Записки научных
семинаров ПОМИ
Том 462, 2017 г.

А. Л. Чистов

СИСТЕМЫ С ПАРАМЕТРАМИ, ИЛИ ЭФФЕКТИВНОЕ РЕШЕНИЕ СИСТЕМ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ 33 ГОДА СПУСТЯ. I

Введение

Пусть k – произвольное поле, содержащее достаточно много элементов, с характеристической экспонентой p. Обозначим через $\overline{k}$ алгебраическое замыкание поля k. Пусть $\nu \geqslant 0$ является целым числом. Пусть $a_1, \ldots, a_\nu$ – семейство независимых переменных (или параметров) над k. Обозначим через $\mathbb{A}^\nu(\overline{k})$ аффинное пространство параметров с координатными функциями $a_1, \ldots, a_\nu$ (в более общей ситуации можно рассматривать алгебраическое многообразие параметров $\mathcal{V} \subset \mathbb{A}^\nu(\overline{k})$, но этот случай легко сводится к частному случаю $\mathcal{V} = \mathbb{A}^\nu(\overline{k})$).

В данной статье мы рассматриваем проблему решения систем полиномиальных уравнений с параметрическими коэффициентами из кольца $k[a_1, \ldots, a_\nu]$. На выходе мы получаем решения, зависящие от этих параметров. Точные формулировки даются ниже, см. теоремы 1 и 2. Чтобы получить требуемые результаты, мы опираемся на наши алгоритмы из [2, 3, 7] для решения обычных систем полиномиальных уравнений. Они имеют наилучшую известную сложность в общем случае. Но оказывается, что эти алгоритмы не являются достаточно явными для целей настоящей статьи. Так что в этой статье мы в значительной степени пересматриваем алгоритмы из [2, 3, 7] и даём новое, вероятно более чёткое и краткое, обоснование для них (хотя основные идеи остаются теми же самыми). Фактически, в данной статье как частный случай $\nu = 0$ нашего основного результата о системах с параметрами мы получаем улучшенные и более явные версии алгоритмов из [2, 3, 7] для решения систем полиномиальных уравнений. Также мы даём замкнутое в себе теоретическое обоснование для этих новых версий. Теперь для удобства читателя мы хотели бы перечислить улучшения

Ключевые слова: параметрические коэффициенты, стратификации, абсолютно неприводимые компоненты, решение систем полиномиальных уравнений.

в этих новых версиях алгоритмов для решения систем полиномиальных уравнений по сравнению с [2, 3, 7].

1) Мы рассматриваем сепарабельные базисы трансцендентности полей рациональных функций неприводимых компонент многообразия решений, см. лемму 7 в разделе 4.[1]
2) Описано более явное сведение к случаю нулевой размерности. Всё сводится к вычислению некоторых определителей и результантов (конечно, они тоже являются определителями).
3) Мы предлагаем новую явную конструкцию общих точек компонент многообразия решений. Координаты этих точек являются отношениями некоторых частных производных, см. разделы 3 и 6.
4) Мы предлагаем новую явную и прозрачную конструкцию систем полиномиальных уравнений, задающих неприводимые компоненты многообразия решений, см. п. (xii) ниже. Эта конструкция пригодна даже для равноразмерностных алгебраических многообразий, см. п. (xi) ниже и лемму 8 в разделе 4.
5) Мы получаем разложение многообразия решений в объединение равноразмерностных алгебраических многообразий. В ненулевой характеристике мы получаем явное разложение многообразия решений в объединение равноразмерностных алгебраических многообразий, определённых над полями k^{1/p^r}, где r – неотрицательное целое число, см. п. (v) ниже.
6) Получен явный критерий для того, чтобы решить, задают ли линейные формы $Y_0, \ldots, Y_s$ сепарабельный базис трансцендентности $Y_1/Y_0, \ldots, Y_s/Y_0$ поля рациональных функций каждой неприводимой компоненты размерности s многообразия решений исходной системы, см. лемму 15 в разделе 6.
7) Даются более точные оценки для степеней, длин записи коэффициентов и времени работы алгоритма. Например, мы используем D'_{n-s}, D_{n-s} (см. ниже) вместо d^{n-s}, ср. [2, 3, 7].

[1]Иногда в данной первой части статьи, главным образом для обзора результатов, мы используем ссылки на леммы, разделы и т.д. из следующей части этой статьи (или следующих частей; это зависит от обстоятельств при публикации). Во всех частях нумерация теорем (соответственно лемм, разделов и т.д.) продолжается из настоящей первой части.

8) Только многочлены от одной переменной раскладываются на неприводимые множители, т.е. достаточно иметь алгоритмы для факторизации лишь для многочленов от одной переменной.
9) Мы исправили неточность в лемме 2.11 работы [2] (следует полностью удалить там эту лемму), см. замечание 8 в разделе 4. Фактически, это простое исправление сделано в [7, стр. 221], но его нельзя найти на английском языке. Всё же странно, что никто не обращал внимания на эту неточность до сих пор (насколько это известно автору).

Теперь мы возвращаемся к системам с параметрами. Пусть $m, n \geqslant 1$ – целые числа. Пусть $f_0, \ldots, f_{m-1} \in k[a_1, \ldots, a_\nu, X_0, \ldots, X_n]$ – однородные относительно $X_0, \ldots, X_n$ многочлены. Предположим, что

$$\deg_{X_0,\ldots,X_n} f_i = d_i \leqslant d, \quad \deg_{a_1,\ldots,a_\nu} f \leqslant d' \tag{1}$$

для некоторых целых чисел $d_0 \geqslant d_1 \geqslant \ldots \geqslant d_{m-1} \geqslant 0$ и $d, d' \geqslant 2$.

Следовательно, каждый многочлен f_i представляется в виде

$$f_i = \sum_{\substack{i_1,\ldots,i_\nu \geqslant 0,\ i_1+\ldots+i_\nu \leqslant d',\\ j_0,\ldots,j_n \geqslant 0,\ j_0+\ldots+j_n = d_i}} f_{i,i_1,\ldots,i_\nu,\,j_0,\ldots,j_n}\, a_1^{i_1} \cdot \ldots \cdot a_\nu^{i_\nu} X_0^{j_0} \cdot \ldots \cdot X_n^{j_n}, \tag{2}$$

где $0 \leqslant i \leqslant m-1$, все $i_1, \ldots, i_\nu$, $j_0, \ldots, j_n$ являются целыми числами и все коэффициенты $f_{i,i_1,\ldots,i_\nu,j_0,\ldots,j_n}$ лежат в k.

Пусть $a^* = (a_1^*, \ldots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$. Обозначим через $V_{a^*} \subset \mathbb{P}^n(\overline{k})$ многообразие всех решений системы полиномиальных уравнений

$$f_0(a_1^*, \ldots, a_\nu^*, X_0, \ldots, X_n) = \cdots = f_{m-1}(a_1^*, \ldots, a_\nu^*, X_0, \ldots, X_n) = 0 \tag{3}$$

(если $\nu = 0$, то $\mathbb{A}^\nu(\overline{k}) = \{()\}$ является множеством, состоящим из одного элемента; если $a^{(0)} = () \in \mathbb{A}^\nu(\overline{k})$, то последовательность $a_1^{(0)}, \ldots, a_\nu^{(0)}$ пуста и мы предполагаем, что $f_i(a_1^{(0)}, \ldots, a_\nu^{(0)}, X_0, \ldots, X_n) = f_i$ для всех i; мы принимаем подобное соглашение и для других многочленов с параметрическими коэффициентами в случае $\nu = 0$).

Для всякой точки $a^* \in \mathbb{A}^\nu(\overline{k})$, для всякого целого s, где $0 \leqslant s \leqslant n$, обозначим через $V_{a^*,s}$ объединение всех неприводимых компонент W многообразия V_{a^*}, таких, что $\dim W = s$. Например, $V_{a^*,s} = \varnothing$, если $n > m$ и $s < n - m$.

Пусть c и c' – целые числа, такие, что $-1 \leqslant c \leqslant n$ и $0 \leqslant c' \leqslant \max\{0, c\}$. Положим $V_{a^*}^{(c',c)} = \bigcup\limits_{c' \leqslant s \leqslant c} V_{a^*,s}$. Так что $V_{a^*}^{(c',c)}$ является объединением всех неприводимых компонент W многообразия V_{a^*}, таких, что $c' \leqslant \dim W \leqslant c$. В частности, $V_{a^*}^{(0,n)} = V_{a^*}$, $V_{a^*}^{(0,0)} = V_{a^*,0}$, и $V_{a^*}^{(0,-1)} = \varnothing$.

Обозначим через $\mathcal{U}_c$ подмножество всех таких $a^* \in \mathbb{A}^\nu(\overline{k})$, что $\dim V_{a^*} \leqslant c$. Можно доказать, что это открытое в топологии Зарисского подмножество аффинного пространства $\mathbb{A}^\nu(\overline{k})$. Следовательно, если $a^* \in \mathcal{U}_c$, то $V_{a^*} = V_{a^*}^{(0,c)}$. Если $a^* \in \mathcal{U}_{-1}$, то $V_{a^*} = \varnothing$.

Рассмотрим проблему, состоящую в том, чтобы представить множество параметров

$$\mathcal{U}_c = \bigcup_{\alpha \in A} \mathcal{W}_\alpha \tag{4}$$

как объединение конечного числа ($\#A < +\infty$) квазипроективных алгебраических многообразий $\mathcal{W}_\alpha$, удовлетворяющих следующим свойствам. Для всякого $\alpha \in A$, для всех $a^* = (a_1^*, \ldots, a_\nu^*) \in \mathcal{W}_\alpha$ подмногообразие решений $V_{a^*}^{(c',c)}$ задано равномерно, т.е. некоторыми алгебраическими формулами (аналогично [2], подробности см. ниже), определёнными везде на $\mathcal{W}_\alpha$ и зависящими от $a_1^*, \ldots, a_\nu^*$ как от параметров.

Для произвольного многочлена $f \in k[a_1, \ldots, a_\nu, X_0, \ldots, X_n]$ и точки $a^* = (a_1^*, \ldots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$ мы будем обозначать $f(a^*, X_0, \ldots, X_n) = f(a_1^*, \ldots, a_\nu^*,\ X_0, \ldots, X_n)$ и использовать другие подобные обозначения.

Обозначим через k_{a^*} поле, порождённое над k координатами точки a^*, т.е. $k_{a^*} = k(a_1^*, \ldots, a_\nu^*)$ (если $\nu = 0$, то мы предполагаем, что $k_{a^*} = k$ для $a^* \in \mathbb{A}^\nu(\overline{k})$; напомним, что $\#\mathbb{A}^\nu(\overline{k}) = 1$ для $\nu = 0$). Так что все многочлены $f_i(a^*, X_0, \ldots, X_n)$ лежат в $k_{a^*}[X_0, \ldots, X_n]$.

Пусть $\mathcal{Z}(f_i(a^*, X_0, \ldots, X_n),\ 0 \leqslant i \leqslant m-1)$ обозначает множество всех общих нулей рассматриваемых полиномов в $\mathbb{P}^n(\overline{k})$. Следовательно, $V_{a^*} = \mathcal{Z}(f_i(a^*, X_0, \ldots, X_n),\ 0 \leqslant i \leqslant m-1)$. Мы будем пользоваться и другими аналогичными обозначениями.

Замечание 1. В дальнейшем мы будем предполагать, что $d_{m-1} \geqslant 1$. Покажем, что это не ограничивает общности. В самом деле, пусть существуют $q \geqslant 1$ многочленов f_i с $d_i = 0$. Тогда для всякого i, где $0 \leqslant i \leqslant m-1$, с $\deg_{X_0,\ldots,X_n} f_i = d_i = 0$ достаточно заменить многочлен f_i на семейство многочленов $\{X_j f_i\}_{0 \leqslant j \leqslant n}$ и m на $m + qn$. После этого

для всякого $a^* \in \mathbb{A}^\nu(\overline{k})$ вновь полученная система (3) эквивалентна первоначальной системе (3).

Теперь мы собираемся придать точный смысл равномерности алгебраических формул, относящихся к (4). Именно, выполняются следующие свойства.

(i) Для всякого $\alpha \in A$ многообразие $\mathcal{W}_\alpha$ непусто. Для всех $\alpha_1, \alpha_2 \in A$ если $\alpha_1 \neq \alpha_2$, то $\mathcal{W}_{\alpha_1} \cap \mathcal{W}_{\alpha_2} = \varnothing$, т.е. эти многообразия $\mathcal{W}_\alpha$ попарно различны; поэтому мы будем называть их стратами и объединение (4) стратификацией.

(ii) Можно представить $\mathcal{W}_\alpha$ в виде

$$\mathcal{W}_\alpha = \mathcal{W}_\alpha^{(1)} \setminus \bigcup_{2 \leqslant \beta \leqslant \mu_\alpha} \mathcal{W}_\alpha^{(\beta)},$$

где каждое $\mathcal{W}_\alpha^{(\beta)} = \mathcal{Z}(\psi_{\alpha,1}^{(\beta)}, \ldots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)})$, $1 \leqslant \beta \leqslant \mu_\alpha$, является множеством всех общих нулей многочленов $\psi_{\alpha,1}^{(\beta)}, \ldots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)} \in k[a_1, \ldots, a_\nu]$ в аффинном пространстве $\mathbb{A}^\nu(\overline{k})$, а $m_{\alpha,\beta}$ – целое число, не меньшее единицы.

Пусть $\alpha \in A$ произвольно. Пусть s – произвольное целое число, такое, что

$$c' \leqslant s \leqslant c$$

(если $c = -1$, то таких целых чисел s не существует).

(iii) Если $V_{a^*,s} = \varnothing$ для некоторого $a^* \in \mathcal{W}_\alpha$, то $V_{a^*,s} = \varnothing$ для всех $a^* \in \mathcal{W}_\alpha$ (если $s \neq n$, то последняя импликация следует также из (iv)).

Если $m-1 < n$, то для всех i из интервала $m-1 \leqslant i \leqslant n$ положим $d_i = 1$ (но в этом случае многочлены f_i для этих i не определены). Положим

$$D'_{n-s} = d_0 d_1 \cdot \ldots \cdot d_{n-s-1}, \quad 0 \leqslant s \leqslant n-1,$$

и $D'_{n-s} = 1$, если $s = n$.

Положим $\rho_s = 0$, если $p = 1$, и $\rho_s = \log_p D'_{n-s}$ в противном случае.

В дальнейшем в статье все константы в $O(\ldots)$ являются абсолютными.

Пусть $\mathcal{I}_\varkappa$ – конечное подмножество в $k \setminus \{0\}$ с числом элементов $\#\mathcal{I}_\varkappa = \varkappa + 1$. Пусть s – целое число, $0 \leqslant s \leqslant n-1$. Положим

$$\mathcal{M}_\varkappa = \Big\{ \sum_{0 \leqslant i \leqslant n} \gamma^i X_i \,:\, \gamma \in \mathcal{I}_\varkappa \Big\}, \quad \mathcal{M}'_{s,\varkappa} = \Big\{ \sum_{s+1 \leqslant i \leqslant n} \gamma^{i-s-1} X_i \,:\, \gamma \in \mathcal{I}_\varkappa \Big\}. \tag{5}$$

Это конечные множества линейных форм с коэффициентами из k.

