{Q}[t_1, \dots, t_l, Z]$. Старший коэффициент $\mathrm{lc}_Z F$ многочлена F равен 1. Пусть даны однородные многочлены $g_0, \dots, g_m \in k[X_0, \dots, X_n]$. Рассмотрим замкнутое алгебраическое множество или алгебраическое многообразие (в этой статье мы не различаем эти понятия)

$$V = \{(x_0 : \ldots : x_n) \, : \, g_i(x_0, \dots, x_n) = 0 \; \forall 0 \le i \le m\} \subset \mathbb{P}^n(\overline{k}).$$

Это множество всех общих нулей многочленов $g_0, \dots, g_m$ в $\mathbb{P}^n(\overline{k})$. В дальнейшем мы будем обозначать для краткости это множество через $\mathcal{Z}(g_0, \dots, g_m)$. Аналогичные обозначения будут также использоваться для множеств всех общих нулей (в аффинных или проективных пространствах, как это будет видно из контекста) других многочленов. Следовательно, $V = \mathcal{Z}(g_0, \dots, g_m)$.

Каждый многочлен $f = g_i$ будем представлять в форме

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

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

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

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

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

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. Мы можем рассматривать различные плотные представления многочленов. Например, можно рассматривать класс многочленов f от $X_0, \dots, X_n$ с $\deg_{X_i} f < d$ для всех $0 \leqslant i \leqslant n$ как базисный в плотном представлении, параметризующемся при помощи d. Тогда длины записи этих многочленов оцениваться сверху $(d^{n+1} d_1 + 1) d_2^l M$. В таком представлении $L(f_i) < (d^{n+1} d_1 + 1) d_2^l M$, и, следовательно, алгоритмы из настоящей статьи являются алгоритмами полиномиальной сложности, ср. [3].

Пусть V_s является объединением всех неприводимых компонент размерности $n - s$ многообразия V, где $0 \leqslant s \leqslant n$. Степень $\deg V_s$ многообразия V_s равна, см. Лемму 1 ниже, $\max_H \# V_s \cap H$, где максимум берется по всем линейным пространствам H в $\mathbb{P}^n(\overline{k})$ размерности s, таким что $\# V_s \cap H < +\infty$.

Теорема 1. *Пусть проективное алгебраическое многообразие V, определенное над полем k, задано как множество всех общих нулей в $\mathbb{P}^n(\overline{k})$ семейства однородных многочленов $g_0, \dots, g_m \in k[X_0, \dots, X_n]$ степеней меньше, чем d. Тогда степени $\deg V_s$ для всех $0 \leqslant s \leqslant n$ могут быть вычислены за полиномиальное время от d^n, d_1, d_2, M, M_1, m.*

Пусть $x \in \mathbb{P}^n(\overline{k})$. Размерность $\dim_x V$ алгебраического многообразия V в точке x (или в окрестности точки x) по определению есть $\max_W \dim W$, где максимум берется по всем неприводимым компонентам W многообразия V, таким что $x \in W$. Обозначим через $\mathcal{W}$ множество всех таких компонент W.

Теорема 2. *Пусть $x \in \mathbb{P}^n(\overline{k})$. Размерности всех неприводимых компонент, содержащих точку x, т.е. множество $\{\dim W : W \in \mathcal{W}\}$, могут быть вычислены за полиномиальное время от d^n, d_1, d_2, M, M_1, m и длины записи точки x. Следовательно, размерность $\dim_x V$ многообразия V в точке x может быть вычислена за то же самое время.*

Пусть теперь точка $x \in V_s$ и $0 \leqslant s \leqslant n$. Обозначим через $\mathcal{L}$ множество всех линейных подпространств L в $\mathbb{P}^n(\overline{k})$, таких что

$\dim L = s$, $x \in L$, и $\#V_s \cap L < +\infty$. Кратность $\mu(x, V_s)$ точки x алгебраического многообразия V_s может быть определена формулой

$$\mu(x, V_s) = \min_{L \in \mathcal{L}} \{1 + \deg V_s - \#V_s \cap L\}, \qquad (1)$$

см. также Следствие 3 и Замечание 5 в Разделе 5. Эта формула может быть объяснена следующим образом, ср. [1]. По своему изначальному смыслу кратность $\mu(x, V_s)$ равна числу точек бесконечно близких к x пересечения многообразия V_s с общим линейным подпространством $\tilde{L}$, $\dim \tilde{L} = s$, которое является бесконечно близким к точке x. Следовательно, $\#V_s \cap \tilde{L} = \deg V_s$. Если сдвинуть это общее линейное подпространство на линейное подпространство $\overline{L}$, содержащее точку x (посредством бесконечно малого сдвига), то все точки пересечения, которые были в инфинитизимальной окрестности точки x, перейдут в x, другие точки пересечения перейдут биективно в $-1 + \#V_s \cap \overline{L} = \max_{L \in \mathcal{L}} \{-1 + \#V_s \cap L\}$ точек. Таким образом, мы получаем формулу для $\mu(x, V_s)$.

Теорема 3. *Кратности $\mu(x, V_s)$ для всех $0 \leqslant s \leqslant n$ могут быть вычислены за полиномиальное время от d^n, d_1, d_2, M, M_1, m и длины записи точки x.*

Теорема 4. *Пусть проективное алгебраическое многообразие V, определенное над полем k, задано как множество общих нулей в $\mathbb{P}^n(\overline{k})$ семейства однородных многочленов $g_0, \ldots, g_m \in k[X_0, \ldots, X_n]$ степеней меньше, чем d. Пусть V_s, как и выше, является объединением всех неприводимых компонент V размерности $n - s$, где $0 \leqslant s \leqslant n$. Тогда можно построить для всякого $0 \leqslant s \leqslant n$ конечное множество A_s гладких точек многообразия V_s и для всякой точки $x \in A_s$ касательное пространство T_x многообразия V_s в точке x. Касательные пространства рассматриваются здесь как линейные подпространства в $\mathbb{P}^n(\overline{k})$. Кроме того, A_s удовлетворяет тому свойству, что для всякой неприводимой компоненты W многообразия V_s существует точка $x \in A_s \cap W$. Точки из A_s являются также гладкими точками многообразия V (т.е. они не принадлежат никакому V_r с $r \neq s$). Число элементов $\#A_s \leqslant d^s$. Время работы алгоритма для построения всех A_s, $0 \leqslant s \leqslant n$ полиномиально от d^n, d_1, d_2, M, M_1, m.*

Теорема 5. *Пусть проективное алгебраическое многообразие V, определенное над полем k, задано как множество общих нулей в*

$\mathbb{P}^n(\overline{k})$ семейства однородных многочленов $g_0, \ldots, g_m \in k[X_0, \ldots, X_n]$ степеней меньше, чем d. Пусть дано семейство $\mathcal{Q}$ рациональных функций $q_{s+1}, \ldots, q_n \in k(X_1/X_0, \ldots, X_n/X_0)$, $0 \leqslant s \leqslant n$. Пусть степени и длины записи целых коэффициентов числителей и знаменателей рациональных функций $q_{s+1}, \ldots, q_n$ ограничены теми же самыми значениями, что и для многочленов $g_0, \ldots, g_m$. Пусть $x \in \mathbb{P}^n(\overline{k})$. Предлагается алгоритм для того, чтобы выяснить, существует ли неприводимая компонента W алгебраического многообразия V, содержащая точку x, и, такая что семейство $\mathcal{Q}$ является базисом трансцендентности поля рациональных функций $\overline{k}(W)$ неприводимой компоненты W. Время работы алгоритма полиномиально от d^n, d_1, d_2, M, M_1, m и длины записи точки x.

Замечание 1. Время работы алгоритмов из теорем 1–5 является по-существу тем же самым, что и при решении систем полиномиальных уравнений с конечным числом решений в проективном пространстве. Поэтому эти теоремы могут быть сформулированы также и в случае, когда l не является фиксированным, см. [3].

Замечание 2. В дальнейшем мы будем предполагать без ограничения общности, что многочлены $g_0, \ldots, g_m$ являются линейно независимыми над k. Следовательно, $\dim V \leqslant n-1$, и $V_0 = \emptyset$.

1. Предварительные сведения

Мы будем использовать в этой статье технику из [8, 6, 7], см. Введения [6, 7]. Именно, мы используем разложения Ньютона–Пюизе и алгоритм Ньютона–Пюизе для построения корней многочлена в поле дробно-степенных рядов от одной переменной, см. также [4], используем бесконечно малые величины, стандартные части, построение вещественных структур.

Вещественная структура на поле k по определению является вложением $k \to K[\sqrt{-1}]$, где K – вещественное упорядоченное поле. Алгоритм полиномиальной сложности для построения вещественной структуры предлагается в [6] для поля k, конечнопорожденного над $\mathbb{Q}$. Здесь важно то, что для заданного элемента $a \in K$ можно выяснить, верно ли, что $a > 0$ за полиномиальное время. Дополнительно $K \subset \overline{k}$ в этой конструкции, где $\overline{k}$ является алгебраическим замыканием поля k. Абсолютная величина $|a|$ элемента из $a \in \overline{k}$ может быть определена естественным образом [6].

Рассмотрим неравенства типа $A < 0$ или $A \leqslant 0$, где $A = \sum_{1\leqslant i\leqslant r} a_i|A_i|^2$, $a_i \in K$, и A_i являются суперпозициями многочленов и функций $B \mapsto |B|^2$ для всякого i. Верхняя граница для степени A может быть легко определена, если мы положим $\deg |B|^2 = 2\deg B$.

Всякая система уравнений и неравенств над $\overline{k}$ эквивалентна системе уравнений и неравенств над $\widetilde{K}$ со в два раза большим числом переменных. Применяя алгоритм из [6] для построения вещественных структур, принцип переноса и [16] в этой ситуации, мы получаем, см. [7], следующий результат.

Предложение 1. *Рассмотрим систему полиномиальных уравнений от n переменных и фиксированного числа неравенств с многочленами и квадратами абсолютных величин (описанного типа $A < 0$ или $A \leqslant 0$) с коэффициентами из поля k, конечнопорожденного над $\mathbb{Q}$. Пусть степени уравнений и неравенств меньше, чем d. Тогда можно построить вещественную структуру на k и выяснить за время полиномиальное от d^n и длины записи входных данных, имеет ли эта система решение в $\mathbb{A}^n(\overline{k})$ относительно построеной вещественной структуры. Если такое решение существует, то его можно построить за то же самое время. Координаты решений принадлежат конечному расширению поля k. Это конечное расширение строится и задано своим примитивным элементом и его минимальным многочленом.*

Поскольку k является произвольным конечнопорожденным полем над $\mathbb{Q}$, этот результат справедлив также в случае, если заменить поле коэффициентов k на расширение k при помощи фиксированного числа бесконечно малых величин. В дальнейшем мы будем использовать много раз Предложение 1 для решения систем полиномиальных уравнений и неравенств с квадратами абсолютных величин и бесконечно малыми величинами без ссылок на это предложение.

Пусть k_1 является алгебраическим расширением поля $\mathbb{Q}(t_1,\dots,t_l)$. Пусть $\varepsilon_i > 0$ – бесконечно малая величина, см. [7], относительно поля $k_1(\varepsilon_1,\dots,\varepsilon_{i-1})$, $1 \leqslant i \leqslant v$. Пусть $0 \leqslant w \leqslant v-1$. Положим $K' = k_1(\varepsilon_1,\dots,\varepsilon_v)$ и $K'' = k_1(\varepsilon_1,\dots,\varepsilon_w)$. Обозначим через

$$\mathrm{st} : \mathbb{P}^n(\overline{K'}) \to \mathbb{P}^n(\overline{K''})$$

отображение стандартной части, см. [7], (стандартная часть элемента $z \in \mathbb{P}^n(\overline{K'})$ – это элемент $z_1 \in \mathbb{P}^n(\overline{K''})$, который является бесконечно близким к z). Мы будем использовать много раз следующий результат, см. [7] Предложение 2.

Предложение 2. *Пусть $W' \subset \mathbb{P}^n$ – алгебраическое многообразие, определенное над полем $\overline{K''}$, и, такое что всякая компонента многообразия W' имеет размерность $n-s$. Пусть $D_i \in \overline{K''}[X_0, \dots, X_n]$, $s+1 \leqslant i \leqslant n$, – линейные формы относительно $X_0, \dots, X_n$ и $\widetilde{D}_i \in \overline{K'}[X_0, \dots, X_n]$, $s+1 \leqslant i \leqslant n$, – линейные формы, все ненулевые коэффициенты которых являются бесконечно малыми величинами относительно поля K''. Тогда условие $\#W' \cap \mathcal{Z}(D_{s+1}, \dots, D_n) < +\infty$ в $\mathbb{P}^n(\overline{K''})$ влечет, что $\#W' \cap \mathcal{Z}(D_{s+1} - \widetilde{D}_{s+1}, \dots, D_n - \widetilde{D}_n) < +\infty$ в $\mathbb{P}^n(\overline{K'})$, и*

$$\mathrm{st}(W' \cap \mathcal{Z}(D_{s+1} - \widetilde{D}_{s+1}, \dots, D_n - \widetilde{D}_n)) = W' \cap \mathcal{Z}(D_{s+1}, \dots, D_n)$$

в $\mathbb{P}^n(\overline{K''})$.

2. Вычисление степени алгебраического многообразия и его гладких точек

Нам потребуется следующая лемма.

Лемма 1. *Пусть V_s, $0 \leqslant s \leqslant n$ – алгебраическое многообразие из утверждения Теоремы 1, и $L_0, L_{s+1}, L_{s+2}, \dots, L_n$ есть $n-s+1$ линейных форм из $\overline{k}[X_0, \dots, X_n]$, такие что $V_s \neq \emptyset$, и*

$$V_s \cap \mathcal{Z}(L_0, L_{s+1}, L_{s+2}, \dots, L_n) = \emptyset$$

в $\mathbb{P}^n(\overline{k})$. Обозначим через

$$p : V_s \longrightarrow \mathbb{P}^{n-s}(\overline{k}), \ (X_0 : \dots : X_n) \mapsto (L_0 : L_{s+1} : \dots : L_n)$$

линейную проекцию, которая является конечным морфизмом. Тогда

(i) *существует непустое открытое в топологии Зарисского подмножество U в $\mathbb{P}^{n-s}(\overline{k})$, такое что для всякого $x \in U$ мощность $\#p^{-1}(x) = \deg V_s$,*

(ii) *если для некоторой точки $x \in \mathbb{P}^{n-s}(\overline{k})$ мощность $\#p^{-1}(x) = \deg V_s$, то для всякой $y \in p^{-1}(x)$ точка y является гладкой точкой алгебраического многообразия V_s, и дифференциал проекции p в точке y*

$$d_y p : T_{y, V_s} \longrightarrow T_{x, \mathbb{P}^{n-s}}$$

является изоморфизмом касательных пространств T_{y,V_s} *и* $T_{x,\mathbb{P}^{n-s}}$ *алгебраических многообразий* V_s *и* $\mathbb{P}^{n-s}(\overline{k})$ *в точках* y *и* x *соответственно.*

Доказательство. Заменяя k на $\overline{k}$, мы можем предполагать без ограничения общности, что $V_s = W$ является неприводимым над $\overline{k}$. Пусть $Y \in \overline{k}[X_0, \ldots, X_n]$ – линейная форма. Рассмотрим морфизм

$$p_1 : W \longrightarrow \mathbb{P}^{n-s+1}(\overline{k}), \ (X_0 : \ldots : X_n) \mapsto (Y : L_0 : L_{s+1} : \ldots : L_n).$$

Поскольку p является конечным морфизмом, $p_1(W)$ является замкнутым подмножество в $\mathbb{P}^{n-s+1}(\overline{k})$, и $p_1(W) = \mathcal{Z}(G)$, где $G \in \overline{k}[Y, L_0, L_{s+1}, \ldots, L_n]$ – неприводимый однородный многочлен со старшим коэффициентом $\mathrm{lc}_Y G = 1$.

По теореме о примитивном элементе для полей существует линейная форма $Y \in \overline{k}[X_0, \ldots, X_n]$, такая что морфизм p_1 индуцирует бирациональный изоморфизм $W \longrightarrow p_1(W)$, который мы будем обозначать p_2. Следовательно, существует открытое подмножество $U_1 \subset W$, такое что $p_2(U_1)$ является открытым в $p_1(W)$, и p_2 индуцирует изоморфизм $U_1 \longrightarrow p_2(U_1)$.

Существует проекция $p_3 : p_1(W) \longrightarrow \mathbb{P}^{n-s}(\overline{k})$, такая что $p = p_3 \circ p_2$. Обозначим через $R = \mathrm{Res}_Y(G, G'_Y)$ дискриминант многочлена G относительно Y. Тогда $0 \neq R$ является однородным многочленом, поскольку G – сепарабельный однородный многочлен. Если $R(x) \neq 0$, то мощность $\# p_3^{-1}(x) = \deg_Y G$, для всякой $y \in p_3^{-1}(x)$ точка y является гладкой точкой алгебраического многообразия $p_1(W)$, и дифференциал отображения p_3 в точке y

$$d_y p_3 : T_{y,p_1(W)} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

является изоморфизмом касательных пространств $T_{y,p_1(W)}$ и $T_{x,\mathbb{P}^{n-s}}$ алгебраических многообразий $p_1(W)$ и $\mathbb{P}^{n-s}(\overline{k})$ в точках y и x соответственно. Последнее утверждение следует здесь просто из того, что $G'_Y(y) \neq 0$, поскольку $R(x) \neq 0$.

Положим $U = \mathbb{P}^{n-s}(\overline{k}) \setminus (\mathcal{Z}(R) \cup p_3(p_2(W) \setminus p_2(U_1)))$. Тогда для всякого $x \in U$

(a) мощность $\# p^{-1}(x) = \deg G$,

(b) для всякой $y \in p^{-1}(x)$ точка y является гладкой точкой многообразия W, и дифференциал отображения p в точке y

$$d_y p : T_{y,W} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

является изоморфизмом касательных пространств $T_{y,W}$ и $T_{x,\mathbb{P}^{n-s}}$ алгебраических многообразий W и $\mathbb{P}^{n-s}(\overline{k})$ в точках y и x соответственно. Покажем, что $\deg G = \deg W$. Пусть $\varepsilon > 0$ – бесконечно малая величина относительно поля k. Следовательно, отображение стандартной части

$$\mathrm{st} \, : \mathbb{P}^r(\overline{k(\varepsilon)}) \longrightarrow \mathbb{P}^r(\overline{k})$$

определено для всякого $r \geqslant 0$, см. [7]. Обозначим через $\mathcal{H}_1$ множество семейств H, состоящих каждое из $n-s+1$ линейных форм $H_0, H_{s+1}, H_{s+2}, \ldots, H_n$ от $X_0, \ldots, X_n$, таких что, если заменить в формулировке Леммы 1 формы $L_0, L_{s+1}, L_{s+2}, \ldots, L_n$ на $H_0, H_{s+1}, H_{s+2}, \ldots, H_n$, то (i) будет удовлетворяться для $U(H)$ и $p(H)$, соответствующих U и p. Рассмотрим $\mathcal{H}_1$ как подмножество в $\mathbb{A}^{(n-s+1)(n+1)}$. Тогда [2], ср. также Раздел 5, $\mathcal{H}_1$ является открытым подмножеством в $\mathbb{A}^{(n-s+1)(n+1)}$ относительно топологии Зарисского.

