Записки научных
семинаров ПОМИ
Том 403, 2012 г.

А. Л. Чистов

ЭФФЕКТИВНАЯ ВЕРСИЯ ПЕРВОЙ ТЕОРЕМЫ БЕРТИНИ В НЕНУЛЕВОЙ ХАРАКТЕРИСТИКЕ И ЕЁ ПРИЛОЖЕНИЯ

Введение

Пусть K – бесконечное поле ненулевой характеристики p. Мы предполагаем, что K конечно порождено над конечным полем $\mathbb{F}_p$ из p элементов и что оно задано аналогично [1]. Именно, пусть $l \geqslant 1$ – целое число и $K = \mathbb{F}_p(T_1, \ldots, T_l)[\eta]$, где $T_1, \ldots, T_l$ являются алгебраически независимыми над $\mathbb{F}_p$ элементами и η – алгебраический сепарабельный элемент над полем $\mathbb{F}_p(T_1, \ldots, T_l)$ с минимальным многочленом $\Phi \in \mathbb{F}_p(T_1, \ldots, T_l)[Z]$ над полем $\mathbb{F}_p(T_1, \ldots, T_l)$. Многочлен Φ задан явно. Мы будем предполагать без ограничения общности, что $\Phi \in \mathbb{F}_p[T_1, \ldots, T_l, Z]$ и $\mathrm{lc}_Z \Phi = 1$, т.е. старший коэффициент многочлена Φ относительно Z равен 1. Пусть $\overline{K}$ – алгебраическое замыкание поля K. Пусть W – определённая над K и неприводимая над $\overline{K}$ компонента аффинного алгебраического многообразия $V = \mathcal{Z}(f_1, \ldots, f_m)$, которое является множеством всех нулей семейства многочленов $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$, $n \geqslant 3$. Мы предполагаем, что W задано точкой $z^{(0)} \in W$, которая принадлежит единственной неприводимой компоненте многообразия V. Пусть $\dim W = n - s$, где $0 \leqslant s \leqslant n - 3$.

Пусть $r \geqslant 3$ – целое число, $e_1, \ldots, e_r \in K[X_1, \ldots, X_n]$,

$$\pi_r : W \to \mathbb{A}^r(\overline{K}), \quad (X_1, \ldots, X_n) \mapsto (e_1, \ldots, e_r),$$

– доминантный морфизм, и

$$\dim \big(W \cap \mathcal{Z}(e_1, \ldots, e_r)\big) \leqslant -2 + \dim W. \tag{1}$$

Таким образом, $n - s \geqslant r$. Пусть $1 \leqslant i_{r+1} < \ldots < i_{n-s} \leqslant n$ – целые числа, такие, что $e_1, \ldots, e_r, X_{i_{r+1}}, \ldots, X_{i_{n-s}}$ образуют базис трансцендентности поля рациональных функций $K(W)$ над K. Кроме того, если морфизм π_r является сепарабельным, то мы будем предполагать,

Ключевые слова: первая теорема Бертини, полиномиальные простые идеалы, системы образующих, нижние оценки.

что этот базис трансцендентности также сепарабелен, т.е. конечное расширение полей

$$K(W) \supset K(e_1, \ldots, e_r, X_{i_{r+1}}, \ldots, X_{i_{n-s}})$$

сепарабельно. Положим $e_j = X_{i_j}$ при $r+1 \leqslant j \leqslant n-s$. Для всякого i, $1 \leqslant i \leqslant n$, пусть $\varepsilon_i \geqslant 0$ – наименьшее целое число, такое, что элемент $X_i^{p^{\varepsilon_i}} \in K(W)$ сепарабелен над подполем $K(e_1, \ldots, e_{n-s})$. Обозначим через ${}^{\pi}W$ определённое над K алгебраическое многообразие с кольцом регулярных определённых над K функций

$$K[{}^{\pi}W] = K[e_1, \ldots, e_{n-s}, X_1^{p^{\varepsilon_1}}, \ldots, X_n^{p^{\varepsilon_n}}] \subset K(W).$$

Таким образом, аффинное алгебраическое многообразие ${}^{\pi}W$ зависит от выбора $i_{r+1}, \ldots, i_{n-s}$. В случае, когда морфизм π_r сепарабелен, мы имеем $\varepsilon_i = 0$ для всех i и ${}^{\pi}W = W$. Теперь включение колец $K[{}^{\pi}W] \supset K[e_1, \ldots, e_{n-s}]$ индуцирует доминантный сепарабельный морфизм $\pi_r' : {}^{\pi}W \to \mathbb{A}^r(\overline{K})$. Далее, расширение полей определённых над K рациональных функций $K({}^{\pi}W) \subset K(W)$ является чисто несепарабельным. Следовательно, вложение колец $K[{}^{\pi}W] \subset K[W]$ индуцирует естественный конечный чисто несепарабельный (и, следовательно, биективный) морфизм $\iota : W \to {}^{\pi}W$. Мы имеем $\pi_r = \pi_r' \circ \iota$. Кроме того, алгебраические многообразия ${}^{\pi}W$ неприводимы над полем $\overline{K}$.

Наша цель (см. теорему 1 ниже) – найти $c_1, \ldots, c_r \in K$, такие, что пересечение ${}^{\pi}W \cap \mathcal{Z}(c_1e_1 + \ldots + c_re_r)$ трансверсально и неприводимо над $\overline{K}$, т.е. доказать эффективную версию первой теоремы Бертини в ненулевой характеристике. Конечно, многообразие $W \cap \mathcal{Z}(c_1e_1 + \ldots + c_re_r)$ также неприводимо над $\overline{K}$ (но, вообще говоря, оно определено над чисто несепарабельным расширением поля K, не определено над K, и это пересечение не трансверсально).

Мы будем представлять каждый многочлен $f = f_j$ в виде

$$f = \frac{1}{a_0} \sum_{i_1, \ldots, i_n} \sum_{0 \leqslant j < \deg_Z \Phi} a_{i_1, \ldots, i_n, j} \eta^j X_1^{i_1} \cdots X_n^{i_n}, \tag{2}$$

где $a_0, a_{i_1, \ldots, i_n, j} \in \mathbb{F}_p[T_1, \ldots, T_l]$, $\mathrm{GCD}_{i_1, \ldots, i_n, j}(a_0, a_{i_1, \ldots, i_n, j}) = 1$. Для любого элемента $a \in \mathbb{F}_p$ положим длину его записи равной $\mathrm{l}(a) = [\log_2 p] + 1$ (здесь $[...]$ обозначает целую часть вещественного числа). Аналогично положим длину записи коэффициентов из $\mathbb{F}_p$ многочлена f равной $\mathrm{l}(f) = [\log_2 p] + 1$ и определим его степень как

$$\deg_{T_\gamma}(f) = \max_{i_1, \ldots, i_n, j} \{\deg_{T_\gamma}(a_0), \deg_{T_\gamma}(a_{i_1, \ldots, i_n, j})\}, \quad 1 \leqslant \gamma \leqslant l. \tag{3}$$

Подобным образом мы будем определять степени и длины записи коэффициентов других многочленов; в частности, определены $\deg_{T_\gamma} F$ и $\mathrm{l}(F)$. Можно аналогично определить $\deg_{T_1,\dots,T_l} f$ и другие степени, ср. с формулировкой леммы 1 из раздела 1.

Мы будем предполагать, что имеются следующие оценки:

$$\deg_{X_1,\dots,X_n}(f_j) < d,\ \deg_{T_\gamma}(f_j) < d_2,$$
$$\deg_{X_1,\dots,X_n} e_i < d,\ \deg_{T_\gamma}(e_i) < d_2,$$
$$\deg_Z(F) < d_1,\ \deg_{T_\gamma}(F) < d_1$$

для всех $1 \leqslant j \leqslant m$, $1 \leqslant i \leqslant r$, $1 \leqslant \gamma \leqslant l$ и целых чисел $d \geqslant 2$, $d_1 \geqslant 1$, $d_2 \geqslant 1$. Положим $M = [\log_2 p] + 1$.

Размер $\mathrm{L}(f)$ многочлена f определяется как произведение $\mathrm{l}(f)$ на число всех коэффициентов из $\mathbb{F}_p$ многочлена f в плотной записи, т.е. это число битов, необходимых для задания этого многочлена в плотном представлении коэффициентов. Мы имеем

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

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

Для всякого j, $1 \leqslant j \leqslant m$, рассмотрим однородный многочлен

$$\overline{f}_j = X_0^{\deg_{X_1,\dots,X_n} f_j} f_j(X_1/X_0, \dots, X_n/X_0) \in K[X_0, \dots, X_n].$$

Многочлен $\overline{f}_j$ является гомогенизацией многочлена f_j. Пусть $\widetilde{V} = \mathcal{Z}(\overline{f}_1, \dots, \overline{f}_m) \subset \mathbb{P}^n(\overline{K})$ – множество всех общих корней многочленов $\overline{f}_1, \dots, \overline{f}_m$ в проективном пространстве. Замыкание в проективном пространстве $\mathbb{P}^n(\overline{K})$ каждой неприводимой компоненты алгебраического многообразия V является неприводимой компонентой многообразия $\widetilde{V}$.

Замечание 1. В дальнейшем мы будем предполагать, что l является константой. Степени многочленов в оценках на $\deg_{T_\gamma}$ различных элементов и время работы в алгоритме из теоремы 1 могут зависеть от l, но, поскольку l – константа, мы не указываем их зависимость от l (хотя это и несложно сделать).