Положим $\varkappa_{1,s} = 2(n-s)D'_{n-s} + s$ и $\varkappa_{2,s} = (n-s)D'_{n-s}(D'_{n-s}-1)/2$. Для всякого s, $0 \leqslant s \leqslant n-1$, определим

$$\mathcal{L}_s = \mathcal{M}_{\varkappa_{1,s}}, \qquad \mathcal{L}'_s = \mathcal{M}'_{s,\varkappa_{2,s}}.$$

Ниже в пунктах (iv)–(xii) мы предполагаем дополнительно, что s – произвольное целое число, такое, что $c' \leqslant s \leqslant \min\{c, n-1\}$. Для любого такого s существуют линейные формы $Y_0, \dots, Y_s \in \mathcal{L}_s$ и $Y_{s+1} \in \mathcal{L}'_s$ (зависящие от α и s; мы будем писать также $Y_i = Y_{s,i}$, если важна зависимость от s, так что $(Y_{s,0}, \dots, Y_{s,s+1}) \in \mathcal{L}_s^{s+1} \times \mathcal{L}'_s$), удовлетворяющие следующим свойствам.

(iv) Для всякого $a^* \in \mathcal{W}_\alpha$ имеем $V_{a^*,s} \cap \mathcal{Z}(Y_0, \dots, Y_s) = \varnothing$ в $\mathbb{P}^n(\overline{k})$.

(v) Линейные формы $Y_0, \dots, Y_{s+1}$ линейно независимы. Для всякого целого числа r, $0 \leqslant r \leqslant \rho_s$, существует ненулевой полином $\Phi_{\alpha,s,r} \in k[a_1, \dots, a_\nu, Y_0, \dots, Y_{s+1}]$, однородный относительно $Y_0, \dots, Y_{s+1}$, такой, что для всякого $a^* \in \mathcal{W}_\alpha$

$$0 \leqslant \deg_{Y_0,\dots,Y_{s+1}} \Phi_{\alpha,s,r} = \deg_{Y_{s+1}} \Phi_{\alpha,s,r}(a^*, Y_0, \dots, Y_{s+1}) \leqslant D'_{n-s}/p^r,$$

старший коэффициент $\mathrm{lc}_{Y_{s+1}} \Phi_{\alpha,s,r}$ лежит в $k[a_1, \dots, a_\nu]$ и

$$\prod_{0 \leqslant r \leqslant \rho_s} \Phi_{\alpha,s,r}^{1/p^r}(a^*, Y_0^{p^r}, \dots, Y_{s+1}^{p^r})$$

является ненулевым многочленом из $\overline{k}[Y_0, \dots, Y_{s+1}]$ минимальной степени, обращающимся в нуль тождественно на проективном алгебраическом многообразии $V_{a^*,s}$. Имеем

$$\deg V_{a^*,s} = \sum_{0 \leqslant r \leqslant \rho_s} \deg_{Y_{s+1}} \Phi_{\alpha,s,r}.$$

Наконец, обозначим через $\Delta_{\alpha,s,r}$ дискриминант многочлена $\Phi_{\alpha,s,r}$ относительно Y_{s+1} (по определению $\Delta_{\alpha,s,r} = 1$, если $\deg_{Y_{s+1}} \Phi_{\alpha,s,r} = 0$). Тогда для всякого $a^* \in \mathcal{W}_\alpha$ имеем $\Delta_{\alpha,s,r}(a^*, Y_0, \dots, Y_s) \neq 0$.

Обозначим через $V_{a^*,s,r}$, $0 \leqslant r \leqslant \rho_s$, объединение всех неприводимых над $\overline{k}$ компонент E алгебраического многообразия $V_{a^*,s}$, таких, что $\Phi_{\alpha,s,r}(a^*, Y_0^{p^r}, \dots, Y_{s+1}^{p^r})$ обращается в нуль тождественно на E. Так что мы имеем $V_{a^*,s} = \bigcup\limits_{0 \leqslant r \leqslant \rho_s} V_{a^*,s,r}$, и если $r_1 \neq r_2$, то многообразия V_{a^*,s,r_1} и V_{a^*,s,r_2} не имеют общих неприводимых компонент.

Алгебраическое многообразие $V_{a^*,s,r}$ определено над полем $k_{a^*}^{1/p^r}$.

(vi) Пусть Z – новая переменная. Существует конечное (или пустое) семейство многочленов $H_j \in k[a_1, \dots, a_\nu, Z]$, $j \in J_{\alpha,s,r}$, удовлетворяющих следующим свойствам. Их степени удовлетворяют неравенствам

$$1 \leqslant \deg_Z H_j \leqslant D'_{n-s}/p^r.$$

Обозначим через Δ_j дискриминант многочлена H_j относительно Z. Тогда $\Delta_j(a^*) \neq 0$ для всякого $a^* \in \mathcal{W}_\alpha$. Обозначим через Ξ_{j,a^*} семейство всех корней из $\overline{k}$ сепарабельного многочлена $H_j(a^*, Z)$. Мы предполагаем, что множества индексов $J_{\alpha,s,r}$ являются попарно непересекающимися.

(vii) Существует семейство многочленов

$$\Phi_j \in k[a_1, \dots, a_\nu, Z, Y_0, \dots, Y_{s+1}],\ j \in J_{\alpha,s,r},$$

и многочлены $\lambda_{\alpha,s,r,0}, \lambda_{\alpha,s,r,1} \in k[a_1, \dots, a_\nu]$, удовлетворяющие следующим свойствам. Для всякого $a^* \in \mathcal{W}_\alpha$ многочлен Φ_j является однородным относительно $Y_0, \dots, Y_{s+1}$,

$$\deg_Z \Phi_j < \deg_Z H_j,$$

$\mathrm{lc}_{Y_{s+1}} \Phi_j \in k[a_1, \dots, a_\nu]$, все многочлены $\Phi_j(a^*, \xi, Y_0, \dots, Y_{s+1})$, $\xi \in \Xi_{j,a^*}$, $j \in J_{\alpha,s,r}$, являются неприводимыми над $\overline{k}$ в кольце

$$\overline{k}[X_0, \dots, X_n]$$

(в частности, они имеют степень $\geqslant 1$),

$$\lambda_{\alpha,s,r,0}(a^*) \neq 0, \quad \lambda_{\alpha,s,r,1}(a^*) \neq 0$$

и

$$\Phi_{\alpha,s,r}(a^*, Y_0, \dots, Y_{s+1}) = \frac{\lambda_{\alpha,s,r,0}(a^*)}{\lambda_{\alpha,s,r,1}(a^*)} \prod_{\substack{j \in J_{\alpha,s,r}, \\ \xi \in \Xi_{j,a^*}}} \Phi_j(a^*, \xi, Y_0, \dots, Y_{s+1}).$$

Следовательно,

$$1 \leqslant \deg_{Y_0,\dots,Y_{s+1}} \Phi_j \leqslant \deg_{Y_0,\dots,Y_{s+1}} \Phi_{\alpha,s,r} \leqslant D'_{n-s}/p^r.$$

(viii) Для всякого $a^* \in \mathcal{W}_\alpha$, для всякого r, $0 \leqslant r \leqslant \rho_s$, неприводимые над $\overline{k}$ компоненты проективного алгебраического многообразия $V_{a^*,s,r}$ находятся во взаимно однозначном соответствии с парами (ξ, j), где $\xi \in \Xi_{j,a^*}$, $j \in J_{\alpha,s,r}$. Обозначим через $W_{j,a^*,\xi}$ неприводимую над $\overline{k}$ компоненту алгебраического многообразия $V_{a^*,s,r}$, соответствующую паре (ξ, j). Мы имеем $\deg W_{j,a^*,\xi} = \deg_{Y_{s+1}} \Phi_j$.

(ix) Пусть Y и Z – переменные, $t_1, \dots, t_s$ – семейство алгебраически независимых элементов над $\overline{k}$, индекс j лежит в $J_{\alpha,s,r}$ и элемент θ является алгебраическим над $\overline{k}(t_1, \dots, t_s)$, таким, что $\Phi_j(a^*, \xi, 1, t_1^{p^r}, \dots, t_s^{p^r}, \theta^{p^r}) = 0$. Тогда существуют многочлены $G_j \in k[a_1, \dots, a_\nu, t_1, \dots, t_s]$, $G_{j,i} \in k[a_1, \dots, a_\nu, Z, t_1, \dots, t_s, Y]$, $0 \leqslant i \leqslant n$, удовлетворяющие следующим свойствам. Многочлен $G_j(a^*, t_1, \dots, t_s)$ ненулевой для всякого $a^* \in \mathcal{W}_\alpha$, выполнены неравенства $\deg_Z G_{j,i} < \deg_Z H_j$, $\deg_Y G_{j,i} < \deg_{Y_{s+1}} \Phi_j$, и все степени

$$\deg_{t_1,\dots,t_s} G_j, \quad \deg_{t_1,\dots,t_s} G_{j,i}$$

ограничены сверху величиной $(D'_{n-s}/p^r)^{O(1)}$. Далее, существует $\overline{k}$-изоморфизм полей $\overline{k}(W_{j,a^*,\xi}) \to \overline{k}(t_1, \dots, t_s)[\theta]$, такой, что $Y_i/Y_0 \mapsto t_i$, $1 \leqslant i \leqslant s$, $Y_{s+1}/Y_0 \mapsto \theta$,

$$(X_i/Y_0)^{p^r} \mapsto G_{j,i}(a^*, \xi, t_1^{p^r}, \dots, t_s^{p^r}, \theta^{p^r})/G_j(a^*, t_1^{p^r}, \dots, t_s^{p^r}), \quad 0 \leqslant i \leqslant n.$$

Следовательно, этот изоморфизм задаёт общую точку алгебраического многообразия $W_{j,a^*,\xi}$. Проективное алгебраическое многообразие $W_{j,a^*,\xi}$ определено над полем $k_{a^*}^{1/p^r}[\xi]$ (хорошо известно, что в этом случае $\xi^{1/p^r} \in k_{a^*}^{1/p^r}[\xi]$).

(x) Более того, существуют многочлены

$$]G_{\alpha,s,r} \in k[a_1, \dots, a_\nu, t_1, \dots, t_s], \quad G_{\alpha,s,r,i} \in k[a_1, \dots, a_\nu, t_1, \dots, t_s, Y],$$

$0 \leqslant i \leqslant n$, удовлетворяющие следующим свойствам. Положим

$$d_j = \deg_Z H_j, \quad d'_j = \deg_{Y_0,\dots,Y_{s+1}} \Phi_j, \quad d_{\alpha,s,r,i} = \deg_Y G_{\alpha,s,r,i}.$$

Для любого i, $0 \leqslant i \leqslant n$, имеем $\deg_Y G_{\alpha,s,r,i} < \deg_{Y_0,\dots,Y_{s+1}} \Phi_{\alpha,s,r}$,

$$\deg_{t_1,\dots,t_s} G_{\alpha,s,r,i} < 2(D'_{n-s})^2, \quad \deg_{t_1,\dots,t_s} G_{\alpha,s,r} < 2(D'_{n-s})^2.$$

Положим $\Phi'_j = \Phi_j(a_1, \dots, a_\nu, Z, 1, t_1, \dots, t_s, Y)$. Для $j \in J_{s,r}$ имеем

$$(\mathrm{lc}_{Y_{s+1}} \Phi_j)^{\max\{d_{\alpha,s,r,i} - d'_j + 1, 0\}} G_{\alpha,s,r,i} = A'_j \Phi'_j + G'_{j,i},$$

где $A'_j, G'_{j,i} \in k[a_1, \dots, a_\nu, Z, t_1, \dots, t_s, Y]$ и $\deg_Y G'_{j,i} = d'_{j,i} < d'_j$. Далее, $(\mathrm{lc}_Z H_j)^{\max\{d'_{j,i} - d_j + 1, 0\}} G'_{j,i} = A_j H_j + G_{j,i}$, где $A_j \in k[a_1, \dots, a_\nu, Z, t_1, \dots, t_s, Y]$. Наконец,

$$G_j = (\mathrm{lc}_{Y_{s+1}} \Phi_j)^{\max\{d_{\alpha,s,r,i} - d'_j + 1, 0\}} \cdot (\mathrm{lc}_Z H_j)^{\max\{d'_{j,i} - d_j + 1, 0\}} \cdot G_{\alpha,s,r}.$$

Поэтому если $s = 0$, то согласно (ix) для всякого $a^* \in \mathcal{W}_\alpha$, для всех $j \in J_{\alpha,0,r_0}$, $\xi \in \Xi_{a^*,j}$, $0 \leqslant r \leqslant \rho_0$

$$W_{j,a^*,\xi} = \mathcal{Z}(G_{j,i}(a^*, \xi) Y_0^{p^r} - G_j(a^*) X_i^{p^r},\ 0 \leqslant i \leqslant n).$$

Если $s = n-1$, то для всякого $a^* \in \mathcal{W}_\alpha$, для всех $j \in J_{\alpha,n-1,r}$, $\xi \in \Xi_{a^*,j}$, $0 \leqslant r \leqslant \rho_{n-1}$, очевидно, $W_{j,a^*,\xi} = \mathcal{Z}(\Phi_j(a^*, \xi, Y_0^{p^r}, \dots, Y_{s+1}^{p^r}))$ и $V_{a^*,s,r} = \mathcal{Z}(\Phi_{\alpha,s,r}(a^*, Y_0^{p^r}, \dots, Y_{s+1}^{p^r}))$.

Пусть $Y^{(i)}$, $0 \leqslant i \leqslant \varkappa_{2,s}$, – все попарно различные линейные формы из $\mathcal{L}'_s$. Заметим, что для всякой формы $Y^{(i)} \in \mathcal{L}'_s$ линейные формы

$$Y_0, \dots, Y_s, Y^{(i)}$$

являются линейно независимыми над k. Пусть t – алгебраически независимый над k элемент. Можно расширить основное поле k до $k(t)$. В следующих пунктах (xi) и (xii) мы предполагаем, что $0 \leqslant s \leqslant n-2$.