Следовательно, существует семейство $H_0, H_{s+1}, H_{s+2}, \ldots, H_n$ в $\mathcal{H}_1(\overline{k(\varepsilon)})$, такое что все формы $H_j - L_j$ имеют бесконечно малые коэффициенты. Таким образом, по Предложению 2 для всякого $x \in U \cap U(H)$ для всякого $y^* \in p(H)^{-1}(x)$ элемент $y = \mathrm{st}\, y^* \in p^{-1}(x)$. Дифференциал проекции p в точке y является изоморфизмом. Следовательно, по теореме о неявной функции существует единственный $y' \in p(H)^{-1}(x)$, такой что $\mathrm{st} y' = y$. Следовательно, $y' = y^*$. Таким образом,

$$\deg W = \#p(H)^{-1}(x) = \#p^{-1}(x) = \deg_Y G,$$

и, поэтому $\deg G = \deg W$. Утверждение (i) доказано.

Чтобы доказать (ii), отметим, что если $R(x) \neq 0$, и $y \in p^{-1}(x)$, то точка $p_1(y)$ является гладкой, локальное кольцо $\mathcal{O}_{p_1(y),p_1(W)}$ многообразия $p_1(W)$ в точке $p_1(y)$ является целозамкнутым. Следовательно, локальное кольцо

$$\mathcal{O}_{y,W} \simeq \mathcal{O}_{p_1(y),p_1(W)},$$

поскольку $\mathcal{O}_{y,W}$ цело над $\mathcal{O}_{p_1(y),p_1(W)}$ и имеет то же самое поле частных. Таким образом, p_1 является изоморфизмом в окрестности каждой точки $y \in p^{-1}(x)$. Теперь (ii) следует из того, что для всякой точки x, для которой $\#p^{-1}(x) = \deg W$, существует линейная форма Y, такая что соответствующее отображение p_1

является бирациональным, $\# p_3^{-1}(x) = \deg W$, и поэтому $R(x) \neq 0$, см. выше. Лемма доказана.

Мы будем предполагать без ограничения общности, что

$$\deg(g_i) = \deg_{X_0,\,\ldots\,,X_n}(g_i) = d$$

для всех $0 \leqslant i \leqslant m$, заменяя при необходимости всякий многочлен g_i на семейство многочленов $\{g_i X_j^{-\deg(g_i)+d}\}_{0\leqslant j\leqslant n}$.

Напомним,что в [7] построен алгоритм полиномиальной сложности, который находит все s, для которых $V_s \neq \emptyset$. Для всякого s на шаге s алгоритм из [7] строит многочлены $h_1, \ldots , h_s$ и линейные формы $L_{s+1}^{(s)}, \ldots , L_n^{(s)}$ от $X_0, \ldots , X_n$ с целыми коэффициентами с длинами записи $O(n \log d)$, такие что

$$h_i = \sum_{0\leqslant j\leqslant m} \lambda_{i,j} g_j , \ \ \lambda_{i,j} \in \mathbb{Z}$$

для всех i, j. Кроме того, выполняется следующее свойство. Пусть

$$W_s = \mathcal{Z}(h_1, \ldots , h_s) \subset \mathbb{P}^n(\overline{k})$$

есть многообразие всех общих нулей многочленов $h_1, \ldots , h_s$ в $\mathbb{P}^n(\overline{k})$, пусть W' – объединение всех неприводимых компонент U_1 многообразия W_s, таких что $\dim U_1 = n - s$, и W'' – объединение всех неприводимых компонент U_1 многообразия W_s, таких что $\dim U_1 > n - s$. Тогда подмножество в $\mathbb{P}^n(\overline{k})$

$$W' \cap \mathcal{Z}(L_{s+1}^{(s)}, \ldots , L_n^{(s)})$$

конечно, и

$$W' \cap \mathcal{Z}(L_{s+1}^{(s)}, \ldots , L_n^{(s)}) \cap W'' = \emptyset .$$

Форма $L_0^{(s)}$ не равна нулю во всякий точке из $W' \cap \mathcal{Z}(L_{s+1}^{(s)}, \ldots , L_n^{(s)})$. Кроме того, W'' состоит из всех компонент U многообразия $\mathcal{Z}(g_0, \ldots , g_m)$ с $\dim U > n - s$.

Мы будем обозначать также $W' = W'_s$, $W'' = W''_s$, когда зависимость от s будет существенна.

Положим $L_{s,j} = L_j^{(s)}$, $s + 1 \leqslant j \leqslant n$ или $j = 0$. Вычислим, см. [7], все точки $\{x_u\}_{1\leqslant u\leqslant N}$ множества $W' \cap \mathcal{Z}(L_{s,s+1}, \ldots , L_{s,n})$. Пусть $x_u = (x_{u,0} : \ldots : x_{u,n})$, где все $x_{u,i}$ – из конечного расширения поля k. Построим вещественную структуру для поля

$K = k(x_{u,0}, \dots, x_{u,n})$, см. [6, 7], которая индуцирует некоторую вещественную структуру на $\overline{k}$ (она однозначно определена с точностью до сопряжения).

Пусть $\varepsilon_1 > 0$ – бесконечно малая величина относительно поля K, и $\varepsilon_2 > 0$ – бесконечно малая величина относительно поля $K(\varepsilon_1)$, поле $K_1 = K(\varepsilon_1, \varepsilon_2)$.

Пусть $Y_0, \dots, Y_n$ – новые переменные. Для всякого $1 \leqslant u \leqslant N$ рассмотрим следующую систему уравнений и неравенств с коэффициентами из K_1

$$\begin{cases} h_i = 0, & 1 \leqslant i \leqslant s, \\ h_i(Y_0, \dots, Y_n) = 0, & 1 \leqslant i \leqslant s, \\ L_{s,j}(X_0 - Y_0, \dots, X_n - Y_n) = 0, & j \in \{0, s+1, \dots, n\}, \\ \sum_{0 \leqslant i \leqslant n} |X_i - x_{u,i}|^2 \leqslant \varepsilon_1, \\ \sum_{0 \leqslant i \leqslant n} |Y_i - x_{u,i}|^2 \leqslant \varepsilon_1, \\ \sum_{0 \leqslant i \leqslant n} |Y_i - X_i|^2 \geqslant \varepsilon_2, \end{cases} \tag{2}$$

Замечание 3 Можно также добавить к этой системе уравнение $L_{s,0}(X_0 - x_{u,0}, \dots, X_n - x_{u,n}) = 0$, однако это необязательно.

Лемма 2. *Пусть $W' = W'_s$. Тогда $N = \deg W'$ в том и только в том случае, если для всякого $1 \leqslant u \leqslant N$ не существует решений системы (2) в $\mathbb{A}^{2n+2}(\overline{K_1})$. Если для всякого $1 \leqslant u \leqslant N$ не существует решений системы (2) в $\mathbb{A}^{2n+2}(\overline{K_1})$, то все точки $\{x_u\}_{1 \leqslant u \leqslant N}$ многообразия W' являются гладкими, и дифференциалы проекции*

$$p : W' \longrightarrow \mathbb{P}^{n-s}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (L_{s,0} : L_{s,s+1} : \ldots : L_{s,n})$$

в точках $\{x_u\}_{1 \leqslant u \leqslant N}$ являются изоморфизмами.

Доказательство. Это следует непосредственно из Леммы 1, если заменить $g_0, \dots, g_m$ на $h_1, \dots, h_s$ и, следовательно, V_s на W'_s, ср. также доказательство Леммы 17 ниже.

Вернемся к описанию алгоритма. Наша цель сейчас – вычислить $\deg W'$. Построим решение системы (2) для некоторого $1 \leqslant u \leqslant N$ или установим, что для всякого $1 \leqslant u \leqslant N$ не существует решений системы (2) в $\mathbb{A}^{2n+2}(\overline{K_1})$. В последнем случае по Лемме 2 степень $\deg W' = N$ уже вычислена. Предположим, что существует решение

$$(x'_0, \dots, x'_n, y'_0, \dots, y'_n) \in \mathbb{A}^{2n+2}(\overline{K_1})$$

системы (2) с $u = u_0$. Обозначим $x' = (x'_0 : \ldots : x'_n)$ и $y' = (y'_0 : \ldots : y'_n)$. Так что $x', y' \in \mathbb{P}^n(\overline{K_1})$. Положим

$$L'_i = L_{s,i} - (L_{s,i}/L_{s,0})(x')L_{s,0},\ s+1 \leqslant i \leqslant n, \quad L'_0 = L_{s,0}.$$

Вычислим, см. [7], все точки множества $W' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n)$ в $\mathbb{P}^n(\overline{K_1})$. Обозначим $N' = \#W' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n)$. По Предложению 2 для всякого $x^* \in W' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n)$ существует $1 \leqslant u \leqslant n$, такое что $\operatorname{st} x^* = x_u$. Следовательно, $N' \geqslant N$. Далее, $x', y' \in W' \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n)$, $x' \neq y'$, и $\operatorname{st} x' = \operatorname{st} y'$. Следовательно, $N' \geqslant N + 1 > N$.

Пусть $D_{s+1}, \ldots, D_n \in \overline{K_1}[X_0, \ldots, X_n]$ – линейные формы (в дальнейшем мы будем рассматривать также другие поля коэффициентов, отличные от K_1). Аналогично определению 1 из [7] свойство $\mathcal{A}$ линейных форм $D_{s+1}, \ldots, D_n$ называется хорошим тогда и только тогда, когда оно удовлетворяет следующему условию. Рассмотрим $\mathcal{A}$ как функцию от $D_{s+1}, \ldots, D_n$. Пусть $D_i = \sum_{0 \leqslant j \leqslant n} l_{i,j} L_j$, где $l_{i,j} \in \overline{K_1}$ для всех i, j. Заменим один произвольный коэффициент $l_{i,j}$ в формах $D_{s+1}, \ldots, D_n$ на ε', где ε' – бесконечно малая величина относительно поля K_1. Мы получаем новую линейную форму D'_i с коэффициентами из $\overline{K_1(\varepsilon')}$. Предположим для удобства обозначений, что мы заменили $l_{s+1,0}$ и получили D'_{s+1}. Условие для свойства $\mathcal{A}$ – следующее. Существует многочлен P, такой что, если свойство $\mathcal{A}$ удовлетворяется для форм $D_{s+1}, \ldots, D_n$, то

(i) оно не удовлетворяется для самое большее $P(d^n)$ произвольных значений ε^* бесконечно малой величины ε' (рассматриваемой как переменная) для форм $D'_{s+1}|_{\varepsilon'=\varepsilon^*}, D_{s+2}, \ldots, D_n$,

(ii) для данного значения ε^* бесконечно малой величины ε' можно проверить свойство $\mathcal{A}$ для форм $D'_{s+1}|_{\varepsilon'=\varepsilon^*}, D_{s+2}, \ldots, D_n$ за полиномиальное время от d^n, d_1, d_2, M_1, M_2 (при условии, что длина записи ε^* ограничена теми же самыми значениями).

Для хорошего свойства $\mathcal{A}$ можно построить, заменяя последовательно коэффициенты линейных форм $D_{s+1}, \ldots, D_n$ на целые коэффициенты (ср. алгоритм из [7] Раздел 3 шаг (24); он называется в [7] вторым вспомогательным алгоритмом), линейные формы $M_{s+2}, \ldots, M_n$ от $X_0, \ldots, X_n$ с целыми коэффициентами с длинами записи $O(n \log d)$, удовлетворяющие свойству $\mathcal{A}$, за полиномиальное время от d^n, d_1, d_2, M_1, M_2. В дальнейшем мы будем использовать несколько раз эту конструкцию (не формулируя явно свойство $\mathcal{A}$ за исключением первого раза), ссылаясь на нее как на аналог второго вспомогательного алгоритма из [7].

Теперь заметим, что согласно [7] свойство, что

$$\#W' \cap \mathcal{Z}(D_{s+1}, \ldots, D_n) \geqslant N', \quad \text{и}$$
$$W' \cap \mathcal{Z}(D_{s+1}, \ldots, D_n) \cap W'' = \emptyset, \quad \text{и} \quad D_0 = L'_0$$

является хорошим.

Так что применим аналог второго вспомогательного алгоритма к линейным формам $L'_0, L'_{s+1}, \ldots, L'_n$ и построим линейные формы $M_0, M_{s+1}, \ldots, M_n$ с коэффициентами из $\mathbb{Z}$ с длинами записи $O(n \log d)$, такие что

$$\#W' \cap \mathcal{Z}(M_{s+1}, \ldots, M_n) \geqslant N',$$
$$W' \cap \mathcal{Z}(M_{s+1}, \ldots, M_n) \cap W'' = \emptyset, \text{ и } M_0 = L'_0.$$

После этого вернемся рекурсивно к началу описываемого алгоритма, заменяя формы $L_{s,0}, L_{s,s+1}, \ldots, L_{s,n}$ на $M_0, M_{s+1}, \ldots, M_n$. Поскольку $N' > N$, то существует самое большее d^s таких возвратов к началу алгоритма.

Таким образом, мы вычислим $\deg W'$ за требуемое время и мы можем предполагать без ограничения общности по Лемме 2, что $N = \deg W'$, все точки x_u, $1 \leqslant u \leqslant N$ являются гладкими на алгебраическом многообразии W', и дифференциалы проекции p, см. Лемму 2, в точках x_u, $1 \leqslant u \leqslant N$ являются изоморфизмами.

Покажем, как выбрать среди точек x_u, $1 \leqslant u \leqslant N$ точки из V_s. Пусть $1 \leqslant u \leqslant N$. Рассмотрим следующую систему уравнений и неравенств относительно $X_0, \ldots, X_n$, Z с коэффициентами из $\overline{k(\varepsilon_1)}$

$$h_1 = \ldots = h_s = h_{s+1}Z - 1 = 0, \sum_{0 \leqslant i \leqslant n} |X_i - x_{u,i}|^2 < \varepsilon_1. \qquad (3)$$

Лемма 3. *Точка $x_u = (x_{u,0} : \ldots : x_{u,n}) \in V_s$ тогда и только тогда, когда система (3) не имеет решений в $\mathbb{A}^{n+1}(\overline{k(\varepsilon_1)})$.*

Доказательство. Это следует непосредственно из того, что точка x_u является гладкой и определения многочленов $h_1, \ldots, h_{s+1}$, см. выше (а также [7]). Лемма доказана.

Теперь построим, ср. [6, 7], решая системы (3), подмножество $A \subset \{1, \ldots, N\}$ всех индексов u, таких что (3) не имеет решений в $\mathbb{A}^{n+1}(\overline{k(\varepsilon_1)})$.

По Лемме 1, Лемме 2 и Лемме 3 мы имеем $\#A = \deg V_s$, множество $V_s \cap \mathcal{Z}(L_{s,s+1}, \ldots, L_{s,n}) = \{x_u : u \in A\}$, и дифференциалы проекции p, см. Лемму 2, в точках x_u, $u \in A$ являются изоморфизмами.

Таким образом, степень $\deg V_s$, и множество гладких точек $\{x_u : u \in A\} \subset V_s$ могут быть вычислены для всякого s. Всякая точка x_u, $u \in A$, не принадлежит W''. Следовательно, точки x_u, $u \in A$ являются гладкими точками многообразия V. Теорема 1 доказана.

Чтобы доказать Теорему 4, достаточно построить касательные пространства многообразия V_s в точках множества $\{x_u : u \in A\}$.

Лемма 4. *Пусть $\phi = (\phi_1, \ldots, \phi_r) : V' \longrightarrow \overline{k}^r$, $r \geqslant 0$, – морфизм алгебраических многообразий, который задан рациональными функциями $\phi_1, \ldots, \phi_r \in \overline{k}(V')$, пусть точка $y \in V'$ является гладкой, рациональные функции $\phi_1, \ldots, \phi_r$ определены в точке y, и дифференциал*

$$d_y\phi : T_{y,V'} \longrightarrow T_{\phi(y),\overline{k}^r}$$

морфизма ϕ в точке y является изоморфизмом касательных пространств $T_{y,V'}$ многообразия V' в точке y и $T_{\phi(y),\overline{k}^r}$ многообразия $\overline{k}^r$ в точке $\phi(y)$. Обозначим

$$C_j = \{(z_1, \ldots, z_r) \in \overline{k}^r : z_m - \phi_m(y) = 0, 1 \leqslant m \leqslant r, m \neq j\}$$

для всякого $1 \leqslant j \leqslant r$. Тогда $D_j = \phi^{-1}(C_j) = \{x \in V' : \phi_m(x) - \phi_m(y) = 0, 0 \leqslant m \leqslant r, m \neq j\}$ является кривой в некоторой окрестности y, точка y является гладкой на D_j. Так что касательное пространство T_{y,D_j} многообразия D_j в точке y является подмножеством $T_{y,D_j} \subset T_{y,V'}$. Наконец, мы имеем $\sum_{1 \leqslant j \leqslant r} T_{y,D_j} = T_{y,V'}$.

Доказательство. В случае, если заменить $\overline{k}$ на $\mathbb{C}$ утверждение леммы следует непосредственно из теоремы о неявной функции. Теперь достаточно использовать принцип переноса для поля, снабженного вещественной структурой, ср. [6], см. [5]. Лемма доказана.

Теперь положим $V' = p^{-1}(\mathbb{P}^{n-s}(\overline{k}) \setminus \mathcal{Z}(L_{s,0})) \subset W'$, где p – проекция из Леммы 2, и $y = x_u$ для некоторогоого $u \in A$. Так что $\mathbb{P}^{n-s}(\overline{k}) \setminus \mathcal{Z}(L_{s,0}) \simeq \overline{k}^{n-s}$. Положим $\phi = p|_{V'}$. Применим Лемму 4.

Мы имеем

$$D_j = \mathcal{Z}(h_1, \dots , h_s) \cap \mathcal{Z}(L_{s,m} - (L_{s,m}/L_{s,0})(x_u)L_{s,0},$$

$$s+1 \leqslant m \leqslant n,\, m \neq s+j)$$

для $1 \leqslant j \leqslant n-s$ в некоторой окрестности x_u.

Таким образом, построим общие точки кривых D_j (более точно неприводимых компонент многообразий D_j в окрестностях точки x_u) и разложения Ньютона–Пюизе координатных функций общих точек D_j относительно униформизующих элементов в некоторой окрестности точки x_u, ср. [6] раздел 3, шаги (11), (12), (13) а также [7], раздел 1, шаг (16). Теперь легко построить касательное пространство T_{x_u,D_j} многообразия D_j в точке x_u. Следовательно, по Лемме 4 все касательные пространства T_{x_u,V_s}, $u \in A$, могут быть построены за требуемое время. Теорема 4 доказана.

Замечание 4 Фактически можно увидеть, что алгоритм из [3] (или его незначительная модификация) дает систему локальных параметров D_j в окрестности гладкой точки x_u. Поэтому необязательно даже рассматривать разложения Ньютона–Пюизе.

3. Размерность компонент, содержащих точку, и доминантность морфизма алгебраических многообразий

Теперь мы собираемся доказать Теорему 2. Эта теорема следует немедленно из следующей леммы.