Теорема 1. *В предыдущих предположениях можно построить многообразие* ${}^{\pi}W$, *т.е. найти индексы* $1 \leqslant i_{r+1} < \dots < i_{n-s} \leqslant n$ *и целые числа* $\varepsilon_i \geqslant 0$, $1 \leqslant i \leqslant n$, *см. выше. В частности, если морфизм* π_r *сепарабелен, то* ${}^{\pi}W = W$. *Далее, можно построить такие*

элементы $c_1, \ldots, c_r \in K$ *с размерами* $O((s+r)\log d + \log n)$ *(мы обозначаем через* $\log(\ldots)$ *логарифм по основанию* e*), что алгебраическое многообразие* ${}^{\pi}W \cap \mathcal{Z}(c_1e_1 + \ldots + c_re_r)$ *является определённым над* K *и неприводимым над* $\overline{K}$ *и последнее пересечение трансверсально (в некоторой гладкой точке этого пересечения, которая является гладкой точкой многообразий* ${}^{\pi}W$ *и* $\mathcal{Z}(c_1e_1 + \ldots + c_re_r)$ *одновременно), т.е. справедливо утверждение первой теоремы Бертини для морфизма* π'_r *и этого пересечения. Более того, для всякой неприводимой над* $\overline{K}$ *компоненты* W' *многообразия* $\mathcal{Z}(f_1, \ldots, f_m)$*, если* $W' \neq W$*, то* $W \cap \mathcal{Z}(c_1e_1 + \ldots + c_re_r) \not\subset W'$*. Можно выбрать* $c_1, \ldots, c_r \in \mathbb{F}_p[T_1, \ldots, T_l]$ *со степенями*

$$\deg_{T_\gamma} c_j = O((((s+r)\log d + \log n)/\log p)^{1/l}) \tag{4}$$

для всех j*,* $1 \leqslant j \leqslant r$*,* $1 \leqslant \gamma \leqslant l$*, с абсолютной константой в* $O(\ldots)$*. Время работы алгоритма для построения элементов* $c_1, \ldots, c_r$ *полиномиально от* $d^{n(s+r)}$*,* d_1*,* d_2*,* p *и длины записи точки* $z^{(0)}$ *(напомним, что мы рассматриваем* l *как константу; так что оценки для времени работы здесь не зависят от* l *явно).*

Доказательство этой теоремы основывается на теореме 2 из [3], конструкции из приложения в [5] и алгоритмов из [1, 4].

Отметим, что можно сформулировать аналог теоремы 3 для нулевой характеристики. Однако в случае нулевой характеристики автором получены более сильные и точные результаты, см. [2]. Из [2] следует, что в теореме 1 для нулевой характеристики можно заменить $d^{n(r+s)}$ на d^n.

Для доказательства теоремы 1 мы используем лемму 1 раздела 1. Эта лемма интересна сама по себе. Применяя её аналог, можно доказать теорему 3 из раздела 1. В этой теореме мы получаем новый алгоритм для решения систем полиномиальных уравнений. Если уточнить оценки на степени исходных многочленов, то время работы этого алгоритма лучше, чем время работы алгоритма из гл. II работы [1] (и [4]) в общем случае (когда размерность многообразия корней рассматриваемой системы не мала).

Замечание 2. В утверждении теоремы 1 можно потребовать дополнительно, чтобы степень $\deg\big(W \cap \mathcal{Z}(c_1e_1 + \ldots + c_re_r)\big)$ была максимально возможной. Заменим везде в формулировке этой теоремы $s+r$ на n.

Тогда можно доказать полученную модифицированную версию утверждения теоремы 1 (и, весьма вероятно, даже без замены $s+r$ на n), однако это не является для нас необходимым в настоящее время.

Замечание 3 Можно выбрать другой план для доказательства теоремы 1, сначала сводя всё к случаю $r=3$. Это может слегка улучшить зависимость от r времени работы в утверждении теоремы.

Доказательство теоремы 1 в произвольной характеристике с временем работы, полиномиальным от d^n вместо d^{n^2} (в общем случае $d^{n(r+s)}$ ограничено сверху величиной d^{n^2}) является очень трудной проблемой. Для её решения понадобится несколько столетий. Подчеркнём здесь, что мы имеем в виду детерминированные алгоритмы с битовой сложностью.

В качестве приложения теоремы 1 мы получаем следующий результат.

Теорема 2. *Существуют константы $c>0$, $n_0>0$, $d_0>0$, такие, что для всякого конечного поля k для всех целых чисел $n>n_0$ и $d>d_0$ существуют однородные многочлены $f_1,\dots,f_\nu\in k[X_0,\dots,X_n]=A$, $\nu\leqslant n$, со степенями*

$$\deg f_i = O(d+\log^2 n(\log d)^{1/\log^2 n}),\quad 1\leqslant i\leqslant \nu \tag{5}$$

(константа в $O(\dots)$ здесь является абсолютной) и однородный простой идеал $\mathfrak{p}\subset A$, удовлетворяющие следующим условиям.

(a) *Множество нулей $\mathcal{Z}(\mathfrak{p})\subset\mathbb{P}^n(\overline{k})$ идеала $\mathfrak{p}$ совпадает с определённой над k и неприводимой над $\overline{k}$ компонентой проективного алгебраического многообразия $\mathcal{Z}(f_1,\dots,f_\nu)\subset\mathbb{P}^n(\overline{k})$ всех общих нулей многочленов $f_1,\dots,f_\nu$. Следовательно, идеал $\overline{k}\otimes_k\mathfrak{p}\subset\overline{k}\otimes_k A$ – простой. Более того, $\mathfrak{p}$ является примарной компонентой идеала $(f_1,\dots,f_\nu)\subset A$ высоты $\operatorname{ht}(\mathfrak{p})=\nu$.*

(b) *Предположим, что характеристическая функция $h(\mathfrak{p},m)$ стабильна для $m\geqslant m_0$, т.е. совпадает с многочленом Гильберта кольца $A/\mathfrak{p}$ для этих m. Тогда $m_0\geqslant d^{2^{cn}}$.*

(c) *Пусть $a_1,\dots,a_m$ – произвольная система образующих идеала $\mathfrak{p}$. Тогда $\max_{1\leqslant i\leqslant m}\deg_{X_0,\dots,X_n} a_i\geqslant d^{2^{cn}}$.*

Ранее известный результат с $d^{2^{c\sqrt{n}}}$ вместо $d^{2^{cn}}$ следует из предложения 1 работы [2]. Теперь оценки из пп. (a) и (b) – почти такие же, как

и в случае бесконечного основного поля, см. теорему 1 из [2]. В последней теореме мы имеем $\deg f_i = O(d)$ для случая бесконечного основного поля. Так что остаётся проблема улучшить (5) до $\deg f_i = O(d)$ в случае конечного основного поля. С помощью теоремы 1 можно получить вместо (5) даже несколько лучшие оценки, но они являются более громоздкими и не дают принципиальных улучшений. Так что мы решили выбрать (5) в формулировке теоремы 2. Заметим также, что из теоремы 1 получается положительный ответ на вопрос, поставленный в замечании 5 из [2]. Мы были не очень точны, формулируя его. Но фактически там мы хотели получить результат, аналогичный теореме 2.

Следствие 1. *В условиях теоремы* 1 *обозначим* $D = \deg \mathcal{Z}(\mathfrak{p})$. *Тогда существует константа* $\gamma > 0$, *такая, что в обозначениях из этой теоремы* $m_0 \geqslant D^{2^{\gamma n}}$ *и* $\max_{1 \leqslant i \leqslant m} \deg_{X_0,\dots,X_n} a_i \geqslant D^{2^{\gamma n}}$

Подобное следствие справедливо и в случае бесконечного поля k, см. [2]. Для конечного поля k из [2] можно получить только аналогичное следствие с $D^{2^{\gamma\sqrt{n}}}$ вместо $D^{2^{\gamma n}}$. Так что здесь мы также имеем улучшение известной дважды экспоненциальной нижней оценки.

§1. Построение пересечения неприводимой компоненты алгебраического многообразия с гиперповерхностью

Обозначим через $K^{p^{-\infty}}$ совершенное замыкание поля K. Для всякого целого числа $\nu \geqslant 0$ положим $K^{p^{-\nu}}$ равным подполю поля $K^{p^{-\infty}}$, состоящему из всех элементов $z \in K^{p^{-\infty}}$, таких, что $z^{p^\nu} \in K$.

Лемма 1. *Пусть* W *– неприводимая компонента из формулировки теоремы* 1, *см. введение. Пусть* $G \in K[X_1, \dots, X_n]$ *– многочлен степени*

$$\deg_{X_1,\dots,X_n} G \leqslant d'$$

и $\deg_{T_\gamma} G \leqslant d'_2$ *при всех* $1 \leqslant \gamma \leqslant l$ *для некоторых целых чисел* $d' \geqslant 2$, $d'_2 \geqslant 1$. *Тогда можно можно выяснить, верно ли, что* $W \not\subset \mathcal{Z}(G)$, *и, если* $W \not\subset \mathcal{Z}(G)$, *то можно построить разложение пересечения*

$$W \cap \mathcal{Z}(G) = \bigcup_{i \in I} W_i$$

на неприводимые над $K^{p^{-\infty}}$ *компоненты. Более того, каждая компонента* W_i *определена над полем* $K^{p^{-\nu}}$, *целое число* p^ν *ограничено сверху величиной* $(d^s d')^{O(1)}$, *и* W_i *задано своей общей точкой аналогично* [1], *т.е. строится* $K^{p^{-\nu}}$*-изоморфизм поля рациональных функций, определённых над* $K^{p^{-\nu}}$,

$$\xi_i \,:\, K^{p^{-\nu}}(W_i) \to K^{p^{-\nu}}(t_1, \ldots, t_{n-s-1})[\theta_i]. \tag{6}$$

Здесь $t_1, \ldots, t_{n-s-1}$ *алгебраически независимы над полем* $K^{p^{-\nu}}$, *а элемент* θ_i *– алгебраический сепарабельный над полем* $K^{p^{-\nu}}(t_1, \ldots, t_{n-s-1})$ *с минимальным многочленом* $\Psi_i \in K^{p^{-\nu}}(t_1, \ldots, t_{n-s-1})[Z]$ *(этот многочлен* Ψ_i *строится алгоритмом); и, далее, существуют индексы* $1 \leqslant j_1 < \ldots < j_{n-s-1} \leqslant n$, *такие, что* $X_{j_\beta} \mapsto t_j$, $1 \leqslant \beta \leqslant n-s-1$, *при изоморфизме* (6). *Мы представляем все* $\Psi_i^{p^\nu}$, $\xi_i(X_j)^{p^\nu}$ *аналогично* (2), *см. введение, но теперь мы имеем трансцендентные элементы* $T_1, \ldots, T_l, t_1, \ldots, t_{n-s-1}$ *вместо* $T_1, \ldots, T_l$. *Для всех* j, i *степени*

$$\deg_{T_\gamma} \Psi_i^{p^\nu}, \quad \deg_{T_\gamma} \xi_i(X_j)^{p^\nu}, \quad 1 \leqslant \gamma \leqslant l,$$

$$\deg_{t_1,\ldots,t_{n-s-1}} \Psi_i^{p^\nu}, \quad \deg_{t_1,\ldots,t_{n-s-1}} \xi_i(X_j)^{p^\nu}, \quad 1 \leqslant \mu \leqslant n-s-1,$$