(xi) Существуют многочлены

$$\Psi_{\alpha,s,r,i_1,i_2} \in k[a_1, \dots, a_\nu, t, Y_0, \dots, Y_s, Z],$$

$0 \leqslant i_1 \leqslant \varkappa_{2,s}$, $s+2 \leqslant i_2 \leqslant n$, однородные относительно $Y_0, \dots, Y_s, Z$ и удовлетворяющие следующим свойствам. Для всякого $a^* \in \mathcal{W}_\alpha$, для всяких i_1 и i_2, где $0 \leqslant i_1 \leqslant \varkappa_{2,s}$, $s+2 \leqslant i_2 \leqslant n$, многочлен $\Psi_{\alpha,s,r,i_1,i_2}(a^*, t, Y_0, \dots, Y_s, Z)$ является ненулевым и $\Psi_{\alpha,s,r,i_1,i_2}(a^*, t^{p^r}, Y_0^{p^r}, \dots, Y_s^{p^r}, (Y^{(i_1)} + tX_{i_2})^{p^r})$ тождественно обращается в нуль на алгебраическом многообразии $V_{a^*,s,r}(\overline{k(t)})$. Далее, для всех s, r многообразие $V_{a^*,s,r}$ совпадает с множеством

$$\mathcal{Z}\left(\Psi_{\alpha,s,r,i_1,i_2}\left(a^*, t^{p^r}, Y_0^{p^r}, \dots, Y_s^{p^r}, (Y^{(i_1)} + tX_{i_2})^{p^r}\right), \forall\, i_1, i_2\right) \cap \mathbb{P}^n(\overline{k}). \tag{6}$$

Старший коэффициент $\mathrm{lc}_Z \Psi_{\alpha,s,r,i_1,i_2}$ лежит в $k[a_1,\dots,a_\nu]$, и для всех $a^* \in \mathcal{W}_\alpha$ мы имеем $(\mathrm{lc}_Z \Psi_{\alpha,s,r,i_1,i_2})(a^*) \neq 0$. Степени удовлетворяют неравенствам

$$\deg_t \Psi_{\alpha,s,r,i_1,i_2} \leqslant \deg_Z \Psi_{\alpha,s,r,i_1,i_2} \leqslant \deg_{Y_{s+1}} \Phi_{\alpha,s,r} \leqslant D'_{n-s}/p^r.$$

Запишем $\Psi_{\alpha,s,r,i_1,i_2} = \sum\limits_{0 \leqslant i_3 \leqslant \deg_t \Psi_{\alpha,s,r,i_1,i_2}} \Psi_{\alpha,s,r,i_1,i_2,i_3} t^{i_3}$, где $\Psi_{\alpha,s,r,i_1,i_2,i_3} \in k[a_1,\dots,a_\nu,Y_0,\dots,Y_s,Y^{(i_1)},X_{i_2}]$ (отметим здесь, что сейчас линейные формы $Y_0,\dots,Y_s,Y^{(i_1)},X_{i_2}$ являются линейно независимыми над k). Тогда (поскольку множество (6) совпадает с $V_{a^*,s,r}$) мы имеем

$$\mathcal{Z}\left(\Psi_{\alpha,s,r,i_1,i_2,i_3}\left(a^*, Y_0^{p^r},\dots,Y_s^{p^r},(Y^{(i_1)})^{p^r},X_{i_2}^{p^r}\right), \forall\, i_1,i_2,i_3\right) = V_{a^*,s,r}.$$

Таким образом, мы получаем систему полиномиальных уравнений с множеством нулей $V_{a^*,s,r}$. Эта система состоит из не более чем $(n-s-1)n(D'_{n-s})^3/(2p^r)$ однородных уравнений степени не больше D'_{n-s}.

(xii) Для всякого $j \in J_{\alpha,s,r}$, $0 \leqslant r \leqslant \rho_s$, существуют многочлены $\Psi_{j,i_1,i_2} \in k[a_1,\dots,a_\nu,Z,t,Y_0,\dots,Y_s,Z_1]$, $0 \leqslant i_1 \leqslant \varkappa_{2,s}$, $s+2 \leqslant i_2 \leqslant n$, однородные относительно $Y_0,\dots,Y_s,Z_1$ и удовлетворяющие следующим свойствам. Степени подчиняются неравенствам $\deg_Z \Psi_{j,i_1,i_2} < \deg_Z H_j$. Для всякого $a^* \in \mathcal{W}_\alpha$, для всякого $\xi \in \Xi_{a^*,j}$, для всех i_1 и i_2, где $0 \leqslant i_1 \leqslant \varkappa_{2,s}$, $s+2 \leqslant i_2 \leqslant n$, многочлен $\Psi_{j,i_1,i_2}(a^*,\xi,t,Y_0,\dots,Y_s,Z)$ ненулевой и

$$\Psi_{j,i_1,i_2}(a^*,\xi,t^{p^r},Y_0^{p^r},\dots,Y_s^{p^r},(Y^{(i_1)}+tX_{i_2})^{p^r})$$

тождественно обращается в нуль на алгебраическом многообразии $W_{j,a^*,\xi}(\overline{k(t)})$. Далее, многообразие $W_{j,a^*,\xi}$ совпадает с множеством

$$\mathcal{Z}\left(\Psi_{j,i_1,i_2}\left(a^*,\xi,t^{p^r},Y_0^{p^r},\dots,Y_s^{p^r},(Y^{(i_1)}+tX_{i_2})^{p^r}\right), \forall\, i_1,i_2\right) \cap \mathbb{P}^n(\overline{k}). \tag{7}$$

Старший коэффициент $\mathrm{lc}_Z \Psi_{j,i_1,i_2}$ лежит в $k[a_1,\dots,a_\nu]$, и для всякого $a^* \in \mathcal{W}_\alpha$ мы имеем $(\mathrm{lc}_Z \Psi_{j,i_1,i_2})(a^*) \neq 0$. Степени подчиняются неравенствам $\deg_t \Psi_{j,i_1,i_2} \leqslant \deg_Z \Psi_{j,i_1,i_2} \leqslant \deg_{Y_{s+1}} \Phi_j \leqslant D'_{n-s}/p^r$.

Запишем $\Psi_{j,i_1,i_2} = \sum_{0 \leqslant i_3 \leqslant \deg_t \Psi_{j,i_1,i_2}} \Psi_{j,i_1,i_2,i_3} t^{i_3}$, где

$$\Psi_{j,i_1,i_2,i_3} \in k[a_1,\dots,a_\nu,Z,Y_0,\dots,Y_s,Y^{(i_1)},X_{i_2}].$$

Тогда (поскольку множество (7) совпадает с $W_{j,a^*,\xi}$) мы имеем

$$\mathcal{Z}\left(\Psi_{j,i_1,i_2,i_3}\left(a^*,\xi,Y_0^{p^r},\dots,Y_s^{p^r},(Y^{(i_1)})^{p^r},X_{i_2}^{p^r}\right),\forall\, i_1,i_2,i_3\right)=W_{j,a^*,\xi}.$$

Таким образом, мы получаем систему полиномиальных уравнений с множеством нулей $W_{j,a^*,\xi}$. Эта система состоит из не более чем $(n-s-1)n(D'_{n-s})^3/(2p^r)$ однородных уравнений степени не больше D'_{n-s}.

Пусть $a^*\in\mathcal{W}_\alpha$. По определению положим

$$c_\alpha=\max\{\dim V_{a^*}^{(c',c)},c'-1\}.$$

Следовательно, c_α зависит только от α и не зависит от выбора a^*.

(xiii) Существуют целое число c'_α и однородные многочлены $q_{\alpha,i,i_1}\in k[X_0,\dots,X_n]$, $1\leqslant i\leqslant n-c'_\alpha$, $0\leqslant i_1\leqslant m-1$, удовлетворяющие следующим свойствам. Справедливо неравенство $c'-1\leqslant c'_\alpha\leqslant c_\alpha$. Положим

$$h_{\alpha,i}=\sum_{0\leqslant i_1\leqslant m-1}q_{\alpha,i,i_1}f_{i_1},\quad 1\leqslant i\leqslant n-c'_\alpha.$$

Положим $d^{(i)}=\deg_{X_0,\dots,X_n}h_{\alpha,i}$ для всех i. Тогда $d^{(i)}\leqslant d_{i-1}$ и для всех i_1 имеем $\deg_{X_0,\dots,X_n}q_{\alpha,i,i_1}=d^{(i)}-d_{i_1}$ при условии, что $q_{\alpha,i,i_1}\neq 0$.

Для всякого $a^*\in\mathcal{W}_\alpha$ положим

$$h_{a^*,i}=\sum_{0\leqslant i_1\leqslant m-1}q_{\alpha,i,i_1}f_{i_1}(a^*,X_0,\dots,\quad X_n).$$

Тогда

$$\mathcal{Z}(h_{a^*,1},\dots,h_{a^*,n-c'_\alpha})=V_{a^*}^{(c',c)}\cup E_{a^*,c'},$$

где $E_{a^*,c'}$ является проективным алгебраическим многообразием размерности $\dim E_{a^*,c'}\leqslant c'-1$. Далее, для всякого целого числа c'', такого, что $c'_\alpha<c''\leqslant c$,

$$\mathcal{Z}(h_{a^*,1},\dots,h_{a^*,n-c''})=V_{a^*}^{(c'',c)}\cup E_{a^*,c''},$$

где $E_{a^*,c''}$ – проективное алгебраическое многообразие, такое, что $\dim E_{a^*,c''}=c''$ и каждая неприводимая над $\overline{k}$ компонента многообразия $E_{a^*,c''}$ не является неприводимой компонентой многообразия V_{a^*}.

Заметим, что если $E_{a^*,c'} = \varnothing$, то $V_{a^*}^{(c',c)} = V_{a^*}$. Далее, можно легко вывести из (xiii), что $h_{a^*,i} \neq 0$ для всякого i, $1 \leqslant i \leqslant c'_\alpha$, для всякого $a^* \in \mathcal{W}_\alpha$.

Для всякого целого числа s, $0 \leqslant s \leqslant n-1$, положим

$$D_{n-s} = \binom{d_0 + \ldots + d_{n-s-1} + 1}{n-s}$$

(это биномиальный коэффициент). Если $s = n$, то положим $D_{n-s} = 1$. Также определим $D_{n+1} = D_n$.

(Битовая) длина записи целого числа $z \in \mathbb{Z}$ определяется формулой $\mathrm{l}(z) = 1 + [\log_2(|z|+1)]$ (здесь $[\ldots]$ обозначает целую часть действительного числа). Если $f_i \in \mathbb{Z}[a_1, \ldots, a_\nu, X_0, \ldots, X_n]$, то по определению длина записи целых коэффициентов многочлена f_i равна

$$\mathrm{l}(f_i) = \max_{i_1,\ldots,i_\nu,\, j_0,\ldots,j_n} \mathrm{l}(f_{i,i_1,\ldots,i_\nu,\, j_0,\ldots,j_n}),$$

см. (2). Аналогичным образом определяются длины записи целых коэффициентов других многочленов с целыми коэффициентами.

Ниже в формулировках теорем 1 и 2 мы предполагаем, что поле k имеет достаточно много элементов. Более точно, достаточно, чтобы $\#k \geqslant D_{n-c'}^C$ для некоторой абсолютной константы $C > 0$ (она может быть легко вычислена явно, если это необходимо).

Теперь мы можем сформулировать наш основной результат.

Теорема 1. *Пусть многочлены*

$$f_0, \ldots, f_{m-1} \in k[a_1, \ldots, a_\nu, X_1, \ldots, X_n],$$

целые числа c, c' и открытое в топологии Зарисского множество $\mathcal{U}_c$ – такие же, как и выше. Тогда существует стратификация (4), *удовлетворяющая свойствам* (i)–(xiii) *и такая, что*

(a) *число элементов $\#A$ и все целые числа μ_α, $m_{\alpha,\beta}$ ограничены сверху величиной $(d')^\nu D_{n-c'}^{O(\nu)}$ с абсолютной константой в $O(\nu)$,*

(b) *степени относительно $a_1, \ldots, a_\nu$ всех многочленов*

$$\psi_{\alpha,1}^{(\beta)}, \ldots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)}$$

ограничены сверху величиной $d' D_{n-c'}^{O(1)}$ с абсолютной константой в $O(1)$.

(c) *для всякого* s, *такого, что* $c' \leqslant s \leqslant \min\{c, n-1\}$, *степени относительно* $a_1, \dots, a_\nu$ *всех многочленов* $\Phi_{\alpha,s,r}$, H_j, Φ_j, $\lambda_{\alpha,s,r,0}, \lambda_{\alpha,s,r,1}$, G_j, $G_{j,i}$, $G_{\alpha,s,r}$, $G_{\alpha,s,r,i}$, $\Psi_{\alpha,s,r,i_1,i_2}$, Ψ_{j,i_1,i_2}, $j \in J_{\alpha,s,r}$, $0 \leqslant r \leqslant \rho_s$, *ограничены сверху величиной* $d' D_{n-s}^{O(1)}$ *с абсолютной константой в* $O(1)$.

Рассмотрим также следующее свойство.

(f) *Поле* k *есть* $\mathbb{Q}$, *и в* (2) *для всякого* i, $0 \leqslant i \leqslant m-1$, *имеем* $f_i \in \mathbb{Z}[a_1, \dots, a_\nu, X_0, \dots, X_n]$ *и* $\mathrm{l}(f_i) \leqslant M$ *для некоторого действительного числа* $M \geqslant 1$.

Далее, для всякого $\varkappa \geqslant 0$ *мы выбираем множество* $\mathcal{I}_\varkappa = \{1, 2, \dots, \varkappa+1\}$.

Тогда дополнительно

(d) *если выполнено условие* (f), *то коэффициенты из* k *всех многочленов из пп.* (b) *и* (c) *фактически принадлежат* $\mathbb{Z}$. *Длины записи целых коэффициентов всех многочленов из п.* (b) *ограничены сверху величиной*

$$(M + c^2 + \nu \log_2 d') D_{n-c'}^{O(1)} \tag{8}$$

с абсолютной константой в $O(1)$. *Длины записи целых коэффициентов всех многочленов из п. (c) ограничены сверху величиной*

$$(M + c^2 + \nu \log_2 d') D_{n-s}^{O(1)} \tag{9}$$

с абсолютной константой в $O(1)$.

При условии (f) мы дадим также хорошие оценки для всех длин записи $\mathrm{l}(h_{\alpha,i})$.

Заметим, что если $c = -1$, то только сама стратификация (4) и многочлены $h_{\alpha,1}, \dots, h_{\alpha,n+1}$ (из пункта (xiii)) фигурируют в формулировке теоремы 1, других объектов в этом случае нет.

Пусть $c = n$. Тогда $V_{a^*,n} = \mathbb{P}^n(\overline{k})$ для некоторого $a^* \in \mathcal{W}_\alpha$ в том и только в том случае, если $c_\alpha = c'_\alpha = n$ (поскольку $h_{a^*,i} \neq 0$ для всякого i, $1 \leqslant i \leqslant n - c'_\alpha$, см. (xiii)), т.е. в том и только в том случае, если нет полиномов $h_{\alpha,i}$, соответствующих α.

Пусть $c' \leqslant s \leqslant \min\{c, n-1\}$. Тогда $V_{a^*,s} = \varnothing$ в том и только в том случае, если $\Phi_{\alpha,s,r} \in k[a_1, \dots, a_\nu]$ при $0 \leqslant r \leqslant \rho_s$, т.е. в том и только в том случае, если $J_{s,r} = \varnothing$ при $0 \leqslant r \leqslant \rho_s$.

Заметим ещё, что можно представить множество A в виде объединения непересекающихся множеств $A = \bigcup\limits_{c'-1\leqslant i\leqslant c} A_i$ так, что для всякого $\alpha \in A_i$, для всякого $a^* \in \mathcal{W}_\alpha$ выполнено равенство $\dim V_{a^*} = i$, если $c' \leqslant i \leqslant c$, и $\dim V_{a^*} \leqslant i$, если $i = c' - 1$.

Для рассматриваемой проблемы ранее известные оценки на степени были дважды экспоненциальными, ср. [1, 9].

Отметим также ещё раз, что алгоритм из [2, гл. 2] можно рассматривать как аналог конструкции из настоящей статьи для $\nu = 0$ (и в этом случае можно опустить a^* в обозначениях).

Замечание 2. Нам необходимо также сформулировать модифицированную версию теоремы 1 для случая покрытия вместо стратификации, т.е. для случая, когда условие (i) не обязательно выполняется.

Именно, если в утверждении теоремы 1 заменить "(i)–(xiii)" на "(ii)–(xiii)", то в п. (a) можно утверждать дополнительно, что $\mu_\alpha = 2$ для всякого $\alpha \in A$.

Аналогичное замечание справедливо для теоремы 1 из [6], см. введение в [6]. Это будет важно в настоящей статье.

В следующей теореме 2 мы сделаем теорему 1 эффективной, в том смысле, что мы предложим алгоритм для построения стратификации (4) (а также соответствующего покрытия, см. замечание 2) и всех относящихся к ней объектов за время, субэкспоненциальное от длины записи входных данных. Но сначала требуется задать явно поле k.