Лемма 5. *Пусть $x \in V$, см. Введение. Тогда можно выяснить верно ли, что $x \in V_s$ за время полиномиальное от d^n, d_1, d_2, M, M_1, m и длины записи точки x.*

Доказательство. Построим множество $\{x_u \,:\, u \in A\}$ гладких точек многообразия V и линейные формы $L_{s,s+1}, \dots , L_{s,n}$, такие что

$$\{x_u \,:\, u \in A\} = V_s \cap \mathcal{Z}(L_{s,s+1}, \dots , L_{s,n}),$$

см. Раздел 2. Построим линейно независимые линейные формы L_i, $s+1 \leqslant i \leqslant n$, обращающиеся в нуль в точке x и, такие что L_i, $s+2 \leqslant i \leqslant n$, являются линейными формами относительно $L_{s,s+1}, \dots , L_{s,n}$. Обозначим $\mathcal{L} = \mathcal{Z}(L_{s+2}, \dots , L_n)$.

Пересечение $\mathcal{L} \cap V_s$ является кривой. Обозначим ее через C_s. Всякая неприводимая компонента C_s является неприводимой компонентой многообразия решений системы

$$h_1 = \ldots = h_s = L_{s+2} = \ldots = L_n = 0. \qquad (4)$$

Существует линейная форма L' (совпадающая с одной из линейных форм $L_{s,s+1}, \ldots, L_{s,n}$), такая что

$$C_s \cap \mathcal{Z}(L') = V_s \cap \mathcal{Z}(L_{s,s+1}, \ldots, L_{s,n}).$$

Следовательно, всякая неприводимая компонента кривой C_s, являясь проективным алгебраическим многообразием, имеет непустое пересечение с $\mathcal{Z}(L')$ и, следовательно, содержит некоторую точку x_u, $u \in A$. Точки $\{x_u \, : \, u \in A\}$ – гладкие на многообразии решений (4) согласно конструкции Раздела 2, и $C_s \supset \{x_u \, : \, u \in A\}$. Поэтому, применяя алгоритм из [3], см. также [6, 7], построим за требуемое время системы уравнений, которые задают одномерные компоненты многообразия решений (4). Затем, подставляя в них координаты точек из $\{x_u \, : \, u \in A\}$, выберем среди этих неприводимых компонент те, которые являются компонентами C_s. Наконец, подставляя в системы уравнений, которые задают неприводимые компоненты C_s координаты точки x, выясним верно ли, что $x \in C_s$, т.е., что $x \in V_s$. Лемма доказана. Теорема 2 доказана.

Следствие 1. *Пусть $\varepsilon > 0$ – бесконечно малая величина относительно поля k. При условиях Леммы 3 для всякого $0 \leqslant s \leqslant n$ можно построить семейство точек $x_\beta \in \mathbb{P}^n(\overline{k(\varepsilon)})$, $\beta \in B_s$, таких что*

- *всякая точка x_β является бесконечно близкой к x,*
- *всякая точка $x_\beta \in V_s$, и x_β – гладкая точка алгебраического многообразия V,*
- *для всякой неприводимой компоненты W_1 многообразия V_s, содержащей точку x, существует $\beta \in B_s$, такое что $x_\beta \in W_1$.*

Доказательство. Выберем $s + 1 \leqslant i_0 \leqslant n$, такое что линейные формы $L_{s,i_0}, L_{s+1}, \ldots, L_n$ являются линейно независимыми. Мы будем предпологать, не умаляя общности, и для удобства обозначений, что $i_0 = s + 1$. Построим изолированные решения системы

$$h_1 = \ldots = h_s = L_{s+1} - \varepsilon L_{s,s+1} = L_{s+2} = \ldots = L_n = 0. \qquad (5)$$

Выберем среди этих решений те, которые являются бесконечно близкими к точке x. Мы утверждаем, что полученное семейство решений дает требуемое семейство x_β, $\beta \in B_s$. Действительно, по Предложению 2 достаточно проверить только, что x_β является гладкой точкой алгебраического многообразия V. Чтобы установить этот факт, отметим, что всякая неприводимая компонента кривой C_s содержит некоторую гладкую точку x_u, $u \in A$ многообразия V, и $x_u \in V_s$. Следовательно, кривая C_s содержит только конечное множество особых точек многообразия V. Поэтому точка x_β является гладкой точкой V, так как она бесконечно близка к x. Следствие доказано.

Теперь наша цель – доказать Теорему 5. Мы можем предполагать без ограничения общности, что V – аффинное алгебраическое многообразие, которое является множеством нулей многочленов $g_0, \dots, g_m \in k[X_1, \dots, X_n]$, рациональные функции $q_{s+1}, \dots, q_n \in k(X_1, \dots, X_n)$, степени (соответственно длины записи целых коэффициентов) многочленов (теперь неоднородных) $g_0, \dots, g_m$, числителей и знаменателей рациональных функций $q_{s+1}, \dots, q_n$ ограничены сверху d (соответственно M). Сначала мы выясняем верно ли, что $V_s \neq \emptyset$, используя алгоритм из [7]. Если $V_s = \emptyset$, то не существует неприводимых компонент многообразия V_s.

Пусть $V_s \neq \emptyset$. Расширяя поле k при помощи бесконечно малой величины $\varepsilon > 0$ (и заменяя k на $k(\varepsilon)$), применяя Следствие 1 и рассматривая отдельно каждую точку x_β, $\beta \in B_s$, мы можем предполагать без ограничения общности, что x – гладкая точка алгебраического многообразия V, и $x \in V_s$, где $0 \leqslant s \leqslant n$ известно. Следовательно, существует только одна неприводимая компонента W_1 алгебраического многообразия V, содержащая точку x, и $W_1 \subset V_s$.

Пусть $q_i = q_i^{(1)}/q_i^{(2)}$, где $q_i = q_i^{(1)}, q_i^{(2)} \in k[X_1, \dots, X_n]$, и $\mathrm{GCD}(q_i^{(1)}, q_i^{(2)}) = 1$ в кольце $k[X_1, \dots, X_n]$ для всякого $s+1 \leqslant i \leqslant n$. Введем новые переменные $Y_{s+1}, \dots, Y_n$, $Z_{s+1}, \dots, Z_n$. Рассмотрим алгебраическое многообразие

$$V' = \mathcal{Z}(g_0, \dots, g_m, q_i^{(2)} Y_i - 1, q_i^{(2)} Z_i - q_i^{(1)}, s+1 \leqslant i \leqslant n) \subset \mathbb{A}^{n+2(n-s)}(\overline{k}).$$

Обозначим через

$$\pi : \mathbb{A}^{n+2(n-s)}(\overline{k}) \to \mathbb{A}^n(\overline{k}),$$
$$(X_1, \dots, X_n, Y_{s+1}, \dots, Y_n, Z_{s+1}, \dots, Z_n) \mapsto (X_1, \dots, X_n)$$

линейную проекцию. Пусть $\varepsilon_1 > 0$ – бесконечно малая величина относительно поля k. Рассмотрим следующую систему алгебраических уравнений и неравенств относительно $X_1, \dots, X_n$, $Y_{s+1}, \dots, Y_n$, $Z_{s+1}, \dots, Z_n$

$$\begin{cases} g_i = 0, & 0 \leqslant i \leqslant m, \\ q_i^{(2)} Y_i - 1 = 0, & s+1 \leqslant i \leqslant n, \\ q_i^{(2)} Z_i - q_i^{(1)} = 0, & s+1 \leqslant i \leqslant n, \\ \sum_{1 \leqslant i \leqslant n} |X_i - X_i(x)|^2 = \varepsilon_1. \end{cases} \tag{6}$$

Покажем, что если семейство $\mathcal{Q}$ алгебраически независимо над $\overline{k}$ в поле $\overline{k}(W_1)$, то существует решение $x' \in \mathbb{A}^{n+2(n-s)}(\overline{k(\varepsilon_1)})$ системы (6). В самом деле, в этом случае существует неприводимая компонента W_1' алгебраического многообразия V', такая что W_1' бирационально изоморфна W_1, и этот бирациональный изоморфизм индуцирован проекцией π. Следовательно, существует решение $x' \in \mathbb{A}^{n+2(n-s)}(\overline{k(\varepsilon_1)})$ системы (6). Отметим, что если существует решение $x' \in \mathbb{A}^{n+2(n-s)}(\overline{k(\varepsilon_1)})$ системы (6), то $x' \in V'$, $q_i^{(2)}(x') \neq 0$, и существует неприводимая компонента W_1' алгебраического многообразия V', такая что W_1' бирационально изоморфна W_1. Рациональные функции q_i совпадают с координатными функциями Z_i на алгебраическом многообразии V', $s+1 \leqslant i \leqslant n$.

Таким образом, заменяя k на $k(\varepsilon_1)$, n на $n+2(n-s)$, алгебраическое многообразие V на V' и точку x на x', мы можем предполагать дополнительно без ограничения общности, что рациональные функции q_i являются координатными функциями Z_i, $s+1 \leqslant i \leqslant n$. Наконец, осуществляя линейное преобразование пространства $\mathbb{A}^n$, мы можем предполагать, не умаляя общности, что q_i являются координатными функциями X_i, $s+1 \leqslant i \leqslant n$, $x = (0, \dots, 0) \in \mathbb{A}^n(\overline{k})$ – гладкая точка алгебраического многообразия V, и $x \in V_s$, где $0 \leqslant s \leqslant n$ известно.

Пусть $\varepsilon_i > 0$ – бесконечно малая величина относительно поля $k(\varepsilon_2, \dots, \varepsilon_{i-1})$, $2 \leqslant i \leqslant 4$. Пусть $\xi = (\xi_1, \dots, \xi_n) \in V_s$. Пусть $s \leqslant r \leqslant n-1$. Пусть $L_{r+1}, \dots, L_n \in \mathbb{Z}[X_0, \dots, X_n]$ – линейные формы с целыми коэффициентами. Рассмотрим следующую систему алгебраических уравнений и неравенств относительно

$X_1, \dots, X_n$, $Y_1, \dots, Y_n$.

$$\begin{cases} g_i = 0, & 0 \leqslant i \leqslant m, \\ g_i(Y_1, \dots, Y_n) = 0, & 0 \leqslant i \leqslant m, \\ \sum_{1 \leqslant i \leqslant n} |X_i - \xi_i|^2 = \varepsilon_2, & \\ \sum_{1 \leqslant i \leqslant n} |X_i - Y_i|^2 = \varepsilon_4^2, & \\ X_i - Y_i = 0, & s+1 \leqslant i \leqslant r, \\ |X_{r+1} - Y_{r+1}|^2 > \varepsilon_4^2 \varepsilon_3. & \end{cases} \tag{7}$$

В дальнейшем мы будем отождествлять для удобства обозначений касательное пространство $\mathcal{Z}(\sum_{1 \leqslant i \leqslant n} a_{\gamma,i} dX_i, \gamma \in \Gamma)$ (где $a_{\gamma,i}$ принадлежит полю коэффициентов) в точке произвольного аффинного алгебраического многообразия с подпространством $\mathcal{Z}(\sum_{1 \leqslant i \leqslant n} a_{\gamma,i} X_i, \gamma \in \Gamma) \subset \mathbb{A}^n$, причем $\mathbb{A}^n$ имеет координатные функции $X_1, \dots, X_n$.

Лемма 6. *Пусть $\xi \in V_s$ – гладкая точка многообразия V. Пусть W_1 – единственная неприводимая компонента алгебраического многообразия V, такая что $\xi \in W_1$. Пусть $s \leqslant r \leqslant n-1$. Пусть пересечение касательного пространства в точке ξ алгебраического многообразия W_1*

$$T_{\xi, W_1} \cap \mathcal{Z}(X_{s+1}, \dots, X_r, L_{r+1}, \dots, L_n) = \{0\} \tag{8}$$

(и следовательно, линейные формы $X_{s+1}, \dots, X_r$, $L_{r+1}, \dots, L_n$ являются алгебраически независимыми в поле рациональных функций $\overline{k}(W_1)$ неприводимой компоненты W_1). Тогда система (7) имеет решение в пространстве $\mathbb{A}^{2n}(\overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)})$ в том и только в том случае, если координатные функции $X_{s+1}, \dots, X_r$, X_{r+1} алгебраически независимы над $\overline{k}$ в поле рациональных функций $\overline{k}(W_1)$ алгебраического многообразия W_1.

Доказательство. Пусть система (7) имеет решение

$$(x'_1, \dots, x'_n, y'_1, \dots, y'_n) \in \mathbb{A}^{2n}(\overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}). \tag{9}$$

Положим $x' = (x'_1, \dots, x'_n)$ и $y' = (y'_1, \dots, y'_n)$. Тогда согласно (8) и, поскольку x' бесконечно близка к ξ, справедливо равенство (8), если заменить ξ на x'. Следовательно, координатные функции X_j, $1 \leqslant j \leqslant n$, на касательном пространстве T_{x', W_1} алгебраического многообразия W_1 в точке x' удовлетворяют равенствам

$$X_j = \sum_{s+1\leqslant i\leqslant r} \alpha_{j,i} X_i + \sum_{r+1\leqslant u\leqslant n} \beta_{j,u} L_u, \quad 1 \leqslant j \leqslant n,$$

для некоторых элементов $\alpha_{j,i} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $s+1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant n$, и $\beta_{j,u} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $r+1 \leqslant u \leqslant n$, $1 \leqslant j \leqslant n$.

Мы можем применить теорему о неявной функции в точке x', когда все координатные функции на W_1 рассматриваются как формальные степенные ряды с коэффициентами в $\overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$ относительно линейных многочленов $X_{s+1} - X_{s+1}(x')$, $\dots, X_r - X_r(x')$, $L_{r+1} - L_{r+1}(x'), \dots, L_n - L_n(x')$. Согласно (8) и, поскольку точка x' бесконечно близка к ξ, все коэффициенты этих формальных степенных рядов не являются бесконечно большими относительно поля k. Согласно (7) $x'_i = y'_i$ для $s+1 \leqslant i \leqslant r$ и $|x'_{r+1} - y'_{r+1}|^2 > \varepsilon_4^2 \varepsilon_3$. Следовательно, теорема о неявной функции влечет, что существует $r+1 \leqslant i_0 \leqslant n$, такое что $\beta_{r+1,i_0} \neq 0$. Мы будем предполагать без ограничения общности для удобства обозначений, что $i_0 = r+1$. Следовательно, координатные функции X_j, $1 \leqslant j \leqslant n$, на касательном пространстве T_{x',W_1} алгебраического многообразия W_1 в точке x' удовлетворяют равенствам

$$X_j = \sum_{s+1\leqslant i\leqslant r+1} \alpha'_{j,i} X_i + \sum_{r+2\leqslant i\leqslant n} \beta'_{j,i} L_i, \quad 1 \leqslant j \leqslant n,$$

для некоторых элементов $\alpha'_{j,i} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $s+1 \leqslant i \leqslant r+1$, $1 \leqslant j \leqslant n$, и $\beta'_{j,i} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $r+2 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$. Следовательно,

$$T_{x',W_1} \cap \mathcal{Z}(X_{s+1}, \dots, X_{r+1}, L_{r+2}, \dots, L_n) = \{0\}. \tag{10}$$

Таким образом, по теореме о неявной функции координатные функции $X_{s+1}, \dots, X_r, X_{r+1}$ алгебраически независимы в поле рациональных функций $\overline{k}(W_1)$ алгебраического многообразия W_1.

Обратно, пусть координатные функции $X_{s+1}, \dots, X_r, X_{r+1}$ алгебраически независимы в поле рациональных функций $\overline{k}(W_1)$ алгебраического многообразия W_1. Тогда существует $r+1 \leqslant i_0 \leqslant n$, такое что линейные формы

$$X_{s+1}, \dots, X_r, X_{r+1}, L_{r+1}, \dots, L_{i_0-1}, L_{i_0+1}, \dots, L_n$$

алгебраически независимы в поле $\overline{k}(W_1)$. Мы будем предполагать, не умаляя общности, для удобства обозначений, что $i_0 = r+1$.

Множество точек $x' \in W_1(\overline{k(\varepsilon_2)})$, таких что справедливо (10), содержит непустое открытое в топологии Зарисского подмножество в $W_1(\overline{k(\varepsilon_2)})$. Следовательно, ср. доказательство Леммы 8 ниже и Леммы 9 из [7], существует гладкая точка $x' = (x'_1, \dots, x'_n) \in W_1(\overline{k(\varepsilon_2)})$, такая что выполнено (10), и $\sum_{1\leqslant i\leqslant n} |x'_i - \xi_i|^2 = \varepsilon_2$.

Мы можем применить теорему о неявной функции в точке x', когда все координатные функции на W_1 рассматриваются как формальные степенные ряды с коэффициентами в $\overline{k(\varepsilon_2)}$ относительно линейных многочленов $X_{s+1} - X_{s+1}(x')$, $\dots, X_r - X_r(x')$, $L_{r+1} - L_{r+1}(x'), \dots, L_n - L_n(x')$. Следовательно, ср. доказательство Леммы 8 ниже и Леммы 9 из [7], система (7) с дополнительными уравнениями

$$L_i(X_1 - Y_1, \dots, X_n - Y_n) = 0, \quad r+2 \leqslant i \leqslant n,$$

имеет решение (9). Лемма доказана.

Следствие 2. *При условиях Леммы 6, если система (7) имеет решение, то можно построить решение (9) этой системы и вычислить i_0 за полиномиальное время от d^n и длины записи входных данных. Так что мы будем предполагать, как и прежде, без ограничения общности, что $i_0 = r+1$. Тогда справедливо равенство (10).*

Доказательство. Достаточно проверить, что можно вычислить i_0. Применяя Лемму 4 к точке x' и морфизму ϕ, заданному линейными формами $X_1, \dots, X_r, L_{r+1}, \dots, L_n$, построим касательное пространство T_{x',W_1}, и затем i_0 может быть вычислено немедленно. Следствие доказано.

Теперь мы можем описать алгоритм, который требуется построить в теореме Теореме 5. Обозначим через W_1 единственную неприводимую компоненту многообразия V_s, такую что $x \in W_1$. Положим $z_s = x = (0, \dots, 0)$. Применяя Лемму 4, построим касательное пространство T_{z_s,W_1}. Затем построим линейные формы $D_i^{(s)}$, $s+1 \leqslant i \leqslant n$, с длинами записей целых коэффициентов $O(n \log d)$, такие что

$$T_{z_s,W_1} \cap \mathcal{Z}(D_{s+1}^{(s)}, \dots, D_n^{(s)}) = \{0\}.$$

Положим $a_i^{(s)} = 0$, $s+1 \leqslant i \leqslant n$.

Пусть $s \leqslant r \leqslant n-1$, и мы уже построили рекурсивно точку $z_r \in W_1$, которая является гладкой точкой многообразия V, линейные формы $D_i^{(r)}$, $s+1 \leqslant i \leqslant n$, с длинами записей целых коэффициентов $O(n \log d)$ и целые числа $a_i^{(r)}$, $s+1 \leqslant i \leqslant n$, с длинами записи $O(n \log d)$, такие что $D_i^{(r)} = X_i$ для всех $s+1 \leqslant i \leqslant r$, точка z_r является изолированной в алгебраическом многообразии

$$\mathcal{Z}(g_0, \dots, g_m, D_{s+1}^{(r)} - a_{s+1}^{(r)}, \dots, D_n^{(r)} - a_n^{(r)}) \subset \mathbb{A}^n(\overline{k}),$$

и пересечение

$$T_{z_r, W_1} \cap \mathcal{Z}(D_{s+1}^{(r)}, \dots, D_n^{(r)}) = \{0\}.$$

База рекурсии есть $r = s$. Мы будем ссылаться на эту рекурсию как на первую. Теперь мы опишем следующий шаг этой рекурсии, т.е. наша цель – построить точку z_{r+1}, линейные формы $D_i^{(r+1)}$ и целые числа $a_i^{(r+1)}$, $s+1 \leqslant i \leqslant n$.