определяются аналогично (3), *см. введение. Справедливы следующие оценки на степени для всех* $1 \leqslant i \leqslant n$, $1 \leqslant \gamma \leqslant l$, $1 \leqslant \mu \leqslant n-s-1$:

$$\begin{aligned}
&\deg_Z \Psi_i \leqslant \deg W_i \leqslant d^s d',\\
&\deg_{T_\gamma} \Psi_i^{p^\nu} = (d_2 + d_2')(d_1 d^s d')^{O(1)},\\
&\deg_{T_\gamma} \xi_i(X_j)^{p^\nu} = (d_2 + d_2')(d_1 d^s d')^{O(1)},\\
&\deg_{t_1,\ldots,t_{n-s-1}} \Psi_i^{p^\nu} = (d^s d')^{O(1)},\\
&\deg_{t_1,\ldots,t_{n-s-1}} \xi_i(X_j)^{p^\nu} = (d^s d')^{O(1)}.
\end{aligned}$$

Число элементов $\#I$ *не превосходит* $d^s d'$ *по теореме Безу. Время работы для построения общих точек всех алгебраических многообразий* W_i, $i \in I$, *полиномиально от* d^{sn}, $(d')^n$, d_1, d_2, p *и длины записи точки* $z^{(0)}$ *(оценка времени работы зависит от* l, *но мы рассматриваем* l *как константу, см. замечание* 1, *так что мы не указываем эту зависимость от* l, *хотя это несложно сделать).*

Доказательство. Мы приведём здесь основные идеи доказательства. Оно использует технику из [1, 4]. Достаточно описать модификации алгоритмов из [1, 4]. Однако мы опустим некоторые детали (мы оставляем их читателю).

Сначала заметим (ср. [1]), что существует полиномиальный алгоритм, выясняющий для данного элемента $z \in K$, верно ли, что $z \in K^p$, и, если $z \in K^p$, находящий $z^{1/p} \in K$ тоже за полиномиальное время (мы оставляем детали читателю). Мы будем использовать этот факт в доказательстве даже без ссылки на него.

Пусть $\overline{W}$ – замыкание алгебраического многообразия W в $\mathbb{P}^n(\overline{K})$. Сначала мы строим, применяя алгоритмы из [1, 4], общие точки всех неприводимых компонент W'' проективного алгебраического многообразия $\widetilde{V} = \mathcal{Z}(\overline{f}_1, \ldots, \overline{f}_m)$, такие, что $\dim W'' \geqslant n - s$. Снова применяя алгоритм из [1, 4], для всякой компоненты W'' мы строим систему полиномиальных уравнений, задающую эту компоненту как множество точек в $\mathbb{P}^n(\overline{K})$. Используя заданную точку $z^{(0)}$ и эти системы полиномиальных уравнений, мы находим среди всех W'' компоненту $\overline{W}$. Более точно, мы находим общую точку $\xi_{\overline{W}}$ алгебраического многообразия $\overline{W}$ или, что то же самое, общую точку алгебраического многообразия W, но в однородных координатах пространства $\mathbb{P}^n(\overline{K})$. Мы получаем также линейно независимые однородные многочлены $\psi_1, \ldots, \psi_N \in K[X_0, \ldots, X_n]$, такие, что $\overline{W} = \mathcal{Z}(\psi_1, \ldots, \psi_N)$ в $\mathbb{P}^n(\overline{K})$. Согласно [1], имеем $\deg_{X_0,\ldots,X_n} \psi_j = d^{O(s)}$, $1 \leqslant j \leqslant N$.

Теперь с помощью $\xi_{\overline{W}}$ мы можем выяснить, верно ли, что $W \subset \mathcal{Z}(G)$. В дальнейшем мы будем предполагать, что $W \not\subset \mathcal{Z}(G)$.

Напомним, что $\overline{G}$ является гомогенизацией многочлена G, см. введение. Сначала нашей целью является построение разложения $\overline{W} \cap \mathcal{Z}(\overline{G}) = \cup_{i \in I'} W_i'$ на неприводимые над $K^{p^{-\infty}}$ компоненты в $\mathbb{P}^n(\overline{K})$. Пусть $K(W)$ – поле определённых над K рациональных функций алгебраического многообразия W. При помощи перебора, см. [1], мы находим линейные формы $Z_0, \ldots, Z_{n-s} \in K[X_0, \ldots, X_n]$ с коэффициентами из K, такие, что

$$\overline{W} \cap \mathcal{Z}(Z_0, \ldots, Z_{n-s}) = \varnothing \tag{7}$$

в $\mathbb{P}^n(\overline{K})$. Заметим, что (7) имеет место в том и только в том случае, если система полиномиальных уравнений

$$\psi_1 = \ldots = \psi_N = Z_0 = \ldots = Z_{n-s} = 0$$

не имеет решений в $\mathbb{P}^n(\overline{K})$. Следовательно, можно выяснить, верно ли, что справедливо (7), за полиномиальное от d^{sn} и длины записи входных данных время, см. [1].

Теперь (ср. с гл. II работы [1]) $Z_1/Z_0, \dots, Z_{n-s}/Z_0$ – базис трансцендентности (не обязательно сепарабельный) поля $K(W)$ над K. Мы находим минимальное целое число $\mu \geqslant 0$, такое, что всякий элемент из $K(W)^{p^\mu}$ сепарабелен над полем $K(Z_1/Z_0, \dots, Z_{n-s}/Z_0) = \mathcal{K}$. Можно доказать, что $p^\mu = d^{O(s)}$, ср. [1] (здесь μ зависит от выбора линейных форм $Z_0, \dots, Z_{n-s}$).

Далее, снова при помощи перебора (ср. [1]), мы строим линейную форму $Z_{n-s+1} \in K[X_0, \dots, X_n]$ с коэффициентами из K, такую, что

$$K(Z_1/Z_0, \dots, Z_{n-s}/Z_0)[(Z_{n-s+1}/Z_0)^{p^\mu}] = \mathcal{K}_1$$

– максимальное сепарабельное над $\mathcal{K}$ подполе поля $K(W)$. Мы находим также минимальный многочлен $\varphi \in \mathcal{K}[Z]$ элемента $(Z_{n-s+1}/Z_0)^{p^\mu} \in \mathcal{K}_1$ над $\mathcal{K}$ и для всякой рациональной функции $(X_j/Z_0)^{p^\mu} \in K(W), 0 \leq j \leq n$, её представление $(X_j/Z_0)^{p^\mu} \in \mathcal{K}[Z]/(\varphi) = \mathcal{K}_1$.

Пусть $N_{\mathcal{K}_1/\mathcal{K}} : \mathcal{K}_1 \to \mathcal{K}$ – норменное отображение полей. Положим $\nu = [\mathcal{K}_1 : \mathcal{K}]\, p^\mu \deg_{X_1,\dots,X_n} G$. Норма всякого элемента $z \in \mathcal{K}_1$ вычисляется как определитель матрицы $\mathcal{K}$-линейного преобразования $\mathcal{K}_1 \to \mathcal{K}_1$, $x \mapsto zx$, в некотором базисе поля $\mathcal{K}_1$ над $\mathcal{K}$. Мы вычисляем однородный многочлен

$$Z_0^\nu N_{\mathcal{K}_1/\mathcal{K}} \left(\overline{G}/Z_0^{\deg_{X_1,\dots,X_n} G}\right)^{p^\mu} = G_0 \in K[Z_0, \dots, Z_{n-s}].$$

Заметим, что $\deg_{Z_0,\dots,Z_{n-s}} G_0 = (d^s d')^{O(1)}$. Осуществляя невырожденное линейное преобразование с коэффициентами из K линейных форм $Z_0, \dots, Z_{n-s}$, мы будем предполагать без ограничения общности, что старший коэффициент $\mathrm{lc}_{Z_{n-s}} G_0$ лежит в K, т.е.,

$$\deg_{Z_{n-s}} G_0 = \deg_{Z_0,\dots,Z_{n-s}} G_0. \tag{8}$$

Рассмотрим линейную проекцию

$$q : \mathbb{P}^n(\overline{K}) \to \mathbb{P}^{n-s}(\overline{K}), \quad (X_0 : \dots : X_n) \mapsto (Z_0 : \dots : Z_{n-s}).$$

Теперь для всякого $i \in I'$ морфизм

$$W_i' \to \mathbb{P}^{n-s-1}(\overline{K}), \quad (X_0 : \dots : X_n) \mapsto (Z_0 : \dots : Z_{n-s-1}),$$

является конечным и $q(\overline{W} \cap \overline{G}) = \mathcal{Z}(G_0)$. Следовательно, для всякого $i \in I'$ имеем $W_i' \cap \mathcal{Z}(Z_0, ..., Z_{n-s-1}) = \varnothing$ в $\mathbb{P}^n(\overline{K})$, и $Z_1/Z_0, ..., Z_{n-s-1}/Z_0$ – базис трансцендентности поля $K^{p^{-\infty}}(W_i')$ над $K^{p^{-\infty}}$.

Мы раскладываем многочлен G_0 в кольце $K^{p^{-\infty}}[Z_0, \ldots, Z_{n-s}]$ на множители при помощи алгоритма из $[1, 4]$ и получаем разложение на неприводимые: $G_0 = \prod_{\gamma \in \Gamma} G_\gamma^{v_\gamma}$, где $v_\gamma > 0$ – целые числа и Γ – конечное множество индексов. Для всякого $\gamma \in \Gamma$ представим $G_\gamma = G'_\gamma(Z_0, \ldots, Z_{n-s-1}, Z_{n-s}^{p^{\mu_\gamma}})$, где $G'_\gamma \in K^{p^{-\infty}}[Z_0, \ldots, Z_{n-s}]$ и целое число $\mu_\gamma \geqslant 0$ является наибольшим возможным (оно однозначно определено). Положим

$$\delta(Z_{n-s}) = \sum_{\gamma \in \Gamma} \deg_{Z_{n-s}} G'_\gamma.$$

Теперь мы хотим варьировать Z_{n-s} таким образом, чтобы оставались справедливыми (7) и (8). Конечно, многочлен G_0 также варьируется. Сверх того, в настоящее время линейная форма Z_{n-s+1} и целое число μ в описанной конструкции также могут изменяться вместе с Z_{n-s}, но в дальнейшем нам нужен только многочлен G_0. Целью сейчас является получить линейную форму Z_{n-s}, такую, что $\delta(Z_{n-s})$ – максимально возможное (среди всех целых чисел $\delta(Z'_{n-s})$ для линейных форм Z'_{n-s}, аналогичных Z_{n-s}, таких, что выполняются (7) и (8) с Z'_{n-s} вместо Z_{n-s}). Положим $\mathcal{K}_2 = K^{p^{-\infty}}(Z_1/Z_0, \ldots, Z_{n-s-1}/Z_0)$. Можно доказать, что $\delta(Z_{n-s})$ максимально возможное в том и только в том случае, если $\#\Gamma = \#I'$ и для всех γ и i из равенства $\mathcal{Z}(G_\gamma) = q(W_i')$ следует, что $\mathcal{K}_2[(Z_{n-s}/Z_0)^{p^{\mu_1}}]$ (здесь мы предполагаем, что $(Z_{n-s}/Z_0)^{p^{\mu_1}} \in K^{p^{-\infty}}(W_i')$) является максимальным сепарабельным над $\mathcal{K}_2$ подполем поля рациональных функций $K^{p^{-\infty}}(W_i')$ для некоторого целого числа $\mu_1 \geqslant 0$, такого, что $p^{\mu_1} = (d^s d')^{O(1)}$ (μ_1 одно и то же для всех $i \in I'$). Более того, можно выбрать μ_1 таким, что для всякого элемента $z \in K^{p^{-\infty}}(W_i')$ будем иметь $z^{p^{\mu_1}} \in \mathcal{K}_2[(Z_{n-s}/Z_0)^{p^{\mu_1}}]$ для всех $i \in I'$.