Мы предполагаем, что поле k является конечно порождённым над подполем k_0, где $k_0 = \mathbb{Q}$, если $p = 1$, и k_0 есть конечное поле $\mathbb{F}_{p^\epsilon}$ порядка p^ϵ, если $p > 1$. В последнем случае ϵ – положительное целое число и поле $\mathbb{F}_{p^\epsilon}$ задано своим базисом с таблицей умножения над полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Положим $k_1 = \mathbb{Z}$, если $p = 1$, и $k_1 = k_0$, если $p > 1$. Если $\mathrm{char}(k_0) = p > 1$ и $z \in k_0$, то по определению длина записи этого элемента есть $\mathrm{l}(z) = \epsilon(1 + [\log_2(p-1)])$.

Мы предполагаем, что $k = k_0(\tau_1, \ldots, \tau_l)[\tau_{l+1}]$, где $l \geqslant 0$ – целое число, а $\tau_1, \ldots, \tau_l$ – алгебраически независимые элементы над полем k_0. Далее, существует ненулевой многочлен $\varphi \in k_1[\tau_1, \ldots, \tau_l, Z]$, такой, что $\deg_Z \varphi \geqslant 1$, $\mathrm{lc}_Z \varphi = 1$, многочлен φ неприводим в кольце $k_0(\tau_1, \ldots, \tau_l)[Z]$ и $\varphi(\tau_1, \ldots, \tau_{l+1}) = 0$. Мы предполагаем, что $\deg_{\tau_1,\ldots,\tau_l,Z} \varphi < d''$ для некоторого целого числа $d'' \geqslant 2$. Если $\mathrm{char}(k) = 0$, то дополнительно предполагается, что $\mathrm{l}(\varphi) \leqslant M_1$, где $M_1 \geqslant 1$. Если $\mathrm{char}(k) > 0$, то положим $M_1 = \epsilon(1 + [\log_2(p-1)])$.

Если $\mathrm{char}(k) = 0$, то для всякого многочлена g с целыми коэффициентами длина записи целых коэффициентов (или коэффициентов из k_1, или просто длина записи коэффициентов, если это не приведёт к двусмысленности) многочлена g определяется как максимум длин записи целых коэффициентов многочлена g.

Если $\mathrm{char}(k) > 0$, то для всякого многочлена g с коэффициентами из k_0 длина записи коэффициентов из k_1 (или просто длина записи коэффициентов, если это не приведёт к двусмысленности) многочлена g определяется формулой $\mathrm{l}(g) = \epsilon(1 + [\log_2(p-1)])$.

Пусть $z \in k_0(\tau_1, \dots, \tau_l)[\tau_{l+1}]$ – произвольный элемент. Мы представляем его в виде $z = (1/z^{(0)}) \sum\limits_{0 \leqslant i < \deg_Z \varphi} z_i \tau_{l+1}^i$, где

$$z^{(0)}, z_i \in k_1[\tau_1, \dots, \tau_l], \quad z^{(0)} \neq 0$$

и наибольший общий делитель всех элементов

$$z^{(0)}, z_0, \dots, z_{\deg_Z \varphi - 1}$$

равен 1 в кольце $k_1[\tau_1, \dots, \tau_l]$. В случае $\mathrm{char}(k) = p > 1$ элемент $z^{(0)}$ однозначно определён с точностью до ненулевого множителя из k_0. Если $\mathrm{char}(k) = 0$, то $z^{(0)}$ однозначно определён с точностью до ненулевого множителя ± 1. В любом случае, если мы фиксируем $z^{(0)}$, то все z_i однозначно определены. Чтобы зафиксировать $z^{(0)}$, мы будем предполагать, что итерированный старший коэффициент $\mathrm{lc}_{\tau_1} \mathrm{lc}_{\tau_2} \dots \mathrm{lc}_{\tau_l}(z^{(0)})$ равен 1, если $\mathrm{char}(k) = p > 0$, и положителен, если $\mathrm{char}(k) = 0$.

Мы определяем степень

$$\deg_{\tau_1, \dots, \tau_l} z = \max_{0 \leqslant i < \deg_Z \varphi} \{\deg_{\tau_1, \dots, \tau_l} z^{(0)}, \deg_{\tau_1, \dots, \tau_l} z_i\}$$

и длину записи коэффициентов $\mathrm{l}(z) = \max_{0 \leqslant i < \deg_Z \varphi} \{\mathrm{l}(z^{(0)}), \mathrm{l}(z_i)\}$.

По определению степень $\deg_{\tau_1, \dots, \tau_l}(f_i)$ многочлена f_i равна максимуму степеней $\deg_{\tau_1, \dots, \tau_l}(f_{i, i_1 \dots, i_\nu, j_0, \dots, j_n})$ по всем индексам $i_1 \dots, i_\nu$, $j_0, \dots, j_n$. Аналогичным образом определены степени относительно $\tau_1, \dots, \tau_l$ других многочленов с коэффициентами из k.

Вернёмся к случаю произвольной характеристики. В этой статье мы будем предполагать, что $f_{i, i_1 \dots, i_\nu, j_0, \dots, j_n} \in k_1[\tau_1, \dots, \tau_{l+1}]$ для всех $i, i_1, \dots, i_\nu, j_0, \dots, j_n$.

Мы предполагаем, что для всякого i, $0 \leqslant i \leqslant m-1$,

$$\deg_{\tau_1, \dots, \tau_l} f_i < d'''$$

для некоторого целого числа $d''' \geqslant 2$ и $\mathrm{l}(f_i) \leqslant M_2$, где $M_2 \geqslant 1$. Так что можно взять $M_2 = \epsilon(1 + [\log_2(p-1)])$, если $\mathrm{char}(k) > 0$.

В [2,3] в случае ненулевой характеристики роль поля k_0 играет поле H. Тогда, чтобы применять алгоритмы из [2,3] для решения систем полиномиальных уравнений, поле H должно иметь достаточно много элементов (например, мы считаем, что $Z_1, \ldots, Z_{n-m+2} \in H[X_0, \ldots, X_n]$, см. утверждение основной теоремы гл. II в [2] и теоремы 1 в [3]). Так что в этих статьях мы при необходимости расширяем поле H, см. замечание 1 в [3]. Фактически, оценки на длины записи коэффициентов из H (или $\widetilde{H}$ в обозначениях работы [3]) дают верхние границы на число элементов расширенного поля H, хотя в [2,3] мы это и не подчёркиваем (поскольку для числа элементов поля H в ненулевой характеристике можно получить даже лучшие оценки).

В последних двух статьях мы получили системы полиномиальных уравнений, задающие неприводимые компоненты многообразия решений и общие точки этих неприводимых компонент. В [2] мы также обсуждаем, как вернуться от этих систем и общих точек с расширенным полем H к аналогичным системам и общим точкам с исходным полем H, если $l > 0$. Заметим, что в случае $l = 0$ такой редукции для систем полиномиальных уравнений, задающих неприводимые компоненты, нет: необходимо расширять поле H (если число его элементов мало), для того чтобы получить такие системы уравнений с требуемыми оценками на их длины записи, см. замечание в конце статьи [2].

Согласно замечанию 1 работы [3], если $l > 0$, то альтернативным образом можно выбрать линейные формы $Z_1, \ldots, Z_{n-m+2}$ с коэффициентами в $H[T_1, \ldots, T_l]$ (в [3] элементы $T_1, \ldots, T_l$ играют роль элементов $\tau_1, \ldots, \tau_l$) и не расширять поле H. Однако в [2,3] мы не приводим явных оценок для степеней относительно $T_1, \ldots, T_l$ всех объектов (особенно это интересно для систем полиномиальных уравнений, задающих неприводимые компоненты) в этом случае. Конечно, время работы алгоритмов из [2,3] для этого альтернативного выбора линейных форм остаётся тем же самым.

В настоящей статье, для того чтобы учесть все случаи, мы используем слегка более общий подход для представления элементов из поля k.

Предположим, что $\mathrm{char}(k) > 0$. Тогда если $l > 0$, то положим

$$\epsilon(\varkappa) = \min\left\{ b \in \mathbb{Z} \,:\, \binom{b+l}{b} \epsilon \log_2 p \geqslant \log_2(\varkappa+1) \;\&\; b \geqslant 0 \right\},\ 0 \leqslant \varkappa \in \mathbb{Z}. \tag{10}$$

В этом случае, согласно (10), мы выбираем и фиксируем $\mathcal{I}_\varkappa$ равным подмножеству множества полиномов из $k_0[\tau_1, \ldots, \tau_l]$ степени $\epsilon(\varkappa)$.

Для всякого s, $0 \leqslant s \leqslant n-1$, положим $\epsilon_s = 0$, если $\epsilon(\varkappa_{1,s}) = 0$, и $\epsilon_s = 1$, если $\epsilon(\varkappa_{1,s}) \geqslant 1$.

Если $l = 0$ или $\mathrm{char}(k) = 0$, то положим $\epsilon_s = 0$ для всех s.

Напомним, что мы предполагаем, что поле k содержит достаточно много элементов, см. выше. Следовательно, если $l = 0$, то поле $k_0[\tau_1]$ содержит достаточно много элементов.

Положим

$$D = \max_{c'-1 \leqslant s \leqslant c} \{ D_{n-s}^{s+\nu+l+2} \}.$$

Таким образом, D зависит от c, c'. Очевидно, $D \leqslant d^{(n+1)(c+\nu+l+2)}$ (эта оценка не зависит от c').

Теорема 2. *При описанных условиях можно построить стратификацию* (4), *удовлетворяющую свойствам* (i)–(xiii) (*соответственно покрытие* (4), *удовлетворяющее свойствам* (ii)–(xiii)), *и все объекты из пунктов* (iv)–(xiii), *относящиеся к ней* (*соответственно к нему*), *см. утверждения* (a)–(c) *теоремы* 1 (*соответственно модифицированной версии теоремы* 1, *см. замечание* 2). *Далее, справедливы следующие утверждения.*

(a) *Все многочлены* $\psi_{\alpha,1}^{(\beta)}, \ldots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)}$ *из утверждения* (b) *теоремы* 1 (*соответственно модифицированной версии теоремы* 1) *принадлежат полю* $k_1[\tau_1, \ldots, \tau_{l+1}, a_1, \ldots, a_\nu]$. *Степени относительно* $\tau_1, \ldots, \tau_l$ *всех этих многочленов ограничены сверху величиной*

$$(d''' + c^2 \epsilon_{c'} + (d'')^2) D_{n-c'}^{O(1)}. \tag{11}$$

Если $\mathrm{char}(k) = 0$, *то длины записи целых коэффициентов всех этих многочленов ограничены сверху величиной*

$$(M_1 + M_2 d'' + c^2 + \nu \log_2 d' + (l+1) \log_2(d'' d''')) D_{n-c'}^{O(1)}. \tag{12}$$

(b) *Для всякого* s, $c' \leqslant s \leqslant \min\{c, n-1\}$, *коэффициенты из* k *всех многочленов из утверждения* (c) *теоремы* 1 (*соответственно модифицированной версии теоремы* 1) *фактически принадлежат полю* $k[\tau_1, \ldots, \tau_{l+1}]$. *Степени относительно* $\tau_1, \ldots, \tau_l$ *всех этих многочленов ограничены сверху величиной*

$$(d''' + c^2\epsilon_s + (d'')^2)D_{n-s}^{O(1)}. \tag{13}$$

Если $\mathrm{char}(k) = 0$, *то длины записи целых коэффициентов всех этих многочленов ограничены сверху величиной*

$$(M_1 + M_2 d'' + c^2 + \nu \log_2 d' + (l+1)\log_2(d''d'''))D_{n-s}^{O(1)}. \tag{14}$$

(c) *Время работы данного алгоритма для построения стратификации* (4) (*соответственно покрытия* (4)) *полиномиально от* D, $(d')^\nu$, $(d'')^{l+1}$, $(d''')^{l+1}$, M_1, M_2 *и* m.

Замечание 3. В случае нулевой характеристики можно изменить конструкцию стратификации (4) (соответственно покрытия (4)) следующим образом. Линейные формы $Y_{s,i}$, $0 \leqslant i \leqslant s+1$, заменяются на некоторые линейные формы $Y_{\alpha,s,i} \in \mathbb{Z}[X_0, \ldots, X_n]$ с длинами записи целых коэффициентов, ограниченными сверху величиной $O(\log_2 D_{n-s})$ для всех i, $0 \leqslant i \leqslant s+1$ (сейчас не обязательно $(Y_{\alpha,s,0}, \ldots, Y_{\alpha,s,s+1}) \in \mathcal{L}_s^{s+1} \times \mathcal{L}'_s$).

В случае ненулевой характеристики и $l > 0$ линейные формы $Y_{s,i}$, $0 \leqslant i \leqslant s+1$, заменяются на некоторые линейные формы $Y_{\alpha,s,i} \in k_0[\tau_1, \ldots, \tau_l][X_0, \ldots, X_n]$ (они являются линейными формами от $X_0, \ldots, X_n$) со степенями относительно $\tau_1, \ldots, \tau_l$ не больше $\epsilon(\varkappa)$, где $\varkappa$ ограничено сверху величиной $O(\log_2 D_{n-s})$ для всех i, $0 \leqslant i \leqslant s+1$.

Тогда в произвольной характеристике основного поля также можно заменить c^2 на c в (8), (9), (11)–(14), и после этой замены все утверждения теоремы 1 и теоремы 2 остаются верными. Но мы не доказываем эти новые версии теоремы 1 и теоремы 2 в настоящей статье (мы оставляем это доказательство заинтересованному читателю; оно не слишком сложно)

Отметим также, что если $n - c > C_1 \log_2 n$ для абсолютной константы $C_1 > 0$, то, очевидно, можно опустить $c^2, c^2\epsilon_{c'}, c^2\epsilon_s$ в (8), (9), (11)–(14).

Замечание 4. Небольшое исправление к статье [6]. В этой статье мы рассматриваем основное поле k с не менее чем $2d^2+1$ элементами. Но

фактически для конструкции, описанной в [6], поле k должно иметь не меньше d^{C_2} элементов для абсолютной константы $C_2 > 0$. С другой стороны, в [6] можно снять все ограничения на число элементов $\#k$, заменяя там поле k на $k(t)$, где t – трансцендентный элемент над k (это требует совсем незначительной модификации конструкции из [6]).

§1. Решение систем линейных уравнений с параметрическими коэффициентами

Известно, что можно реализовать алгоритм исключения по Гауссу для решения систем линейных уравнений так, что на каждом шаге все коэффициенты преобразуемой матрицы являются частными некоторых миноров исходной расширенной матрицы рассматриваемой линейной системы. Это даёт алгоритм, соответствующий лесу вычислений для решения линейных систем с хорошими оценками на степени относительно параметров.

Всё же мы опишем здесь модификацию этого алгоритма в удобной для наших целей форме. Пусть дана линейная система

$$\sum_{1\leqslant j\leqslant m} a_{i,j}X_j = a_{i,m+1}, \quad 1\leqslant i\leqslant n, \tag{15}$$

где $a_{i,j}\in\overline{k}$. Обозначим через A расширенную матрицу

$$(a_{i,j})_{1\leqslant i\leqslant n,\,1\leqslant j\leqslant m+1}$$

этой линейной системы.

Мы используем рекурсию по r, где $0\leqslant r\leqslant \min\{n,m\}-1$.

(**) Предположим, что построены индексы $1\leqslant i_1<\ldots<i_r\leqslant n$, $1\leqslant j_1<\ldots<j_r\leqslant m+1$ и минор $\det((a_{i_\alpha,j_\beta})_{1\leqslant\alpha,\beta\leqslant r})\neq 0$.