Используя Лемму 6 для $\xi = z_r$, мы выясним верно ли, что $X_{s+1}, \dots, X_{r+1}$ алгебраически независимы в поле рациональных функций $\overline{k}(W_1)$ алгебраического многообразия W_1.

В случае, когда $X_{s+1}, \dots, X_{r+1}$ алгебраически зависимы над полем $\overline{k}$ в поле рациональных функциях $\overline{k}(W_1)$, координатные функции $X_{s+1}, \dots, X_n$ также алгебраически зависимы в этом поле, и описываемый алгоритм заканчивает свою работа.

В случае, когда $X_{s+1}, \dots, X_{r+1}$ являются алгебраически независимыми, мы применяем Следствие 2, строим точку (x', y') (она зависит от r), которая является решением (9) системы (7) с $\xi = z_r$, и вычисляем i_0. Определим семейство $D_i^{(r+1)}$, $r+2 \leqslant i \leqslant n$, равным семейству $D_i^{(r)}$, $r+1 \leqslant i \leqslant n$, $i \neq i_0$. Мы будем предполагать без ограничения общности, что $i_0 = r+1$. Затем положим $D_i^{(r+1)} = D_i^{(r)}$, $r+2 \leqslant i \leqslant n$, и $D_i^{(r+1)} = X_i$ для всех $s+1 \leqslant i \leqslant r+1$.

Покажем, как построить требуемые целые числа $a_i^{(r+1)}$, $s+1 \leqslant i \leqslant n$ и точку z_{r+1}. Положим $b_i = D_i^{(r+1)}(x')$, $s+1 \leqslant i \leqslant n$. Положим $z'_s = x'$. Предположим, что $s \leqslant j \leqslant n-1$, и что мы уже построили рекурсивно целое число $a_i^{(r+1)}$, $s+1 \leqslant i \leqslant j$ с длиной записи $O(n \log d)$, и $z'_j \in W_1$, которая является гладкой точкой многообразия V и, такой что

$$z'_j \in V^{(j)} = \mathcal{Z}(g_0, \dots, g_m, D_{s+1}^{(r+1)} - a_{s+1}^{(r+1)}, \dots, D_j^{(r+1)} - a_j^{(r+1)},$$
$$D_{j+1}^{(r+1)} - b_{j+1}, \dots, D_n^{(r+1)} - b_n) \subset \mathbb{A}^n(\overline{k}),$$

и пересечение

$$T_{z'_j,W_1} \cap \mathcal{Z}(D_{s+1}^{(r+1)},\dots,D_n^{(r+1)}) = \{0\}. \tag{11}$$

Отметим, что (11) влечет, что z'_j – изолированная точка алгебраического многообразия $V^{(j)}$.

База рекурсии есть $j = s$. Мы будем ссылаться на эту рекурсию как на вторую. Теперь мы опишем следующий шаг этой рекурсии, т.е. наша цель – построить точку z'_{j+1} и целое число $a_{j+1}^{(r+1)}$.

Поскольку z'_j – гладкая точка многообразия V, алгебраическое многообразие

$$\mathcal{Z}(g_0,\dots,g_m, D_{s+1}^{(r+1)} - a_{s+1}^{(r+1)},\dots,D_j^{(r+1)} - a_j^{(r+1)},$$
$$D_{j+2}^{(r+1)} - b_{j+2},\dots,D_n^{(r+1)} - b_n) \subset \mathbb{A}^n(\overline{k})$$

содержит единственную неприводимую компоненту C'_j, такую что точка $z'_j \in C'_j$. Компонента C'_j является кривой, и степень $\deg C'_j$ ограничена сверху многочленом от d^s по неравенству Безу. Построим общую точку C'_j и систему полиномиальных уравнений, задающую кривую C'_j, используя алгоритм из [3]. Существует, см. напр. [9], семейство $\psi_1,\dots,\psi_s$ локальных параметров алгебраического многообразия W_1 в точке z'_j со степенями полиномиальными от d^s. Следовательно, по (11) кривая C'_j содержит только полиномиальное от d^n число точек z'' многообразия V, таких что не выполнено равенство

$$T_{z'',V} \cap \mathcal{Z}(D_{s+1}^{(r+1)},\dots,D_n^{(r+1)}) = \{0\}. \tag{12}$$

В частности кривая C'_j содержит только полиномиальное от d^n число особых точек V. Для заданной точки $z'' \in C'_j$ можно вычислить, применяя алгоритм Теоремы 3 из Раздела 4 и Раздела 6, все кратности $\mu(z'', V_i)$, $0 \leqslant i \leqslant n$, за полиномиальное время от d^n и длины записи входных данных, включая длину записи точки z'' (алгоритм из Раздела 4 и Раздела 6 не использует описываемый алгоритм). Теперь z'' – гладкая точка многообразия V тогда и только тогда, когда $\mu(z'', V_s) = 1$ и $\mu(z'', V_u) = 0$ для всех $u \neq s$.

Алгоритм из Раздела 4 и Раздела 6 также позволяет построить для $z'' \in W_1$, которая является гладкой точкой V, семейство линейных форм $\phi_{s+1}, \dots, \phi_n$ от $X_1, \dots, X_n$ с длинами записей целых коэффициентов $O(n \log d)$, таких что

$$T_{z'', W_1} \cap \mathcal{Z}(\phi_{s+1}, \dots, \phi_n) = \{0\}$$

(касательное пространство гладкой точки совпадает с касательным конусом в этой точке). Следовательно, мы можем применить Лемму 4 и построить касательное пространство T_{z'', W_1}. Таким образом, можно выяснить для заданной точки $z'' \in C'_j$ верно ли, что выполняется (12) за полиномиальное время от d^n и длины записи входных данных, включая длину записи точки z''.

Теперь будем перебирать целые числа $a = 0, 1, \dots$. Построим, ср. [7] шаг (16), пересечение

$$B_j = C'_j \cap \mathcal{Z}(D^{(r+1)}_{j+1} - a) \subset \mathbb{A}^n(\overline{k}).$$

Если B_j бесконечно, то мы переходим к следующему значению a.

Если B_j конечно, то будем перебирать точки $z'' \in B_j$. Для рассматриваемой точки z'' выясним, выполняется ли (12). Если равенство (12) не выполняется, то мы переходим к следующему элементу $z'' \in B_j$. Если все элементы из B_j перебраны, то мы переходим к следующему значению a. Если равенство (12) выполняется, то положим $a^{(r+1)}_{j+1} = a$ и $z'_{j+1} = z''$.

Таким образом, согласно предыдущим рассмотрениям мы построим требуемую z'_{j+1} и целое число $a^{(r+1)}_{j+1}$ с длиной записи $O(n \log d)$.

Если $j < n-1$, то заменим j на $j+1$ и перейдем к следующему шагу второй рекурсии. Если $j = n-1$, то положим $z_{r+1} = z'_{j+1}$ и, если $r < n-1$, заменим r на $r+1$ и перейдем к следующему шагу первой рекурсии. Если $j = n-1$ и $r = n-1$, алгоритм завершает свою работу.

Таким образом, мы выясним в конечном счете верно ли, что семейство $X_{s+1}, \dots, X_n$ алгебраически независимо в поле $\overline{k}(W_1)$. Оценка для времени работы описанного алгоритма следует немедленно из оценок для времени работы примененных алгоритмов. Теорема 5 доказана.

4. Вычисление кратности точки

Цель этого и следующих разделов доказать Теорему 3. Рассмотрим алгебраическое многообразие V, такое как во Введении и точку x. Обозначим через $\mathrm{con}(x, V)$ касательный конус многообразия V в точке x. Если x не является изолированной точкой V, то $\mathrm{con}(x, V)$ состоит по определению из всех прямых, содержащих точку x, которые являются пределами секущих многообразия V, содержащих x, когда другая точка пересечения секущей с V стремится к x (вырожденный случай, когда прямая l является, такой что $x \in l \subset V$ не исключается: в этом случае прямая $l \subset \mathrm{con}(x, V)$). Строго говоря, это определение справедливо для случая, когда основное поле – $\mathbb{C}$. Другое определение $\mathrm{con}(x, V)$ справедливо для произвольных полей (и в случае, когда x – произвольная необязательно изолированная точка V или даже, когда $x \notin V$). Конус определяется как многообразие нулей идеала, порожденного формами наименьшей степени элементов идеала исходного многообразия в случае, когда оно аффинное, и точка x имеет нулевые координаты, см. чуть ниже. Фактически, если использовать второе определение, то во многих случаях можно придать смысл первому.

Мы можем осуществить линейный автоморфизм пространства $\mathbb{P}^n(\overline{k})$ и будем предполагать без ограничения общности (может быть, заменяя основное поле k), что $x = (1 : 0 : \ldots : 0)$. Мы будем использовать следующее определение касательного конуса $\mathrm{con}(x, V)$. Отождествим $\mathbb{A}^n(\overline{k}) = \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(X_0)$. Пусть $X_1, \ldots, X_n$ – координатные функции в $\mathbb{A}^n(\overline{k})$, соответствующие $X_1/X_0, \ldots, X_n/X_0$ в $\mathbb{P}^n(\overline{k})$. Обозначим $U = V \setminus \mathcal{Z}(X_0) \subset \mathbb{A}^n(\overline{k})$. Пусть $I(U) \subset k[X_1, \ldots, X_n]$ – идеал аффинного алгебраического многообразия U. Всякий ненулевой элемент $F \in k[X_1, \ldots, X_n]$ представляется как сумма $F = F_r + F_{r+1} + \ldots + F_m$ однородных относительно $X_1, \ldots, X_n$ многочленов F_j, таких что $\deg F_j = j$, и $F_r \neq 0$. Таким образом для всякого ненулевого элемента $F \in k[X_1, \ldots, X_n]$ определена форма наименьшей степени $F_r \neq 0$. Определим также форму наименьшей степени нулевого многочлена равной нулю. Обозначим через $I'(U)$ (соответственно $I'(V)$) идеал кольца $k[X_1, \ldots, X_n]$ (соответственно $k[X_0, \ldots, X_n]$), порожденный формами наименьшей степени элементов $I(U)$. Тогда $\mathrm{con}(x, U)$ (соответственно $\mathrm{con}(x, V)$) есть множество нулей идеала $I'(U)$ в $\mathbb{A}^n(\overline{k})$ (соответственно $I'(V)$ в $\mathbb{P}^n(\overline{k})$). Другие определения касательного конуса, доказательство эквивалентности определения касательного конуса с секущими и того, которым мы пользуемся, см. в [11, 17] и Лемме 7 ниже.

Теперь пусть $x = (0,\ldots,0) = (1:0:\ldots:0)$, и Z – новая переменная. Введем многообразие секущих $\sec(x,U) \subset (\mathbb{A}^n \times \mathbb{A}^1)(\overline{k})$ многообразия U следующим образом. Пусть I_1 – идеал $k[X_1\ldots,X_n,Z]$, порожденный всеми многочленами $p(ZX_1,\ldots,ZX_n)$ для всех $p \in I(U)$. Тогда $\sec(x,U)$ является объединением всех компонент U_1 многообразия нулей идеала I_1 в $(\mathbb{A}^n \times \mathbb{A}^1)(\overline{k})$, таких что $U_1 \not\subset \mathcal{Z}(Z)$.

Лемма 7. *Справедливо равенство* $\mathrm{con}(x,U) = \sec(x,U) \cap \mathcal{Z}(Z)$. *Если* $x \in U$, *то размерность в точке* $\dim_x U = \dim \mathrm{con}(x,U)$.

Доказательство. Если x является изолированной точкой U или $x \notin U$, то доказательство – непосредственное. Так что мы будем предполагать, что x не является изолированной точкой U. Мы имеем изоморфизм алгебраических многообразий

$$\begin{aligned} &U \times (\mathbb{A}^1 \setminus \{0\}) \simeq \sec(x,U) \setminus \mathcal{Z}(Z), \\ &((X_1,\ldots,X_n),Z) \mapsto ((X_1/Z,\ldots,X_n/Z),Z), \end{aligned} \tag{13}$$

который индуцирует изоморфизм колец регулярных функций

$$\begin{aligned} \overline{k}[X_1,\ldots,X_n]/I(U) \otimes_{\overline{k}} \overline{k}[Z,Z^{-1}] \simeq \\ \simeq \overline{k}[Z,Z^{-1}] \otimes_{\overline{k}[Z]} \overline{k}[X_1,\ldots,X_n,Z]/I_1. \end{aligned}$$

Пусть многочлен F обращается в нуль тождественно на $\mathrm{con}(x,U)$. Тогда F^a – форма наименьшей степени некоторого многочлена $F_1 \in I(U)$ для некоторого целого числа $a \geqslant 1$. Следовательно, $F^a = F_1(ZX_1,\ldots,ZX_n)/Z^{a \deg F} + ZF_2$ для некоторого многочлена F_2. Поэтому F обращается в нуль тождественно на $\sec(x,U) \cap \mathcal{Z}(Z)$. Обратно, пусть многочлен $F \in \overline{k}[X_1,\ldots,X_n,Z]$. Покажем, что F может быть единственным образом представлен в виде

$$F = \sum_{i \in J} Z^i F_i(ZX_1,\ldots,ZX_n), \tag{14}$$

где $F_i \in \overline{k}[X_1,\ldots,X_n]$, $Z^iF_i(ZX_1,\ldots,ZX_n) \in \overline{k}[X_1,\ldots,X_n,Z]$, и $J \subset \mathbb{Z}$ – конечное множество. Достаточно проверить, (14) для мономов, и этот случай доказывается непосредственно. Заметим, что (14) индуцирует градуировку на алгебре $\overline{k}[X_1,\ldots,X_n,Z]$, такую что $Z^iF_i(ZX_1,\ldots,ZX_n)$ является градуированной компонентой F степени i. Поскольку I_1 имеет систему однородных образующих степени 0 относительно этой градуировки, то идеал I_1

является градуированным идеалом относительно рассматриваемой градуировки. Если F обращается в нуль тождественно на $\sec(x, U)$, то $Z^b F \in I_1$ для некоторого целого числа $b \geqslant 1$. Так как однородные компоненты элемента градуированного идеала принадлежат этому идеалу, то $Z^{b+i} F_i(ZX_1, \dots, ZX_n) \in I_1$. Поскольку Z не обращается в нуль тождественно на всякой компоненте $\sec(x, U)$, то многочлены $F_i(ZX_1, \dots, ZX_n)$ обращаются в нуль тождественно на $\sec(x, U)$ для всех $i \in J$. Следовательно, $F_i \in I(U)$, $i \in J$, так как мы имеем сюръективную проекцию

$$\sec(x, U) \setminus \mathcal{Z}(Z) \to U \setminus \{x\},\ (X_1, \dots, X_n, Z) \mapsto (ZX_1, \dots, ZX_n),$$

и $U \setminus \{x\}$ является плотным подмножеством U в топологии Зарисского, в силу того, что x – не изолированная точка U. Положим $J_1 = \{i \in J : Z^i F_i(ZX_1, \dots, ZX_n)|_{Z=0} \neq 0\}$. Тогда $\sum_{i \in J_1} Z^i F_i(ZX_1, \dots, ZX_n)|_{Z=0}$ принадлежит идеалу, порожденному формами наименьшей степени идеала $I(U)$. Теперь предположим, что многочлен G обращается в нуль тождественно на $\sec(x, U) \cap \mathcal{Z}(Z)$. Тогда существует многочлен G_1 и целое число $a \geqslant 1$, такие что $F = G^a + ZG_1$ обращается в нуль тождественно на $\sec(x, U)$. Следовательно, $G^a = \sum_{i \in I_1} Z^i F_i(ZX_1, \dots, ZX_n)|_{Z=0}$ обращается в нуль тождественно на $\operatorname{con}(x, U)$. Поэтому G также обращается в нуль тождественно на $\operatorname{con}(x, U)$. Первое утверждение леммы доказано.

Заметим, что (13) влечет, что $\dim \sec(x, U) = 1 + \dim U$. Согласно (13) для всяких алгебраических многообразий U_1 и U_2 справедливо равенство $\sec(x, U_1 \cup U_2) = \sec(x, U_1) \cup \sec(x, U_2)$. Следовательно, для того, чтобы доказать последнее утверждение, мы можем предполагать без ограничения общности, что U неприводимо, и $x \in U$. Тогда (13) влечет, что $(x, 0) \in \sec(x, U)$. Таким образом, $\sec(x, U)$ имеет непустое пересечение с $\mathcal{Z}(Z)$. Следовательно, $\dim \operatorname{con}(x, U) = \dim_x U$. Лемма доказана.

Фактически эквивалентность определения касательного конуса с секущими и второго с идеалом форм наименьшей степени следует из доказанной леммы.

Рассмотрим подробно случай, когда V – кривая. Нам потребуется следующее определение. Пусть даны алгебраическая кривая $V \subset \mathbb{P}^n(\overline{k})$, и ее ветвь V^* в точке $x = (1 : 0 : \ldots : 0)$ с униформизующим элементом τ, т.е. мы имеем представления координатных функций многообразия V как формальных степенных рядов

$$(X_i/X_0)|_V = \gamma_{i,m}\tau^m + \sum_{m<j\in\mathbb{Z}} \gamma_{i,j}\tau^j, \quad 1 \leqslant i \leqslant n,$$

где $\gamma_{i,j} \in \overline{k}$ для всех $1 \leqslant i \leqslant n, 0 < m \in \mathbb{Z}$, и $(\gamma_{1,m}, \dots, \gamma_{n,m}) \neq (0, \dots, 0)$. Тогда касательная прямая l к этой ветви есть замыкание в $\mathbb{P}^n$ аффинной прямой l', определенной формулой

$$l' = \{(\gamma_{1,m}t, \dots, \gamma_{n,m}t) \,:\, t \in \overline{k}\}.$$

Заметим, что l не зависит от выбора униформизующего элемента τ. Оказывается, что $\mathrm{con}(x, V) = \cup_{i\in I} l_i$ – объединение всех касательных прямых l_i ко всем ветвям кривой V, содержащим точку $x = (1 : 0 : \dots : 0)$.

Теперь мы переходим к описанию алгоритма для вычисления кратности точки алгебраического многообразия. Мы будем использовать конструкцию из [7] и обозначения W_s, W_s', W_s'', $h_1, \dots h_s$, $L_{s+1}^{(s)}, \dots, L_n^{(s)}$ для $1 \leqslant s \leqslant n-1$, и $W^{(1)}$, см. Раздел 2. Напомним,что $W^{(1)}$ является объединением всех компонент U_1 многообразия W_s', таких что $U_1 \cap \mathcal{Z}(h_{s+1}) \neq U_1$. Следовательно, V_{s+1} – объединение некоторых компонент пересечения $W^{(1)} \cap \mathcal{Z}(h_{s+1})$.

Если $s = 0$, положим $W_s' = W^{(1)} = \mathbb{P}^n(\overline{k})$, $W_s'' = \emptyset$ и $L_n^{(s)} = X_j$ для $1 \leqslant j \leqslant n$. Так что мы можем предполагать далее, что $0 \leqslant s \leqslant n-1$. Наша цель – вычислить кратность $\mu(x, V_{s+1})$ для $0 \leqslant s \leqslant n-2$. Случай $s = n-1$ – тривиальный, так как в этом случае V_{s+1} состоит из точек. Далее, выясним, используя алгоритм из Раздела 3, верно ли, что $x \in V_{s+1}$. Если $x \notin V_{s+1}$, то $\mu(x, V_{s+1}) = 0$. Поэтому в дальнейшем мы будем предполагать без ограничения общности, что $x \in V_{s+1}$.