Опишем, как построить требуемую линейную форму Z_{n-s}. Мы выбираем подмножество $J_0 \subset K$ с достаточно большим числом элементов. Более точно, существует многочлен $P \in \mathbb{Z}[Z]$ (многочлен P является абсолютным, т.е. его коэффициенты – абсолютные константы; они не зависят от чего-либо), такой, что если $\#J_0 = P(d^s d')$, то описываемый алгоритм работает корректно. Дополнительно мы выбираем $J_0 \subset \mathbb{F}_p[T_1, \ldots, T_l]$ так, что для всякого $\alpha \in J_0$ степени $\deg_{T_\gamma}$ имеем

$\alpha = O(((\log d' + s\log d)/\log p)^{1/l})$ для всех $1 \leqslant \gamma \leqslant l$ (с абсолютной константой в $O(\dots)$). Мы используем рекурсию по $0 \leqslant i \leqslant n$. Линейная форма Z_{n-s} изменяется на каждом шаге рекурсии.

Для рассматриваемого i, $0 \leqslant i \leqslant n$, на i-м шаге рекурсии мы перебираем линейные формы $Z_{n-s} + \alpha X_i$, $\alpha \in J_0$. Обозначим через J_0' подмножество всех $\alpha \in J_0$, таких, что (7) и (8) выполняются для $Z_{n-s}+\alpha X_i$ вместо первоначальной линейной формы Z_{n-s}. Если $\alpha \in J_0'$, то мы вычисляем $\delta(Z_{n-s} + \alpha X_i)$. Выберем элемент $\alpha_i \in J_0$, такой, что $\delta(Z_{n-s} + \alpha_i X_i) = \max_{\alpha \in J_0'} \delta(Z_{n-s} + \alpha X_i)$. После этого мы заменяем Z_{n-s} на $Z_{n-s} + \alpha_i X_i$ и, если $i + 1 \leqslant n$, переходим к $(i + 1)$-му шагу рекурсии. Можно доказать, что в конце рекурсии получается линейная форма Z_{n-s} с максимально возможным $\delta(Z_{n-s})$ (если P выбран заранее подходящим образом).

В дальнейшем мы будем предполагать, что $\delta(Z_{n-s})$ является максимально возможным. Мы отождествляем множества индексов Γ и I'. Именно, положим $i = \gamma$ тогда и только тогда, когда $\mathcal{Z}(G_\gamma) = q(W_i')$. Рассматривая $G_i(1, Z_1/Z_0, \dots, Z_{n-s}/Z_0)$, несложно построить минимальный многочлен $\widetilde{G}_i \in \mathcal{K}_2[Z]$ элемента $(Z_{n-s}/Z_0)^{p^{\mu_1}} \in K^{p^{-\infty}}(W_i')$ над $\mathcal{K}_2$. Положим $\mathcal{K}_{3,i} = \mathcal{K}_2[Z]/(\widetilde{G}_i)$. Определим

$$z_i = (Z_{n-s}/Z_0)^{p^{\mu_1}} \bmod \widetilde{G}_i \in \mathcal{K}_{3,i}.$$

Таким образом, $\mathcal{K}_2[z_i]$ является максимальным сепарабельным над $\mathcal{K}_2$ подполем поля $K^{p^{-\infty}}(W_i')$ для всякого $i \in I'$.

Расширим основное поле K до $K(t)$, где t – трансцендентный элемент над полем K. Заменим линейную форму Z_{n-s} на $Z_{n-s} + tX_j$ (мы осуществляем это для всех j, $0 \leqslant j \leqslant n$, последовательно). Многочлен G_0 соответствует Z_{n-s}. Аналогичным образом, пусть многочлен $G_{0,j}$ соответствует линейной форме $Z_{n-s} + tX_j$. Мы вычисляем $G_{0,j}$ для всякого j, $0 \leqslant j \leqslant n$. Разложим на неприводимые множители многочлен

$$G_{0,j}^{p^{\mu_1}}(1, Z_1/Z_0, \dots, Z_{n-s-1}/Z_0, Z^{p^{-\mu_1}}) \in (\mathcal{K}_2(t))^{p^{-\infty}}[Z] \tag{9}$$

над полем $(\mathcal{K}_2(t))^{p^{-\infty}}$ при помощи алгоритма из [1,4] (мы оставляем подробности читателю). Многочлен (9) имеет один и только один корень $z_i + tx_i$ кратности p^{μ_2} для некоторого целого числа $\mu_2 \geqslant 0$ (оно может зависеть от j и i), такой, что $x_i \in \mathcal{K}_{3,i}$ (этот элемент x_i однозначно определён). Теперь x_i отождествляется с $(X_i/Z_0)^{p^{\mu_1}} \in K^{p^{-\infty}}(W_i')$ для

всякого $i \in I'$. Это определяет общую точку ξ'_i алгебраического многообразия W'_i, ср. [1], заданную относительно рациональных функций Z_i/Z_0, $1 \leqslant i \leqslant n-s$.

С помощью алгоритма из [1] мы находим подмножество $I \subset I'$, такое, что $i \in I$ тогда и только тогда, когда $W'_i \not\subset \mathcal{Z}(X_0)$. Положим $W_i = W'_i \setminus \mathcal{Z}(X_0) \subset \mathbb{A}^n(\overline{K})$ для всякого $i \in I$. Далее мы собираемся построить требуемые общие точки ξ_i для всякого $i \in I$. С этой целью для фиксированного i мы перебираем наборы, состоящие каждый из $(n-s-1)$ целых чисел $(j_1, \ldots, j_{n-s-1})$, таких, что $1 \leqslant j_1 < \cdots < j_{n-s-1} \leqslant n$. Используя общие точки ξ'_i и алгоритмы из [1], можно выяснить, верно ли, что элементы $X_{j_1}, \ldots, X_{j_{n-s-1}} \in K^{p^{-\infty}}(W_i)$ являются алгебраически независимыми над $K^{p^{-\infty}}$. Здесь достаточно решить подходящую линейную систему над полем K относительно коэффициентов многочлена, дающего возможное алгебраическое соотношение между $X_{j_1}^{p^{\mu_1}}, \ldots, X_{j_{n-s-1}}^{p^{\mu_1}}$. Этот многочлен имеет степень, ограниченную сверху величиной $(d^s d')^{O(1)}$. Заметим, что в однородных координатах X_{j_β} соответствует функции $(X_{j_\beta}/Z_0)/(X_0/Z_0)$. Так что в аффинных координатах каждый элемент $X_{j_\beta}^{p^{\mu_1}}$ может быть вычислен при помощи общей точки ξ'_i.

Предположим, что $X_{j_1}, \ldots, X_{j_{n-s-1}} \in K^{p^{-\infty}}(W_i)$ являются алгебраически независимыми. Тогда аналогичным образом, используя алгоритм из [1], для заданной линейной формы L относительно $X_1, \ldots, X_n$ можно найти минимальный многочлен $\varphi \in K^{p^{-\infty}}(X_{j_1}, \ldots, X_{j_{n-s-1}})[Z]$ элемента $L \in K^{p^{-\infty}}(W_i)$ над полем $K^{p^{-\infty}}(X_{j_1}, \ldots, X_{j_{n-s-1}})$. В частности, можно выяснить, верно ли, что L сепарабельна над этим полем. Таким образом, мы можем найти сепарабельный базис трансцендентности $X_{j_1}, \ldots, X_{j_{n-s-1}} \in K^{p^{-\infty}}(W_i)$ последнего поля над $K^{p^{-\infty}}$. Далее, аналогично тому, как это было сделано для Z_{n-s}, можно построить линейную форму L_i, такую, что

$$K^{p^{-\infty}}(X_{j_1}, \ldots, X_{j_{n-s-1}})[L_i] = K^{p^{-\infty}}(W_i).$$

Наконец, раскладывая многочлены на неприводимые множители (ср. с конструкцией выше с основным полем $K(t)$), находим требуемые общие точки ξ_i.

Оценки на степени из утверждения леммы и время работы всего этого алгоритма немедленно следуют из описанной конструкции и [1, 4]. Лемма доказана. $\square$

Отметим, что при помощи [1] в доказательстве леммы 1 можно получить оценку для времени работы, полиномиальную от $(d_1 d_2)^n$ вместо $d_1 d_2$. Основная теорема гл. II работы [1] даёт оценку на время работы, полиномиальную от $d_1 d_2$, только если размерность $\dim W$ мала (или равна константе). Так что улучшение алгоритма из [1], полученное в [4], сейчас существенно.

Можно слегка модифицировать формулировку леммы 1. Теперь мы предполагаем, что W является произвольным неприводимым над $K^{p^{-\infty}}$ (соответственно над $\overline{K}$) аффинным алгебраическим многообразием, заданным своей общей точкой. Оценки на степени всех элементов из представления этой общей точки заданы. Отсюда естественным образом вытекают изменения оценок на целое число p^ν и на степени относительно $X_1, \ldots, X_n$; $t_1, \ldots, t_{n-s-1}$ и T_γ многочлена Ψ_i и общих точек ξ_i, $i \in I$, на выходе алгоритма в лемме. Последовательно используя эту модифицированную версию леммы 1, можно доказать следующий результат (при этом хорошие верхние границы на степени всех строящихся элементов надо получить заранее с помощью U-результантов и идей из [1, 4]; иначе при последовательном применении модификации леммы 1 может возникнуть оценка, зависящая от d_1^n вместо d_1, см. формулировку следующей теоремы).