Наша цель состоит в том, чтобы построить i_{r+1}, j_{r+1}, такие, что свойство (**) выполняется для $r+1$ вместо r, или установить, что такой пары i_{r+1}, j_{r+1} не существует. Для удобства обозначений мы можем, не умаляя общности, предполагать (только в описании рекурсивного шага), что $i_\alpha=\alpha$, $j_\beta=\beta$ при $1\leqslant\alpha,\beta\leqslant r$.

Обозначим через $\tilde{A}_r$ присоединённую матрицу к матрице $A_r = (a_{\alpha,\beta})_{1\leqslant\alpha,\beta\leqslant r}$. Положим $\delta_r=\det(A_r)\neq 0$. Пусть E_w – единичная матрица порядка w, где $w\geqslant 1$. Положим

$$G'_r = \begin{pmatrix} \tilde{A}_r, & 0 \\ 0, & \delta_r E_{n-r} \end{pmatrix}, \quad A'_r = G'_r A = \begin{pmatrix} \delta_r E_r, & B_r \\ \delta_r C_r, & \delta_r D_r \end{pmatrix},$$

$$G_r = \begin{pmatrix} \tilde{A}_r, & 0 \\ -C_r\tilde{A}_r, & \delta_r E_{n-r} \end{pmatrix}, \quad A''_r = G_r A = \begin{pmatrix} \delta_r E_r, & B_r \\ 0, & F_r \end{pmatrix}.$$

Здесь B_r, C_r, D_r, F_r – однозначно определённые матрицы с коэффициентами в k. Заметим, что все коэффициенты матрицы F_r являются некоторыми минорами (с точностью до знака) порядка $r+1$ матрицы A.

Теперь если $F_r = 0$, то не существует требуемой пары i_{r+1}, j_{r+1}. В этом случае положим $\rho = r$, $G = G_\rho$, $A'' = A''_\rho$. Мы имеем $\rho = \mathrm{rank}(A)$.

Если

$$F_r = (f_{r,i,j})_{r+1 \leqslant i \leqslant n,\, r+1 \leqslant j \leqslant m+1} \neq 0,$$

то положим $j_{r+1} = \min\{j \,:\, \exists i\, (f_{r,i,j} \neq 0)\}$, $i_{r+1} = \min\{i \,:\, f_{r,i,j_{r+1}} \neq 0\}$ и определим $J_r = \{(i,j) \,:\, ((r+1 \leqslant j < j_{r+1})\&(r+1 \leqslant i \leqslant n)) \vee ((j = j_{r+1})\&(r+1 \leqslant i < i_{r+1}))\}$. Следовательно, $f_{r,i,j} = 0$ для всех $(i,j) \in J_r$.

Таким образом, в итоге можно преобразовать матрицу A к канонической трапециевидной форме A'' (с точностью до перестановок строк и столбцов матрицы A'') с $F_\rho = 0$, применяя невырожденное преобразование строк матрицы A. Это преобразование является умножением матрицы A на матрицу $G = (g_{i,j})_{1 \leqslant i,j \leqslant n}$ слева. Поэтому можно построить фундаментальное семейство решений линейной системы (15) (или установить, что эта система не имеет решений). Отметим также, что индексы $j_1, \ldots, j_\rho$ являются минимально возможными, для которых выполняется свойство (**). Это немедленно следует из описанной рекурсивной конструкции.

Теперь мы изменим обозначения. В дальнейшем мы будем предполагать, что $a = \{a_{i,j}\}_{1 \leqslant i \leqslant n,\, 1 \leqslant j \leqslant m+1}$ является семейством алгебраически независимых параметров над полем k. Пусть аффинное пространство $\overline{k}^{(m+1)n}$ имеет координатные функции из семейства a. Мы будем обозначать через $a^* = \{a^*_{i,j}\}_{1 \leqslant i \leqslant n,\, 1 \leqslant j \leqslant m+1}$ элемент из $\overline{k}^{(m+1)n}$. Обозначим через $\mathfrak{A}$ кольцо многочленов над k относительно всех переменных из семейства a. Для всякого $\psi \in \mathfrak{A}$ пусть $\deg_a \psi$ обозначает степень многочлена ψ относительно всех переменных из семейства a. Теперь все матрицы $A, A_r, G'_r, A'_r, G_r, A''_r, B_r, C_r, D_r, G$, введённые выше, имеют коэффициенты в $\mathfrak{A}$, все элементы δ_r, $g_{i,j}$ являются полиномами из $\mathfrak{A}$. Обозначим через $\delta'_1, \ldots, \delta'_\mu$ все попарно различные элементы семейства $\{f_{r,i,j}\}$, $(i,j) \in J_r$, $1 \leqslant r \leqslant \rho$. Тогда каждый элемент δ'_i является минором матрицы A (с точностью до знака). Мы будем писать

$G(a^*) = G|_{a=a^*} = (g_{i,j}(a^*))_{1\leqslant i,j\leqslant n}$ и использовать другие подобные обозначения.

Мы доказали следующую лемму.

Лемма 1. *Если $k = \overline{k}$, то описанная конструкция определяет функцию*

$$\bigcup_{n,m\geqslant 1} \overline{k}^{(m+1)n} \to \bigcup_{n\geqslant 1} \overline{k}^{n^2},$$

$$a^* \mapsto G(a^*) \quad \textit{тогда и только тогда, когда}$$

$$a^* \in \mathcal{Z}(\delta'_1, \ldots, \delta'_\mu) \setminus \mathcal{Z}(\delta_1 \cdot \ldots \cdot \delta_\rho).$$

Эта функция является алгоритмом, соответствующим лесу вычислений $\{T_{m,n}\}_{m,n\geqslant 1}$. Каждое дерево $T_{m,n}$ является деревом вычислений над k с входными параметрами из семейства a, имеющее уровень не больше $\min\{m+1, n\}$. Для всякого листа $v \in L(T_{m,n})$ выход, ему соответствующий, является матрицей G с коэффициентами из $\mathfrak{A}$, такой, что $\deg_a g_{i,j} \leqslant \min\{m+1, n\} - 1$ для всех i, j. Квазипроективное алгебраическое многообразие $\mathcal{W}_v \subset \overline{k}^{(m+1)n}$, соответствующее листу v, имеет вид

$$\mathcal{W}_v = \mathcal{Z}(\delta'_1, \ldots, \delta'_\mu) \setminus \mathcal{Z}(\delta_1 \cdot \ldots \cdot \delta_\rho),$$

где $\rho = \mathrm{rank} A(a^*)$. Кроме того, индексы $1 \leqslant i_1 < \ldots < i_\rho \leqslant n$, $1 \leqslant j_1 < \ldots < j_\rho \leqslant m+1$ соответствуют листу v и $\mathrm{rank}(A_r(a^*)) = \rho$. Для всякого $a^* \in \mathcal{W}_v$ матрица $G(a^*)A(a^*)$ имеет каноническую трапециевидную форму (см. выше) с точностью до перестановки строк и столбцов.

Теперь мы хотим получить некоторые следствия из [8]. Они близко соотносятся с решением линейных систем. Но сначала введем некоторые обозначения. Пусть K – произвольное поле. Мы будем обозначать через $M_{n,m}(K)$ множество всех матриц с коэффициентами из K с n строками и m столбцами.

Лемма 2. *Пусть k и K – поля и $K \supset k$. Пусть $m, n, r \geqslant 1$ – целые числа, такие, что $r \leqslant \min\{m, n\}$. Предположим, что поле k содержит не меньше $\min\{(m-r)r, (n-r)r\} + 1$ элементов. Тогда существуют матрицы $B_i = (b_{i,\alpha,\beta})_{1\leqslant\alpha\leqslant r,\, 1\leqslant\beta\leqslant n} \in M_{r,n}(k)$, $0 \leqslant i \leqslant (n-r)r$, и $C_j = (c_{j,\alpha,\beta})_{1\leqslant\alpha\leqslant m,\, 1\leqslant\beta\leqslant r} \in M_{m,r}(k)$, $0 \leqslant j \leqslant (m-r)r$, удовлетворяющие следующему свойству.*

Пусть $A = (a_{i,j})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m} \in M_{n,m}(K)$ *– произвольная матрица. Тогда* $\mathrm{rank}(A) \geqslant r$ *в том и только в том случае, если существуют* i *и* j*, где* $0 \leqslant i \leqslant (n-r)r$ *и* $0 \leqslant j \leqslant (m-r)r$*, такие, что* $\det(B_i A C_j) \neq 0$.

Или, что эквивалентно, все миноры порядка r *матрицы* A *равны нулю в том и только в том случае, если* $\det(B_i A C_j) = 0$ *для всех* i, j.

Доказательство. В [8] построено семейство матриц $D_j \in M_{m-r,m}(k)$, $0 \leqslant j \leqslant (m-r)r$, удовлетворяющее следующему свойству.

- Для всякой матрицы $Q \in M_{r,m}(K)$ с $\mathrm{rank}(Q) = r$ существует такое j, $0 \leqslant j \leqslant (m-r)r$, что $\det \begin{pmatrix} Q \\ D_j \end{pmatrix} \neq 0$.

Построим матрицу $D'_j \in M_{r,m}(k)$, такую, что $\delta_j = \det \begin{pmatrix} D'_j \\ D_j \end{pmatrix} \neq 0$. Обозначим через $\tilde{D}_j$ присоединённую матрицу к квадратной матрице $\begin{pmatrix} D'_j \\ D_j \end{pmatrix}$. Представим ее в виде $\tilde{D}_j = (C_j, C'_j)$, где $C_j \in M_{m,r}(k)$, $C'_j \in M_{m,m-r}(k)$. Тогда $\begin{pmatrix} Q \\ D_j \end{pmatrix} \tilde{D}_j = \begin{pmatrix} Q_1, & Q_2 \\ 0, & \delta_j E_{m-r} \end{pmatrix}$ для некоторых матриц Q_1, Q_2. Поэтому $Q_1 = QC_j$ и $\det(QC_j) \neq 0$. Мы будем писать также $C_j = C_j^{(r,m)}$, $0 \leqslant j \leqslant (m-r)r$.

Следовательно, $\mathrm{rank}(A) \geqslant r$ тогда и только тогда, когда существует индекс j, $0 \leqslant j \leqslant r(m-r)$, такой, что $\mathrm{rank}(AC_j) = r$. Обозначим через $(AC_j)^t$ транспонированную матрицу к матрице AC_j. Тогда согласно доказанному (с n вместо m) существует индекс i, $0 \leqslant i \leqslant r(n-r)$, такой, что $\det((AC_j)^t C_i^{(r,n)}) \neq 0$. Следовательно, можно взять $B_i = (C_i^{(r,n)})^t$ для всех i, $0 \leqslant i \leqslant r(n-r)$. Лемма доказана. □

Замечание 5. Можно использовать лемму 2 в разделе 3 работы [6]. Именно, там мы отметили следующее: "*Применяя результат из* [8], *можно заменить все миноры* Δ_i *на некоторые их линейные комбинации и предполагать в дальнейшем без ограничения общности, что* $m_3 = d^{O(1)}$".

Эти Δ_i – из формулы (20) работы [6]. Фактически, чтобы получить $m_3 = d^{O(1)}$, следует применить здесь лемму 2 три раза: сначала к $\Delta_1, \ldots, \Delta_{m_1}$, затем к $\Delta_{m_1+1}, \ldots, \Delta_{m_2}$ и, наконец, к $\Delta_{m_2+1}, \ldots, \Delta_{m_3}$.

После этого можно упростить конструкцию многочленов $\psi^{(1)}$ и $\psi^{(2)}$. Именно, можно положить

$$\psi^{(1)} = \mathrm{G\,C\,D}_{Y_1,X,v_3,\dots,v_n}\Big(\sum_{1\leqslant i\leqslant m_1} Y_1^i\tilde{\Delta}_i, f(X,0)\Big) \in k[v][X], \tag{16}$$

$$\psi^{(2)} = \mathrm{G\,C\,D}_{Y_2,Y_3,X,v_3,\dots,v_n}\Big(\psi^{(1)}, \sum_{\substack{m_1<i_2\leqslant m_2,\\ m_2<i_3\leqslant m_3}} Y_2^{i_2}Y_3^{i_3}\tilde{\Delta}_{i_2}\tilde{\Delta}_{i_3}\Big) \in k[v][X]. \tag{17}$$

Функцию $\varkappa$ в разделе 3 работы [6] не следует вводить вовсе. Конечно, число линейно независимых над $\overline{k}$ миноров Δ_i ограничено сверху величиной $D_n^{O(1)}$. Мы пытались использовать этот факт и определили функцию $\varkappa$. Но это может показаться слегка непонятным (когда строится соответствующий лес вычислений) и требует дополнительных пояснений. Например, здесь можно применить лемму 1 для обоснования конструкции с функцией $\varkappa$. Но всё же лучше применить в [6] лемму 2.

Конечно, для того чтобы получить основной результат работы [6], можно действовать более простым способом. Именно, пусть $Z_1,\dots,Z_{m_3}$ – новые переменные. Тогда в формуле (16) для $\psi^{(1)}$ (с произвольным m_1, мы не используем сейчас лемму 2) достаточно заменить $Y_1, X, v_3,\dots,v_n$ на $Z_1,\dots,Z_{m_1}, X, v_3,\dots,v_n$ и Y_1^i на Z_i. В формуле (17) для $\psi^{(2)}$ (с произвольными m_2, m_3) достаточно заменить $Y_2, Y_3, X, v_3,\dots,v_n$ на $Z_{m_1+1},\dots,Z_{m_3}, X, v_3,\dots,v_n$ и $Y_2^{i_2}Y_3^{i_2}$ на $Z_{i_2}Z_{i_3}$. Но здесь присутствует слишком много переменных Z_i, если мы пожелаем построить стратификацию из теоремы 1 работы [6] за субэкспоненциальное время.

§2. Многозначные деревья и леса вычислений

В [5] вводятся деревья и леса вычислений. Согласно разделу 1 работы [5] (мы используем обозначения оттуда),

(*) для всякой вершины v дерева вычислений T, для всякой точки $a^* = (a_1^*,\dots,a_\nu^*) \in \mathcal{W}_v$ существует не более одного сына w вершины v, такого, что $\mathcal{A}_w(a_1^*,\dots,a_\nu^*) = \mathrm{true}$.

В [5] свойство (*) формулируется в эквиваленой форме, см. формулу (3) в разделе 1 этой работы.

Определение многозначного дерева вычислений – такое же, как в [5], с той лишь разницей, что свойство (*) не обязательно выполняется. Так что для многозначного дерева вычислений определены все объекты, введённые в [5]. В [5] (см. формулу (5) в конце раздела 1)

$$\mathcal{S}(T) = \bigcup_{v \in L(T)} \mathcal{W}_v \tag{18}$$

– стратификация конструктивного множества $\mathcal{S}(T)$, т.е. $\mathcal{W}_{v_1} \cap \mathcal{W}_{v_2} = \varnothing$ для всех попарно различных $v_1, v_2 \in L(T)$. Теперь для многозначного дерева вычислений (18) является покрытием множества $\mathcal{S}(T)$.

Аналогично [5] (мы оставляем подробности читателю) определено поддерево многозначного дерева вычислений. Любое такое поддерево является многозначным деревом вычислений. Многозначное дерево вычислений T является несократимым в том и только в том случае, если для любого его поддерева T', такого, что $T' \neq T$, мы имеем $\mathcal{S}(T') \neq \mathcal{S}(T)$. Если T является деревом вычислений в смысле [5], то T несократимо тогда и только тогда, когда $T = \mathrm{IRD}(T)$, см. раздел 2 в [5].