Покажем, что если даны линейные формы $D_{s+2}, \dots, D_n$ от $X_0, \dots, X_n$ с коэффициентами из расширения k_1 поля k, такие что $W^{(4)} = W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(D_{s+2}, \dots, D_n)$ является конечным множеством в $\mathbb{P}^n(\overline{k_1})$, то можно построить за полиномиальное время от длины записи входных данных и d^{s+1} все точки из этого конечного множества. Действительно, если $W^{(4)}$ конечно, то конструкция из [7] немедленно влечет, что $W^{(1)} \cap \mathcal{Z}(D_{s+2}, \dots, D_n)$ является объединением всех неприводимых компонент C размерности один многообразия $\mathcal{Z}(h_1, \dots, h_s, D_{s+2}, \dots, D_n)$, таких что h_{s+1} не равен тождественно нулю на C. Используя алгоритм из

[3], построим общие точки и системы полиномиальных уравнений, задающие все такие кривые C и, может быть некоторые дополнительные кривые C', которые содержатся в компонентах размерности больше, чем один, алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_s, D_{s+2}, \ldots, D_n)$. Время работы алгоритма для построения всех этих кривых полиномиально от d^n и длины записи входных данных. Заметим, что h_{s+1} равен нулю тождественно на всякой C'. Следовательно, мы можем выбрать требуемые кривые C среди построенных.

Теперь объединение всех пересечений $C \cap \mathcal{Z}(h_{s+1})$ и есть требуемое множество $W^{(4)}$. Следовательно, достаточно построить все пересечения $C \cap \mathcal{Z}(h_{s+1})$. Алгоритм для этого, использующий разложения Ньютона–Пюизе, в случае, когда h_{s+1} – линейная форма, описан в [7, 6]. Общий случай может быть сведен к этому следующим образом. Пусть ξ – построенная общая точка C, и $k_1(\xi)$ – поле, порожденное координатами ξ. Следовательно, согласно [3] ξ – алгебраическая над полем $k_1(t)$, где $t = D'/D''$ является рациональной функцией на C, которая равна частному двух линейных форм D' и D'' с коэффициентами из k, и степень $[k_1(\xi) : k_1(t)]$ ограничена сверху полиномом от d^{s+1}. Существуют самое большее $\mathcal{P}(d^{s+1})$ (для некоторого полинома $\mathcal{P}$) значений t из $\overline{k_1}$, в которых специализации точки ξ не определены. Множество этих значений включается в множество корней многочлена $F_1 \in k_1[t]$, который известен, когда построена общая точка. При этом $\deg_t F_1 \leqslant \mathcal{P}(d^{s+1})$. Пусть $N_{k_1(\xi)/k_1(t)}$ обозначает норму из поля $k_1(\xi)$ в поле $k_1(t)$. Вычислим $N_{k_1(\xi)/k_1(t)}(h_{s+1}(\xi)) = F_2/F_3$, где $F_2, F_3 \in k_1[t]$, и $\deg_t F_2 \leqslant \mathcal{P}(d^{s+1})$, $\deg_t F_1 \leqslant \mathcal{P}(d^{s+1})$. Тогда множество значений из k_1, которые может принимать t на $C \cap \mathcal{Z}(h_{s+1})$ включается в множество корней многочлена $F = F_1F_2F_3$. Построим все корни y этого многочлена и множество T_1 всех точек из пересечения $C \cap \mathcal{Z}(D' - D''y)$ а также $C \cap \mathcal{Z}(D'')$. Затем построим множество T_2 всех точек $z \in T_1$, таких что $h_{s+1}(z) = 0$. Таким образом, мы получим требуемое множество $C \cap \mathcal{Z}(h_{s+1}) = T_2$.

В [7] построены линейные формы $L_{s+2}^{(s+1)}, \ldots, L_n^{(s+1)}$ с целыми коэффициентами с длиной записи $O(n \log d)$. Из [7] следует, что для всякой неприводимой компоненты U_1 многообразия W'_s с $U_1 \cap \mathcal{Z}(h_{s+1}) \neq U_1$, множество

$$U_1 \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}^{(s+1)}, \ldots, L_n^{(s+1)})$$

является конечным подмножеством в $\mathbb{P}^n(\overline{k})$. Построим все точки множества

$$W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)}).$$

Построим линейную форму L_0'' с целыми коэффициентами с длиной записи $O(n \log d)$, которая не обращается в нуль ни в какой точке множества $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)})$ и в точке x. Поэтому $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_0'', L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)}) = \emptyset$.

Положим $L_j = L_j^{(s+1)} - (L_j^{(s+1)}/L_0'')(x)L_0''$ для всех $s+2 \leqslant j \leqslant n$ и $L_0 = L_0''$. Тогда $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}, \dots, L_n)$ – конечное множество, содержащее x, и $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_0, L_{s+2}, \dots, L_n) = \emptyset$. Кроме того, $L_{s+2}, \dots, L_n$ – линейные формы относительно $X_1, \dots, X_n$, так как $x = (1 : 0 : \dots : 0)$.

Положим $V' = W^{(1)} \cap \mathcal{Z}(h_{s+1})$ и $U' = V' \setminus \mathcal{Z}(X_0) \subset \mathbb{A}^n(\overline{k})$. Следовательно, размерность всякой неприводимой компоненты многообразия V' равна $n - s - 1$, и $x \in V'$.

Наша цель теперь – построить семейство линейных форм $M_0, M_{s+2}, M_{s+3}, \dots, M_n$ с коэффициентами из $\mathbb{Z}$ с длиной записи $O(n \log d)$, таких что $M_0 = L_0$, формы $M_{s+2}, \dots, M_n \in k[X_1, \dots, X_n]$, и

$$V' \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \dots, M_n) = \emptyset,$$
$$\operatorname{con}(x, V') \cap \mathcal{Z}(M_0, M_{s+2}, \dots, M_n) = \emptyset$$

в $\mathbb{P}^n(\overline{k})$.

Как и в Разделе 2, построим вещественную структуру для поля k, см. [6, 7], которая индуцирует некоторую вещественную структуру на $\overline{k}$. Пусть $\varepsilon_i > 0$ – бесконечно малая величина относительно поля $k(\varepsilon_0, \dots, \varepsilon_{i-1})$, $0 \leqslant i \leqslant 2$, и поле $K_2 = k(\varepsilon_0, \varepsilon_1, \varepsilon_2)$.

Если $z \in \overline{k(\varepsilon_0, \dots, \varepsilon_i)}$, $0 \leqslant i \leqslant 2$, – не бесконечно большой относительно поля $\overline{k(\varepsilon_0, \dots, \varepsilon_{i-1})}$, то определена стандартная часть $\mathrm{st}_{\varepsilon_i}(z) \in \overline{k(\varepsilon_0, \dots, \varepsilon_{i-1})}$, см. [7], Если $z = (z_1, \dots z_n) \in \mathbb{A}^n(\overline{k(\varepsilon_0, \dots, \varepsilon_i)})$, и все стандартные части $\mathrm{st}_{\varepsilon_i}(z_j)$, $1 \leqslant j \leqslant n$ определены, то положим

$$\mathrm{st}_{\varepsilon_i}(z) = (\mathrm{st}_{\varepsilon_i}(z_1), \dots, \mathrm{st}_{\varepsilon_i}(z_n)) \in \mathbb{A}^n(\overline{k(\varepsilon_0, \dots, \varepsilon_{i-1})}).$$

Кроме того, определены отображения стандартных частей

$$\mathrm{st}_{\varepsilon_i} : \mathbb{P}^n(\overline{k(\varepsilon_0, \dots, \varepsilon_i)}) \longrightarrow \mathbb{P}^n(\overline{k(\varepsilon_0, \dots, \varepsilon_{i-1})}),$$

см. [7], для $i = 0, 1, 2$.

Обозначим $L = \mathcal{Z}(L_{s+2}, \dots, L_n) \subset \mathbb{A}^n(\overline{k})$, где $\mathbb{A}^n$ имеет координатные функции $X_1, \dots, X_n$. Рассмотрим следующую систему уравнений и неравенств с коэффициентами из поля K_2 относительно $X_1 \dots, X_n, Y_1 \dots, Y_n, Z_1, \dots, Z_n, Z$

$$\begin{cases} h_i(1, Z_1, \dots, Z_n) = 0, & 1 \leqslant i \leqslant s, \\ h_{s+1}(1, Z_1, \dots, Z_n)Z - 1 = 0, & \\ h_i(1, X_1, \dots, X_n) = 0, & 1 \leqslant i \leqslant s+1, \\ \sum_{1 \leqslant i \leqslant n} |X_i - Z_i|^2 \leqslant \varepsilon_2, & \\ \sum_{1 \leqslant i \leqslant n} |X_i|^2 = \varepsilon_1^2, & \\ L_j(Y_1, \dots, Y_n) = 0, & s+2 \leqslant j \leqslant n, \\ \sum_{1 \leqslant i \leqslant n} |X_i - Y_i|^2 < \varepsilon_0 \varepsilon_1^2. & \end{cases} \tag{15}$$

Лемма 8. *Пусть семейство $L_0, L_{s+2}, L_{s+3}, \dots, L_n$ линейных форм – такое же, как и выше. Следующие условия эквивалентны:*

(i) $\mathrm{con}(x, V') \cap \mathcal{Z}(L_0, L_{s+2}, L_{s+3}, \dots, L_n) = \emptyset$ *в* $\mathbb{P}^n(\overline{k})$

(ii) $\mathrm{con}(x, U') \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \dots, L_n) = \{x\}$ *в* $\mathbb{A}^n(\overline{k})$

(iii) *система (15) не имеет решений в* $\mathbb{A}^{3n+1}(\overline{K_2})$.

Доказательство. Эквивалентность (i) и (ii) доказывается непосредственно.

Предположим, что существует решение

$$(x_1^*, \dots, x_n^*, y_1^*, \dots, y_n^*, z_1^*, \dots, z_n^*, z') \in \mathbb{A}^{3n+1}(\overline{K_2})$$

системы (15). Обозначим $x^* = (x_1^*, \dots, x_n^*)$ и $y^* = (y_1^*, \dots, y_n^*)$. Мы имеем

$$\begin{aligned} h_i(1, z_1^* \dots, z_n^*) &= 0, \quad 1 \leqslant i \leqslant s, \\ h_{s+1}(1, z_1^* \dots, z_n^*) &\neq 0, \\ h_i(1, x_1^* \dots, x_n^*) &= 0, \quad 1 \leqslant i \leqslant s+1, \\ \sum_{1 \leqslant i \leqslant n} |x_i^* - z_i^*|^2 &\leqslant \varepsilon_2, \end{aligned}$$

Следовательно, $\sum_{1 \leqslant i \leqslant n} |\mathrm{st}_{\varepsilon_2} x_i^* - z_i^*|^2$ – бесконечно малая относительно поля $k(\varepsilon_0, \varepsilon_1)$. Точка $\mathrm{st}_{\varepsilon_2} x^*$ определена над полем $\overline{k(\varepsilon_0, \varepsilon_1)}$. Следовательно, многочлены $h_1, \dots, h_s$ обращаются в нуль в точке $\mathrm{st}_{\varepsilon_2} x^*$. Многочлен h_{s+1} не обращается в нуль в точке x^*, которая бесконечно близка к $\mathrm{st}_{\varepsilon_2} x^*$. Таким образом, $\mathrm{st}_{\varepsilon_2} x^* \in U'$, ср. также

[7] доказательство Леммы 13. Следовательно, прямая (стандартные части рассматриваются здесь в $\mathbb{A}^n$)

$$l = \{(\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(\mathrm{st}_{\varepsilon_2} y^*/\varepsilon_1)t \,:\, t \in \overline{k}\} \subset \mathrm{con}(x, U') \cap \mathcal{Z}(L_{s+2}, \ldots, L_n),$$

так как l есть множество нулей соответствующего идеала форм наименьшей степени.

Обратно, предположим, что существует прямая $l \subset \mathrm{con}(x, U') \cap \mathcal{Z}(L_{s+2}, \ldots, L_n)$, $x \in l$. Выберем точку $x \neq (l_1, \ldots, l_n) \in l \subset \mathbb{A}^n(\overline{k})$. Тогда существует алгебраическая кривая $C \subset \sec(x, U')$, такая что $\{(l_1, \ldots, l_n)\}$ является компонентой пересечения $C \cap \mathcal{Z}(Z)$. Следовательно, существует ветвь C^* кривой C в точке $(l_1, \ldots, l_n)$ с униформизующим элементом τ, такая что соответствующие представления координатных функций на C как формальных степенных рядов имеют вид

$$Z|_C = z_m\tau^m + \sum_{m<j\in\mathbb{Z}} z_j\tau^j,$$
$$X_i|_C = l_i + \sum_{0<j\in\mathbb{Z}} x_{i,j}\tau^j, \quad 1 \leqslant i \leqslant n,$$

где $0 < m \in \mathbb{Z}$, $z_j, x_{i,j} \in \overline{k}$ для всех j, $z_m \neq 0$. Рассмотрим неприводимую алгебраическую кривую C_1, которая имеет ветвь C_1^* в точке x с униформизующим элементом τ, такую что

$$X_i|_{C_1} = (z_m\tau^m + \sum_{m<j\in\mathbb{Z}} z_j\tau^j)(l_i + \sum_{0<j\in\mathbb{Z}} x_{i,j}\tau^j), \quad 1 \leqslant i \leqslant n.$$

Тогда C_1 содержится в U' и имеет касательную прямую l. Выберем новый униформизующий элемент τ_1 ветви C_1^*, такой что $\tau_1 \in \overline{k}(C_1)$, где $\overline{k}(C_1)$ – поле рациональных функций на C_1. Так что мы имеем

$$X_i|_{C_1} = w_{i,m}\tau_1^m + \sum_{m<j\in\mathbb{Z}} w_{i,j}\tau_1^j, \quad 1 \leqslant i \leqslant n,$$

где $w_{i,j} \in \overline{k}$ для всех j, и $x \neq (w_{1,m}, \ldots, w_{n,m}) \in l$. Обозначим $X_i|_{C_1} = w_i$ для $1 \leqslant i \leqslant n$. Следовательно, $(w_1, \ldots, w_n) \in C_1$ в $\mathbb{A}^n(\overline{k((\tau_1))})$, где $k((\tau_1))$ – поле формальных степенных рядов от τ_1, и $(w_1, \ldots, w_n)$ соответствует вложению $\overline{k}[C_1] \hookrightarrow \overline{k}[[\tau_1]]$, где $\overline{k}[C_1]$ – кольцо регулярных функций на C_1, и $\overline{k}[[\tau_1]]$ – кольцо формальных степенных рядов от τ_1.

Пусть вещественная структура поля $\overline{k}$ задана изоморфизмом $\overline{k} \simeq \widetilde{K}[\sqrt{-1}]$, где $\widetilde{K}$ – вещественно замкнутое поле. По определению вещественная структура на поле $\overline{k(\varepsilon_1)}$ индуцирована вещественной структурой на поле формальных степенных рядов от ε_1 с коэффициентами из $\overline{k}$. Вещественные элементы из этого поля суть дробно–степенные ряды с коэффициентами из $\widetilde{K}$.

Покажем, что существует точка $x^* \in C_1$ из $\mathbb{A}^n(\overline{k(\varepsilon_1)})$, такая что $|x^*|^2 = \varepsilon_1^2$, и $x \neq \mathrm{st}_{\varepsilon_1}(x^*/\varepsilon_1) \in l$. Кроме того, эта точка x^* будет определена сквозным гомоморфизмом

$$\overline{k}[C_1] \hookrightarrow \overline{k}[[\tau_1]] \to \overline{k}[[\varepsilon_1^{1/m}]],$$

таким что $\tau_1 \mapsto \tau^* \in \widetilde{K}[[\varepsilon_1^{1/m}]]$. Здесь $\overline{k}[[\varepsilon_1^{1/m}]]$ – кольцо формальных степенных рядов от $\varepsilon_1^{1/m}$.

Для того, чтобы доказать это утверждение, представим $w_{i,j} = u_{i,j} + \sqrt{-1}v_{i,j}$, где $u_{i,j}, v_{i,j} \in \widetilde{K}$ для всех i, j. Положим

$$u_i = u_{i,m}\tau_1^m + \sum_{m<j\in\mathbb{Z}} u_{i,j}\tau_1^j,\ v_i = v_{i,m}\tau_1^m + \sum_{m<j\in\mathbb{Z}} v_{i,j}\tau_1^j,\ 1 \leqslant i \leqslant n.$$

Так что $w_i = u_i + \sqrt{-1}v_i$ для $1 \leqslant i \leqslant n$.

Функции w_i – алгебраические над полем $\overline{k}(\tau_1)$ и, следовательно, они – алгебраические над полем $\widetilde{K}(\tau_1)$ для $1 \leqslant i \leqslant n$. Мы имеем вложение $\overline{k}[C_1] \hookrightarrow \widetilde{K}[\sqrt{-1}]((\tau_1))$ кольца $\overline{k}[C_1]$ в поле формальных степенных рядов $\widetilde{K}[\sqrt{-1}]((\tau_1))$. Следовательно, функции $u_i - \sqrt{-1}v_i$ – также алгебраические над полем $\widetilde{K}(\tau_1)$. Поэтому u_i, v_i – алгебраические над $\widetilde{K}(\tau_1)$ и над $\overline{k}(\tau_1)$ для всех $1 \leqslant i \leqslant n$.

Существуют формальные степенные ряды $\tau^* \in \widetilde{K}((\varepsilon_1^{1/m}))$, такие что

$$\tau^* = (\sum_{1\leqslant i\leqslant n} |w_{i,m}|^2)^{-1/(2m)}\varepsilon_1^{1/m} + \sum_{m<j\in\mathbb{Z}} \tau_j^*\varepsilon_1^{j/m},\ \tau_j^* \in \widetilde{K},$$

и подстановка $\tau_1 \mapsto \tau^*$ определяет изоморфизм $\psi : \overline{k}[[\tau_1]] \to \overline{k}[[\varepsilon_1^{1/m}]]$, для которого $\sum_{1\leqslant i\leqslant n}(u_i^2+v_i^2)|_{\tau_1=\tau^*} = \varepsilon_1^2$ (это просто обращение функции в кольце формальных степенных рядов).

Элемент $\tau^* \in \overline{k(\varepsilon_1)}$, поскольку ψ – гомоморфизм, и $\sum_{1\leqslant i\leqslant n}(u_i^2 + v_i^2)$ и τ_1 алгебраически зависимы над $\overline{k}$. Теперь положим $x_i^* = w_i|_{\tau_1=\tau^*}$ для $1 \leqslant i \leqslant n$. Тогда аналогично $x_i^* \in \overline{k(\varepsilon_1)}$ для $1 \leqslant i \leqslant$

n. Положим $x^* = (x_1^*, \ldots, x_n^*)$. Тогда $x^* \in C_1$, $|x^*|^2 = \varepsilon_1^2$, и $x \neq \mathrm{st}_{\varepsilon_1}(x^*/\varepsilon_1) \in l$, поскольку ψ – гомоморфизм. Наше утверждение доказано.

