Записки научных
семинаров ПОМИ
Том 507, 2021 г.

А. Л. Чистов

ЭФФЕКТИВНАЯ КОНСТРУКЦИЯ МАЛОГО ЧИСЛА УРАВНЕНИЙ, ЗАДАЮЩИХ АЛГЕБРАИЧЕСКОЕ МНОГООБРАЗИЕ

Введение

Пусть F – поле произвольной характеристики с алгебраическим замыканием $\overline{F}$. В дальнейшем в алгоритмах мы будем предполагать, что F конечно порождено над его примитивным подполем, см. подробности ниже. Кроме того, мы предполагаем, что F содержит достаточно много элементов (если оно конечно). Если $\mathrm{char}(F) > 0$, то положим $p = \mathrm{char}(F)$. Если $\mathrm{char}(F) = 0$, то положим $p = 1$.

Пусть $f_0, \dots, f_{k-1} \in F[X_1, \dots, X_n]$ – многочлены с $\deg f_i \leqslant d$, где $d \geqslant 2$ и $k \geqslant 1$ (в дальнейшем для краткости deg обозначает $\deg_{X_1,\dots,X_n}$). Мы будем считать, что все эти многочлены линейно независимы над F (в частности, $f_0 \neq 0$). Положим $V = \mathcal{Z}(f_0, \dots, f_{k-1})$ равным алгебраическому многообразию всех общих нулей полиномов $f_0, \dots, f_{k-1}$ в аффинном пространстве $\mathbb{A}^n(\overline{k})$ (мы будем использовать аналогичные обозначения $\mathcal{Z}(\dots)$ также для других семейств многочленов).

В [1], см. также [2–4], мы описываем алгоритм для решения систем полиномиальных уравнений. В этих статьях основным является однородный случай, когда $f_0, \dots, f_{k-1}$ – однородные многочлены. Но случай неоднородных f_i легко сводится к однородному (с числом переменных на единицу больше).

Используя работу [1], можно решить систему однородных уравнений $f_0 = \dots = f_{k-1} = 0$ за время, полиномиальное от $d^{n(c_0+1)}$, p и длины записи входных данных, где c_0 – размерность алгебраического многообразия V. На выходе алгоритма из [1] каждая неприводимая компонента W многообразия V размерности $\dim W = n - s$ задаётся её общей точкой и семейством полиномов $g_1, \dots, g_N$, таким, что $W = \mathcal{Z}(g_1, \dots, g_N)$, $\deg g_i \leqslant d^{2s}$, $1 \leqslant n \leqslant N$, и N ограничено сверху полиномом от d^s.

Ключевые слова: алгебраические многообразия, эффективные алгоритмы, задающие уравнения, число уравнений.

Однако уже давно было известно, что любое алгебраическое многообразие в $\mathbb{A}^n(\overline{k})$ может быть задано $n+1$ уравнениями [8]. Хотя в настоящее время конструкция этих уравнений стала естественной и прозрачной, кажется, что до сих пор никто не дал явной оценки на сложность построения этих $n+1$ уравнений. Заметим, что степени этих $n+1$ уравнений, определяющих алгебраическое многообразие V (соответственно неприводимую компоненту W), ограничены сверху d, см. теорему 1 (соответственно d^{2s}, см. следствие 1) ниже.

Может возникнуть вопрос, почему мы не использовали такие системы уравнений в [1]. Ответ прост: в общем случае мы не можем построить эти системы уравнений, задающие неприводимые компоненты многообразия V, за время, полиномиальное от d^{n^2}, p и длины записи входных данных. Однако, см. следствие 1 (a), можно построить эти $n+1$ уравнений за время, полиномиальное от d^{n^3}, p и длины записи входных данных, применяя несколько раз оригинальный алгоритм из [1].

Только в случае нулевой характеристики основного поля, привлекая наши глубокие результаты о новой модели задания алгебраических многообразий, см. [5], можно получить алгоритм для построения этих $n+1$ уравнений, определяющих алгебраическое многообразие V (соответственно неприводимые компоненты многообразия V), за время, полиномиальное от d^n (соответственно d^{n^2}) и длины записи входных данных, см. теорему 1 (b) (соответственно следствие 1 (b)).

Далее, мы хотели бы рассмотреть проблему построения n уравнений, задающих алгебраическое многообразие V. Известно, что существуют n многочленов $h_1, \ldots, h_n \in F[X_1, \ldots, X_n]$, таких, что $V = \mathcal{Z}(h_1, \ldots, h_n)$, см. [9,10] и [11, гл. V, разд. 1]. Конструкция этих уравнений по существу одна и та же во всех этих работах. И всё же до сих пор никто не получил явной оценки на степени этих n уравнений и сложность алгоритма для их построения. Мы доказываем теорему 2, см. ниже, где предлагаем алгоритм для построения $h_1, \ldots, h_n$ и получаем требуемые явные верхние оценки на степени этих многочленов и сложность полученного алгоритма. Данные оценки дважды экспоненциальны от n, но, по-видимому, это неизбежно, по крайней мере при рассматриваемом подходе.

В доказательствах теорем 1 и 2 ниже мы широко используем алгоритм для решения систем полиномиальных уравнений из [1]. К настоящему времени мы значительно улучшили результаты из [1] и их

изложение в [2–4] (имеется также третья часть работы [3, 4], но она посвящена главным образом системам с параметрами). Сейчас можно было бы ссылаться на эти статьи вместо [1] в том, что касается решения систем полиномиальных уравнений. Так что мы рекомендуем статьи [2–4] заинтересованному читателю. Отметим, что конструкция системы уравнений, задающей неприводимую компоненту, улучшена в [3] (а также в [3] исправлена небольшая неточность из [1]).

Перейдём к точным формулировкам. Поле F конечно порождено над полем H, где H есть $\mathbb{Q}$ или конечное поле $\mathbb{F}_p$ из p элементов, если $p > 1$. Мы предполагаем, что $F = H(T_1, \dots, T_l)[\eta]$, элементы $T_1, \dots, T_l$ алгебраически независимы над H и элемент η алгебраический сепарабельный над полем $H(T_1, \dots, T_l)$, причем задан минимальный многочлен $\varphi \in H(T_1, \dots, T_l)[Z]$ элемента η над полем $H(T_1, \dots, T_l)$.

Мы представляем многочлен в виде $\varphi = 1/\varphi^{(2)} \sum\limits_{0 \leqslant i \leqslant \deg_Z \varphi} \varphi_i^{(1)} Z^i$, где $\varphi_i^{(1)}$, $\varphi^{(2)} \in \widetilde{H}[T_1, \dots, T_l]$, $\widetilde{H} = \mathbb{Z}$, если $\operatorname{char}(F) = 0$, $\widetilde{H} = H$, если $\operatorname{char}(F) = p > 0$, и $\operatorname{GCD}_i\{\varphi_i^{(1)}, \varphi^{(2)}\} = 1$ в кольце $\widetilde{H}[T_1, \dots, T_l]$. Каждый элемент $f \in F[X_1, \dots, X_n]$ представляется в виде

$$f = \frac{1}{b} \sum_{0 \leqslant i \leqslant \deg_Z \varphi, i_1, \dots, i_n} a_{i,i_1,\dots,i_n} \eta^i X_1^{i_1} \cdot \ldots \cdot X_n^{i_n},$$