Для всякого многозначного дерева вычислений T существует несократимое поддерево T' в T с $\mathcal{S}(T') = \mathcal{S}(T)$, но это поддерево в общем случае не является единственным.

Аналогично [5] можно определить полные сигнатуры, сигнатуры и метки, соответствующие многозначным деревьям вычислений и их вершинам (мы оставляем подробности читателю).

Пусть $a'_1, \ldots, a'_\varkappa$ – некоторые алгебраически независимые над k параметры и $c_1, \ldots, c_\nu \in k[a'_1, \ldots, a'_\varkappa]$. В [5] в конце раздела 2 определены дерево вычислений $T(c)$ и неполное дерево $T'(c)$, соответствующие дереву вычислений T и семейству элементов $c = \{c_i\}_{1 \leqslant i \leqslant \nu}$ (фактически там определены $T(b)$ и $T'(b)$, но для удобства мы заменяем здесь обозначения b на c и μ на $\varkappa$). Дерево $T(c)$ имеет семейство входных параметров $a'_1, \ldots, a'_\varkappa$. Предположим теперь, что T является многозначным деревом вычислений. Тогда, заменяя везде в определениях деревьев $T(c)$ и $T'(c)$ в [5] дерево вычислений T на многозначное дерево вычислений T, мы получаем (по определению) многозначное дерево вычислений $T(c)$ и неполное многозначное дерево вычислений $T'(c)$, соответствующие многозначному дереву вычислений T и семейству элементов c. Грубо говоря, для того чтобы получить $T'(c)$, следует

подставить $c_1, \ldots, c_\nu$ вместо $a_1, \ldots, a_\nu$ везде в объекты, относящиеся к T. После этого, чтобы определить $T(c)$, надо приклеить новый корень к $T'(c)$.

Заменим везде в определении леса вычислений деревья на многозначные деревья. Тогда мы получим определение многозначного леса вычислений. Так что многозначный лес вычислений является семейством $\{T_\sigma\}_{\sigma\in\Sigma}$ многозначных деревьев вычислений.

В [5, раздел 3] определена функция $\mathfrak{F} : \mathcal{S}(T) \to \mathcal{K}$, соответствующая каждому лесу T.

Теперь пусть T является многозначным лесом вычислений. Заменим в определении этой функции $\mathfrak{F}$ из [5, раздел 3] лес вычислений на многозначный лес вычислений T (для которого мы используем то же самое обозначение T). Тогда мы получим бинарное отношение $\mathfrak{F} \subset \mathcal{S}(T) \times \mathcal{K}$, соответствующее многозначному лесу вычислений T (вместо функции $\mathfrak{F}$). Здесь $\mathfrak{F}$ можно рассматривать как многозначную функцию. Мы будем писать $\mathfrak{F} = \mathfrak{F}(T)$.

По определению бинарное отношение $\mathfrak{F}(T)$ является алгоритмом, соответствующим многозначному лесу вычислений T. Произвольное бинарное отношение $\mathfrak{Q}$ является алгоритмом, соответствующим многозначному лесу вычислений, в том и только в том случае, если существует многозначный лес вычислений T, такой, что $\mathfrak{Q} = \mathfrak{F}(T)$.

Как мы отметили в [5], на практике алгоритм, соответствующий лесу вычислений T, возникает из некоторого алгоритма в обычном смысле этого слова. Последний имеет множество входных данных $\mathcal{S}(T)$, его выходные данные принадлежат $\mathcal{K}$, и он вычисляет функцию $\mathfrak{F}(T)$.

Аналогичным образом на практике алгоритм, соответствующий многозначному лесу вычислений, скажем $T = \{T_\sigma\}_{\sigma\in\Sigma}$, возникает из многозначного алгоритма. В последнем алгоритме на некоторых шагах выбираются некоторые объекты (например, линейные формы или матрицы из заданных конечных множеств, см. последующие разделы). Рассматриваются все возможные выборы. Но некоторые из них дают выходные данные (с предписанной сигнатурой, см. подробности в [5]), а другие нет. Так что выходные данные этого алгоритма зависят от выбора этих объектов. Здесь получается многозначная функция из области входных данных этого алгоритма в область его выходных данных, или, что то же самое, бинарное отношение $\mathfrak{Q}$ (так что $\mathfrak{Q} = \mathfrak{F}(T)$).

Зафиксируем $\sigma \in \Sigma$. Предположим, что шаг рассматриваемого многозначного алгоритма с выбором объектов соответствует вершине v' дерева T_σ. Тогда все сыновья v вершины v' находятся во взаимно однозначном соответствии со всеми возможными выборами рассматриваемых объектов. Обозначим через $L(v, T_\sigma)$ множество листьев w дерева вычислений T_σ, таких, что w является потомком вершины v. Тогда выбор объектов, соответствующих вершине v, не даёт никакого требуемого выхода в том и только в том случае, если $\mathcal{W}_w = \varnothing$ для всякого листа $w \in L(v, T_\sigma)$. Вот не вполне формальное пояснение этого факта: данный многозначный алгоритм решает некоторую задачу (например, находит все решения системы полиномиальных уравнений), и каждый его выход из $\mathcal{K}$ даёт решение этой задачи. Других выходов нет.

Часто алгоритм $\mathfrak{Q}$, соответствующий многозначному лесу вычислений, определяет алгоритм в обычном (или классическом) смысле. Именно, предположим, что $\mathfrak{Q}$ возникает из многозначного алгоритма. В этом многозначном алгоритме выбираются некоторые объекты. В соответствующем ему алгоритме в классическом смысле эти объекты перебираются до первого, который задаёт выход (конечно, следует уточнить метод этого перебора; отметим также, что шагов с переборами может быть много). Последний алгоритм вычисляет функцию (в обычном смысле) $\mathfrak{Q}' : \mathcal{S}(T) \to \mathcal{K}$, которая является ограничением бинарного отношения $\mathfrak{Q}$.

Обратно, пусть задан алгоритм с переборами в обычном смысле, вычисляющий функцию $\mathfrak{Q}' : \mathcal{S} \to \mathcal{K}$. Тогда ему соответствует многозначный алгоритм $\mathfrak{Q} : \mathcal{S} \to \mathcal{K}$. Для того чтобы определить $\mathfrak{Q}$, следует использовать все возможные выборы рассматриваемых объектов вместо их переборов. Так что здесь $\mathfrak{Q}'$ снова является ограничением бинарного отношения $\mathfrak{Q}$.

Мы будем говорить, что алгоритм с переборами (в обычном смысле), вычисляющий функцию $\mathfrak{Q}'$, соответствует многозначному лесу вычислений T, в том и только в том случае, если соответствующая ему многозначная функция $\mathfrak{Q}$ является алгоритмом, соответствующим лесу вычислений T. Мы будем говорить, что алгоритм с переборами (в обычном смысле) соответствует многозначному лесу вычислений, если существует многозначный лес вычислений T, такой, что этот алгоритм ему соответствует.

Аналогично [5, раздел 3] можно определить композицию $T_2 \circ T_1$ многозначных лесов вычислений T_1 и T_2. Она определена в том и

только том случае, когда определена композиция бинарных отношений $\mathfrak{F}(T_2) \circ \mathfrak{F}(T_1)$. Более того, в этом случае мы имеем $\mathfrak{F}(T_2 \circ T_1) = \mathfrak{F}(T_2) \circ \mathfrak{F}(T_1)$.

Аналогично [5, раздел 3] можно определить набор $\langle T_1, \dots, T_N \rangle$ из N многозначных лесов вычислений $T_1, \dots, T_N$. Таким образом, $\langle T_1, \dots, T_N \rangle$ является многозначным лесом вычислений.

Теперь мы собираемся сформулировать аналог теоремы 1 работы [5] для многозначных деревьев вычислений. Это теорема 3, см. ниже. Она может рассматриваться как фундаментальный результат в теории многозначных деревьев и лесов вычислений.

Но сначала нам надо усилить лемму 5 из раздела 6 статьи [6]. В указанной статье для квазипроективного алгебраического многообразия $V \subset \mathbb{A}^\mu(\overline{k})$ мы используем следующие обозначения: $D_a(V)$ – степень (см. подробности в разделе 6 статьи [6]) объединения всех неприводимых компонент многообразия V размерности a, где $0 \leqslant a \leqslant \mu$; для целого числа $D \geqslant 2$ положим $\delta_1(V, D) = \sum\limits_{0 \leqslant a \leqslant \mu} D_a(V) D^a$ и $\delta(V, D) = \sum\limits_{0 \leqslant a \leqslant \mu} D_a(V)(D^{a+1} - 1)/(D - 1)$.

В формулировке следующей леммы имеются две верхние границы на степень – D_1 и D – вместо одной границы D в лемме 5 работы [6]. Тем не менее, пункты (b)–(d) следующей леммы совпадают с соответствующими пунктами (b)–(d) леммы 5 работы [6].

Лемма 3. *Пусть V является квазипроективным алгебраическим многообразием в $\mathbb{A}^\mu(\overline{k})$. Пусть $\{\mathcal{W}_\gamma\}_{\gamma \in \Gamma}$ – семейство квазипроективных алгебраических многообразий в $\mathbb{A}^\mu(\overline{k})$. Предположим, что для всякого $\gamma \in \Gamma$*

$$\mathcal{W}_\gamma = \mathcal{Z}(\psi_{\gamma,1}, \dots, \psi_{\gamma,\mu_{\gamma,1}}) \setminus \mathcal{Z}(\psi_{\gamma,\mu_{\gamma,1}+1}, \dots, \psi_{\gamma,\mu_{\gamma,2}}) \subset \mathbb{A}^\mu(\overline{k})$$

для некоторых многочленов $\psi_{\gamma,i} \in \overline{k}[b_1, \dots, b_\mu]$, таких, что

$$\deg_{b_1,\dots,b_\mu} \psi_{\gamma,i} \leqslant D_1$$

при $1 \leqslant i \leqslant \mu_{\gamma,1}$ и $\deg_{b_1,\dots,b_\mu} \psi_{\gamma,i} \leqslant D$ при $\mu_{\gamma,1} + 1 \leqslant i \leqslant \mu_{\gamma,2}$ для некоторых целых чисел $D_1 \geqslant D \geqslant 2$. Предположим, что $\bigcup_{\gamma \in \Gamma} \mathcal{W}_\gamma \supset V$. Тогда существует семейство квазипроективных алгебраических многообразий $\{\mathcal{W}_\beta\}_{\beta \in B}$, удовлетворяющее следующим свойствам.

(a) *Для всякого* $\beta \in B$

$$\mathcal{W}_\beta = \mathcal{Z}(\psi^{(1)}_{\beta,1}, \ldots, \psi^{(1)}_{\beta,\mu_{\beta,1}}) \setminus \bigcup_{2 \leqslant j \leqslant m_\beta} \mathcal{Z}(\psi^{(j)}_{\beta,1}, \ldots, \psi^{(j)}_{\beta,\mu_{\beta,j}}) \subset \mathbb{A}^\mu(\overline{k})$$

для некоторого целого числа $m_\beta \geqslant 2$ *и некоторых многочленов* $\psi^{(j)}_{\beta,i} \in \overline{k}[b_1, \ldots, b_\mu]$, *таких, что* $\deg_{b_1,\ldots,b_\mu} \psi^{(1)}_{\beta,i} \leqslant D_1$ *при* $1 \leqslant i \leqslant \mu_{\beta,1}$ *и* $\deg_{b_1,\ldots,b_\mu} \psi^{(j)}_{\beta,i} \leqslant D$ *при* $1 \leqslant i \leqslant \mu_{\beta,j}$, $2 \leqslant j \leqslant m_\beta$.

(b) *Для всякого* $\beta \in B$ *целое число* m_β *ограничено сверху величиной* $\delta_1(V, D)$.

(c) *Набор* $\{V \cap \mathcal{W}_\beta\}_{\beta \in B}$ *является стратификацией алгебраического многообразия* V, *т.е.* $\bigcup_{\beta \in B}(V \cap \mathcal{W}_\beta) = V$, *и для всех попарно различных* β_1, β_2 *пересечение* $(V \cap \mathcal{W}_{\beta_1}) \cap (V \cap \mathcal{W}_{\beta_2})$ *пусто.*

(d) *Для всякого* $\beta \in B$ *существует элемент* $\gamma \in \Gamma$, *такой, что* $\mathcal{W}_\beta \subset \mathcal{W}_\gamma$.

(e) *Число элементов* $\#B$ *не превосходит* $\delta(V, D)$.

Доказательство. Совпадает с доказательством леммы 5 раздела 6 работы [6]. □

Теорема 3. *Пусть* T *– многозначное дерево вычислений со входными параметрами* $a_1, \ldots, a_\nu$ *над основным полем* k *и* $l(T) = w$. *Предположим, что для всякой вершины* v *дерева* T *условие* $\mathcal{A}_v$ *имеет вид*

$$(\varphi_{v,1} = 0) \wedge \ldots \wedge (\varphi_{v,\mu_{v,1}} = 0) \wedge ((\varphi_{v,\mu_{v,1}+1} \neq 0) \vee \ldots \vee (\varphi_{v,\mu_{v,2}} \neq 0)), \quad (19)$$

где $\wedge$, $\vee$ *обозначают логические конъюнкцию и дизъюнкцию, все*

$$\varphi_{v,\beta} \in k[a_1, \ldots, a_\nu], \quad 1 \leqslant \beta \leqslant \mu_{v,2},$$

являются многочленами для некоторых целых чисел $\mu_{v,2} \geqslant \mu_{v,1} \geqslant 0$ *и* $\deg_{a_1,\ldots,a_\nu} \varphi_{v,\beta} \leqslant d$ *при* $\mu_{1,v} < \beta \leqslant \mu_{2,v}$, *см.* (19), *для некоторого целого числа* $d \geqslant 2$. *Пусть* $\mathcal{S}(T) = \bigcup_{1 \leqslant j \leqslant N} S_j$, *где все* S_j *являются алгебраическими многообразиями в* $\mathbb{A}^\nu(\overline{k})$. *Тогда существует несократимое многозначное поддерево* T' *дерева* T, *такое, что* $\mathcal{S}(T') = \mathcal{S}(T)$ *и*

$$\#L(T') \leqslant \sum_{1 \leqslant j \leqslant N} \delta(S_j, wd).$$

В частности, если $\mathcal{S}(T) = \mathbb{A}^\nu(\overline{k})$, *то*

$$\#L(T') \leqslant \frac{(wd)^{\nu+1} - 1}{wd - 1}.$$

Доказательство. Применим лемму 3 с $\mu = \nu$, $V = S_j$ для всякого j, $D = wd$, $\Gamma = L(T)$. Тогда сначала мы получим стратификацию каждого многообразия S_j и после этого, согласно утверждению (d) леммы, покрытие каждого S_j. Это даёт покрытие $\{\mathcal{W}_v\}_{v\in\Gamma'}$ множества $\mathcal{S}(T) = \bigcup\limits_{1\leqslant j\leqslant N} S_j$ с $\Gamma' \subset \Gamma$ и $\#\Gamma' \leqslant \sum\limits_{1\leqslant j\leqslant N} \delta(S_j, wd)$. Теперь положим T' равным минимальному многозначному поддереву в T, такому, что $L(T') = \Gamma'$. Для этого поддерева T' справедливо утверждение теоремы. Теорема доказана. $\square$

В качестве примера заметим, что покрытие из модифицированной версии теоремы 1 работы [6] (см. замечание 2 из введения) получается при помощи многозначного леса вычислений. Здесь мы оставляем подробности читателю.