Теорема 3. *Пусть $f_1, \ldots, f_m$ – многочлены из формулировки теоремы 1. Предположим дополнительно, что $\deg_{X_1,\ldots,X_n} f_i = D_i$, $1 \leqslant i \leqslant m$, и $D_1 \geqslant D_2 \geqslant \ldots \geqslant D_m$, $d = D_1 \geqslant 2$. Пусть $\nu = \min\{m, n\}$. Тогда можно построить разложение алгебраического многообразия $\mathcal{Z}(f_1, \ldots, f_m)$ на неприводимые над $K^{p^{-\infty}}$ (соответственно над $\overline{K}$) компоненты в смысле [1], т.е. построить общие точки всех этих неприводимых компонент и системы полиномиальных уравнений, задающие их как алгебраические многообразия в $\mathbb{A}^n(\overline{K})$. Время работы этого алгоритма полиномиально от $(D_1 \cdot \ldots \cdot D_\nu)^n$, d_1, d_2, m и p (напомним снова, что мы рассматриваем l как константу, но несложно аналогично [1, 4] дать оценки на время работы, зависящие от l, для произвольного l).*

В общем случае оценка времени работы с $(D_1 \cdot \ldots \cdot D_\nu)^n$ в этой теореме является более сильной, чем соответствующая оценка с d^{n^2} из основной теоремы гл. II работы [1]. С другой стороны, если $\beta = 1 + \dim \mathcal{Z}(\overline{f}_1, \ldots, \overline{f}_m)$, то [1] даёт более точную границу $d^{\beta n}$. Отметим, что $d^{\beta n}$ может быть меньше $(D_1 \cdot \ldots \cdot D_\nu)^n$, если β мало.

Заметим также, что теорема 3 (и аналог леммы 1) могут быть сформулированы в произвольной характеристике основного поля аналогичным образом. В случае нулевой характеристики в формулировках учитываются длины записи элементов из основного поля, ср. [1, 4].

§2. Доказательство теоремы 1

При помощи алгоритмов из [1], используя данную точку $z^{(0)}$, мы строим общую точку алгебраического многообразия W и систему полиномиальных уравнений, задающих эту компоненту. Пусть $K(W)$ – поле определённых над K рациональных функций алгебраического многообразия W. Пусть $\dim W = n - s$. Заметим, что $n - s \geqslant 3$. Пусть $x' = (0, \ldots, 0) \in \mathbb{A}^r(\overline{K})$. Существуют индексы $1 \leqslant i_{r+1} < \ldots < i_{n-s} \leqslant n$, такие, что морфизм

$$\pi : W \to \mathbb{A}^{n-s}(\overline{K}), \quad (X_1, \ldots, X_n) \mapsto (e_1, \ldots, e_r, X_{i_{r+1}}, \ldots, X_{i_{n-s}}), \quad (10)$$

является доминантным и дополнительно сепарабельным при условии, что морфизм π_r сепарабелен. Чтобы построить $(i_{r+1}, \ldots, i_{n-s})$, мы перебираем все возможные наборы $(j_{r+1}, \ldots, j_{n-s})$, такие, что $1 \leqslant j_{r+1} < \ldots < j_{n-s} \leqslant n$. Для каждого $(n - s - r)$-набора целых чисел $(j_{r+1}, \ldots, j_{n-s})$, используя [1], можно выяснить, верно ли, что элементы

$$e_1, \ldots, e_r, X_{j_{r+1}}, \ldots, X_{j_{n-s}} \in K(W) \quad (11)$$

алгебраически независимы над полем K. Положим $K_1 = K(e_1, \ldots, e_r, X_{j_{r+1}}, \ldots, X_{j_{n-s}})$. Если элементы (11) алгебраически независимы, то можно построить для всякого i, $1 \leqslant i \leqslant n$, минимальный многочлен из $K_1[Z]$ элемента $X_i \in K(W)$. Следовательно, можно найти также наименьшее целое число $\varepsilon_i \geqslant 0$, такое, что $X_i^{p^{\varepsilon_i}}$ сепарабелен над полем K_1. В частности, можно выяснить, верно ли, что $e_1, \ldots, e_r, X_{j_{r+1}}, \ldots, X_{j_{n-s}}$ образуют сепарабельный базис трансцендентности поля $K(W)$ над K, т.е. верно ли, что расширение полей $K(W) \supset K_1$ является конечным сепарабельным. Если морфизм π_r сепарабелен, то мы устанавливаем этот факт, выбираем индексы $1 \leqslant j_{r+1} < \ldots < j_{n-s} \leqslant n$, такие, что расширение $K(W) \supset K_1$ конечно сепарабельно. Если π_r является доминантным, но не сепарабельным, то мы выбираем индексы $1 \leqslant j_{r+1} < \ldots < j_{n-s} \leqslant n$, такие, что расширение $K(W) \supset K_1$ – конечное (алгебраическое). В любом случае обозначим $i_v = j_v$, $r+1 \leqslant v \leqslant n-s$, и $e_j = X_{i_j}$, $r + 1 \leqslant j \leqslant n - s$. Определим кольцо определённых над K

регулярных функций алгебраического многообразия ${}^{\pi}W$

$$K[{}^{\pi}W] = K[e_1, \dots, e_{n-s}, X_1^{p^{\varepsilon_1}}, \dots, X_n^{p^{\varepsilon_n}}].$$

Если морфизм π_r сепарабелен, то, очевидно, ${}^{\pi}W = W$. Таким образом, определённое над K и неприводимое над $\overline{K}$ аффинное алгебраическое многообразие ${}^{\pi}W$ построено. Пусть

$$\pi' : {}^{\pi}W \to \mathbb{A}^{n-s}(\overline{K}), \quad z \mapsto (e_1(z), \dots, e_{n-s}(z)),$$

– морфизм аффинных алгебраических многообразий. Теперь $\pi = \pi' \circ \iota$. Положим $x = (0, \dots, 0) \in \mathbb{A}^{n-s}(\overline{K})$.

Пусть $Y_1, \dots, Y_{n-s}$ – новые переменные. Рассмотрим аффинное алгебраическое многообразие $V' = \mathcal{Z}(f_1, \dots, f_m, e_1 - Y_1, \dots, e_{n-s} - Y_{n-s}) \subset \mathbb{A}^{2n-s}(\overline{K})$. Здесь последнее аффинное пространство имеет координатные функции $X_1, \dots, X_n, Y_1, \dots, Y_{n-s}$. Теперь W отождествляется с неприводимой компонентой многообразия V'. Следовательно, $Y_j \in K({}^{\pi}W)$, для всех j, расширение $K(W) \supset K(Y_1, \dots, Y_{n-s})$ конечно, расширение $K({}^{\pi}W) \supset K(Y_1, \dots, Y_{n-s})$ конечно сепарабельно. Используя теорему Безу, получаем, что степень $[K(W) : K(Y_1, \dots, Y_{n-s})]$ ограничена сверху величиной d^{s+r} (мы оставляем подробности читателю).

Снова применяя алгоритм из [1], мы строим такой элемент

$$y = \sum_{1 \leqslant i \leqslant n} l_i X_i^{p^{\varepsilon_i}} \in K({}^{\pi}W),$$

что все коэффициенты $l_i \in K$ имеют размер $O((s+r)\log d)$ и y является примитивным элементом расширения $K({}^{\pi}W) \supset K(e_1, \dots, e_{n-s})$. Более точно, мы строим минимальный многочлен $f \in K(Y_1, \dots, Y_{n-s})[Y]$ элемента y над полем $K(Y_1, \dots, Y_{n-s})$. Поскольку многообразие ${}^{\pi}W$ неприводимо над $\overline{K}$, многочлен f неприводим над полем $\overline{K}(Y_1, \dots, Y_{n-s})$. Следовательно, многочлен f сепарабелен относительно переменной Y, и $\deg_Y f \geqslant 1$. В дальнейшем мы будем предполагать без ограничения общности, что $f \in K[Y_1, \dots, Y_{n-s}, Y]$ является неприводимым над $\overline{K}$. При помощи теоремы Безу и [1] мы получаем, что $\deg_{Y_1, \dots, Y_{n-s}, Y} f \leqslant d^{s+r}$ и $\deg_{T_\gamma} f$ ограничена сверху величиной $d_2(d_1 d^{s+r})^{O(1)}$ для всякого γ, $1 \leqslant \gamma \leqslant l$.

Теперь напомним некоторые подробности из приложения работы [5]. Мы слегка меняем обозначения. Именно, мы заменяем в [5] многообразие V на ${}^{\pi}W$, морфизм p на π', поле $\overline{k}$ на $\overline{K}$, целое число n на $n-s$ и $X_1, \dots, X_n$ на $Y_1, \dots, Y_{n-s}$. Положим $\deg_{Y_1, \dots, Y_{n-s}, Y} f = m_1$ и положим

$f^{(m_1)}$ равным однородной относительно $Y_1, \ldots, Y_{n-s}, Y$ форме степени m_1 многочлена f.

Положим $B = \overline{K}[{}^{\pi}W]$ равным кольцу определённых над $\overline{K}$ регулярных функций алгебраического многообразия ${}^{\pi}W$. Пусть B' – целое замыкание кольца B в его поле частных. Для конечно порождённого B-модуля M обозначим через $\mathrm{Ass}_B(M)$ множество всех ассоциированных простых идеалов модуля M (они являются примарными идеалами кольца B).

Обозначим через

$$\Delta_1 = \mathrm{Res}_Y(f, \partial f/\partial Y) \in K[Y_1, \ldots, Y_{n-s}] \tag{12}$$

дискриминант многочлена f относительно Y. Тогда $\Delta_1 \neq 0$, поскольку f является сепарабельным. Мы вычисляем $\Delta_1 \in K[Y_1, \ldots, Y_{n-s}]$. Имеем $\deg_{Y_1,\ldots,Y_{n-s}} \Delta_1 = O(d^{2(r+s)})$, и $\deg_{T_\gamma} \Delta_1$ ограничена сверху величиной $d_2(d_1 d^{r+s})^{O(1)}$ для всякого γ, $1 \leqslant \gamma \leqslant l$.