где $a_{i,i_1,\dots,i_n}, b \in \widetilde{H}[T_1, \dots, T_l]$ и $\operatorname{GCD}_{i,i_1,\dots,i_n}\{a_{i,i_1,\dots,i_n}, b\} = 1$ в последнем кольце. Положим

$$\deg_{T_1,\dots,T_l} f = \max\{\deg_{T_1,\dots,T_l} a_{i,i_1,\dots,i_n}, \deg_{T_1,\dots,T_l} b\}. \tag{1}$$

Длина записи $\mathrm{l}(h)$ целого числа $h \in \mathbb{Z}$ есть его битовая длина. Длина записи $\mathrm{l}(h)$ элемента $h \in \mathbb{F}_p$ равна $[\log_2 p] + 1$. Обозначим через $\mathrm{l}(f)$ максимум длин записи коэффициентов из H (фактически из $\widetilde{H}$) при мономах от $T_1, \dots, T_l$ полиномов $a_{i,i_1,\dots,i_n}, b$. Аналогичным образом определяются степени $\deg_{T_1,\dots,T_l,Z} \varphi$ и длины записи коэффициентов $\mathrm{l}(\varphi)$. Мы будем предполагать, что при $0 \leqslant i \leqslant k-1$

$$\deg_{T_1,\dots,T_l,Z} \varphi < d_1, \quad \deg_{T_1,\dots,T_l} f_i < d_2, \quad \deg_{X_1,\dots,X_n} f_i \leqslant d,$$
$$\mathrm{l}(\varphi) \leqslant M_1, \quad \mathrm{l}(f_i) \leqslant M_2$$

для некоторых положительных целых чисел $d \geqslant 2$, d_1, d_2, M_1, M_2.

Мы хотели бы избежать зависимости от l оценок в формулировках теорем ниже. Я думаю, что здесь (и почти во всех других моих статьях) эффективные конструкции и алгоритмы сами по себе являются

более важными, чем оценки их сложности. Так что в дальнейшем для простоты мы будем предполагать, что l является фиксированной константой. Однако заинтересованный читатель может получить оценки, зависящие от l, ср. [2].

В дальнейшем в этой статье мы используем обозначение $\mathcal{P}$ для полинома от одной переменной с целыми неотрицательными коэффициентами. Если не оговорено противное, мы не предполагаем, что этот полином является одним и тем же в разных местах текста статьи (даже близко друг к другу).

При $0 \leqslant i \leqslant n$ выберем конечное множество $\mathcal{I}(d,i) \subset F$, такое, что $\#\mathcal{I}(d,i) = d^i + 1$ и $\mathrm{l}(c) = O(1 + i\log_2 d)$ для всякого $c \in \mathcal{I}(d,i)$ с абсолютной константой в $O(\ldots)$.

Рассмотрим случай, когда все многочлены $f_0, \ldots, f_{k-1}$ являются однородными относительно $X_1, \ldots, X_n$. Положим $f_{i,j} = f_i X_j^{d-\deg f_i}$. Тогда, очевидно, $V = \mathcal{Z}(f_0, \ldots, f_{k-1}) = \mathcal{Z}(\{f_{i,j},\, 0 \leqslant i \leqslant k-1,\, 1 \leqslant j \leqslant n\})$ и все $f_{i,j}$ являются однородными многочленами степени d.

Теорема 1. *Пусть $f_0, \ldots, f_{k-1}$ – многочлены (соответственно однородные многочлены одной и той же степени d), такие же, как и выше. Тогда можно построить элементы $c_{i,j} \in \mathcal{I}(d, i-1)$, $1 \leqslant i \leqslant n+1$, $0 \leqslant j \leqslant k-1$, удовлетворяющие следующим свойствам. Положим $g_i = \sum_{1 \leqslant j \leqslant k-1} c_{i,j} f_j$, $1 \leqslant i \leqslant n+1$. Пусть α – целое число, такое, что $1 \leqslant \alpha \leqslant n+1$, и W – произвольная неприводимая компонента алгебраического многообразия $\mathcal{Z}(g_1, \ldots, g_\alpha)$, которая не является неприводимой компонентой многообразия V. Тогда $\dim W = n - \alpha$. В частности, $V = \mathcal{Z}(g_1, \ldots, g_{n+1})$. Заметим, что $\deg g_i \leqslant d$ (соответственно все ненулевые g_i являются однородными многочленами степени d).*

(a) *Время работы алгоритма для построения $g_1, \ldots, g_{n+1}$ (и семейства элементов $\{c_{i,j}\}$, $1 \leqslant i \leqslant n+1$, $0 \leqslant j \leqslant k-1$) полиномиально от d^{n^2}, d_1, d_2, M_1, M_2 и p.*

(b) *Более того, если основное поле F имеет характеристику нуль, то можно предложить другой аналогичный алгоритм, но со временем работы, полиномиальным от d^n, d_1, d_2 и M_1, M_2.*

Замечание 1. Фактически в утверждении теоремы 1 можно избежать зависимости времени работы от p, используя алгоритм разложения в объединение равноразмерностных компонент вместо неприводимых

компонент, ср. [3, 4]. Но здесь мы оставляем подробности заинтересованному читателю.

Обозначим через $F_{\mathrm{pf}} = \bigcup_{\alpha \geqslant 0} F^{p^{-\alpha}}$ совершенное замыкание поля F. Пусть $V = \bigcup_{j \in J} W_j$ – разложение алгебраического многообразия V в объединение неприводимых над полем F_{pf} компонент W_j, $j \in J$. Предположим, что $\dim W_j = n - s_j$.

Следствие 1. *В условиях теоремы* 1 *можно построить для каждой определённой и неприводимой над* F_{pf} *компоненты* W_j *многообразия* V *многочлены (соответственно однородные многочлены)*

$$g_{j,1}, \ldots, g_{j,n+1} \in F[X_1, \ldots, X_n],$$

такие, что $W_j = \mathcal{Z}(g_{j,1}, \ldots, g_{j,n+1})$ *и*

$$\deg g_{j,i} \leqslant d^{2s_j}, \quad \deg_{T_1,\ldots,T_l} g_{j,i} \leqslant d_2 \mathcal{P}(d_1 d^{s_j}),$$
$$\mathrm{l}(g_{j,i}) \leqslant (M_1 + M_2 + d_2 + n)\mathcal{P}(d_1 d^{s_j}).$$

(a) *Время работы алгоритма для построения всех многочленов* $g_{j,i}$ *полиномиально от* d^{n^3}, d_1, d_2, M_1, M_2 *и* p.

(b) *Более того, если основное поле* F *имеет характеристику нуль, то можно предложить другой аналогичный алгоритм, но со временем работы, полиномиальным от* d^{n^2}, d_1, d_2 *и* M_1, M_2.

Доказательство. Это немедленно вытекает из теоремы 1 и оценок для степеней и длин записи коэффициентов уравнений, определяющих компоненту W_j, из алгоритма для решения системы полиномиальных уравнений, см. [1, 2]. Следствие доказано (по модулю теоремы 1). □

Обозначим через $\mathfrak{a}$ идеал кольца $F[X_1, \ldots, X_n]$, порождённый многочленами $f_0, \ldots, f_{k-1}$.