Положим $y^* = \varepsilon_1 \mathrm{st}_{\varepsilon_1}(x^*/\varepsilon_1)$. Поскольку $x^* \in W^{(1)} \cap \mathcal{Z}(h_{s+1})$, то существует точка $z^* \in \mathbb{A}^n(\overline{K_2})$, такая что $(x^*, y^*, z^*, h_{s+1}(z^*)^{-1})$ задает решение системы (15). Лемма доказана.

Возвратимся к описанию алгоритма. Выясним, имеет ли система (15) решение. Если система (15) не имеет решений, то по Лемме 8 мы можем положить $M_i = L_i$ для $i = 0, s+2, \ldots, n$. Предположим, что система (15) имеет решение. Построим такое решение $(x^*, y^*, z^*, h_{s+1}(z^*)^{-1}) \in \mathbb{A}^{3n+1}(\overline{K_2})$, см. [6, 7]. Напомним, что $L = \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n)$. Построим, см. доказательство Леммы 8, прямую

$$l = \{(\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(\mathrm{st}_{\varepsilon_2} y^*/\varepsilon_1)t \,:\, t \in \overline{k}\} \subset \mathrm{con}(x, U') \cap L.$$

Построим линейную форму L_1 от $X_1, \ldots, X_n$, такую что L_1 не равна тождественно нулю на прямой l. Обозначим $L' = \mathcal{Z}(L_1, L_{s+2}, L_{s+3}, \ldots, L_n)$. Это линейное подпространство, такое что $L' + l = L$.

Определим прямую

$$l' = \{x^* t \,:\, t \in \overline{K_2}\}.$$

Построим линейное пространство $L' + l'$. Тогда подпространство $L' + l'$ бесконечно близко к $L' + l$, поскольку x^*, y^* получены из решения системы (15). Подпространство $L' + l' = \mathcal{Z}(L'_{s+2}, \ldots, L'_n)$ в $\mathbb{A}^n(\overline{K_2})$, где $L'_j = L_j - \delta_j L_1$, и δ_j – бесконечно малые величины относительно поля k для $s+2 \leqslant j \leqslant n$. Построим такие линейные формы $L'_{s+2}, \ldots, L'_n \in \overline{K_2}[X_1, \ldots, X_n]$. Положим также $L'_0 = L_0$.

Теперь согласно Предложению 2 мы имеем

$$\#V' \cap \mathcal{Z}(L_{s+2}, \ldots, L_n) \leqslant \#V' \cap \mathcal{Z}(L'_{s+2}, \ldots, L'_n) < +\infty.$$

Далее, существуют точки $x, x^* \in V' \cap \mathcal{Z}(L'_{s+2}, L'_{s+3}, \ldots, L'_n)$, такие что их стандартные части в $\mathbb{P}^n(\overline{k})$ равны x. Следовательно,

$$N = \#V' \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n) < \#V' \cap \mathcal{Z}(L'_{s+2}, L'_{s+3}, \ldots, L'_n) = N'.$$

Положим $M_0 = L_0$. Теперь наша цель – применить аналог второго вспомогательного алгоритма из [7] к линейным формам $L'_0, L'_{s+2}, \ldots, L'_n$ и построить линейные формы $M_{s+2}, \ldots, M_n$

от $X_1, \dots, X_n$, которые имеют целые коэффициенты с длинами записи $O(n \log d)$, такие что $\#V' \cap \mathcal{Z}(M_{s+2}, \dots, M_n) \geqslant N'$, и $V' \cap \mathcal{Z}(M_0, M_{s+2}, \dots, M_n) = \emptyset$. Заметим, что второе условие может быть проверено в ходе этого вспомогательного алгоритма. Действительно, предположим, что мы заменили один коэффициент, скажем в M_{s+2} (мы не вводим новых обозначений для линейных форм, которые появляются в ходе второго вспомогательного алгоритма, а используем обозначения $M_{s+2}, \dots, M_n$). Тогда, как это известно из предыдущего шага осуществляемого алгоритма, $\#V' \cap \mathcal{Z}(M_0, M_{s+3}, \dots, M_n) < +\infty$, и, следовательно, точки этого множества могут быть вычислены, как это описано выше. Далее, мы можем подставить координаты этих точек в M_{s+1} с замененным коэффициентом и, таким образом, выяснить верно ли, что $V' \cap \mathcal{Z}(M_0, M_{s+2}, \dots, M_n) = \emptyset$ для вновь полученных линейных форм.

Если это второе условие удовлетворено, то $\#V' \cap \mathcal{Z}(M_{s+2}, \dots, M_n) < +\infty$, и первое условие также может быть проверено, как это описано выше. Таким образом, мы можем применить аналог второго вспомогательного алгоритма из [7] к линейным формам $L'_0, L'_{s+2}, \dots, L'_n$ и построить требуемые формы $M_{s+2}, \dots, M_n$ относительно $X_1, \dots, X_n$.

После этого возвратимся рекурсивно к началу описываемого алгоритма, заменяя линейные формы $L_0, L_{s+2}, \dots, L_n$ на $M_0, M_{s+2}, \dots, M_n$. Так как $N' > N$, в алгоритме может быть самое большее d^{s+1} таких возвратов.

Таким образом, мы получим в конечном счете согласно Лемме 8 семейство линейных форм $M_0, M_{s+2}, M_{s+3}, \dots, M_n$, таких что $M_0 = L_0$, формы $M_{s+2}, \dots, M_n \in k[X_1, \dots, X_n]$ имеют целые коэффициенты с длинами записи $O(n \log d)$,

$$V' \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \dots, M_n) = \emptyset,$$
$$\mathrm{con}(x, V') \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \dots, M_n) = \emptyset$$

в $\mathbb{P}^n(\overline{k})$. Мы будем предполагать, заменяя, как это описано выше, формы $L_0, L_{s+2}, \dots, L_n$ на $M_0, M_{s+2}, \dots, M_n$, что эти свойства удовлетворяются для $L_0, L_{s+2}, \dots, L_n$, т.е. формы $L_{s+2}, L_{s+3}, \dots, L_n \in k[X_1, \dots, X_n]$ имеют целые коэффициенты с длинами записи

$O(n \log d)$, и

$$V' \cap \mathcal{Z}(L_0, L_{s+2}, L_{s+3}, \dots, L_n) = \emptyset,$$
$$\operatorname{con}(x, V') \cap \mathcal{Z}(L_0, L_{s+2}, L_{s+3}, \dots, L_n) = \emptyset$$

в $\mathbb{P}^n(\overline{k})$.

Построим, см. выше, все точки x_u, $1 \leqslant u \leqslant N$, множества

$$V' \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \dots, L_n)$$

в $\mathbb{P}^n(\overline{k})$. Мы можем предполагать без ограничения общности, что $x_1 = x$. Построим линейную форму L_{s+1} от $X_1, \dots, X_n$ с коэффициентами из $\mathbb{Z}$ с длиной записи $O(n \log d)$, такую что $L_{s+1}(x_u) \neq 0$ для всех $2 \leqslant j \leqslant N$. Обозначим через

$$p_x : V' \backslash \{x\} \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}), \qquad (X_0 : \ldots : X_n) \mapsto (L_{s+1} : L_{s+2} : \ldots : L_n)$$

линейную проекцию.

5. Леммы для обоснования алгоритма

Пусть $W \subset \mathbb{P}^n(\overline{k})$ – неприводимое алгебраическое многообразие размерности $\dim W = n - s - 1$, и L_{s+1}, $L_{s+2}, \dots, L_n \in \overline{k}[X_1, \dots, X_n]$ – линейные формы. Рассмотрим следующие условия. Пересечение

$$W \cap \mathcal{Z}(L_{s+1}, \dots, L_n) \setminus \{x\} = \emptyset. \tag{16}$$

Выполняется равенство (16), и проекция

$$p : W \setminus \{x\} \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (L_{s+1} : L_{s+2} : \ldots : L_n)$$

является доминантным морфизмом, т.е. замыкание в топологии Зарисского

$$\overline{p(W \setminus \{x\})} = \mathbb{P}^{n-s-1}(\overline{k}). \tag{17}$$

Пересечение

$$\operatorname{con}(x, W) \cap \mathcal{Z}(L_{s+1}, L_{s+2}, \dots, L_n) \setminus \{x\} = \emptyset, \quad \text{если} \quad x \in W. \tag{18}$$

Лемма 9. *Пусть* $W \subset \mathbb{P}^n(\overline{k})$ *– неприводимое алгебраическое многообразие размерности* $\dim W = n - s - 1$, *и линейные формы* L_{s+1}, $L_{s+2}, \dots, L_n \in \overline{k}[X_1, \dots, X_n]$ *удовлетворяют условию* (16). *Пусть*

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

в $\mathbb{P}^n(\overline{k})$. *Тогда морфизм* p *– доминантный, т.е. выполняется равенство* (17).

Доказательство. Действительно, нам следует показать, что замыкание F в топологии Зарисского образа $p(W \setminus \{x\})$ совпадает с $\mathbb{P}^{n-s-1}(\overline{k})$. Согласно Предложению 2 для всяких $\lambda_{s+2}, \dots, \lambda_n \in \overline{k(\varepsilon)}$, которые являются бесконечно малыми относительно поля поля k множество $W \cap \mathcal{Z}(L_{s+2} - \lambda_{s+2} L_{s+1}, \dots, L_n - \lambda_n L_{s+1}) \setminus \{x\} \neq \emptyset$ в $\mathbb{P}^n(\overline{k(\varepsilon)})$. Следовательно, $p^{-1}((1 : \lambda_{s+2} : \dots : \lambda_n))$ непусто в $\mathbb{P}^{n-s}(\overline{k(\varepsilon)})$. Следовательно,

$$F(\overline{k(\varepsilon)}) = \mathbb{P}^{n-s-1}(\overline{k(\varepsilon)}),$$

и $F = \mathbb{P}^{n-s-1}(\overline{k})$. Лемма доказана.

Лемма 9 влечет, что условие (17) удовлетворяется для любой компоненты W многообразия V', такой что существует $x_u \in W$, $u \geqslant 2$, и линейные формы, $L_{s+1}, L_{s+2}, \dots, L_n$, построенные в Разделе 4.

Обозначим через $\mathcal{H}$ множество всех семейств H, состоящих каждое из $n - s$ линейных форм $H_{s+1}, H_{s+2}, \dots, H_n \in \overline{k}[X_1, \dots, X_n]$. Мы будем отождествлять $\mathcal{H}$ с алгебраическим многообразием $\mathbb{A}^{(n-s)n}(\overline{k})$.

Обозначим через $\mathcal{H}_1$ подмножество в $\mathcal{H}$ всех семейств H , состоящих каждое из $n-s$ линейных форм $H_{s+1}, H_{s+2}, \dots, H_n$, таких что

$$W \cap \mathcal{Z}(H_{s+1}, H_{s+2}, \dots, H_n) = \{x\}.$$

Лемма 10. *Пусть* $W \subset \mathbb{P}^n(\overline{k})$ *– неприводимое алгебраическое многообразие размерности* $\dim W = n - s - 1$, *такое что существуют линейные формы* L_{s+1}, $L_{s+2}, \dots, L_n \in \overline{k}[X_1, \dots, X_n]$, *удовлетворяющие* (16) *и* (17). *Тогда* $\mathcal{H}_1$ *содержит непустое открытое подмножество* $\mathcal{H}$ *в топологии Зарисского.*

Доказательство. В самом деле, обозначим через

$$\pi : \mathbb{P}^n \setminus \{x\} \to \mathbb{P}^{n-1}, \ (X_0 : \ldots : X_n) \mapsto (X_1 : \ldots : X_n)$$

линейную проекцию. Заметим, что замыкание в топологии Зарисского образа $\pi(W \setminus \{x\})$ является неприводимым алгебраическим многообразием размерности $n-s-1$, так как замыкание в топологии Зарисского множества $p(W \setminus \{x\})$ есть $\mathbb{P}^{n-s-1}$. Следовательно, существуют однородные многочлены $F_1, \ldots, F_s \in K[X_1 \ldots, X_n]$, такие что $\dim \mathcal{Z}(F_1, \ldots, F_s) = n-s-1$ в $\mathbb{P}^{n-1}$, и $\pi(W \setminus \{x\}) \subset \mathcal{Z}(F_1, \ldots, F_s)$. Условие

$$T = \mathcal{Z}(F_1, \ldots, F_s, H_{s+1}, H_{s+2}, \ldots, H_n) = \emptyset$$

в $\mathbb{P}^{n-1}(\overline{k})$ влечет, что $W \cap \mathcal{Z}(H_{s+1}, H_{s+2}, \ldots, H_n) \setminus \{x\} = \emptyset$. Но $T = \emptyset$ эквивалентно условию, что по меньшей мере один коэффициент соответствующего U-результанта не равен нулю. Теперь утверждение леммы следует из того, что коэффициенты U-результанта являются многочленами от коэффициентов линейных форм $H_{s+1}, H_{s+2}, \ldots, H_n$. Лемма доказана.

Лемма 11. *Пусть* $W \subset \mathbb{P}^n(\overline{k})$ *– неприводимое алгебраическое многообразие размерности* $\dim W = n-s-1$, *такое что существуют линейные формы* $L_{s+1}, L_{s+2}, \ldots, L_n \in \overline{k}[X_1, \ldots, X_n]$, *удовлетворяющие условию* (18). *Пусть* $x \in W$. *Тогда существует непустое открытое подмножество* U_4 *в* $\mathbb{P}^{n-s-1}(\overline{k})$, *такое что* $U_4 \subset \mathbb{P}^{n-s-1}(\overline{k}) \setminus \mathcal{Z}(L_{s+1})$, *и, если* $(1 : \lambda_{s+1} : \ldots : \lambda_n) \in U_4$, *то*

$$\operatorname{con}(x, W) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}) = \{x\}.$$

Доказательство. Мы имеем $\dim \pi(\operatorname{con}(x, W) \setminus \{x\}) \leqslant n-s-2$, и

$$\pi(\operatorname{con}(x, W) \setminus \{x\}) \cap \mathcal{Z}(L_{s+1}, \ldots, L_n) = \emptyset.$$

Таким образом, существует непустое открытое подмножество $U_4 \subset \mathbb{P}^{n-s-1}(\overline{k}) \setminus \mathcal{Z}(L_{s+1})$, такое что, если $(1 : \lambda_{s+1} : \ldots : \lambda_n) \in U_4$, то

$$\pi(\operatorname{con}(x, W) \setminus \{x\}) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}) = \emptyset.$$

Следовательно, если $(1 : \lambda_{s+1} : \ldots : \lambda_n) \in U_4$, то

$$\operatorname{con}(x, W) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}) = \{x\}.$$

Лемма доказана.

Пусть W – неприводимое алгебраическое многообразие из формулировки Леммы 10, и H – семейство $n-s$ линейных форм $H_{s+1}, H_{s+2}, \ldots, H_n$ от $X_1, \ldots, X_n$ с коэффициентами из $\overline{k}$. Пусть $H \in \mathcal{H}_1$. Обозначим через $p(H) : W \setminus \{x\} \to \mathbb{P}^{n-s-1}$ проекцию, соответствующую p, если мы заменим $L_{s+1}, L_{s+2}, \ldots, L_n$ на $H_{s+1}, H_{s+2}, \ldots, H_n$. Положим

$$\begin{aligned} &U_3(H) = \{z \in \mathbb{P}^{n-s} : \#p(H)^{-1}(z) < +\infty\,\}, \\ &\delta(H) = \sup\{\#p(H)^{-1}(z) : z \in U_3(H)\,\}, \\ &U(H) = \{z \in U_3(H) : \#p(H)^{-1}(z) = \delta(H)\}, \\ &\delta = \sup\{\#p(H)^{-1}(z) : z \in U_3(H), H \in \mathcal{H}_1\,\}. \end{aligned} \tag{19}$$

Заметим, что если $H \in \mathcal{H}_1$, и проекция $p(H)$ не является доминантной, то по Лемме 9 $\delta(H) = 0$, и $U_3(H) = U(H)$ содержит непустое открытое в топологии Зарисского подмножество в $\mathbb{P}^{n-s-1}(\overline{k})$.

Обозначим через $\widetilde{H}$ семейство $\widetilde{H}_{s+1}, \widetilde{H}_{s+2}, \ldots, \widetilde{H}_n$, которое является общим элементом $\mathcal{H}_1$, т.е. поле K, порожденное коэффициентами линейных форм из $\widetilde{H}$ над k является чисто трансцендентным над $\overline{k}$ степени трансцендентности $(n-s)n$.

Лемма 12. *Пусть W – алгебраическое многообразие из формулировки Леммы 10, и $H \in \mathcal{H}_1$ является, таким что проекция $p(H)$ – доминантный морфизм. Тогда $0 < \delta(H) < +\infty$, и $U(H)$ содержит непустое открытое в топологии Зарисского подмножество U в $\mathbb{P}^{n-s-1}(\overline{k})$, такое что для всякого $x^* \in U$ для всякой $y \in p^{-1}(x^*)$ точка y является гладкой точкой многообразия W, и дифференциал проекции p в точке y*

$$d_y p : T_{y,W} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

является изоморфизмом касательных пространств $T_{y,W}$ и $T_{x,\mathbb{P}^{n-s}}$ алгебраических многообразий W и $\mathbb{P}^{n-s}(\overline{k})$ в точках y и x соответственно.

Доказательство. Пусть $Y \in \overline{k}[X_0, \ldots, X_n]$ – линейная форма. Рассмотрим линейную проекцию

$$p_1 : W \setminus \{x\} \longrightarrow \mathbb{P}^{n-s}(\overline{k}),$$

$$(X_0 : \ldots : X_n) \mapsto (Y : H_{s+1} : H_{s+2} : \ldots : H_n).$$

Так как $p(H)$ – доминантный морфизм, то существует неприводимый однородный многочлен $G \in \overline{k}[Y, H_{s+1}, H_{s+2}, \ldots, H_n]$, такой что замыкание множества $p_1(W)$ в топологии Зарисского $\overline{p_1(W)} = \mathcal{Z}(G)$, и $p_1(W)$ содержит открытое подмножество замкнутого множества $\mathcal{Z}(G)$.

По теореме о примитивном элементе для полей существует линейная форма $Y \in \overline{k}[X_0, \ldots, X_n]$, такая что морфизм p_1 индуцирует бирациональный изоморфизм $W \setminus \{x\} \longrightarrow \mathcal{Z}(G)$, который мы будем обозначать p_2. Следовательно, существует открытое подмножество $U_1 \subset W$, такое что $p_2(U_1)$ открыто в $\mathcal{Z}(G)$, и p_2 индуцирует изоморфизм $U_1 \to p_2(U_1)$.

Обозначим $U_2 = \mathcal{Z}(G) \setminus \mathcal{Z}(H_{s+1}, H_{s+2}, \ldots, H_n)$. Существует проекция $p_3 : U_2 \longrightarrow \mathbb{P}^{n-s}(\overline{k})$, такая что $p = p_3 \circ p_2$ (на открытом подмножестве, где определены правая и левая части). Обозначим через $R = \mathrm{Res}_Y(G, G'_Y)$ дискриминант многочлена G относительно Y. Тогда $0 \neq R$ – однородный многочлен, так как G – сепарабельный однородный многочлен.