Отождествим множество всех линейных форм из $\overline{K}[Y_1, \ldots, Y_{n-s}]$ с аффинным пространством $\mathbb{A}^{n-s}(\overline{K})$. Пусть $\mathfrak{P}$ – простой идеал кольца $\overline{K}[Y_1, \ldots, Y_{n-s}]$ (соответственно B, B'). Предположим, что

$$\mathcal{Z}(\mathfrak{P}) \not\subset \mathcal{Z}(Y_1, \ldots, Y_{n-s}),$$

где $\mathcal{Z}(Y_1, \ldots, Y_{n-s})$ и $\mathcal{Z}(\mathfrak{P})$ рассматриваются как подмногообразия пространства $\mathbb{A}^{n-s}(\overline{K})$ (соответственно многообразия ${}^{\pi}W$, нормализации многообразия ${}^{\pi}W$). Тогда множество $S_{\mathfrak{P}}$ линейных форм $L \in \overline{K}[Y_1, \ldots, Y_{n-s}]$, таких, что $L \notin \mathfrak{P}$, является непустым открытым в топологии Зариского в $\mathbb{A}^{n-s}(\overline{K})$, поскольку

$$S_{\mathfrak{P}} = \bigcup_{z \in \mathcal{Z}(\mathfrak{P})} \Big\{ L \in \mathbb{A}^{n-s}(\overline{K}) \,:\, L(z) \neq 0 \Big\}.$$

Рассмотрим B'/B как B-модуль. Положим

$$\mathcal{B}_0 = \mathrm{Ass}_B(B'/B), \quad \mathcal{B}_2 = \{\mathfrak{P} \in \mathcal{B}_0 \,:\, \dim \mathcal{Z}(\mathfrak{P}) = n - s - 1\}.$$

Рассмотрим множество $\mathcal{U}_2$ (мы не используем множество $\mathcal{U}_1$ из [5]) линейных форм L от $Y_1, \ldots, Y_{n-s}$ таких, что $L \notin \mathfrak{P}$ для всякого $\mathcal{B}_2$. Тогда $\mathcal{U}_2$ является непустым открытым в топологии Зариского подмножеством пространства $\mathbb{A}^{n-s}(\overline{K})$.

Лемма 2. *Можно построить многочлен $\Delta_2 \in K[X_1, \ldots, X_n]$ со степенями $\deg_{X_1,\ldots,X_n} \Delta_2 = (d^s)^{O(1)}$ и $\deg_{T_\gamma} \Delta_2$, ограниченными сверху величиной $d_2(d_1 d^s)^{O(1)}$ для всех γ, $1 \leqslant \gamma \leqslant l$, такой, что $W \not\subset \mathcal{Z}(\Delta_2)$ и*

для всякого $\mathfrak{P} \in \mathcal{B}_2$ алгебраическое многообразие $\iota^{-1}(\mathcal{Z}(\mathfrak{P}))$ является определённой над $\overline{K}$ и неприводимой над $\overline{K}$ компонентой пересечения $W \cap \mathcal{Z}(\Delta_2)$.

Далее, пусть $W \cap \mathcal{Z}(\Delta_2) = \bigcup\limits_{i \in I_2} W_i$ – разложение пересечения $W \cap \mathcal{Z}(\Delta_2)$ на неприводимые над $K^{p^{-\infty}}$ компоненты. Тогда, применяя лемму 1, можно построить все общие точки ξ_i алгебраических многообразий W_i, $i \in I_2$. Имеем $\#I_2 = (d^s)^{O(1)}$ по теореме Безу. Время работы алгоритмов для построения многочлена Δ_2 и всех общих точек алгебраических многообразий W_i, $i \in I_2$, полиномиально от d^{sn}, d_1, d_2 и p.

Доказательство. Обозначим через $\mathrm{Sing}\,(W)$ и $\mathrm{Sing}\,({}^{\pi}W)$ многообразия всех особых точек многообразий W и ${}^{\pi}W$ соответственно. Заметим, что для всякого $\mathfrak{P} \in \mathcal{B}_2$ имеем $\mathcal{Z}(\mathfrak{P}) \subset \mathrm{Sing}({}^{\pi}W)$.

Покажем, что для всякого $\mathfrak{P} \in \mathcal{B}_2$ имеет место вложение $\iota^{-1}(\mathcal{Z}(\mathfrak{P})) \subset \mathrm{Sing}(W)$. Действительно, предположим противное. Тогда существует многочлен $0 \neq \psi \in K[X_1^{p^{\varepsilon_1}}, \ldots, X_n^{p^{\varepsilon_n}}]$, такой, что $\mathcal{Z}(\mathfrak{P}) \setminus \mathcal{Z}(\psi) \neq \varnothing$, многообразие $W \setminus \mathcal{Z}(\psi)$ является гладким и, следовательно, кольцо $\overline{K}[W \setminus \mathcal{Z}(\psi)]$ целозамкнуто. Это кольцо цело над $\overline{K}[{}^{\pi}W \setminus \mathcal{Z}(\psi)]$, и каждый элемент из $\overline{K}[W \setminus \mathcal{Z}(\psi)] \setminus \overline{K}[{}^{\pi}W \setminus \mathcal{Z}(\psi)]$ является чисто несепарабельным над полем $K({}^{\pi}W)$ со степенью несепарабельности > 1. С другой стороны, кольцо $\overline{K}[{}^{\pi}W \setminus \mathcal{Z}(\psi)]$ не является целозамкнутым, поскольку $\mathfrak{P} \in \mathcal{B}_2$ и $\mathcal{Z}(\mathfrak{P}) \setminus \mathcal{Z}(\psi) \neq \varnothing$. Поэтому существует элемент $a \in \overline{K}(W) \setminus \overline{K}[{}^{\pi}W \setminus \mathcal{Z}(\psi)]$, который цел над $\overline{K}[{}^{\pi}W \setminus \mathcal{Z}(\psi)]$. Очевидно, $a \in \overline{K}[W \setminus \mathcal{Z}(\psi)] \setminus \overline{K}[{}^{\pi}W \setminus \mathcal{Z}(\psi)]$, и a имеет степень несепарабельности 1 над $\overline{K}({}^{\pi}W)$. Полученное противоречие доказывает требуемое утверждение.

Мы используем обозначения из доказательства леммы 1. Сначала мы строим общую точку многообразия $\overline{W}$, многочлены $\psi_1, \ldots, \psi_N$ и линейные формы $Z_0, \ldots, Z_{n-s} \in K[X_0, \ldots, X_n]$, такие, что $\overline{W} \cap \mathcal{Z}(Z_0, \ldots, Z_{n-s}) = \varnothing$ в $\mathbb{P}^n(\overline{K})$. Мы также находим перебором (ср. доказательство леммы 1) сепарабельный базис трансцендентности $X_{i_1}/Z_0, \ldots, X_{i_{n-s}}/Z_0$ поля $K(W)$ над K.

Можно доказать, что всякое конечное подмножество в $\mathbb{F}_p[T_1, \ldots, T_l]$ с $nd^{O(s)}$ элементами (здесь константа в $O(s)$ достаточно большая, она является абсолютной) содержит элемент t', такой, что

- $\overline{W} \cap \mathcal{Z}(Z_0, Z_1 + t'X_{i_1}, \ldots, Z_{n-s} + t'X_{i_{n-s}}) = \varnothing$ в $\mathbb{P}^n(\overline{K})$,

- $(Z_1 + t'X_{i_1})/Z_0, \ldots, (Z_{n-s} + t'X_{i_{n-s}})/Z_0$ – сепарабельный базис трансцендентности поля $K(W)$ над K

(мы оставляем детали читателю). Поэтому при помощи перебора можно найти элемент $t' \in \mathbb{F}_p[T_1, \ldots, T_l]$, удовлетворяющий этим двум свойствам, такой, что $\deg_{T_\gamma} t' = O(((\log n + s \log d)/\log p)^{1/l})$ для всех γ, $1 \leqslant \gamma \leqslant l$.

Положим $L_0 = Z_0$, $L_j = Z_j + t'X_{i_j}$ для всех j, $1 \leqslant j \leqslant n-s$. Затем мы строим (см. [1] и ср. доказательство леммы 1) линейную форму $L_{n-s+1} \in K[X_0, \ldots, X_n]$, такую, что L_{n-s+1}/L_0 является примитивным элементом сепарабельного расширения полей

$$K(W) \supset K(L_1/L_0, \ldots, L_{n-s}/L_0).$$

Мы вычисляем ненулевой полином $\varphi_L \in K[X_0, \ldots, X_{n-s+1}]$ минимальной степени, такой, что $\varphi_L(L_0, \ldots, L_{n-s+1})$ обращается в нуль тождественно на многообразии $\overline{W}$ (т.е. он обращается в нуль в общей точке алгебраического многообразия W).

Рассмотрим морфизмы проективных алгебраических многообразий

$$p_L : \overline{W} \to \mathbb{P}^{n-s}(\overline{K}), \qquad (X_0 : \ldots : X_n) \mapsto (L_0 : \ldots : L_{n-s}),$$
$$q_L : \overline{W} \to \mathbb{P}^{n-s+1}(\overline{K}), \quad (X_0 : \ldots : X_n) \mapsto (L_0 : \ldots : L_{n-s+1}).$$

Тогда морфизм p_L является конечным сепарабельным, $q_L(\overline{W}) = \mathcal{Z}(\varphi_L)$ в $\mathbb{P}^{n-s+1}(\overline{K})$, и морфизм $\overline{W} \to q_L(\overline{W})$ является конечным сепарабельным, доминантным и бирациональным.

Согласно основной теореме Зариского,

$$\overline{W} \cap \mathcal{Z}((\partial\varphi_L/\partial X_{n-s+1})(L_0, \ldots, L_{n-s+1})) \supset \mathrm{Sing}(\overline{W}).$$

Следовательно, можно взять $\Delta_2 = (\partial\varphi_L/\partial X_{n-s+1})(L_0, ..., L_{n-s+1})\big|_{X_0=1}$. Мы имеем $\deg_{X_1,\ldots,X_n} \Delta_2 = d^{O(s)}$.

Оценка на время работы этого алгоритма немедленно следует из описанной конструкции и [1, 4]. Лемма доказана. □

С помощью леммы 2 мы строим все объекты, которые получаются на выходе алгоритмов из формулировки этой леммы, и фиксируем их.