Теорема 2. *Предположим, что* $f_0, \ldots, f_{k-1}$ *– произвольные многочлены, такие же, как и выше (соответственно предположим, что* $f_0, \ldots, f_{k-1}$ *– однородные многочлены относительно* $X_1, \ldots, X_n$, *такие же, как и выше, и дополнительно предположим, что прямая* $\mathcal{Z}(X_1, \ldots, X_{n-1})$ *содержится в* V*). Тогда можно построить многочлены*

$h_1, \dots, h_n \in \mathfrak{a}$ *(соответственно однородные многочлены* $h_1, \dots, h_{n-1} \in \mathfrak{a}$ *и* $h_n = 0$*), такие, что* $V = \mathcal{Z}(h_1, \dots, h_n)$ *и при* $1 \leqslant i \leqslant n$

$$\deg h_i \leqslant d^{2^{ci}}, \quad \deg_{T_1,\dots,T_l} h_i \leqslant d_2 \mathcal{P}(d_1^i d^{2^{ci}}),$$
$$\mathrm{l}(h_i) \leqslant (M_1 + M_2 + d_2 + n)\mathcal{P}(d_1^i d^{2^{ci}})$$

для абсолютной константы $c > 0$ *(эта константа может быть вычислена явно).*

Время работы алгоритма для построения многочленов $h_1, \dots, h_n$ *полиномиально от* $d^{2^{cn}}$, d_1^n, d_2, M_1, M_2 *и р.*

Замечание 2. Можно осуществить линейное преобразование координат $X_1, \dots, X_n$. Следовательно, в утверждении теоремы 2 можно заменить условие "$\mathcal{Z}(X_1, \dots, X_{n-1}) \subset V$" на "существует прямая $\mathcal{L}$, определённая над полем F, такая, что $\{0\} \subset \mathcal{L} \subset V$". Конечно, последнее условие выполняется, если заменить поле F на его алгебраическое замыкание и $V \neq \{0\}$. Без этого условия вопрос о том, верно ли, что для заданных однородных полиномов $f_0, \dots, f_{k-1}$ существуют однородные полиномы $h_1, \dots, h_{n-1} \in F[X_1, \dots, X_n]$, такие, что $V = \mathcal{Z}(h_1, \dots, h_{n-1})$, до сих пор является открытой проблемой. Эта проблема сформулирована в [11, гл. V, с. 127].

§1. Доказательство теоремы 1

Используя алгоритм из [1], построим общую точку ξ_j каждой неприводимой компоненты W_j, $j \in J$, см. введение.

Теперь мы опишем рекурсивную конструкцию для нахождения многочленов $g_1, \dots, g_{n+1} \in F[X_1, \dots, X_n]$. Положим $g_1 = f_0$ (напомним, что $f_0 \neq 0$). Предположим, что $1 \leqslant i \leqslant n$ и $g_1, \dots, g_i$ построены и удовлетворяют следующим свойствам. Положим $V_i = \mathcal{Z}(g_1, \dots, g_i)$. Тогда для всякого $j \in J$, такого, что $\dim W_j \geqslant n - i$, многообразие W_j является неприводимой компонентой многообразия V_i. Если W – определённая над F_{pf} компонента алгебраического многообразия V_i, которая не является компонентой многообразия V, то $\dim W = n - i$. Очевидно, эти свойства выполняются для базы рекурсии $i = 1$.

Покажем, как построить многочлен g_{i+1}. Пусть $V_i = \bigcup\limits_{j \in J_i} W_{i,j}$ является разложением алгебраического многообразия V_i в объединение неприводимых над F_{pf} компонент $W_{i,j}$, $j \in J_i$.

Опишем шаг рекурсии для утверждения (a). Для всякого $j \in J_i$, используя алгоритм из [1], построим общую точку $\xi_{i,j}$ компоненты $W_{i,j}$. Теперь $W_{i,j}$ является неприводимой компонентой многообразия V в том и только в том случае, если $f_u(\xi_{i,j}) = 0$ при $0 \leqslant u \leqslant k-1$. Поэтому мы можем построить подмножество J'_i всех $j \in J_i$, таких, что $W_{i,j}$ не является неприводимой компонентой многообразия V.

По теореме Безу $\#J'_i \leqslant d^i$. Значит, можно построить элементы $c_{i+1,u} \in \mathcal{I}(d,i)$, такие, что $\sum\limits_{0\leqslant u\leqslant k-1} c_{i+1,u} f_u(\xi_{i,j}) \neq 0$ для всех $j \in J'_i$ (мы оставляем детали читателю). Положим $g_{i+1} = \sum_{0\leqslant u\leqslant k-1} c_{i+1,u} f_u$. Рекурсивный шаг для утверждения (a) описан.

Опишем рекурсивный шаг для утверждения (b). Применяя алгоритм из [5], построим семейство точек $\xi_\gamma \in \mathbb{A}^n(\overline{F})$, $\gamma \in \Gamma_i$, удовлетворяющее следующему свойству: $\#\Gamma_i \leqslant d^i$, и для всякого $j \in J_i$ существует индекс $\gamma_j \in \Gamma_i$, такой, что $\xi_{\gamma_j} \in W_{i,j}$ и ξ_{γ_j} – гладкая точка алгебраического многообразия V_i (индекс γ_j определён неоднозначно; фактически, согласно [5], имеется в точности $\deg W_{i,j}$ индексов $\gamma \in \Gamma_i$, аналогичных γ_j). Теперь $W_{i,j}$ является неприводимой компонентой многообразия V в том и только в том случае, если $f_u(\xi_{\gamma_j}) = 0$ при $0 \leqslant u \leqslant k-1$.

Обозначим через Γ''_i подмножество всех индексов $\gamma \in \Gamma_i$, таких, что $f_u(\xi_\gamma) = 0$ при $0 \leqslant u \leqslant k-1$. Положим $\Gamma'_i = \Gamma_i \setminus \Gamma''_i$. Можно построить элементы $c_{i+1,u} \in \mathcal{I}(d,i)$, такие, что $\sum\limits_{0\leqslant u\leqslant k-1} c_{i+1,u} f_u(\xi_{\gamma_j}) \neq 0$ при $j \in \Gamma'_i$ (здесь мы оставляем детали читателю). Положим $g_{i+1} = \sum\limits_{0\leqslant u\leqslant k-1} c_{i+1,u} f_u$. Рекурсивный шаг для утверждение (b) описан.

Таким образом, в конечном счёте мы построим требуемые многочлены $g_1, \ldots, g_{n+1}$. Оценка на время работы описанного алгоритма следует из [1] для утверждения (a) и из [5] для утверждения (b). Теорема доказана. □

§2. Доказательство теоремы 2

Для всякого идеала $\mathfrak{b}$ коммутативного кольца Λ обозначим через $\mathfrak{N}(\mathfrak{b})$ нильрадикал идеала $\mathfrak{b}$. В дальнейшем в доказательстве "(соответственно ...)" относится к случаю "(соответственно ...)" из формулировки теоремы 2. Также мы предполагаем без ограничения общности, что $n \geqslant 2$.

Сначала мы применим теорему 1 (а) и построим многочлены (соответственно однородные многочлены) $g_1, \dots, g_{n+1}$, такие, что

$$\mathcal{Z}(f_0, \dots, f_{k-1}) = \mathcal{Z}(g_1, \dots, g_{n+1}).$$

Заменяя $f_0, \dots, f_{k-1}$ на максимальное линейно независимое подсемейство семейства $g_1, \dots, g_{n+1}$, мы будем считать, не умаляя общности, что $1 \leqslant k \leqslant n+1$.

Пусть $A^{(0)} = F[X_1, \dots, X_n]$, $B^{(0)} = F[X_1, \dots, X_{n-1}]$, $A = A^{(0)} \otimes_F F_{\mathrm{pf}}$, $B = B^{(0)} \otimes_F F_{\mathrm{pf}}$, и рассмотрим идеал $\mathfrak{a}' = \mathfrak{a} \otimes_F F_{\mathrm{pf}} \subset A$. Заметим, что $\deg z = \deg_{X_1,\dots,X_{n-1}} z$ для всякого полинома z из кольца B.