Если $R(x^*) \neq 0$, то мощность $\# p_3^{-1}(x^*) = \deg_Y G$, для всякой $y \in p_3^{-1}(x^*)$, точка y является гладкой точкой многообразия U_2, и дифференциал отображения p_3 в точке y

$$d_y p_3 \, : \, T_{y,U_2} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

является изоморфизмом касательных пространств $T_{y,p_1(W)}$ и $T_{x,\mathbb{P}^{n-s}}$ алгебраических многообразий U_2 и $\mathbb{P}^{n-s}(\overline{k})$ в точках y и x соответственно. Последнее утверждение следует здесь просто из того, что $G'_Y(y) \neq 0$, поскольку $R(x^*) \neq 0$.

Обозначим через F замыкание в топологии Зарисского множества $p_3(U_2 \setminus p_2(U_1))$. Положим $U = \mathbb{P}^{n-s-1}(\overline{k}) \setminus (\mathcal{Z}(R) \cup F)$ (следовательно, $U \neq \emptyset$). Тогда для всякого $x^* \in U$

(a) мощность $\# p(H)^{-1}(x^*) = \deg_Y G$,

(b) для всякой $y \in p(H)^{-1}(x^*)$ точка y является гладкой точкой многообразия W, и дифференциал проекции p в точке y

$$d_y p \, : \, T_{y,W} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

является изоморфизмом касательных пространств $T_{y,W}$ и $T_{x,\mathbb{P}^{n-s}}$ алгебраических многообразий W и $\mathbb{P}^{n-s}(\overline{k})$ в точках y и x соответственно.

Пусть $\varepsilon > 0$ – бесконечно малая величина относительно поля K. Теперь, если $z^* \in U(H)$, то существует точка $z \in U$ в

$\mathbb{P}^{n-s-1}(\overline{K(\varepsilon)})$, которая бесконечно близка к z^*. Следовательно, по Предложению 2 $\#p(H)^{-1}(z^*) \leqslant \#p(H)^{-1}(z)$. Следовательно, $\delta(H) = \deg_Y G$, и $U \subset U(H)$. Лемма доказана.

Лемма 13. *Пусть W – такое же, как и в формулировке Леммы 10. Для всякого $z \in U(\widetilde{H})$ справедливо равенство*

$$\delta = \delta(\widetilde{H}) = \#p(\widetilde{H})^{-1}(z)$$

Следовательно, δ – целое число, которое зависит только от W и x.

Доказательство. Равенство $\delta(\widetilde{H}) = \#p(\widetilde{H})^{-1}(z)$ следует из Леммы 12. Далее, если $H \in \mathcal{H}_1$ и $z \in U_3(H)$ – произвольные, то мы можем положить коэффициенты форм $H_j - \widetilde{H}_j$ равными бесконечно малым величинам для всех j, и по Предложению 2 точка $z \in U_3(\widetilde{H})$, и $\#p(\widetilde{H})^{-1}(z) \geqslant \#p(H)^{-1}(z)$. Следовательно, $\delta = \delta(\widetilde{H})$. Лемма доказана.

Лемма 14. *Пусть $q : V_1 \to V_2$ – доминантный регулярный морфизм неприводимых алгебраических многообразий V_1 и V_2, определенный над полем k. Пусть $\dim V_1 = \dim V_2$. Пусть $z \in V_2$, и*

$$\#q^{-1}(z) = [k(V_1) : k(V_2)],$$

т.е. число элементов обратного образа точки z совпадает со степенью расширения полей рациональных функций многообразий V_1 и V_2. Тогда существует открытое в топологии Зарисского подмножество $U' \subset V_2$, такое что $z \in U'$, и морфизм

$$q^{-1}(U') \to U',$$

индуцированный q, конечен.

Доказательство. Обозначим $[k(V_1) : k(V_2)] = \alpha$. Обозначим через $\widetilde{V}_i$, $i = 1, 2$, нормализацию алгебраического многообразия V_i в поле $k(V_1)$, см. [2]. Следовательно, мы имеем коммутативную диаграму морфизмов алгебраических многообразий

$$\begin{tikzcd} \widetilde{V}_1 \arrow[r, "\widetilde{q}"] \arrow[d, "\pi_1"'] & \widetilde{V}_2 \arrow[d, "\pi_2"'] \\ V_1 \arrow[r, "q"] & V_2, \end{tikzcd}$$

где π_1 и π_2 – конечные морфизмы, и $\widetilde{q}$ – бирациональный изоморфизм, индуцированный q. Мы имеем $\#\pi_2^{-1}(z) \leqslant \alpha$, поскольку π_2 конечен. Согласно основной теореме Зарисского $\widetilde{q}$ является обратимым в некоторой окрестности в топологии Зарисского каждой точки $z' \in \pi_2^{-1}(z)$, если $\widetilde{q}^{-1}(z') \neq \emptyset$. Следовательно, $\#\pi_2^{-1}(z) \geqslant \#\pi_1^{-1}(q^{-1}(z))$. Но $\#q^{-1}(z) = \alpha$. Следовательно, $\#\pi_2^{-1}(z) = \#\pi_1^{-1}(q^{-1}(z))$, и $\widetilde{q}$ обратим в некоторой окрестности в топологии Зарисского U'' конечного множества $\pi_2^{-1}(z)$. Так что мы имеем изоморфизм алгебраических многообразий

$$\widetilde{q}^{-1}(U'') \simeq U'',$$

индуцированный $\widetilde{q}$. Положим $U' = V_2 \setminus \pi_2(\widetilde{V}_2 \setminus U'')$. Тогда $z \in U'$, и морфизм

$$\pi_1^{-1}(q^{-1}(U')) = \widetilde{q}^{-1}(\pi_2^{-1}(U')) \to U'$$

конечен. Следовательно, морфизм $q^{-1}(U') \to U'$ также конечен. Лемма доказана.

Лемма 15. *Пусть $W \subset \mathbb{P}^n(\overline{k})$ – неприводимое алгебраическое многообразие размерности $\dim W = n - s - 1$, линейные формы $L_{s+1}, \dots, L_n \in \overline{k}[X_1, \dots, X_n]$ удовлетворяют* (16), (17) *и* (18). *Тогда*

(i) *существует непустое открытое в топологии Зарисского подмножество U в $\mathbb{P}^{n-s}(\overline{k})$, такое что для всякого $x^* \in U$ мощность $\#p^{-1}(x^*) = \delta > 0$, и δ – целое число, определенное в* (19), *которое зависит только от W и x.*

(ii) *если для некоторой точки $x^* \in \mathbb{P}^{n-s}(\overline{k})$ мощность $\#p^{-1}(x^*) = \delta$, то для всякой $y \in p^{-1}(x^*)$ точка y является гладкой точкой алгебраического многообразия W, и дифференциал проекции p в точке y*

$$d_y p : T_{y,W} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

является изоморфизмом касательных пространств $T_{y,W}$ и $T_{x^*,\mathbb{P}^{n-s}}$ алгебраических многообразий W и $\mathbb{P}^{n-s}(\overline{k})$ в точках y и x^* соответственно.

(iii) *если для некоторой точки $x^* \in \mathbb{P}^{n-s}(\overline{k})$ мощность $\#p^{-1}(x^*) < +\infty$, то $\#p^{-1}(x^*) \leqslant \delta$.*

Доказательство. Семейство $L_{s+1}, \dots, L_n$ принадлежит $\mathcal{H}_1$. Положим в Лемме 12 семейство H равным $L_{s+1}, \dots, L_n$. Мы будем использовать обозначения Y, p_1, p_2, p_3, G, R, U из доказательства Леммы 12 и U_4 из Леммы 11. Покажем, что $\deg_Y G = \delta$. Определим коэффициенты форм $\widetilde{H}_j - L_j$ как бесконечно малые величины относительно поля k для всех j. Так что определено отображение стандартной части

$$\mathrm{st} : \mathbb{P}^r(\overline{K}) \longrightarrow \mathbb{P}^r(\overline{k}).$$

Таким образом, согласно Предложению 2 для всякого $x^* \in U \cap U(\widetilde{H}) \cap U_4$ для всякого $y^* \in p(\widetilde{H})^{-1}(x^*)$ элемент $y = \mathrm{st}\, y^* \in p^{-1}(x^*)$, или $x = \mathrm{st}\, y^*$. Дифференциал проекции p в точке $y \in p^{-1}(x^*)$ – изоморфизм. Если $y \in p^{-1}(x^*)$, то по теореме о неявной функции существует единственное $y' \in p(\widetilde{H})^{-1}(x^*)$, такое что $\mathrm{st}(y') = y$. Следовательно, в этом случае $y' = y^*$.

Покажем, что не существует y^* такого, как выше, для которого $x = \mathrm{st}\, y^*$. Действительно, предположим обратное, что $x = \mathrm{st}\, y^*$. Обозначим $y^* = (y_1^*, \ldots, y_n^*) \in \mathbb{A}^n(\overline{k})$ и $x^* = (1 : \lambda_{s+1} : \ldots : \lambda_n)$. Положим $|y^*| = (\sum_{1 \leqslant i \leqslant n} |y_i^*|^2)^{1/2}$. Тогда

$$x \neq \mathrm{st}(y^*/|y^*|) \in \mathrm{con}(x, W) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}),$$

так как, если $F \in \overline{k}[X_1, \ldots, X_n]$, $F(y^*) = 0$, и F_r – форма наименьшей степени многочлена F, то $F_r(\mathrm{st}(y^*/|y^*|)) = 0$. Полученное противоречие доказывает наше утверждение.

Таким образом,

$$\delta = \# p(\widetilde{H})^{-1}(x^*) = \# p^{-1}(x^*) = \deg_Y G,$$

и, следовательно, $\deg G = \delta$, и (i) доказано.

Теперь (iii) следует из (i) и определения δ.

Чтобы доказать (ii) заметим, что согласно Лемме 14 (с k, замененным на $\overline{k}$) для всякой точки x^* с $\# p^{-1}(x^*) = \delta = [\overline{k}(W) : \overline{k}(\mathbb{P}^{n-s-1})]$ (здесь включение $\overline{k}(\mathbb{P}^{n-s-1}) \subset \overline{k}(W)$ полей рациональных функций индуцировано p) существует открытое множество U' в топологии Зарисского, такое что $x^* \in U'$, и морфизм $p^{-1}(U') \to U'$, индуцированный p, конечен. Теперь существует линейная форма Y, такая что соответствующее p_1 бирационально, $\# p_1(p^{-1}(x^*)) = \delta$. Для этой формы старший коэффициент $(\mathrm{lc}_Y G)(x^*) \neq 0$, так как морфизм $p^{-1}(U') \to U'$ конечен, и $x^* \in U'$. Следовательно, $p_3^{-1}(x^*) < +\infty$. Следовательно, $p_3^{-1}(x^*) = p_1(p^{-1}(x^*)) = \delta$. Таким образом, $R(x^*) \neq 0$.

Далее, если $R(x^*) \neq 0$, $\#p^{-1}(x^*) = \delta$, и $y \in p^{-1}(x^*)$, то точка $p_1(y)$ – гладкая, локальное кольцо $\mathcal{O}_{p_1(y),p_1(W)}$ многообразия $p_1(W)$ в точке $p_1(y)$ целозамкнуто. Следовательно, по основной теореме Зарисского локальные кольца

$$\mathcal{O}_{y,W} \simeq \mathcal{O}_{p_1(y),p_1(W)}.$$

Таким образом, p_1 – изоморфизм в окрестности всякой точки $y \in p^{-1}(x^*)$. Отсюда и (a) и (b), доказанных ранее, утверждение (ii) следует немедленно. Лемма доказана.

Следствие 3. *При условиях Леммы* 15 *кратность* $\mu(x, V_{s+1}) = \deg V_{s+1} - \delta$.

Доказательство. Это следует из определения кратности (1), данного во Введении, и лемм, доказанных в этом разделе.

Замечание 5. Согласно Следствию 4 из Леммы 16, см. ниже, Лемма 15 и Следствие 3 также выполняются, когда условие (17) не удовлетворяется. В этом случае $\delta = 0$, и $W = \mathrm{con}(x, W)$.

Лемма 16. *Пусть* W *– неприводимое алгебраическое многообразие размерности* $n - s - 1$, *и линейные формы* $L_0, L^{(i)}_{s+2}, \ldots, L^{(i)}_n \in \overline{k}[X_0, \ldots, X_n]$, $i = 0, 1$ *являются, такими что*

$$L^{(i)}_{s+2}, \ldots, L^{(i)}_n \in \overline{k}[X_1, \ldots, X_n],$$
$$W \cap \mathcal{Z}(L_0, L^{(0)}_{s+2}, \ldots, L^{(0)}_n) = \emptyset,$$
$$\mathrm{con}(x, W) \cap \mathcal{Z}(L_0, L^{(0)}_{s+2}, \ldots, L^{(0)}_n) = \emptyset, \quad \text{если} \quad x \in W,$$
$$W \cap \mathcal{Z}(L^{(1)}_{s+2}, \ldots, L^{(1)}_n) < +\infty$$

в $\mathbb{P}^n(\overline{k})$. *Далее, пусть все точки* $W \cap \mathcal{Z}(L^{(0)}_{s+2}, \ldots, L^{(0)}_n) \setminus \{x\}$ *– гладкие, и дифференциалы проекции*

$$p^{(0)} : W \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (L_0 : L^{(0)}_{s+2} : \ldots : L^{(0)}_n)$$

являются изоморфизмами во всех точках из $W \cap \mathcal{Z}(L^{(0)}_{s+2}, \ldots, L^{(0)}_n) \setminus \{x\}$. *Тогда*

$$\#W \cap \mathcal{Z}(L^{(0)}_{s+2}, \ldots, L^{(0)}_n) \geqslant \#W \cap \mathcal{Z}(L^{(1)}_{s+2}, \ldots, L^{(1)}_n).$$

Доказательство. Предположим противное, что

$$\#W \cap \mathcal{Z}(L^{(0)}_{s+2}, \ldots, L^{(0)}_n) < \#W \cap \mathcal{Z}(L^{(1)}_{s+2}, \ldots, L^{(1)}_n).$$

Пусть $\varepsilon > 0$ – бесконечно малая величина относительно поля k. Так что определено отображение стандартной части

$$\mathrm{st} : \mathbb{P}^n(\overline{k(\varepsilon)}) \longrightarrow \mathbb{P}^n(\overline{k}).$$

Мы имеем, ср. [3], $+\infty > \#W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0,\ s+2 \leqslant j \leqslant n\} \geqslant \#W \cap \mathcal{Z}(L_{s+2}^{(1)}, \dots, L_n^{(1)})$ (здесь можно использовать Предложение 2, если сейчас, только на один момент, рассмотреть $1/\varepsilon$ как бесконечно малую величину). Пусть $x^* \in W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0,\ s+2 \leqslant j \leqslant n\}$. Тогда $\mathrm{st}(x^*) \in W \cap \mathcal{Z}(L_{s+2}^{(0)}, \dots, L_n^{(0)})$ по Предложению 2. Дифференциалы проекции $p^{(0)}$ суть изоморфизмы во всех точках из $W \cap \mathcal{Z}(L_{s+2}^{(0)}, \dots, L_n^{(0)}) \setminus \{x\}$. Таким образом, по теореме о неявной функции (примененной к формальным степенным рядам) для всякого $x'' \in W \cap \mathcal{Z}(L_{s+2}^{(0)}, \dots, L_n^{(0)}) \setminus \{x\}$ существует единственный $x^* \in W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0,\ s+2 \leqslant j \leqslant n\}$, такой что $\mathrm{st}(x^*) = x''$. Следовательно, $x \in W$, и существует по меньшей мере один $x' \in W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0,\ s+2 \leqslant j \leqslant n\}$, такой что $\mathrm{st}(x') = x$.

Обозначим $x' = (x'_1, \dots, x'_n) \in \mathbb{A}^n$. Положим $|x'| = (\sum_{1 \leqslant i \leqslant n} |x'_i|^2)^{1/2}$. Мы имеем $\mathrm{st}(x') = x$, и, следовательно,

$$x \neq \mathrm{st}(x'/|x'|) \in \mathrm{con}(x, W) \cap \mathcal{Z}(L_{s+2}^{(0)}, \dots, L_n^{(0)}),$$

так как, если $F \in \overline{k}[X_1, \dots, X_n]$, $F(x') = 0$, и F_r – форма наименьшей степени многочлена F, то $F_r(\mathrm{st}(x'/|x'|)) = 0$. Полученное противоречие доказывает лемму.

Следствие 4. *Пусть W, и $L_{s+2}^{(i)}, \dots, L_n^{(i)}$, $i = 1, 2$, – такие же, как и в формулировке Леммы* 16. *Пусть*

$$W \cap \mathcal{Z}(L_{s+2}^{(0)}, \dots, L_n^{(0)}) = \{x\}.$$

Тогда

$$W \cap \mathcal{Z}(L_{s+2}^{(1)}, \dots, L_n^{(1)}) = \{x\}.$$

Более того, в этом случае $W = \mathrm{con}(x, W)$.

Доказательство. Необходимо доказать только последнее утверждение. Рассмотрим проекцию $\pi : \mathbb{P}^n(\overline{k}) \setminus \{x\} \to \mathbb{P}^{n-1}(\overline{k})$, определенную в доказательстве Леммы 10.

Покажем, что замыкание W_1 в топологии Зарисского множества $\pi(W \setminus \{x\})$ имеет размерность $n-s-2$. В самом деле, иначе, эта размерность равна $n-s-1$. Следовательно, существуют линейные формы $H_{s+1}, H_{s+2}, \ldots , H_n$ от $\overline{k}[X_1, \ldots , X_n]$, такие что

$$W_1 \cap \mathcal{Z}(H_{s+1}, \ldots , H_n) = \emptyset.$$

Следовательно, морфизм $W \setminus \{x\} \to \mathbb{P}^{n-s-1}(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (H_{s+1} : \ldots : H_n)$ является доминантным. Поэтому существуют $z_1, \ldots , z_n \in \overline{k}$, такие что

$$W \cap \mathcal{Z}(H_{s+2} - z_{s+2}H_{s+1}, \ldots , H_n - z_n H_{s+1}) \setminus \{x\}$$

является непустым конечным множеством. Теперь положим $L_j^{(1)} = H_j - z_j H_{s+1}$, $s+2 \leqslant j \leqslant n$. Следовательно, $\#W \cap \mathcal{Z}(L_{s+2}^{(1)}, \ldots , L_n^{(1)}) \setminus \{x\} \geqslant 1$, что приводит к противоречию. Наше утверждение доказано.

Теперь неприводимое алгебраическое многообразие $\pi^{-1}(W_1) \supset W \setminus \{x\}$, и $\dim \pi^{-1}(W_1) = \dim W$. Следовательно, $W = \operatorname{con}(x, W) = \pi^{-1}(W_1) \cup \{x\}$. Следствие доказано.

6. Завершение описания алгоритма для вычисления кратности точки

Наша цель теперь – построить семейство линейных форм $M_0, M_{s+2}, M_{s+3}, \ldots , M_n$, таких что $M_0 = L_0$, формы $M_{s+2}, M_{s+3}, \ldots , M_n \in k[X_1, \ldots , X_n]$ имеют коэффициенты из $\mathbb{Z}$ с длиной записи $O(n \log d)$,

$$V' \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \ldots , M_n) = \emptyset,$$

$$\operatorname{con}(x, V') \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \ldots , M_n) = \emptyset$$

в $\mathbb{P}^n(\overline{k})$, все точки из $V' \cap \mathcal{Z}(M_{s+2}, M_{s+3}, \ldots , M_n) \setminus \{x\}$ являются гладкими точками алгебраического многообразия V', и пересечение касательных пространств

$$T_{x_1,V'} \cap \mathcal{Z}(M_{s+2}, M_{s+3}, \ldots , M_n) = \{x_1\}$$

для всякой точки $x_1 \in V' \cap \mathcal{Z}(M_{s+2}, M_{s+3}, \ldots , M_n) \setminus \{x\}$.