Теперь мы снова возвращаемся к подробностям из [5]. Пусть $L \in \overline{K}[Y_1, \ldots, Y_{n-s}]$ – ненулевая линейная форма. Рассмотрим B/LB как B-модуль. Положим

$$\mathcal{B}_{2,L} = (\mathcal{B}_0 \setminus \mathcal{B}_2) \cap \mathrm{Ass}_B(B/LB).$$

Далее, покажем, что существует ненулевой полином

$$\Delta_3 \in K[Y_1, \dots, Y_{n-s}],$$

такой, что расширение колец

$$B[\Delta_3^{-1}] \supset \overline{K}[Y_1, \dots, Y_{n-s}, \Delta_3^{-1}][y] \supset \overline{K}[Y_1, \dots, Y_{n-s}][\Delta_3^{-1}] \tag{13}$$

является целым. В самом деле, можно выбрать Δ_3 равным произведению $\mathrm{lc}_Y f$ и всех старших коэффициентов минимальных многочленов над $K[Y_1, \dots, Y_{n-s}]$ элементов $X_1^{p^{\varepsilon_1}}, \dots, X_n^{p^{\varepsilon_n}} \in B$. При помощи алгоритмов из [1] мы строим и фиксируем такой многочлен Δ_3. Заметим, что $\deg_{Y_1,\dots,Y_{n-s}} \Delta_3 = n(d^{s+r})^{O(1)}$ и $\deg_{T_\gamma} \Delta_3$ ограничены сверху величиной $nd_2(d_1 d^{s+r})^{O(1)}$ для всех γ, $1 \leqslant \gamma \leqslant l$. Положим $\widetilde{\Delta}_3 = \Delta_3(e_1, \dots, e_{n-s}) \in K[X_1, \dots, X_n]$.

Положим $\mathcal{B}_3 = \mathrm{Ass}_{B'}(B'/\Delta_3 B')$, где $B'/\Delta_3 B'$ рассматривается как B'-модуль. Тогда элементы из $\mathcal{B}_3$ являются простыми идеалами кольца B'. Обозначим через $\mathcal{U}_3$ множество всех таких линейных форм $L \in \overline{K}[Y_1, \dots, Y_{n-s}]$, что $L \notin \mathfrak{P}$ для всякого $\mathfrak{P} \in \mathcal{B}_3$. Поскольку B' целозамкнуто, $\dim \mathcal{Z}(\mathfrak{P}) = n - s - 1$ для всякого $\mathfrak{P} \in \mathcal{B}_3$. Поэтому $\mathcal{U}_3$ – непустое открытое в топологии Зариского подмножество пространства $\mathbb{A}^{n-s}(\overline{K})$. Заметим, что если $L \in \mathcal{U}_3$, то L не делит Δ_3 в кольце $K[Y_1, \dots, Y_{n-s}]$.

Пусть

$$W \cap \mathcal{Z}(\widetilde{\Delta}_3) = \bigcup_{i \in I_3} W_i$$

– разложение пересечения $W \cap \mathcal{Z}(\widetilde{\Delta}_3)$ на неприводимые над $K^{p^{-\infty}}$ компоненты. Применяя лемму 1, мы строим все общие точки ξ_i, $i \in I_3$, определённых над $K^{p^{-\infty}}$ и неприводимых над $K^{p^{-\infty}}$ компонент пересечения $W \cap \mathcal{Z}(\widetilde{\Delta}_3)$. Имеем $\#I_3 = n(d^{s+r})^{O(1)}$ по лемме 1.

Напомним, что мы отождествляем многообразия V и V', см. выше. Согласно данным определениям, мы имеем

$$W \cap \mathcal{Z}(\widetilde{\Delta}_3) = \bigcup_{\mathfrak{P} \in \mathcal{B}_3} \iota^{-1}(\mathcal{Z}(\mathfrak{P} \cap B)).$$

Поэтому для всякого $i \in I_3$ всякая неприводимая над $\overline{K}$ компонента многообразия W_i имеет вид $\iota^{-1}(\mathcal{Z}(\mathfrak{P} \cap B))$ для некоторого $\mathfrak{P} \in \mathcal{B}_3$.

Напомним, что $n - s \geqslant 3$. Теперь, согласно теореме 3 из приложения статьи [5], справедливы следующие утверждения (мы опустили здесь

утверждение (v), поскольку в настоящее время нам оно не потребуется, и слегка ослабили утверждение (iii)).

(i) Существует ненулевая линейная форма $L \in \overline{K}[Y_1, \dots, Y_{n-s}]$ от $Y_1, \dots, Y_{n-s}$, такая, что идеал $(f, L) \subset \overline{K}[Y_1, \dots, Y_{n-s}, Y]$ является простым. Элемент $\Delta_1 \bmod L \in \overline{K}[Y_1, \dots, Y_{n-s}]/(L)$ – ненулевой (т.е. L не делит Δ_1), и элемент

$$f^{(m_1)} \bmod L \in (\overline{K}[Y_1, \dots, Y_{n-s}]/(L))[Y]$$

также является ненулевым.

(ii) Множество $\mathcal{U}_4$ линейных форм L, удовлетворяющее свойствам из (i), является непустым открытым в топологии Зариского подмножеством в $\mathbb{A}^{n-s}(\overline{K})$.

(iii) Пусть $L \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$. Тогда

$$LB = \mathfrak{p} \cap \mathfrak{q},$$

где идеал $\mathfrak{p}$ является радикалом идеала LB и $\mathfrak{p}$ – простой идеал. Идеал $\mathfrak{q}$ является пересечением $\mathfrak{P}$-примарных идеалов для всех простых идеалов $\mathfrak{P} \in \mathcal{B}_{2,L}$, причём здесь мы предполагаем, что пересечение по пустому множеству индексов (когда $\mathcal{B}_{2,L} = \varnothing$) равно B. Сверх того, для всякого $\mathfrak{P} \in \mathcal{B}_{2,L}$ имеем $\dim \mathcal{Z}(\mathfrak{P}) \leqslant n-s-2$ и, следовательно, $\mathfrak{P}$-примарная компонента идеала LB является вложенной.

(iv) Пусть $L \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$. Тогда алгебраическое многообразие ${}^{\pi}W \cap \mathcal{Z}(L)$ имеет размерность $\dim({}^{\pi}W) - 1$ и неприводимо над $\overline{K}$. Далее, проекция

$$ {}^{\pi}W \cap \mathcal{Z}(L) \to \mathcal{Z}(L), \tag{14}$$

индуцированная морфизмом π, является доминантным сепарабельным морфизмом алгебраических многообразий (в левой части формулы (14) имеем $\mathcal{Z}(L) \subset \mathbb{A}^{n-s}(\overline{K})$). Кроме того, если морфизм π конечен, то морфизм (14) также конечен.

Обозначим через $\overline{K}({}^{\pi}W \cap \mathcal{Z}(L))$ поле рациональных функций алгебраического многообразия ${}^{\pi}W \cap \mathcal{Z}(L)$. Тогда

$$[\overline{K}({}^{\pi}W \cap \mathcal{Z}(L)) : \overline{K}(\mathcal{Z}(L))] = [\overline{K}({}^{\pi}W) : \overline{K}(Y_1, \dots, Y_{n-s})]. \tag{15}$$

Обозначим через $y \bmod L$ образ элемента y в $\overline{K}[{}^{\pi}W \cap \mathcal{Z}(L)]$. Тогда минимальный многочлен элемента $y \bmod L$ над $\overline{K}(\mathcal{Z}(L))$ равен $f \bmod L$, и $y \bmod L$ является примитивным элементом поля рациональных функций $\overline{K}({}^{\pi}W \cap \mathcal{Z}(L))$ над $\overline{K}(\mathcal{Z}(L))$.

(vi) Пусть $\mathcal{L}$ – линейное подпространство пространства всех линейных форм из $\overline{K}[Y_1, \ldots, Y_{n-s}]$ и $\dim \mathcal{L} \geqslant 3$. Тогда $\mathcal{L} \cap \mathcal{U}_4 \neq \varnothing$.

Отметим, что утверждения (i), (ii) и (vi) следуют также из теоремы 2 работы [3] и, возможно, доказательство в [3] является более поучительным.

Теперь мы переходим к описанию алгоритма для теоремы 1. Обозначим через $\overline{W}$ замыкание алгебраического многообразия W в проективном пространстве $\mathbb{P}^n(\overline{K})$. Тогда с помощью алгоритма из [1, 4] мы строим следующие объекты.

- Однородные многочлены $h_1, \ldots, h_s \in K[X_0, \ldots, X_n]$, такие, что всякая неприводимая компонента W'' алгебраического многообразия $\widetilde{V}$ (см. введение) с $\dim W'' \geqslant n - s$ является неприводимой компонентой проективного алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_s)$ и каждый многочлен h_j, $1 \leqslant j \leqslant s$, есть линейная комбинация многочленов $\overline{f}_1, \ldots, \overline{f}_m$ с коэффициентами из K.
- Общие точки ξ_i, $i \in I_1'$, всех неприводимых над $K^{p^{-\infty}}$ компонент W_i, $i \in I_1'$, алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(X_0) = \mathcal{Z}(h_1, \ldots, h_s) \cap \mathbb{A}^n(\overline{K})$.
- Для всякого $i \in I_1'$ семейство многочленов $\varphi_{i,j} \in K[X_1, \ldots, X_n]$, $j \in J^{(i)}$, такое, что $\mathcal{Z}(\{\varphi_{i,j}\}_{j \in J^{(i)}}) = \mathcal{Z}(W_i) \setminus \mathcal{Z}(X_0)$; т.е. мы строим системы полиномиальных уравнений, задающих неприводимые компоненты алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(X_0)$ (фактически, гомогенизации многочленов $\varphi_{i,j}$ имеют специальный вид, описанный в §2 гл. II работы [1]).

Заметим, что W является неприводимой компонентой алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(X_0)$ и для всякой неприводимой компоненты W' алгебраического многообразия V, такой, что $W' \neq W$, существует неприводимая компонента W''' алгебраического многообразия $\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(X_0)$, удовлетворяющая условию $W''' \supset W'$.

Положим

$$I_1 = \{i \in I_1' \,:\, \exists\, \alpha\, (1 \leqslant \alpha \leqslant r \,\&\, e_\alpha(\xi_i) \neq 0)\},$$

где $e_\alpha(\xi_i) = \xi_i(e_\alpha)$ – значение многочлена e_α в точке ξ_i (можно записать здесь $\xi_i(e_\alpha)$, если ξ_i рассматривается как гомоморфизм). Мы строим множество индексов I_1. Имеем $\#I_1 \leqslant d^s$ по теореме Безу.