Мы опишем рекурсию, состоящую из n шагов (соответственно опишем рекурсию, состоящую из $n-1$ шагов, и положим $h_n = 0$, $u_n = 1$). На i-м шаге этой рекурсии, $1 \leqslant i \leqslant n$ (соответственно $1 \leqslant i \leqslant n-1$), мы построим многочлены (соответственно однородные многочлены) $u_i \in B^{(0)}$ и $h_i \in A^{(0)}$, удовлетворяющие следующим свойствам. Рассмотрим алгебраическое многообразие $E_i = \mathcal{Z}(u_1, \dots, u_i) \subset \mathbb{A}^{n-1}(\overline{F})$ (здесь аффинное пространство $\mathbb{A}^{n-1}(\overline{F})$ имеет координаты $X_1, \dots, X_{n-1}$). Тогда $\dim E_i = n - 1 - i$. Далее,

$$u_i \mathfrak{a} \subset \mathfrak{N}(A^{(0)} h_i + A^{(0)} u_1 + \ldots + A^{(0)} u_{i-1}) \subset A^{(0)}.$$

Мы увидим, что последнее равенство справедливо для $i = n$ также в случае "(соответственно ...)".

Если эти свойства выполняются при $1 \leqslant i \leqslant n$, то согласно [9, 10] и [11, гл. V] мы имеем $\mathfrak{a} = \mathfrak{N}(A^{(0)} h_1 + \ldots + A^{(0)} h_n)$. После этого для доказательства теоремы 2 остаётся только установить требуемые оценки на степени и длины записи коэффициентов полиномов h_i из формулировки теоремы.

Предположим, что $1 \leqslant i \leqslant n-1$ (соответственно $1 \leqslant i \leqslant n-2$) и многочлены (соответственно однородные многочлены) $u_1, \dots, u_{i-1}$ и $h_1, \dots, h_{i-1}$, удовлетворяющие требуемым свойствам, построены. Опишем i-й шаг рекурсии, т.е. построим u_i и h_i.

Используя алгоритм из [1] и [3, разд. 4], мы вычисляем разложение алгебраического многообразия $E_{i-1} = \bigcup\limits_{j \in I_{i-1}} W_j$ в объединение определённых и неприводимых над полем F_{pf} компонент W_j (чтобы избежать двусмысленности в дальнейшем, мы предполагаем, что все индексы из I_{i-1} не являются целыми числами). Для всякого $j \in I_{i-1}$ мы имеем $\dim W_j = n - i$ согласно рекурсивному предположению.

Более того, при $i > 1$ мы строим линейно независимые над F линейные многочлены (соответственно линейные формы) $L_1, \dots, L_{n-i+1} \in F[X_1, \dots, X_n]$, удовлетворяющие формулируемым ниже свойствам (i) и (ii). Фактически это условия "общего положения" для линейных многочленов (соответственно линейных форм) $L_1, \dots, L_{n-i}$.

(i) Морфизм $E_{i-1} \to \mathbb{A}^{n-i}(\overline{F})$, $(X_1, \dots, X_{n-1}) \mapsto (L_1, \dots, L_{n-i})$, является конечным доминантным сепарабельным (это означает, что ограничение этого морфизма на каждую неприводимую компоненту W_j, $j \in I_{i-1}$, является конечным доминантным сепарабельным).

Для всякого $j \in I_{i-1}$ мы строим неприводимый многочлен

$$\Phi_j \in F_{\mathrm{pf}}[L_1, \dots, L_{n-i+1}],$$

обращающийся в нуль тождественно на W_j и такой, что $\mathrm{lc}_{L_{n-i+1}} \Phi_j = 1$ (этот многочлен однозначно определён).

(ii) Для всякого $j \in I_{i-1}$ имеем $\deg_{L_{n-i}} \Phi_j = \deg_{L_1,\dots,L_{n-i+1}} \Phi_j = \deg W_j$, и все многочлены Φ_j, $j \in I_{i-1}$, попарно различны и сепарабельны относительно L_{n-i}.

Следовательно, для всякого $j \in I_{i-1}$ мы имеем общую точку

$$\xi_j : F_{\mathrm{pf}}[W_j] \to F_{\mathrm{pf}}(L_1, \dots, L_{n-i-1})[L_{n-i+1}]/(\Phi_j)$$

алгебраического многообразия W_j. Мы строим все эти общие точки ξ_j, т.е. все элементы $\xi_j(X_i)$, $1 \leqslant i \leqslant n-1$, $j \in I_{i-1}$.

В дальнейшем, если не оговорено противное, мы предполагаем, что $i > 1$. Существует линейный многочлен (соответственно линейная форма) $L \in F[X_1, \dots, X_n]$, такой, что $\dim W_j \cap \mathcal{Z}(L) = -1 + \dim W_j$ для всякого $j \in I_{i-1}$. Мы строим такой линейный многочлен (соответственно такую линейную форму) L.

Обозначим через $\mathfrak{p}_j \subset B$ идеал (соответственно однородный идеал) компоненты W_j. Для всякого многочлена $z \in A$ обозначим через $z \bmod \mathfrak{p}_j$ образ этого многочлена в кольце $B/\mathfrak{p}_j[X_n]$ при естественном гомоморфизме $B[X_n] \to B/\mathfrak{p}_j[X_n]$ (мы будем использовать это обозначение $z \bmod \mathfrak{p}_j$ также для элементов z из других колец многочленов над B). Если $z \in B$, то, очевидно, $z \bmod \mathfrak{p}_j \in B/\mathfrak{p}_j$. Положим K_j равным полю частных кольца $B/\mathfrak{p}_j$. Мы отождествляем K_j с $F_{\mathrm{pf}}(L_1, \dots, L_{n-i})[L_{n-i+1}]/(\Phi_j)$. Положим $\Phi = \Phi_{i-1} = \prod\limits_{j \in I_{i-1}} \Phi_j$. В дальнейшем удобно рассматривать Φ и Φ_j как многочлены от $L_1, \dots, L_{n-i+1}$.

Обозначим через Δ_j дискриминант многочлена Φ_j относительно L_{n-i+1} для всякого $j \in I_{i-1}$. Обозначим через Δ_{i-1} дискриминант многочлена Φ_{i-1} относительно L_{n-i+1}. Для краткости положим $\Delta = \Delta_{i-1}$. Заметим, что $\Delta \notin \bigcup\limits_{j\in I_{i-1}} \mathfrak{p}_j$. Также $L \notin \bigcup\limits_{j\in I_{i-1}} \mathfrak{p}_j$. Хорошо известно, что $\deg \Delta \leqslant (-1+\deg\Phi)\deg\Phi$ (соответственно $\deg\Delta = (-1+\deg\Phi)\deg\Phi$).