§3. Случай конечного числа решений в проективном пространстве

Сначала мы рассмотрим случай $c = 0$. Сейчас для всякого $a^* \in \mathcal{U}_c$ система (3) имеет конечное (или пустое) множество решений в $\mathbb{P}^n(\overline{k})$. Пусть $B = \overline{k}[a_1, \ldots, a_\nu]$. Пусть $Y_0, Y_1, \ldots, Y_n \in B[X_0, \ldots, X_n]$ – произвольные линейные формы от переменных $X_0, \ldots, X_n$ с коэффициентами в B, а $U_0, U_1, \ldots, U_n$ – новые переменные. Положим $f_m = U_0Y_0 + U_1Y_1 + \ldots + U_nY_n$.

Пусть $\deg_{X_0,\ldots,X_n} f_i = d_i$ при $0 \leqslant i \leqslant m-1$. Положим $d_m = 1$. Напомним, что $d_0 \geqslant d_1 \geqslant \ldots \geqslant d_{m-1} \geqslant 1$, см. замечание 1 во введении. Пусть $D' = d_0 + \sum\limits_{1\leqslant i\leqslant \min\{m-1,n\}} (d_i - 1)$. Пусть $\mathcal{H}_i$, $1 \leqslant i \leqslant m$ (соответственно $\mathcal{H}$), является $B[U_0, \ldots, U_n]$-модулем всех многочленов $g \in B[U_0, \ldots, U_n][X_0, \ldots, X_n]$, однородных относительно $X_0, \ldots, X_n$ степени $\deg_{X_0,\ldots,X_n} g = D' - d_i$ (соответственно $\deg_{X_0,\ldots,X_n} g = D'$). Следовательно, $\mathcal{H}_i$ (соответственно $\mathcal{H}$) является свободным $B[U_0, \ldots, U_n]$-модулем ранга $\gamma_i = \binom{D'-d_i+n}{n}$ (соответственно $\gamma = \binom{D'+n}{n}$). Рассмотрим гомоморфизм свободных $B[U_0, \ldots, U_n]$-модулей

$$\mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \ldots \oplus \mathcal{H}_m \to \mathcal{H}, \quad (g_0, \ldots, g_m) \mapsto g_0f_0 + \ldots + g_mf_m. \tag{20}$$

Выберем базис каждого модуля $\mathcal{H}_i$ (соответственно $\mathcal{H}$), состоящий из мономов от $X_0, \ldots, X_n$ с коэффициентами 1 степени $D' - d_i$ (соответственно D'). Тогда гомоморфизм (20) в этих базисах задаётся

матрицей $\mathcal{A}$ с γ строками и $\sum\limits_{0\leqslant i\leqslant m}\gamma_i$ столбцами. Можно представить $\mathcal{A}$ в виде $\mathcal{A}=(\mathcal{A}',\mathcal{A}'')$, где $\mathcal{A}'$ является подматрицей в $\mathcal{A}$, состоящей из первых $\sum\limits_{0\leqslant i\leqslant m-1}\gamma_i$ столбцов. Следовательно, коэффициенты матрицы $\mathcal{A}'$ являются элементами кольца B, и коэффициенты матрицы $\mathcal{A}''$ являются линейными формами от $U_0,\dots,U_n$ с коэффициентами из B.

Для всякого $a^*\in\mathbb{A}^\nu(\overline{k})$ положим $\mathcal{A}(a^*)=\mathcal{A}|_{a_1=a_1^*,\dots,a_\nu=a_\nu^*}$ равным результату подстановки a_i^* вместо a_i, $1\leqslant i\leqslant\nu$, в матрицу $\mathcal{A}$. Аналогично определяются матрицы $\mathcal{A}'(a^*)$, $\mathcal{A}''(a^*)$. Так что $\mathcal{A}'(a^*)$ – матрица с коэффициентами из k_{a^*}, все коэффициенты матрицы $\mathcal{A}''(a^*)$ являются линейными формами от $U_0,\dots,U_n$ с коэффициентами из k_{a^*}, и $\mathcal{A}(a^*)=(\mathcal{A}'(a^*),\mathcal{A}''(a^*))$. Обозначим через Δ_{a^*} наибольший общий делитель в кольце $k_{a^*}[U_0,\dots,U_n]$ всех миноров порядка γ матрицы $\mathcal{A}(a^*)$ (он однозначно определён с точностью до ненулевого множителя из k_{a^*}).

Сформулируем результат из [10,11].

Лемма 4. *Пусть $a^*\in\mathbb{A}^\nu(\overline{k})$. Пусть V_{a^*} – множество всех решений (или корней) системы* (3) *в $\mathbb{P}^n(\overline{k})$. Тогда справедливы следующие утверждения.*

(a) *Если $\#V_{a^*}=+\infty$ (или, что то же самое, $\dim V_{a^*}>0$), то $\Delta_{a^*}=0$.*

(b) *Если $\#V_{a^*}<+\infty$, то*

$$\Delta_{a^*}=\lambda\prod_{\eta=(\eta_0:\dots:\eta_n)\in V_{a^*}}\Big(\sum_{0\leqslant i\leqslant n}U_iY_i(\eta_0,\dots,\eta_n)\Big)^{e_\eta},$$

где $e_\eta\geqslant 1$ – кратность корня η системы (3), *и $0\neq\lambda\in\overline{k}$, все η_i лежат в $\overline{k}$, $0\leqslant i\leqslant n$ (заметим, что здесь линейные формы $\sum\limits_{0\leqslant i\leqslant n}U_iY_i(\eta_0,\dots,\eta_n)\in\overline{k}[U_0,\dots,U_n]$, $\eta\in V_{a^*}$, не обязательно попарно различны, поскольку Y_i являются произвольными).*

(c) *Предположим, что $\#V_{a^*}<+\infty$ и для всякого решения $\eta=(\eta_0:\dots:\eta_n)\in V_{a^*}$ мы имеем $\sum\limits_{0\leqslant i\leqslant n}U_iY_i(\eta_0,\dots,\eta_n)\neq 0$. Тогда $\deg_{U_0,\dots,U_n}\Delta_{a^*}=\gamma-\operatorname{rank}\mathcal{A}'(a^*)$.*

Доказательство. Если $Y_i=X_i$ для всех i, то это доказано в [10,11]. Случай произвольных Y_i легко сводится к частному случаю $Y_i=X_i$, $0\leqslant i\leqslant n$, при помощи невырожденного линейного преобразования

линейных форм и некоторой подстановки (мы оставляем подробности читателю). □

Напомним, что конечные множества линейных форм $\mathcal{L}_0 = \mathcal{M}_{\varkappa_{1,0}}$, $\mathcal{L}'_0 = \mathcal{M}'_{0,\varkappa_{2,0}}$ определены во введении. Напомним также, что $\varkappa_{1,0} = 2nD'_n$ и $\varkappa_{2,0} = nD'_n(D'_n - 1)/2$.

Лемма 5. *Пусть $a^* \in \mathcal{U}_0$. Тогда существует пара линейных форм $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}'_0$, такая, что для всякого $\eta \in V_{a^*}$ имеем $Y_0(\eta) \neq 0$ и для любых двух различных $\eta_1, \eta_2 \in V_{a^*}$ имеем $(Y_1/Y_0)(\eta_1) \neq (Y_1/Y_0)(\eta_2)$.*

Доказательство. Получается непосредственно, ср. [2]. □

Ослабим теорему 1 (соответственно модифицированную версию теоремы 1) для $c = 0$ следующим образом. Заменим в её формулировке "(i)–(xiii)" на "(i)–(ix)" (соответственно "(ii)–(xiii)" на "(ii)–(ix)") и опустим "$\Psi_{\alpha,s,r,i_1,i_2}$, Ψ_{j,i_1,i_2}" в утверждении (c). Теперь мы собираемся построить многозначный лес вычислений T_0, чтобы доказать ослабленную теорему 1 (соответственно ослабленную модифицированную версию теоремы 1) для $c = 0$. Рассмотрим систему (3) с $a^* \in \mathcal{U}_0$. Сначала мы опишем алгоритм (с переборами, см. раздел 2) для решения этой системы. Он следует методу из [10, 11] с некоторыми изменениями. После этого мы увидим, что это алгоритм, соответствующий многозначному лесу вычислений в смысле раздела 2.

Мы перебираем пары линейных форм $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}'_0$.

Пусть $Y_0, Y_1 \in k[X_0, \ldots, X_n]$ – произвольные линейные формы. Положим $Y_i = 0$ при $2 \leqslant i \leqslant n$. Наша цель – найти многочлен Δ_{a^*}, см. лемму 5 (c). Построим матрицу $\mathcal{A} = (\mathcal{A}', \mathcal{A}'')$, см. выше. Затем, используя лемму 1, построим матрицу $\mathcal{G}$, такую, что $\mathcal{G}\mathcal{A}'(a^*)$ имеет каноническую трапециевидную форму с точностью до перестановок строк и столбцов этой матрицы. Пусть $\mathcal{G}\mathcal{A}'(a^*) = \begin{pmatrix} \mathcal{A}_1 \\ 0 \end{pmatrix}$, где $\operatorname{rank}(\mathcal{A}_1) = \operatorname{rank}(\mathcal{A}'(a^*))$ есть число строк матрицы $\mathcal{A}_1$. Следовательно, после перестановки строк и столбцов матрицы $\mathcal{G}\mathcal{A}(a^*)$ эта матрица имеет вид $\begin{pmatrix} \mathcal{A}_1, & \mathcal{A}_2 \\ 0, & \mathcal{A}_3 \end{pmatrix}$, где все коэффициенты матриц $\mathcal{A}_2$, $\mathcal{A}_3$ являются линейными формами из $k_{a^*}[U_0, U_1]$ и $\operatorname{rank}(\mathcal{A}_3) = \gamma - \operatorname{rank}(\mathcal{A}'(a^*))$.

Теперь применим лемму 2 к матрице $\mathcal{A}_3$ (вместо A). Согласно этой лемме мы получаем семейство матриц C_j, $0 \leqslant j \leqslant N$, с коэффициентами из k, такое, что $\mathcal{A}_3 C_j$ является квадратной матрицей для всякого

j. Мы перебираем матрицы C_j для $j = 1, 2, \ldots, N$. Если $\det(\mathcal{A}_3 C_j) = 0$ для всякого j, то $\operatorname{rank}(A) < \gamma$ и $\Delta_{a^*} = 0$.

Пусть $\det(\mathcal{A}_3 C_{j_0}) \neq 0$ для некоторого индекса j_0 и $\det(\mathcal{A}_3 C_j) = 0$ при $1 \leqslant j < j_0$. Тогда по лемме 5 (а) мы имеем $\Delta_{a^*} = \det(\mathcal{A}_3 C_{j_0})$ (с точностью до ненулевого множителя из k_{a^*}; мы будем предполагать, не умаляя общности, что этот множитель равен 1). Таким образом, вычислен ненулевой многочлен $\Delta_{a^*} \in k_{a^*}[U_0, U_1]$.

Замечание 6. Предположим, что $\nu = 0$, $a^{(0)} \in \mathbb{A}^\nu(\overline{k})$, $Y_0 \neq 0$. По определению положим

$$\widetilde{\Delta}_{k;X_0,\ldots,X_n;f_0,\ldots,f_{m-1};Y_0,Y_1} = \Delta_{a^{(0)}},$$

где многочлен $\Delta_{a^{(0)}}$ однозначно определён согласно описанной конструкции.

При этих условиях мы вводим обозначение

$$\Delta_{k;X_0,\ldots,X_n;f_0,\ldots,f_{m-1};Y_0,Y_1} = \begin{cases} \Delta_{a^{(0)}}/\mathrm{lc}_{U_0}(\Delta_{a^{(0)}}), & \text{если} \quad \Delta_{a^{(0)}} \neq 0, \\ 0, & \text{если} \quad \Delta_{a^{(0)}} = 0. \end{cases}$$

Оно будет использоваться в последующих разделах.

Пусть $a^* \in \mathcal{U}_0$. Теперь мы перебираем пары линейных форм

$$(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}_0'.$$

Положим $Y_i = 0$ при $2 \leqslant i \leqslant n$ и вычислим соответствующий многочлен Δ_{a^*}, как это было описано выше.

Если $\Delta_{a^*} = 0$, то пара линейных форм не удовлетворяет утверждению леммы 5 и мы переходим к следующей паре $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}_0'$.

Если $\Delta_{a^*} \neq 0$ и U_1 делит Δ_{a^*}, то $Y_0(\eta) = 0$ для некоторого $\eta \in V_{a^*}$. В этом случае мы переходим к следующей паре $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}_0'$.

Наконец, по лемме 5 и лемме 4 мы найдём такую пару (Y_0, Y_1), что соответствующий многочлен Δ_{a^*} не равен нулю и U_1 не делит Δ_{a^*}. В этом случае мы применим результат из [6, раздел 2] и построим сепарабельные многочлены

$$\Delta_{a^*,j} = \mathrm{SQF}_{j,Z}(\Delta_{a^*}(Z, -1)) \in k_{a^*}[Z], \quad 1 \leqslant j \leqslant \deg_{U_0} \Delta_{a^*},$$

задающие разложение на бесквадратные множители многочлена

$$\Delta_{a^*}(Z, -1)$$

в смысле (21), см. ниже. Для всякого j имеем

$$0 \leqslant \deg_Z \Delta_{a^*,j} \leqslant (\deg_{U_0} \Delta_{a^*})/j.$$

Напомним, что целое число ρ_0 определено во введении, см. п. (iv) с $s = 0$. Если характеристическая экспонента p равна 1, то по определению $B_0 = \{1, \dots, \deg_Z \Delta_{a^*}(Z, -1)\}$, $B_1 = \varnothing$. Если $p > 1$, то $B_r = \{jp^r \,:\, 1 \leqslant j \leqslant (\deg_Z \Delta_{a^*}(Z, -1))/p^r\}$ для всякого целого числа $r \geqslant 0$, см. [6, раздел 2]. По определению положим $r(j) = r$ в том и только в том случае, если $j \in B_r \setminus B_{r+1}$.

В этих обозначениях многочлен

$$\prod_{0 \leqslant r \leqslant \rho_0} \prod_{j \in B_r \setminus B_{r+1}} \Delta_{a^*,j}^{j/p^r}(Z^{p^r}) = \lambda'_{a^*} \Delta_{a^*}(Z, -1), \tag{21}$$

где $0 \neq \lambda'_{a^*} \in k_{a^*}$, и многочлены $\Delta_{a^*,j}(Z^{p^{r(j)}})$, $1 \leqslant j \leqslant \deg_{U_0} \Delta_{a^*}$, попарно взаимно просты, см. [6, раздел 2]. Положим

$$g_{a^*,r} = \prod_{j \in B_r \setminus B_{r+1}} \Delta_{a^*,j} \in k_{a^*}[Z], \quad 0 \leqslant r \leqslant \rho_0.$$

Следовательно, каждый многочлен $g_{a^*,r} \in k_{a^*}[Z]$ сепарабелен. Заметим, что

$$\sum_{0 \leqslant r \leqslant \rho_0} \deg_Z g_{a^*,r} = \#\{(Y_1/Y_0)(\eta) \,:\, \eta \in V_{a^*}\} \tag{22}$$

(здесь мы оставляем подробности читателю).