Пусть $\#(I_2 \cup I_3) = N$. Тогда $N = n(d^{s+r})^{O(1)}$ с абсолютной константой в $O(1)$. Обозначим через $\xi_1, \ldots, \xi_N$ общие точки ξ_i, $i \in I_2 \cup I_3$.

Пусть $J_1 \subset K$ – произвольное множество с числом элементов $\#J_1 = N+1$ и $0 \notin J_1$. Покажем, что существует линейная форма $L' = l_1 Y_1 + \cdots + l_r Y_r$, такая, что все $l_i \in J_1$, $1 \leqslant i \leqslant r$, и $L'(\xi_i) = (l_1 e_1 + \cdots + l_r e_r)(\xi_i) \neq 0$ для всех i, $1 \leqslant i \leqslant N$. Мы будем строить и доказывать существование L' при помощи рекурсии по j. Предположим, что для некоторого j, $0 \leqslant j < N$, построена линейная форма $L^{(j)} = l_1^{(j)} Y_1 + \cdots + l_r^{(j)} Y_r$, такая, что $l_v^{(j)} \in J_1$ для всех j и $L^{(j)}(\xi_i) \neq 0$ для всех i, $1 \leqslant i \leqslant j$ (база рекурсии $j = 0$ тривиальна). Тогда существует α, $1 \leqslant \alpha \leqslant r$, такое, что $e_\alpha(\xi_{j+1}) \neq 0$. Положим $l_i^{(j+1)} = l_i^{(j)}$ при $1 \leqslant i \leqslant r$, $j \neq \alpha$. Теперь существует $l_\alpha^{(j+1)} \in J_1$, такое, что $L^{(j+1)}(\xi_i) = (l_1^{(j+1)} e_1 + \cdots + l_r^{(j+1)} e_r)(\xi_i) \neq 0$ для всех i, $1 \leqslant i \leqslant j+1$. Наконец, положим $L' = L^{(N)}$.

Линейные формы $L', Y_2, \ldots, Y_{n-s}$ являются линейно независимыми, поскольку $0 \neq l_1 \in J_1$. Поэтому существует такой многочлен $\widetilde{\Delta}_1 \in K[Y_1, \ldots, Y_{n-s}]$, что

$$\Delta_1 = \widetilde{\Delta}_1(L', Y_2, \ldots, Y_{n-s}).$$

Пусть $J_2 \subset K$ – произвольное подмножество с числом элементов $\#J_2 = N + 1 + \deg_{Y_1,\ldots,Y_{n-s}} \Delta_1$. Существуют $\alpha_1, \alpha_2 \in J_2$, такие, что

(a) $(Y_r - \alpha_2 L')(\xi_i) \neq 0$ для всякого i, $1 \leqslant i \leqslant N$,
(b) $\widetilde{\Delta}_1(L', Y_2, \ldots, Y_{r-2}, \alpha_1 L', \alpha_2 L', Y_{r+1}, \ldots, Y_{n-s}) \neq 0$.

Мы строим такие элементы $\alpha_1, \alpha_2 \in J_2$.

Положим $L_1 = Y_{r-1} - \alpha_1 L'$ и $L_2 = Y_r - \alpha_2 L'$. Обозначим через (L_1, L_2) идеал кольца $K[Y_1, \ldots, Y_{n-s}]$, порождённый L_1 и L_2. Мы имеем $\Delta_1 \notin (L_1, L_2)$ согласно (b). Напомним, что $m_1 = \deg_{Y_1,\ldots,Y_{n-s}} f$. Пусть $J_3 \subset K$ – произвольное подмножество с числом элементов $\#J_3 = N + 1 + 56 m_1^8 + d^{2s}$. Согласно (a) и теореме 2 работы [3], существует подмножество $J_3' \subset J_3$, такое, что $\#J_3' \geqslant 1 + d^{2s}$ и для всякого $t^* \in J_3'$

(c) $(L_2 - t^* L_1)(\xi_i) \neq 0$ для всех i, $1 \leqslant i \leqslant N$,
(d) $L_2 - t^* L_1 \in \mathcal{U}_4$

(отметим здесь, что условие $f^{(m_1)} \bmod (L_2 - t^* L_1) \neq 0$ выполняется автоматически, как только справедливо утверждение теоремы 2 работы [3] в рассматриваемой нами ситуации). Для всякого $t^* \in J_3$ мы проверяем, верно ли, что $t^* \in J_3'$, с помощью алгоритмов из [1,4]. Пусть

$t^* \in J_3'$. Положим $L^* = L_2 - t^* L_1$. В силу (c) имеем $L^*(\xi_i) \neq 0$ для всякого $i \in I_2$ (соответственно $i \in I_3$). Отсюда следует, что $L^* \in \mathcal{U}_2$ (соответственно $L^* \in \mathcal{U}_3$). Поэтому $L^* \in \mathcal{U}_2 \cap \mathcal{U}_3 \cap \mathcal{U}_4$. Следовательно, согласно утверждениям (iii) и (iv), алгебраическое многообразие ${}^{\pi}W \cap \mathcal{Z}(L^*)$ определено над K, неприводимо над $\overline{K}$, и последнее пересечение трансверсально (в некоторой гладкой точке этого пересечения, ср. с формулировкой теоремы 1). Отсюда вытекает, что

$$\dim({}^{\pi}W \cap \mathcal{Z}(L_1, L_2)) = n - s - 2 \tag{16}$$

(мы оставляем подробности читателю).

Наконец, обозначим через $\mathcal{C}_4$ множество всех неприводимых над $\overline{K}$ алгебраических многообразий E, таких, что E является неприводимой компонентой пересечения $W \cap W_i$ для некоторого $i \in I_1$ с $W_i \neq W$ и $\dim E = n - s - 1$. Согласно теореме Безу, $\#\mathcal{C}_4 \leqslant d^{2s}$. В силу (16) для всякого $E \in \mathcal{C}_4$ существует самое большее один элемент $t^* \in J_3'$, такой, что L^* обращается в нуль тождественно на E. Следовательно, существует элемент $t' \in J_3'$, такой, что линейная форма $L = L_1 - t' L_2$ не обращается в нуль тождественно на E для всякого $E \in \mathcal{C}_4$. Теперь из определений множеств индексов I_1' и I_1 мы выводим, что для всякой неприводимой над $\overline{K}$ компоненты W''' многообразия $\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(X_0)$, если $W''' \neq W$, то

$$W \cap \mathcal{Z}(L(e_1, \ldots, e_{n-s})) \not\subset W'''.$$

Для того чтобы найти t', мы перебираем $t^* \in J_3'$ и с помощью леммы 1 строим общую точку ξ^* пересечения $W \cap \mathcal{Z}(L^*(e_1, \ldots, e_{n-s}))$. Затем полагаем $t' = t^*$ для элемента t^*, такого, что для всякого $i \in I_1$ с $W \neq W_i$ выполнено условие $\varphi_{i,j}(\xi^*) \neq 0$ для некоторого $j \in J^{(i)}$.

Мы выбираем J_1, J_2, J_3 так, что все их элементы имеют размер $O((s+r)\log d + \log n)$. Это возможно, поскольку число элементов $\#J_i$ ограничено сверху величиной $n(d^{r+s})^{O(1)}$. Более точно, можно выбрать J_1, J_2, J_3 так, что для всякого $a \in J_1 \cup J_2 \cup J_3$ элемент a лежит в $\mathbb{F}_p[T_1, \ldots, T_l]$ и степень $\deg_{T_\gamma} a$ ограничена сверху величиной

$$O((((s+r)\log d + \log n)/\log p)^{1/l})$$

для всех γ, $1 \leqslant \gamma \leqslant l$.

Пусть $L = c_1 Y_1 + \ldots + c_r Y_r$. Тогда $c_1, \ldots, c_r$ – требуемые элементы.

Оценка на время работы этого алгоритма немедленно следует из описанной конструкции и [1, 4]. Теорема доказана. $\square$

§3. Доказательство теоремы 2

Теперь доказательство этой теоремы становится коротким. Положим $l = [2\log^2 n]$. Пусть k – конечное поле и $T_1, \dots, T_l$ – алгебраически независимые элементы над k. В формулировке теоремы 1 работы [2] положим основное поле равным $k(T_1, \dots, T_l)$ (вместо k в обозначениях из [2]). Пусть $\mathfrak{p} \subset k(T_1, \dots, T_l)[X_0, \dots, X_n]$ – идеал, построенный в доказательстве теоремы 1 работы [2] над бесконечным полем $k(T_1, \dots, T_l)$.

Согласно доказательству предложения 1 из [2], для того чтобы доказать теорему 2, достаточно установить следующее. Применяя первую теорему Бертини, можно выбрать все коэффициенты $\lambda_{v,w} \in k[T_1, \dots, T_l]$ многочленов f_{v+1} и коэффициенты $l_{i,j} \in k[T_1, \dots, T_l]$ линейных форм L_i (см. [2]) со степенями $\deg_{T_1,\dots,T_l} \lambda_{v,w}$, $\deg_{T_1,\dots,T_l} l_{i,j}$, ограниченными сверху величиной

$$O(\log^2 n (\log d)^{1/(2\log^2 n)}).$$

Но это немедленно следует из теоремы 1, см. [4]. Теорема доказана.□

Список литературы

1. 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.
2. А. Л. Чистов, *Дважды экспоненциальная нижняя оценка на степень системы образующих полиномиального простого идеала.* — Алгебра и анализ **20**, вып. 6 (2008), 186–213.
3. А. Л. Чистов, *Оценка степени системы уравнений, задающей многообразие приводимых многочленов.* — Алгебра и анализ **24**, вып. 3 (2012), 199–222.
4. A. L. Chistov, *An improvement of the complexity bound for solving systems of polynomial equations.* — Зап. научн. семин. ПОМИ **390** (2011), 299–306.
5. A. L. Chistov, *A deterministic polynomial-time algorithm for the first Bertini theorem.* — Preprint of the St.Petersburg Mathematical Society (2004), `http://www.mathsoc.spb.ru/preprint/2004/index.html`.

Chistov A. L. An effective version of the first Bertini theorem in nonzero characteristic and its applications.

We suggest an effective algorithm for the first Bertini theorem in nonzero characteristic of the ground field. This allows us to improve the double-exponential lower bound for the degree of any system of generators of a polynomial ideal over a finite ground field.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
наб. р. Фонтанки, д. 27,
191023 С.-Петербург, Россия
E-mail: alch@pdmi.ras.ru

Поступило 8 октября 2012 г.