Положим

$$B_{i-1} = F_{\mathrm{pf}}[L_1,\dots,L_{n-i}]/(\Phi) \quad \text{и} \quad B_{i-1,j} = F_{\mathrm{pf}}[L_1,\dots,L_{n-i}]/(\Phi_j)$$

для всякого $j \in I_{i-1}$. Очевидно, существует естественное вложение $B_{i-1} \subset B/\bigcap\limits_{j\in I_{i-1}} \mathfrak{p}_j$. Обозначим через $\overline{B}_{i-1}$ целое замыкание кольца B_{i-1} в его полном кольце частных $\prod\limits_{j\in I_{i-1}} K_j$. Для всякого $j \in I_{i-1}$ обозначим через $\overline{B}_{i-1,j}$ целое замыкание кольца $B_{i-1,j}$ в его поле частных K_j. Положим $K = F_{\mathrm{pf}}(L_1,\dots,L_{n-i})$. Многочлен Φ сепарабелен относительно L_{n-i+1}. Поэтому $\prod\limits_{j\in I_{i-1}} K_j$ является сепарабельной алгеброй над полем K. Кольцо B_{i-1} является свободным $F_{\mathrm{pf}}[L_1,\dots,L_{n-i}]$-модулем, его базис $\{L_{n-i+1}^{\alpha}\}_{0\leqslant\alpha<\deg\Phi}$ над кольцом $F_{\mathrm{pf}}[L_1,\dots,L_{n-i}]$ является базисом алгебры $\prod\limits_{j\in I_{i-1}} K_j$ над K. Хорошо известно, что в этом случае $B/\bigcap\limits_{j\in I_{i-1}} \mathfrak{p}_j \subset \overline{B}_{i-1} \subset (1/\Delta)B_{i-1}$. Аналогично, $B/\mathfrak{p}_j \subset \overline{B}_{i-1,j} \subset (1/\Delta)B_{i-1,j}$ для всякого $j \in I_{i-1}$.

Для всех попарно различных элементов $j_1, j_2 \in I_{i-1}$ положим $R_{j_1,j_2} = \mathrm{Res}_{L_{n-i}}(\Phi_{j_1},\Phi_{j_2})$ равным результанту относительно L_{n-i+1} полиномов Φ_{j_1},Φ_{j_2}. Заметим, что $R_{j_1,j_2} = \pm R_{j_2,j_1}$ и R_{j_1,j_2}^2 делит Δ для всякой пары (j_1,j_2) попарно различных элементов $j_1, j_2 \in I_{i-1}$. Построим линейный порядок $<$ на множестве I_{i-1}. Вычислим полином

$$\Delta' = \Big(\prod_{j\in I_{i-1}} \Delta_j\Big)\Big(\prod_{j_1,j_2\in I_{i-1},\, j_1<j_2} R_{j_1,j_2}\Big).$$

Заметим, что $\Delta' = \pm\Delta/\prod\limits_{j_1,j_2\in I_{i-1},\, j_1<j_2} R_{j_1,j_2}$.

Рассмотрим естественное вложение

$$\iota : B/\cap_{j\in I_{i-1}} \mathfrak{p}_j \longrightarrow \prod_{j\in I_{i-1}} B/\mathfrak{p}_j, \quad z \mapsto \{z \bmod \mathfrak{p}_j\}_{j\in I_{i-1}}.$$

Если все многочлены $f_0, \dots, f_{k-1}$ являются однородными, то $\prod\limits_{j \in I_{i-1}} B/\mathfrak{p}_j$ является градуированным кольцом: однородная компонента степени m этого кольца является прямым произведением $\prod\limits_{j \in I_{i-1}} (B/\mathfrak{p}_j)_m$ однородных компонент степени m колец $B/\mathfrak{p}_j$. В этом случае ι является однородным гомоморфизмом степени 0.

Лемма 1. *Пусть $z_j \in B$, $j \in I_{i-1}$, – произвольное семейство элементов. Тогда существует многочлен $z \in F_{\mathrm{pf}}[L_1, \dots, L_{n-i+1}] \subset B$, такой, что $\iota(z \bmod \bigcap\limits_{j \in I_{i-1}} \mathfrak{p}_j) = \{\Delta' z_j \bmod \mathfrak{p}_j\}_{j \in I_{i-1}}$. Следовательно, фактически $B/\bigcap\limits_{j \in I_{i-1}} \mathfrak{p}_j \subset (1/\Delta')B_{i-1}$.*

Если все многочлены $f_0, \dots, f_{k-1}$ однородны и $\deg z_j = m$ для всех $j \in I_{i-1}$, таких, что z_j не равен нулю, то можно выбрать z равным однородному многочлену степени $\deg z = m + \deg \Delta'$.

Если задано семейство $\{z_j\}_{j \in I_{i-1}}$, то можно построить этот многочлен z при помощи общих точек ξ_j, $j \in I_{i-1}$, и китайской теоремы об остатках.

Доказательство. Чтобы доказать первое и третье утверждения, заметим, что $\Delta_j \prod\limits_{j_1 \in I_{i-1},\, j_1 \neq j} R_{j_1,j}$ делит Δ'. Для всякого $j \in I_{i-1}$ вычислим многочлен $\Delta'_j = \Delta'/(\Delta_j \prod\limits_{j_1 \neq j} R_{j_1,j})$. Согласно китайской теореме об остатках, для всякого $j \in I_{i-1}$ существует элемент (соответственно однородный элемент) $\delta_j \in F_{\mathrm{pf}}(L_1, \dots, L_{n-i})[L_{n-i+1}]$, такой, что $\delta_j \bmod \Phi_j = \prod\limits_{j_1 \neq j} R_{j_1,j} \bmod \Phi_j$ и $\delta_j \bmod \Phi_{j_1} = 0$ для всякого $j_1 \in I_{i-1}$, $j_1 \neq j$. Мы строим все δ_j, решая линейные системы по правилу Крамера, и устанавливаем, что фактически можно выбрать $\delta_j \in F_{\mathrm{pf}}[L_1, \dots, L_{n-i+1}]$.

После этого для всякого $j \in I_{i-1}$, используя общую точку ξ_j, построим элемент $\widetilde{z}_j \in F_{\mathrm{pf}}[L_1, \dots, L_{n-i+1}]$, такой, что $\widetilde{z}_j = \Delta_j z_j \bmod \Phi_j$. Наконец, положим $z = \sum\limits_{j \in I_{i-1}} \Delta'_j \delta_j \widetilde{z}_j$. Тогда $z = \Delta' z_j \bmod \mathfrak{p}_j$ для всякого $j \in I_{i-1}$.

Второе утверждение следует из однородности вложения ι в рассматриваемом случае. Лемма доказана. □

Далее для всякого $j \in I_{i-1}$ мы выясняем, верно ли, что $f_\alpha(\xi_j) = 0$ (или, что то же самое, $\xi_j(f_\alpha) = 0$) при $1 \leqslant \alpha \leqslant k-1$. Если $f_\alpha(\xi_j) = 0$ при $1 \leqslant \alpha \leqslant k-1$, то положим $v'_{i,j} = L$ и $h'_{i,j} = 0$.

В дальнейшем GCD обозначает наибольший общий делитель. Если $f_\alpha(\xi_j) \neq 0$ для некоторого α, то мы выбираем такое α_j, $1 \leqslant \alpha_j \leqslant k-1$, что $f_{\alpha_j}(\xi_j) \neq 0$. В этом случае мы собираемся вычислить полином $h'_{i,j} \in A = B[X_n]$, такой, что

$$h'_{i,j} \bmod \mathfrak{p}_j = \mathrm{GCD}_{X_n}(f_1 \bmod \mathfrak{p}_j, , \ldots, f_n \bmod \mathfrak{p}_j) \tag{2}$$

в кольце $K_j[X_n]$ и $\deg_{X_n} h'_{i,j} = \deg_{X_n}(h'_{i,j} \bmod \mathfrak{p}_j)$. Заметим, что тогда $h'_{i,j} \notin \mathfrak{p}_j$.