Напомним, что в Разделе 4 построены точки x_u, $1 \leqslant u \leqslant N$, причем $x_1 = x$. Пусть $x_u = (x_{u,0} : \ldots : x_{u,n})$, где все $x_{u,i}$ – из конечного расширения поля k. Построим вещественную структуру для поля $K = k(x_{u,0}, \dots, x_{u,n})$, см. [6, 7], которая индуцирует вещественную структуру на $\overline{k}$.

Пусть бесконечно малые величины $\varepsilon_0, \varepsilon_1, \varepsilon_2$ и поле $K_2 = k(\varepsilon_0, \varepsilon_1, \varepsilon_2)$ – такие же, как и в Разделе 4.

Пусть $Y_0, \dots, Y_n$, $Z_0, \dots, Z_n$, $T_0, \dots, T_n$, Z, T – новые переменные. Для всякого $2 \leqslant u \leqslant N$ рассмотрим следующую систему уравнений и неравенств с коэффициентами из K_2

$$\begin{cases} h_i = 0, & 1 \leqslant i \leqslant s+1, \\ h_i(Y_0, \dots, Y_n) = 0, & 1 \leqslant i \leqslant s+1, \\ h_i(Z_0, \dots, Z_n) = 0, & 1 \leqslant i \leqslant s, \\ h_i(T_0, \dots, T_n) = 0, & 1 \leqslant i \leqslant s, \\ h_{s+1}(Z_0, \dots, Z_n)Z - 1 = 0, & \\ h_{s+1}(T_0, \dots, T_n)T - 1 = 0, & \\ \sum_{0 \leqslant i \leqslant n} |X_i - Z_i|^2 \leqslant \varepsilon_2, & \\ \sum_{0 \leqslant i \leqslant n} |Y_i - T_i|^2 \leqslant \varepsilon_2, & \\ L_j(X_0 - Y_0, \dots, X_n - Y_n) = 0, & s+1 \leqslant j \leqslant n, \\ L_{s+1}(X_0 - x_{u,0}, \dots, X_n - x_{u,n}) = 0, & \\ \sum_{0 \leqslant i \leqslant n} |X_i - x_{u,i}|^2 \leqslant \varepsilon_0, & \\ \sum_{0 \leqslant i \leqslant n} |Y_i - x_{u,i}|^2 \leqslant \varepsilon_0, & \\ \sum_{0 \leqslant i \leqslant n} |Y_i - X_i|^2 \geqslant \varepsilon_1, & \end{cases} \tag{20}$$

Мы имеем следующий аналог Леммы 2.

Лемма 17. *Пусть V', и проекция $p_x : V' \setminus \{x\} \longrightarrow \mathbb{P}^{n-s-1}(\overline{k})$ – такие же, как в Разделе 4. Если для всякого $2 \leqslant u \leqslant N$ не существует решений системы (20) в $\mathbb{A}^{4n+2}(\overline{K_2})$, то все точки $\{x_u\}_{2 \leqslant u \leqslant N}$ алгебраического многообразия V' являются гладкими и дифференциалы проекции p_x в точках $\{x_u\}_{2 \leqslant u \leqslant N}$ – изоморфизмы.*

Доказательство. Пусть $\varepsilon_3 > 0$ – бесконечно малая величина относительно поля $k(\varepsilon_0)$, такая что ε_1 – бесконечно малая величина относительно поля $k(\varepsilon_0, \varepsilon_3)$. Предположим, что по крайней мере одна точка x_{u_0} не является гладкой, или она является гладкой, но дифференциал проекции p в точке x_{u_0} – не изоморфизм. Обозначим $p_x(x_{u_0}) = w \in \mathbb{P}^{n-s-1}(\overline{k})$.

Предположим, что существует только одна компонента W многообразия V', такая что $x_{u_0} \in W$. Обозначим через $A(W)$ множество всех индексов u, таких что $x_u \in W$, $1 \leqslant u \leqslant N$, и положим $p = p_x|_{W\setminus\{x\}}$, $N(W) = \#A(W)$. Применим Лемму 15. Тогда по этой лемме $N(W) - 1 < \delta$, и существует $w^* \in \mathbb{P}^{n-s-1}(\overline{k(\varepsilon_3)})$, такое что $\mathrm{st}_{\varepsilon_3}(w^*) = w$ и $\#p^{-1}(w^*) = \delta$. Согласно Предложению 2 существуют два различных элемента $x', y' \in \#p^{-1}(w^*)$, таких что $\mathrm{st}_{\varepsilon_3}(x') = \mathrm{st}_{\varepsilon_3}(y') = x_{u_1}$ для некоторого $u_1 \in A(W)$.

Напомним,что $L = \mathcal{Z}(L_{s+2}, L_{s+3}, \dots, L_n)$. Обозначим $\mathrm{st} = \mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_3}$. Покажем, что $u_1 \neq 1$. Действительно, иначе, $x \neq \mathrm{st}(x'/|x'|) \in \mathrm{con}(x, W) \subset \mathrm{con}(x, V')$, так как, если $F \in \overline{k}[X_1, \dots, X_n]$, $F(x') = 0$, и F_r – форма наименьшей степени многочлена F, то $F_r(\mathrm{st}(x'/|x'|)) = 0$. Далее,

$$(L_j - (L_j/L_{s+1})(w^*)L_{s+1})(x'/|x'|) = 0,$$

и $(L_j/L_{s+1})(w^*)$ – бесконечно малая величина для всякого $s+2 \leqslant j \leqslant n$. Следовательно, мы имеем $L_j(\mathrm{st}(x'/|x'|)) = 0$ для всякого $s+2 \leqslant j \leqslant n$. Поэтому $x \neq \mathrm{st}(x'/|x'|) \in \mathrm{con}(x, V') \cap L$. Полученное противоречие доказывает наше утверждение.

Следовательно, $u \geqslant 2$. Из того, что $x', y' \in W \subset V'$, мы получаем существование $z', t' \in \mathbb{P}^n(\overline{k(\varepsilon_3, \varepsilon_2)})$, таких что $h_i(z') = h_i(t') = 0$ для $1 \leqslant i \leqslant s$, $h_{s+1}(z') \neq 0$, $h_{s+1}(t') \neq 0$, и $\mathrm{st}_{\varepsilon_2}(z') = x'$, $\mathrm{st}_{\varepsilon_2}(t') = y'$. Таким образом, система (20) с $u = u_1$ имеет решение в $\mathbb{P}^n(\overline{k(\varepsilon_3, \varepsilon_2)})$. Теперь изоморфизм полей с вещественными структурами $\overline{k(\varepsilon_3, \varepsilon_2)} \simeq \overline{k(\varepsilon_0^a, \varepsilon_2)}$, индуцированный $\varepsilon_3 \mapsto \varepsilon_0^a$ для достаточно больших $0 < a \in \mathbb{Z}$ задает решение системы (20) с $u = u_1$ в $\mathbb{P}^n(\overline{k(\varepsilon_0, \varepsilon_2)})$.

Если существуют две различные компоненты W_1 и W_2 многообразия W, то существует точка $w^* \in \mathbb{P}^{n-s-1}(\overline{k(\varepsilon_3)})$, такая что $w^* \notin p(W_1 \cap W_2)$, и $\mathrm{st}_{\varepsilon_3}(w^*) = w$. Тогда по Предложению 2 существуют две различные $x', y' \in \#p^{-1}(w^*)$, такие что $x' \in W_1$, $y' \in W_2$, $\mathrm{st}_{\varepsilon_3}(x') = \mathrm{st}_{\varepsilon_3}(y') = x_{u_0}$. Далее доказательство аналогично рассмотреному случаю одной компоненты W. Лемма доказана.

Вернемся к описанию алгоритма. Построим решение системы (20) для некоторого u или установим, что для всякого $2 \leqslant u \leqslant N$ не существует решений системы (20) в $\mathbb{A}^{4n+2}(\overline{K_2})$. В последнем случае по Лемме 17 все точки $\{x_u\}_{2 \leqslant u \leqslant N}$ многообразия V' – гладкие, и дифференциалы проекции p_x в точках $\{x_u\}_{2\leqslant u\leqslant N}$ – изоморфизмы.

Предположим, что существует решение

$$(x'_0, \dots , x'_n, y'_0, \dots , y'_n, z'_0, \dots , z'_n, t'_0, \dots , t'_n, z, t) \in \mathbb{A}^{4n+2}(\overline{K_2})$$

некоторой системы (20) с $u = u_0$. Обозначим $x' = (x'_0 : \dots : x'_n)$ и $y' = (y'_0 : \dots : y'_n)$. Следовательно, $x', y' \in \mathbb{P}^n(\overline{K_2})$. Вычислим $x^* = \mathrm{st}_{\varepsilon_2}(x')$ и $y^* = \mathrm{st}_{\varepsilon_2}(y')$. Тогда $x^*, y^* \in V'$, так как многочлены $h_1, \dots , h_s$ обращаются в нуль в этих точках, многочлен h_{s+1} не обращается в нуль в точках $(z'_0, \dots , z'_n)$ и $(t'_0, \dots , t'_n)$, которые бесконечно близки к x^* и y^* соответственно. Положим

$$L'_i = L_i - (L_i/L_{s+1})(x^*)L_{s+1},\ s + 2 \leqslant i \leqslant n.$$

Вычислим все точки множества $V' \cap \mathcal{Z}(L'_{s+2}, \dots , L'_n)$ в $\mathbb{P}^n(\overline{K_2})$. Обозначим $N' = \#V' \cap \mathcal{Z}(L'_{s+2}, \dots , L'_n)$. По Предложению 2 для всякого $x'' \in V' \cap \mathcal{Z}(L'_{s+2}, \dots , L'_n)$ существует $1 \leqslant u \leqslant N$, такое что $(\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(x'') = x_u$. Так что $N' \geqslant N$. Далее, $x^*, y^* \in V' \cap \mathcal{Z}(L'_{s+2}, \dots , L'_n)$, $x^* \neq y^*$, и $(\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(x^*) = (\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(y^*)$. Следовательно, $N' \geqslant N + 1 > N$.

Применим аналог второго вспомогательного алгоритма из [7], описанного в Разделе 4, к линейным формам $L'_{s+2}, \dots , L'_n$ и построим линейные формы $M_{s+2}, \dots , M_n$ от $X_1, \dots , X_n$ с коэффициентами из $\mathbb{Z}$ с длиной записи $O(n \log d)$, такие что

$$\#V' \cap \mathcal{Z}(M_{s+2}, \dots , M_n) \geqslant N' > N,$$
$$V' \cap \mathcal{Z}(L_0, M_{s+2}, \dots , M_n) = \emptyset$$

в $\mathbb{P}^n(\overline{k})$. Положим также $M_0 = L_0$.

После этого возвратимся рекурсивно к началу описываемого алгоритма, заменяя линейные формы $L_0, L_{s+2}, \dots , L_n$ на $M_0, M_{s+2}, \dots , M_n$. Поскольку $N' > N$, то может быть самое большее d^{s+1} таких возвратов в алгоритме.

Таким образом, осуществляя эту рекурсивную процедуру до конца, мы можем предполагать без ограничения общности по Лемме 17, что все точки x_u, $2 \leqslant u \leqslant N$ (если они существуют) являются гладкими точками алгебраического многообразия V', и дифференциалы проекции p_x, см. Лемму 17, в точках x_u, $2 \leqslant u \leqslant N$ – изоморфизмы.

Условие, что дифференциалы проекции

$$\widetilde{p} : W \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}),\ (X_0 : \dots : X_n) \mapsto (L_0 : L_{s+2} : \dots : L_n)$$

являются изоморфизмами во всех точках из $V'\cap\mathcal{Z}(L_{s+2},\ldots,L_n)\setminus\{x\}$ следует из условия, что дифференциалы проекции

$$p_x : V'\setminus\{x\}\longrightarrow\mathbb{P}^{n-s-1}(\overline{k}),\ (X_0:\ldots:X_n)\mapsto(L_{s+1}:L_{s+2}:\ldots:L_n).$$

являются изоморфизмами во всех точках из $W\cap\mathcal{Z}(L_{s+2},\ldots,L_n)\setminus\{x\}$. Оба условия эквивалентны тому, что пересечение касательных пространств $T_{x_u,V'}\cap\mathcal{Z}(L_{s+2},L_{s+3},\ldots,L_n)=\{x_u\}$ для всякой точки $x_u\in V'\cap\mathcal{Z}(L_{s+2},\ L_{s+3},\ \ldots,L_n)\setminus\{x\}$. Таким образом, мы имеем требуемые линейные формы $M_j=L_j$, $j=0,s{+}2,s{+}3,\ldots,n$.

Теперь построим, применяя Лемму 5, подмножество индексов $A\subset\{2,\ldots,N\}$, таких что

$$\{x_u : u\in A\}=V_{s+1}\cap\mathcal{Z}(L_{s+2},\ldots,L_n) \tag{21}$$

в $\mathbb{P}^n(\overline{k})$.

Лемма 18. *Пусть* $\mu(x,V_{s+1})$ *– кратность точки* x *многообразия* V_{s+1}. *Тогда*

$$\mu(x,V_{s+1})=\deg V_{s+1}-\#A. \tag{22}$$

Доказательство. Пусть W – произвольная неприводимая компонента многообразия V', и $A(W)\subset\{1,\ldots,N\}$ – подмножество индексов, таких что

$$\{x_u : u\in A(W)\}=W\cap\mathcal{Z}(L_{s+2},\ldots,L_n)$$

в $\mathbb{P}^n(\overline{k})$.

Рассмотрим множество семейств H, состоящих каждое из $n-s-1$ линейных форм $H_{s+2},\ldots,H_n$ от $X_1,\ldots,X_n$ с коэффициентами из $\overline{k}$. Так что по определению кратности существует такое семейство $H=\{H_j\}_{s+2\leqslant j\leqslant n}$, для которого $\#(W\cap\mathcal{Z}(H_{s+2},\ldots,H_n)\setminus\{x\})<+\infty$, и $\mu(x,W)=\deg W-\#(W\cap\mathcal{Z}(H_{s+2},\ldots,H_n)\setminus\{x\})$. Условия Леммы 16 удовлетворяются для $L_j^{(0)}=L_j$, $j=0,s+2,\ldots,n$ и $L_j^{(1)}=H_j$, $j=s+2,\ldots,n$. Теперь, применяя Лемму 16, мы получаем, что

$$\#(W\cap\mathcal{Z}(L_{s+2},\ldots,L_n)\setminus\{x\})\geqslant\#(W\cap\mathcal{Z}(H_{s+2},\ldots,H_n)\setminus\{x\}).$$

Следовательно, по определению кратности

$$\begin{aligned}&\#A(W)=\#(W\cap\mathcal{Z}(L_{s+2},\ldots,L_n)\setminus\{x\})=\\&\#(W\cap\mathcal{Z}(H_{s+2},\ldots,H_n)\setminus\{x\})=\deg W-\mu(x,W).\end{aligned}$$

Следовательно, $\sum_{W\subset V_{s+1}}\mu(x,W)=\deg V_{s+1}-\#A$. Но $\mu(x,V_{s+1})\geqslant \sum_{W\subset V_{s+1}}\mu(x,W)$, что является простым следствием определения кратности. Поэтому $\mu(x,V_{s+1})\geqslant \deg V_{s+1}-\#A$. Наконец, мы имеем $-1+\deg V_{s+1}-\#V_{s+1}\cap\mathcal{Z}(L_{s+2},\dots,L_n)=\deg V_{s+1}-\#A$, и, следовательно, $\mu(x,V_{s+1})=\deg V_{s+1}-\#A$. Лемма доказана.

Таким образом, согласно Лемме 18 мы можем вычислить кратность $\mu(x,V_{s+1})$. Алгоритм для вычисления кратности точки описан полностью. Теорема 3 доказана.

Литература

1. Д. Мамфорд, *Алгебраическая геометрия И. Комплексные проективные многообразия.* М., Мир, 1979.
2. Р. Хартсхорн, *Алгебраическая геометрия.* М., Мир, 1981.
3. А. Л. Чистов, *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время.* — Зап. научн. семин. ЛОМИ **137** (1984), 124–188.
4. А. Л. Чистов, *Алгоритмы полиномиальной сложности для вычислительных задач в теории алгебраических кривых.* — Зап. научн. семин. ЛОМИ **176** (1989), 127–150.
5. J. Bochnak, M. Coste, and M.-F. Roy, *Géométrie algébrique réelle.* Springer–Verlag, Berlin, Heidelberg, New York, 1987.
6. A. L. Chistov, *Polynomial-time computation of the dimension of algebraic varieties in zero-characteristic.* — J. Sym. Comp. **22**, No. **1** (1996), 1–25.
7. A. L. Chistov, *Polynomial-time computation of the dimensions of components of algebraic varieties in zero-characteristic.* — J. Pure Appl. Algebra **117, 118** (1997), 145–175.
8. A. L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm.* Lecture Notes Computer Science, Vol. 233, Springer, New York, Berlin, Heidelberg, 1986, pp. 247–255.
9. A. L. Chistov, M. Karpinski, *Complexity of Deciding Solvability of Polynomial Equations over p-adics.* Research Report No. 85183-CS, Institut fur Informatik der Universitat Bonn, May 1997.
10. M. Giusti, J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial.* Proc. Int. Meeting on Commutative Algebra, Cortona (1993).
11. J. Igusa, *Mem. Coll. Sci. Univ.*. Kyoto 27 (1951), 189–201.
12. L. Kroneker, *Grundzüge einer arithmetischen theorie der algebraischen grossen.* — J. Reine Angew. Math. **92** (1882), 1–122.
13. D. Lazard, *Algèbre linéaire sur* $k[x_1,\dots,x_n]$ *et élimination.* — Bul. S.M.F. **105** (1977), 165–190.
14. D. Lazard, *Résolution des systèmes d'équations algébrique.* — Theor. Comp. Sci. **15** (1981), 77–110.

15. J. Milnor, *On Betti numbers of real varieties.* — Proc. Amer. Math. Soc. **15 (2)** (1964), 275–280.
16. J. Renegar, *A faster PSPACE algorithm for deciding the existential theory of reals.* Proc. 29th Annual Symp. on Foundations of Computer Sci., October 24–26, 1988, pp. 291–295.
17. P. Samuel, *Métodes d'algebre abstracte en géométrie algébrique.* B. 1967.

Chistov A. L. Polynomial-time computation of degrees of algebraic varieties in zero-characteristic and its applications.

Consider an algebraic variety over a zero–characteristic ground field which is given as a set of all common zeros of a family of polynomials of the degree less than d in n variables. In this paper the following algorithms with the working time polynomial in the size of input and d^n are constructed: an algorithm for the computation of the degrees of algebraic varieties, an algorithm for the computation of the dimension of a given algebraic variety in the neighbourhood of a given point, an algorithm for the computation of the multiplicity of a given point of an algebraic variety, an algorithm for the computation of a representative system of smooth points with their tangent spaces on each component of a given algebraic variety, an algorithm for deciding whether a given morphism of algebraic varieties is dominant.

Санкт-Петербургский институт
информатики и автоматизации
Российской академии наук

Поступило 22 июля 1999 г.