Выберем подмножество $\mathcal{J}(n,d) \subset F$ с числом элементов $\#\mathcal{J}(n,d) = (2d+1)n+1$ и такое, что $\mathrm{l}(c) = O(\log_2(nd))$ для всякого $c \in \mathcal{J}(n,d)$ с абсолютной константой в $O(\ldots)$.

Более точно, если $\mathrm{char}(F) = 0$, то мы предполагаем, что $\mathcal{J}(n,d) \subset \mathbb{Z}$. В этом случае найдём простое число q, такое, что $q > (2d+1)n+1$. Для всякого $c \in \mathcal{J}(n,d)$ и целого числа α, где $0 \leqslant \alpha \leqslant n$, положим $c^{(\alpha)}$ равным целому числу, такому, что $0 \leqslant c^{(\alpha)} < q$ и $c^{(\alpha)} = c^\alpha \bmod q$.

Если $\mathrm{char}(F) = p > 1$ и поле F не является конечным, то мы предполагаем, что $\mathcal{J}(n,d) \subset \mathbb{F}_p[t]$ для некоторого элемента $t \in F$, трансцендентного над $\mathbb{F}_p$, с небольшой длиной записи $\mathrm{l}(t)$. В этом случае мы находим неприводимый многочлен $q \in \mathbb{F}_p[t]$ наименьшей степени, такой, что $\#\mathbb{F}_p[t]/(q) > (2d+1)n+1$. Для всякого $c \in \mathcal{J}(n,d)$ и целого числа α, где $0 \leqslant \alpha \leqslant n$, положим $c^{(\alpha)}$ равным элементу из $\mathbb{F}_p[t]$, такому, что $\deg_t(c^{(\alpha)}) < \deg_t(q)$ и $c^{(\alpha)} = c^\alpha \bmod q$ в кольце $\mathbb{F}_p[t]/(q)$.

Кроме того, мы предполагаем, что $\#\mathcal{J}(n,d) = \#(\mathcal{J}(n,d) \bmod q)$.

Для всякого $c \in \mathcal{J}(n,d)$ положим $\varphi_c = f_0 + \sum\limits_{1 \leqslant \alpha \leqslant k-1} c^{(\alpha)} f_\alpha$ (напомним, что $k = n+1$). Обозначим через $\mathcal{J}'(n,d)$ подмножество всех $c \in \mathcal{J}(n,d)$, таких, что $\deg(\varphi_c \bmod \mathfrak{p}_j) = \max_{0 \leqslant \alpha \leqslant k-1} \deg(f_\alpha \bmod \mathfrak{p}_j)$. Мы строим это подмножество $\mathcal{J}'(n,d)$, используя общую точку ξ_j. Тогда, очевидно, $\#\mathcal{J}'(n,d) \geqslant 2nd+1$.

Теперь мы утверждаем, что существует элемент $c \in \mathcal{J}'(n,d)$, такой, что $\deg_{X_n} \mathrm{GCD}(f_{\alpha_j} \bmod \mathfrak{p}_j, \varphi_c \bmod \mathfrak{p}_j) = \deg_{X_n} h'_{i,j}$. Это может быть легко выведено, например, из [6, разд. 2], см. там определение $(**)$.

Общая точка ξ_j компоненты W_j известна. Поэтому для вычисления коэффициентов наибольшего общего делителя многочленов по модулю $\mathfrak{p}_j$ можно использовать субрезультантный алгоритм, см., например, [7],

а также [6, разд. 2], где более подробно рассмотрена наша ситуация. Более точно, пусть $f_\alpha = \sum\limits_{\beta\geqslant 0} f_{\alpha,\beta}X_n^\beta$, где $f_{\alpha,\beta}\in B^{(0)}$ для всех α,β. Положим $d_{j,\alpha} = \deg_{X_n}(f_\alpha \bmod \mathfrak{p}_j)$ и $\widetilde{f}_\alpha = \sum\limits_{0\leqslant\beta\leqslant d_{j,\alpha}} f_{\alpha,\beta}X_n^\beta$. Для всякого $c\in\mathcal{J}'(n,d)$ мы применяем субрезультантный алгоритм для вычисления наибольшего общего делителя относительно X_n многочленов $\widetilde{f}_{\alpha_j} \bmod \mathfrak{p}_j$ и $(\widetilde{f}_0 + \sum\limits_{1\leqslant\alpha\leqslant k-1} c^\alpha \widetilde{f}_\alpha) \bmod \mathfrak{p}_j$. На выходе получаем полином $h'_{i,j,c}\in A^{(0)}$, такой, что $h'_{i,j,c} \bmod \mathfrak{p}_j$ является наибольшим общим делителем этих многочленов и $\deg_{X_n}(h'_{i,j,c} \bmod \mathfrak{p}_j) = \deg_{X_n} h'_{i,j,c}$. Выберем $c_0\in\mathcal{J}'(n,d)$ так, что $\deg_{X_n} h'_{i,j,c_0} = \min\{\deg_{X_n} h_{i,j,c} : c\in\mathcal{J}'(n,d)\}$ и положим $h'_{i,j} = h'_{i,j,c_0}$. Тогда выполняется условие (2).

Таким образом, согласно субрезультантному алгоритму, $h'_{i,j}\in A$ является многочленом (соответственно однородным многочленом), таким, что $\deg h'_{i,j} < 2d^2$ (фактически здесь можно заменить $< 2d^2$ на $\leqslant d^2$), $\deg_{T_1,\dots,T_l} h'_{i,j} \leqslant d_2\mathcal{P}(d_1 d)$ и $\mathrm{l}(h'_{i,j}) \leqslant (M_1+M_2+d_2+n)\mathcal{P}(d_1 d)$.

Пусть $d'_i = \max_{j\in I_{i-1}} \deg h'_{i,j}$. Положим $h_{i,j} = L^{d'_i - \deg h'_{i,j}} h'_{i,j}$ для всех $j\in I_{i-1}$. Тогда условие $h_{i,j}\neq 0$ влечёт, что $\deg h_{i,j} = d'_i$, т.е. ненулевые $h_{i,j}$ являются многочленами (соответственно однородными многочленами) одной и той же степени для всех $j\in I_{i-1}$.

Если $h_{i,j}\neq 0$, то положим $v'_{i,j} = \mathrm{lc}_{X_n} h_{i,j}$ равным старшему коэффициенту полинома $h_{i,j}$ относительно X_n. Теперь $v'_{i,j}\notin\mathfrak{p}_j$ для всех $j\in I_{i-1}$. Положим $d''_i = \max_{j\in I_{i-1}} \deg v'_{i,j} < 2d^2$, $d''_{i,j} = \deg v'_{i,j}$ и $v_{i,j} = L^{d''_i - d''_{i,j}} v'_{i,j}$, $j\in I_{i-1}$. Тогда $v_{i,j}\neq 0$ и $\deg v_{i,j} = d''_i \geqslant 1$ для всех $j\in I_{i-1}$. Положим $I'_{i-1} = \{j\in I_{i-1} : \deg_{X_n} h_{i,j} > 0\}$,

$$\nu_i = \max(\{\deg_{X_n} f_\alpha - \deg_{X_n} h_{i,j} + 1 : 0\leqslant\alpha\leqslant k-1,\ j\in I'_{i-1}\}\cup\{1\}) \quad (3)$$

и $u_{i,j} = L v_{i,j}^{\nu_i}$ (мы вводим здесь множитель L, чтобы гарантировать, что $\dim W_j\cap\mathcal{Z}(u_{i,j}) = -1 + \dim W_j$ для всякого $j\in I_i$, поскольку иначе, без этого множителя L, может случиться, что $0\neq u_{i,j}\in F$ и $W_j\cap\mathcal{Z}(u_{i,j}) = \varnothing$; в этом случае можно было бы слегка модифицировать описываемую конструкцию и обойтись без множителя L, но мы не делаем этого). Следовательно, $\deg u_{i,j} = \nu_i d''_i + 1$ для всех $j\in I_{i-1}$. Заметим, что также $\deg_{X_n}(f_\alpha \bmod \mathfrak{p}_j) \leqslant \deg_{X_n} f_\alpha$ и это неравенство может быть строгим для некоторых α и j, однако $\deg_{X_n} h_{i,j} = \deg_{X_n}(h_{i,j} \bmod \mathfrak{p}_j) \leqslant \max_\alpha\{\deg_{X_n}(f_\alpha \bmod \mathfrak{p}_j)\}$, см. выше.

Если $h_{i,j} \neq 0$, то, согласно (3) и определениям $v'_{i,j}$, $v_{i,j}$ и $u_{i,j}$, можно записать $u_{i,j}f_\alpha = q_{\alpha,i,j}h_{i,j} + r_{\alpha,i,j}$, где $q_{\alpha,i,j}, r_{\alpha,i,j} \in A$, $\deg_{X_n} r_{\alpha,i,j} < \deg_{X_n} h_{\alpha,i,j}$ и если $q_{\alpha,i,j} \neq 0$, то $\deg_{X_n} q_{\alpha,i,j} = \deg_{X_n} f_\alpha - \deg_{X_n} h_{i,j}$. Далее, согласно (2) мы имеем $r_{\alpha,i,j} \bmod \mathfrak{p}_j = 0$. Следовательно, $u_{i,j}f_\alpha = q_{\alpha,i,j}h_{i,j} \bmod \mathfrak{p}_j$. Дополнительно в случае "(соответственно ...)" многочлены $q_{\alpha,i,j}$, $r_{\alpha,i,j}$ являются однородными и справедливы следующие два утверждения. Либо $q_{\alpha,i,j} = 0$, либо $\deg q_{\alpha,i,j} = \nu_i d''_i + 1 + d - d'_i$. Либо $r_{\alpha,i,j} = 0$, либо $\deg r_{\alpha,i,j} = \nu_i d''_i + 1 + d$.

Если $h_{i,j} = 0$, то положим $q_{\alpha,i,j} = L^{\nu_i d''_i + 1 + d - d'_i}$. Напомним, что в этом случае $f_\alpha \bmod \mathfrak{p}_j = 0$ для всех α. Поэтому снова $u_{i,j}f_\alpha = q_{\alpha,i,j}h_{i,j} \bmod \mathfrak{p}_j$ и $\deg q_{\alpha,i,j} = \nu_i d''_i + 1 + d - d'_i$.

Для краткости обозначим $\mathfrak{q} = \cap_{j \in I_{i-1}} \mathfrak{p}_j$. Построим, см. лемму 1, многочлены (соответственно однородные многочлены) $u'_i \in B$ и $h'_i \in A$, такие, что

$$\iota(u'_i \bmod \mathfrak{q}) = \{(\Delta')^2 u_{i,j} \bmod \mathfrak{p}_j\}_{j \in I_{i-1}},$$
$$\iota(h'_i \bmod \mathfrak{q}) = \{\Delta' h_{i,j} \bmod \mathfrak{p}_j\}_{j \in I_{i-1}}.$$

Далее, существует элемент $q_{\alpha,i} \in A$, такой, что

$$\iota(q_{\alpha,i} \bmod \mathfrak{q}) = \{\Delta' q_{\alpha,i,j} \bmod \mathfrak{p}_j\}_{j \in I_{i-1}}.$$

Теперь при $1 \leqslant \alpha \leqslant k-1$ мы имеем

$$\iota(u'_i f_\alpha \bmod \mathfrak{q}) = \{(\Delta')^2 u'_{i,j} f_\alpha \bmod \mathfrak{p}_j\}_{j \in I_{i-1}}$$
$$= \{(\Delta' q_{\alpha,i,j})(\Delta' h_{i,j}) \bmod \mathfrak{p}_j\}_{j \in I_{i-1}} = \iota(q_{\alpha,i} h'_i \bmod \mathfrak{q}).$$

Это означает, что

$$u'_i \mathfrak{a}' \subset A h'_i + \mathfrak{q} = A h'_i + \mathfrak{N}(A u'_1 + \ldots + A u'_{i-1}) \subset \mathfrak{N}(A h'_i + A u'_1 + \ldots + A u'_{i-1})$$

в кольце A. Пусть $b_i \geqslant 0$ – наименьшее целое число, такое, что $(u'_i)^{p^{b_i}} \in B^{(0)}$, и $a_i \geqslant 0$ – наименьшее целое число, такое, что $(h'_i)^{p^{a_i}} \in A^{(0)}$. Положим $u_i = (u'_i)^{p^{b_i}}$ и $h_i = (h'_i)^{p^{a_i}}$. Мы вычисляем a_i и b_i. Тогда, очевидно, $u_i \mathfrak{a} \subset \mathfrak{N}(A^{(0)} h_i + A^{(0)} u_1 + \ldots + A^{(0)} u_{i-1})$ в кольце $A^{(0)}$.

Заметим, что элемент u_i не является делителем нуля в кольце $B^{(0)}/(u_1, \ldots, u_{i-1})$, поскольку для всякого $j \in I_{i-1}$

$$\mathcal{Z}(u_i) \cap W_j = \mathcal{Z}(u'_i) \cap W_j = \mathcal{Z}(\Delta^2 u_{i,j}) \cap W_j \neq W_j.$$

Более того, $\dim \mathcal{Z}(u_i) \cap W_j = -1 + \dim W_j$ для всякого $j \in I_{i-1}$, поскольку $u_{i,j} = L v_{i,j}^{\nu_i}$. Поэтому $\dim E_i = n - 1 - i$. Рекурсивный шаг описан в случае $i > 1$.

Пусть $i = n-1$. Пусть все многочлены $f_0, \dots, f_{k-1}$ однородны и $\mathfrak{a} \subset AX_1 + \dots + AX_{n-1}$. Тогда из рекурсивного предположения вытекает, что $A^{(0)}X_1 + \dots + A^{(0)}X_{n-1} = \mathfrak{N}(A^{(0)}u_1 + \dots + A^{(0)}u_{n-1})$. Следовательно, $u_n\mathfrak{a} \subset \mathfrak{N}(A^{(0)}h_n + A^{(0)}u_1 + \dots + A^{(0)}u_{n-1})$ с $h_n = 0$ и $u_n = 1$.

Рассмотрим случай $i = 1$. Если $i = 1$, то имеется много упрощений. Именно, $\#I_1 = 1$, и $W_j = \mathbb{A}^{n-1}(\overline{F})$ для $j \in I_1$. Далее, идеал $\mathfrak{p}_j$ алгебраического многообразия W_j равен $\{0\}$. Мы определяем $h'_{1,j}$ по формуле (2) (сейчас можно совсем опустить $\mathrm{mod}\mathfrak{p}_j$ везде в (2)) и полагаем $h_1 = h_{1,j} = h'_{1,j}$. Имеем $h_1 \neq 0$, поскольку $f_0 \neq 0$. Положим $v_{1,j} = \mathrm{lc}_{X_n} h_{1,j}$. Целое число ν_1 определяется снова по формуле (3). Положим $L = X_1$, $u_1 = Lv_{1,j}^{\nu_1}$. Теперь $u_1 \neq 0$ и $u_1\mathfrak{a} \subset A^{(0)}h_1 \subset \mathfrak{N}(A^{(0)}h_1)$. Рекурсивный шаг описан в случае $i = 1$.

Остаётся получить оценки на степени и длины записи коэффициентов построенных объектов. Положим $D_i = \max\{\deg u_1, \dots, \deg u_i, d\}$ и

$$D'_i = D_1 D_2 \cdot \ldots \cdot D_i, \quad 1 \leqslant i \leqslant n. \tag{4}$$

Тогда $\deg E_i \leqslant D'_i$ по теореме Безу. Также известно, ср., например, [1] и [3, 4], что алгебраическое многообразие E_i и все неприводимые компоненты $W_{i,j}$, $j \in I_i$, определены над полем $F^{p^{-\mu_i}}$, где $\mu_i \geqslant 0$ – наименьшее целое число, такое, что $p^{\mu_i+1} > D'_i$. Имеем $D'_1 = D_1 \leqslant 2d^2$.

Пусть $1 < i \leqslant n$. Согласно описанной конструкции,

$$\deg u'_i \leqslant 2\deg\Delta + d''_i\nu_i + 1 \leqslant 2(D'_{i-1})^2 + 2d^3,$$
$$\deg h'_i \leqslant \deg\Delta + 2d^2 \leqslant (D'_{i-1})^2 + 2d^2.$$

Многочлен u'_i лежит в $F^{p^{-\mu_{i-1}}}[X_1, \dots, X_n]$. Это следует из китайской теоремы об остатках, см. лемму 1. Поэтому $b_i \leqslant \mu_{i-1}$ и

$$\deg u_i \leqslant 2D'_{i-1}((D'_{i-1})^2 + d^3).$$

Следовательно,

$$D_i \leqslant 2D'_{i-1}((D'_{i-1})^2 + d^3), \quad 1 < i \leqslant n. \tag{5}$$

Аналогично, $h'_i \in F^{p^{-\mu_{i-1}}}[X_1, \dots, X_n]$, и $a_i \leqslant \mu_{i-1}$. Следовательно,

$$\deg h_i \leqslant D'_{i-1}((D'_{i-1})^2 + 2d^2). \tag{6}$$

Пусть $1 \leqslant i \leqslant n$. Тогда положим $D''_i = \max\limits_{1\leqslant\alpha\leqslant i}\{\deg_{T_1,\dots,T_l}\deg u_\alpha, d_2\}$ и $M''_i = \max\{\mathrm{l}(u_1), \dots, \mathrm{l}(u_i), M_1 + M_2 + d_2 + n\}$. Согласно [1] (и также [3, 4]), при $1 < i \leqslant n$ имеем $\deg_{T_1,\dots,T_l}(\Phi_{i-1}) \leqslant D''_{i-1}\mathcal{P}(d_1(D_{i-1})^{i-1})$. Поэтому согласно описанной конструкции получаем последовательно,

что также степени относительно $T_1, \dots, T_l$ многочленов Δ_{i-1}, u'_i, h'_i, u_i и h_i ограничены сверху величиной $D''_{i-1}\mathcal{P}(d_1(D_{i-1})^{i-1})$. Следовательно,

$$D''_i \leqslant D''_{i-1}\mathcal{P}(d_1(D_{i-1})^{i-1}), \quad 1 < i \leqslant n. \tag{7}$$

Положим $M'''_{i-1} = M''_{i-1} + M_1 + D''_{i-1} + n$. Тогда, аналогично, согласно [1] (и также [3, 4]) имеем $\mathrm{l}(\Phi_{i-1}) \leqslant M'''_{i-1}\mathcal{P}(d_1(D_{i-1})^{i-1})$. Поэтому согласно описанной конструкции получаем последовательно, что также $\mathrm{l}(\Delta_{i-1})$, $\mathrm{l}(u'_i)$, $\mathrm{l}(h'_i)$, $\mathrm{l}(u_i)$ и $\mathrm{l}(h_i)$ ограничены сверху величиной $M'''_{i-1}\mathcal{P}(d_1(D_{i-1})^{i-1})$. Следовательно,

$$M''_i \leqslant (M''_{i-1} + M_1 + D''_{i-1} + n)\mathcal{P}(d_1(D_{i-1})^{i-1}), \quad 1 < i \leqslant n. \tag{8}$$

Теперь из (4)–(8) следует, что существует константа $c_1 > 0$, такая, что $D_i \leqslant d^{2^{c_1 i}}$, $D''_i \leqslant d_2\mathcal{P}(d_1^i d^{i\,2^{c_1 i}})$ и $M''_i \leqslant (M_1+M_2+d_2+n)\mathcal{P}(d_1^i d^{i\,2^{c_1 i}})$ при $1 \leqslant i \leqslant n$ (здесь мы оставляем подробности читателю). Следовательно, снова по (4)–(8) существует константа $c > 0$, такая, что выполняются оценки из формулировки теоремы 2. Теорема доказана. □

Замечание 3. Фактически несложно привести более точные оценки, чем оценки из теоремы 2, а также уточнить c. Но эти оценки остаются дважды экспоненциальными от n. Так что мы не делаем этого.

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. A. L. Chistov, *An improvement of the complexity bound for solving systems of polynomial equations.* — Зап. научн. семин. ПОМИ **390** (2011), 299–306.
3. А. Л. Чистов, *Системы с параметрами, или эффективное решение систем полиномиальных уравнений* 33 *года спустя.* I. — Зап. научн. семин. ПОМИ **462** (2017), 122–166.
4. А. Л. Чистов, *Системы с параметрами, или эффективное решение систем полиномиальных уравнений* 33 *года спустя.* II. — Зап. научн. семинаров ПОМИ **468** (2018), 138–176.
5. А. Л. Чистов, *Алгоритмы полиномиальной сложности для новой модели представления алгебраических многообразий.* — Зап. научн. семин. ПОМИ **378** (2010), 133–170.
6. А. Л. Чистов, *Эффективное разложение многочленов с параметрическими коэффициентами на абсолютно неприводимые множители.* — Зап. научн. семин. ПОМИ **448** (2016), 286–325.
7. G. E. Collins, *Polynomial remainder sequences and determinants.* — Amer. Math. Monthly **73**, No. 7 (1966), 708–712.

8. L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.* — J. reine angew. Math. **92** (1882), 1–123.
9. U. Storch, *Bemerkung zu einem Satz von M. Kneser.* — Arch. Math. **23** (1972), 403–404.
10. D. Eisenbud, E. G. Evans, Jr. *Every algebraic set in n-space is the intersection of n hypersurfaces.* — Inv. Math. **19** (1973), 107–112.
11. E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.

Chistov A. L. An effective construction of a small number of equations defining an algebraic variety.

Consider a system of polynomial equations in n variables of degrees at most d with the set of all common zeros V. We suggest subexponential time algorithms (in the general case and in the case of zero characteristic) for constructing $n+1$ equations of degrees at most d defining the algebraic variety V.

Further, we construct n equations defining V. We give an explicit upper bound on the degrees of these n equations. It is double exponential in n. The running time of the algorithm for constructing them is also double exponential in n.

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

Поступило 15 сентября 2021 г.