Пусть t – трансцендентный элемент над k. Расширим основное поле k до $k(t)$. Для всякого i, $0 \leqslant i \leqslant n$, мы применяем описанную конструкцию к $k(t)$, $Y_0, Y_1 + tX_i$ вместо k, Y_0, Y_1 с тем же самым j_0, фиксированным ранее (т.е. мы не перебираем снова матрицы C_j; система (3) также остаётся той же самой). Положим $\tau_r = t^{p^r}$. Мы получаем многочлены $\Delta_{a^*,i} \in k_{a^*}[t, U_0, U_1]$ и $g_{a^*,r,i} \in k_{a^*}[\tau_r, Z]$ вместо Δ_{a^*} и $g_{a^*,r}$ соответственно, $0 \leqslant r \leqslant \rho_0$. Имеем

$$\sum_{0 \leqslant r \leqslant \rho_0} \deg_Z g_{a^*,r,i} = \#\{((Y_1 + tX_i)/Y_0)(\eta) \,:\, \eta \in V_{a^*}\}. \tag{23}$$

Лемма 6. *В обозначениях леммы* 4 (b) *пусть* $e_\eta = p^{r_\eta} e'_\eta$, *где* r_η, e'_η *– целые числа,* $0 \leqslant r_\eta \leqslant \rho_0$, $e'_\eta \geqslant 1$, $\mathrm{G\,C\,D}\,(e'_\eta, p) = 1$, *для всякого* $\eta \in V_{a^*}$. *Предположим, что* U_1 *не делит* Δ_{a^*}. *Тогда пара линейных форм* $(Y_0, Y_1) \in \mathcal{L}_0 \times \mathcal{L}'_0$ *удовлетворяет утверждению леммы* 5 *в том и только в том случае, если выполняются следующие эквивалентные условия*:

(a) $\sum_{0 \leqslant r \leqslant \rho_0} \deg_Z g_{a^*,r,i} = \sum_{0 \leqslant r \leqslant \rho_0} \deg_Z g_{a^*,r}$ *для всех* i,

(b) $\deg_Z g_{a^*,r,i} = \deg_Z g_{a^*,r}$ *для всех* i, r,

(c) *для всякого* r, $0 \leqslant r \leqslant \rho_0$, *многочлен* $g_{a^*,r}(Z^{p^r})$ *совпадает с*

$$\prod_{\eta \in V_{a^*},\, r_\eta = r} (Z - (Y_1/Y_0)(\eta))^{p^r}$$

с точностью до ненулевого множителя из $\overline{k}$, *и для всех* i, $0 \leqslant i \leqslant n$, *и* r, $0 \leqslant r \leqslant \rho_0$, *многочлен* $g_{a^*,r,i}(Z^{p^r})$ *совпадает с*

$$\prod_{\eta \in V_{a^*},\, r_\eta = r} (Z - (Y_1/Y_0)(\eta) - t(X_i/Y_0)(\eta))^{p^r}$$

с точностью до ненулевого множителя из $\overline{k}(\tau_r)$.

Доказательство. Очевидно, из (c) следует (b), а из (b) следует (a). Докажем, что из (a) следует (c). Для всякого $\eta \in V_{a^*}$ обозначим через e''_η (соответственно $e''_{\eta,i}$) кратность корня $Z = (Y_1/Y_0)(\eta)$ (соответственно $Z = ((Y_1/Y_0) + t(X_i/Y_0))(\eta)$) многочлена $\Delta_{a^*}(Z, -1) \in k_{a^*}[Z]$ (соответственно $\Delta_{a^*,i}(t, Z, -1) \in k_{a^*}(t)[Z]$). Тогда, $e''_\eta \geqslant e''_{\eta,i} \geqslant e_\eta$ для всякого η и всякого i. Поэтому согласно (22) и (23)

$$\sum_{0 \leqslant r \leqslant \rho_0} \deg_Z g_{a^*,r} = \sum_{\eta \in V_{a^*}} 1/e''_\eta \leqslant \sum_{\eta \in V_{a^*}} 1/e''_{\eta,i} = \sum_{0 \leqslant r \leqslant \rho_0} \deg_Z g_{a^*,r,i}. \quad (24)$$

Если $e''_\eta > e_\eta$ для некоторого η, то существует элемент $\eta^{(1)} \in V_{a^*}$, такой, что $(Y_1/Y_0)(\eta^{(1)}) = (Y_1/Y_0)(\eta)$, но $(X_i/Y_0)(\eta^{(1)}) \neq (X_i/Y_0)(\eta)$ для некоторого i, $0 \leqslant i \leqslant n$. Следовательно, в этом случае существует такое i, $0 \leqslant i \leqslant n$, что $e''_\eta > e''_{\eta,i}$.

Поэтому в (24) равенство имеет место для всякого i, $0 \leqslant i \leqslant n$, тогда и только тогда, когда $e_\eta = e''_\eta$ для всякого $\eta \in V_{a^*}$. Отсюда (c) следует немедленно. Лемма доказана. □

Предположим, что пара (Y_0, Y_1) удовлетворяет утверждению леммы 5. Пусть $\mathrm{lc}_Z(g_{a^*,r,i})$ – старший коэффициент многочлена $g_{a^*,r,i}$ относительно Z. Тогда $g_{a^*,r,i}/\mathrm{lc}_Z(g_{a^*,r,i}) \in k_{a^*}[\tau_r, Z]$, поскольку корни этого многочлена являются целыми над $k_{a^*}[\tau_r]$. Так что, применяя лемму 2 работы [6], можно заменить $g_{a^*,r,i}$ на многочлен, совпадающий с $g_{a^*,r,i}/\mathrm{lc}_Z(g_{a^*,r,i})$ с точностью до ненулевого множителя из k_{a^*}. Следовательно, в дальнейшем мы можем предполагать без ограничения общности, что $\mathrm{lc}_Z(g_{a^*,r,i}) \in k_{a^*}$.

Теперь для всякого r и для всякого i многочлен $g_{a^*,r,i}(0, Z)$ совпадает с $g_{a^*,r}$ с точностью до ненулевого множителя из k_{a^*}. Пусть $\mu_{a^*,r} = \mathrm{lc}_Z g_{a^*,r}$ (соответственно $\mu_{a^*,r,i} = \mathrm{lc}_Z g_{a^*,r,i}$, $0 \leqslant i \leqslant n$). Заменяя

многочлен $g_{a^*,r}$ на $\left(\prod\limits_{0\leqslant j\leqslant n}\mu_{a^*,r,j}\right)g_{a^*,r}$ и каждый многочлен $g_{a^*,r,i}$ на $\mu_{a^*,r}\left(\prod\limits_{0\leqslant j\neq i\leqslant n}\mu_{a^*,r,j}\right)g_{a^*,r,i}$, мы будем предполагать, не умаляя общности, что $g_{a^*,r,i}(0,Z)=g_{a^*,r}$ для всякого i.

Если $\deg_Z g_{a^*,r}=0$, то положим $J_{a^*,r}=\varnothing$ и $V_{a^*,0,r}=\varnothing$. Пусть $\deg_Z g_{a^*,r}>0$. Тогда положим $J_{a^*,r}$ равным одноэлементному множеству. Обозначим $H_{a^*,j}=g_{a^*,r}$ для $j\in J_{a^*,r}$. Мы предполагаем, что множества $J_{a^*,r}$ попарно различны. Сейчас мы собираемся определить и вычислить многообразие $V_{a^*,0,r}$ в рассматриваемом случае. Так что в дальнейшем в доказательстве, если не оговорено противное, мы предполагаем, что $\deg_Z g_{a^*,r}>0$.

Для всякого r, $0\leqslant r\leqslant\rho_0$, мы строим многочлен $Q\in k_{a^*}[Y,Z]$, такой, что $g_{a^*,r}=(Z-Y)Q+g_{a^*,r}(Y)$. Для всякого корня ξ полинома $g_{a^*,r}$ мы имеем $(Z-\xi)Q(\xi,Z)=0$. Положим $g'_{a^*,r}=\frac{d}{dZ}(g_{a^*,r})=Q(Z,Z)$.

Для всякого i имеем $g_{a^*,r,i}=g_{a^*,r}+\sum\limits_{j\geqslant 0}g_{a^*,r,i,j}\tau_r^j\in k_{a^*}((\tau_r))[Z]$, где $g_{a^*,r,i,j}\in k_{a^*}[Z]$. Теперь применим подъём по лемме Гензеля к многочлену $g_{a^*,r,i}$ и разложению $g_{a^*,r,i}(0,Z)=(Z-\xi)Q(\xi,Z)$ и получим корень $Z=\xi_i\in k_{a^*}[[\tau_r]]$ этого многочлена $g_{a^*,r,i}$, такой, что $\xi_i(0)=\xi_i|_{\tau_r=0}=\xi$. Далее,

$$\frac{d}{d\tau_r}(\xi_i)\Big|_{\tau_r=0}=-\left(\frac{\partial g_{a^*,r,i}}{\partial\tau_r}\right)\Big/\left(\frac{\partial g_{a^*,r,i}}{\partial Z}\right)\Big|_{\tau_r=0,Z=\xi}=-g_{a^*,r,i,1}(\xi)/g'_{a^*,r}(\xi).$$

По лемме 4 фактически корень ξ_i является линейным полиномом от τ_r и

$$\xi_i=\xi-\tau_r\frac{g_{a^*,r,i,1}(\xi)}{g'_{a^*,r}(\xi)},\quad 0\leqslant i\leqslant n.$$

Напомним, что сейчас $\mu_{a^*,r}=\mathrm{lc}_Z g_{a^*,r}=\mathrm{lc}_Z g_{a^*,r,i}$ для всех i. Пусть $\delta_{a^*,r}$ является дискриминантом многочлена $g_{a^*,r}$. Существуют многочлены $A,B\in k_{a^*}[Z]$, такие, что $\deg_Z A<\deg_Z g_{a^*,r}$, $\deg_Z B<\deg_Z g'_{a^*,r}$ и $-g_{a^*,r,i,1}\delta_{a^*,r}=Ag'_{a^*,r}+Bg_{a^*,r}$ (фактически, коэффициенты многочленов A и B являются полиномами от коэффициентов многочленов $g_{a^*,r,i,1}$, $g'_{a^*,r}$, $g_{a^*,r}$). Положим $A=\delta_{a^*,r,i}$. Следовательно, можно записать $-g_{a^*,r,i,1}(\xi)/g'_{a^*,r}(\xi)=\delta_{a^*,r,i}(\xi)/\delta_{a^*,r}$.

Если $J_{a^*,r}=\varnothing$, то положим $\delta_{a^*,r}=1$ и $\delta_{a^*,r,i}=0$ для всякого i, $0\leqslant i\leqslant n$.

Обозначим через $\Xi_{a^*,r}$ множество корней многочлена $g_{a^*,r}$. Пусть $\xi \in \Xi_{a^*,r}$. Положим $W_{a^*,r,\xi} = \{(\eta_0 : \ldots : \eta_n)\}$, где $\eta_i^{p^r} = \delta_{a^*,r,i}(\xi)/\delta_{a^*,r}$ для всякого i, $0 \leqslant i \leqslant n$. Положим

$$V_{a^*,0,r} = \bigcup_{\xi \in \Xi_{a^*,r}} W_{a^*,r,\xi}$$

для всякого r, $0 \leqslant r \leqslant \rho_0$, такого, что $\deg_Z g_{a^*,r} > 0$, и $V_{a^*,0,r} = \varnothing$ для всякого r, $0 \leqslant r \leqslant \rho_0$, такого, что $\deg_Z g_{a^*,r} = 0$.

Теперь мы собираемся доказать модифицированную версию ослабленной теоремы 1, см. замечание 2 во введении, для случая $c = 0$.

Пусть $\mu = \gamma_0 + \ldots + \gamma_{m-1}$ и $b = \{b_i\}_{1 \leqslant i \leqslant \mu}$ – семейство алгебраически независимых элементов над k. Сначала мы предположим, что

($\mathfrak{g}$) $\mu = \nu$, элементы a_i и b_i совпадают при $0 \leqslant i \leqslant \mu$ и $b_1, \ldots, b_\mu$ является семейством всех коэффициентов многочленов $f_0, \ldots, f_{m-1}$, т.е. семейство коэффициентов этих многочленов имеет максимальную возможную степень трансцендентности над k.

Таким образом, сейчас $d' = 1$.

При условии ($\mathfrak{g}$) описанная конструкция определяет многозначную функцию (или бинарное отношение)

$$\mathfrak{F} : \bigcup_{n,d_0,\ldots,d_{m-1}} \overline{k}^{\gamma_0+\ldots+\gamma_{m-1}} \to \mathcal{K},$$

$$a^* \mapsto \left(\{g_{a^*,r}\}_{0 \leqslant r \leqslant \rho_0},\ \{\delta_{a^*,i}\}_{\substack{0 \leqslant r \leqslant \rho_0, \\ 0 \leqslant i \leqslant n}} \right),$$

которое является алгоритмом, соответствующим многозначному лесу вычислений $T_0 = \{T_{0,n,d_0,\ldots,d_{m-1}}\}$ в смысле раздела 2 (напомним, что $\mathcal{K}$ является универсальной областью значений алгоритмов, соответствующих многозначным лесам вычислений, см. [5] и раздел 2). Напомним, что все многочлены $g_{a^*,r}$, $\delta_{a^*,r,i}$ зависят от пары линейных форм (Y_0, Y_1) и матрицы C_{j_0}, см. выше.

Таким образом, $\mathfrak{F} = \mathfrak{F}(T_0)$. Уровень каждого многозначного дерева вычислений $l(T_{0,n,d_0,\ldots,d_{m-1}})$ есть $D_n^{O(1)}$. Для всякой вершины v дерева $T_{0,n,d_0,\ldots,d_{m-1}}$ имеем

$$\mathcal{W}_v = \mathcal{Z}(\psi_{v,1}, \ldots, \psi_{v,\mu_{v,1}}) \setminus \mathcal{Z}(\psi_{v,\mu_{v,1}+1}, \ldots, \psi_{v,\mu_{v,2}}),$$

где все многочлены $\psi_{v,j}$ лежат в $k[a_1,\dots,a_\nu]$ и имеют степени, ограниченные сверху величиной $\binom{n+D'}{n}^{O(1)}$. Положим $A = L(T_{0,n,d_0,\dots,d_{m-1}})$ равным множеству листьев дерева $T_{0,n,d_0,\dots,d_{m-1}}$.

Теперь для всякого $\alpha \in A$, $0 \leqslant r \leqslant \rho_0$, $0 \leqslant i \leqslant n$ в вершине α вычисляются многочлены $g_{\alpha,r} \in k[a_1,\dots,a_\nu,Z]$, $\delta_{\alpha,r,i} \in k[a_1,\dots,a_\nu,Z]$. Они удовлетворяют следующим свойствам. Их степени подчиняются неравенствам $\deg_Z g_{\alpha,r} \leqslant D_n/p^r$, $\deg_Z \delta_{\alpha,r,i} < \deg_Z g_{\alpha,r}$. Степени относительно $a_1,\dots,a_\nu$ многочленов $g_{\alpha,r}$, $\delta_{\alpha,r,i}$ ограничены сверху величиной $\binom{n+D'}{n}^{O(1)}$, и для всякого $a^* \in \mathcal{W}_\alpha$ имеем $\deg_Z g_{\alpha,r} = \deg_Z g_{\alpha,r}(a^*,Z)$,

$$g_{\alpha,r}(a^*,Z) = g_{a^*,r}, \quad \delta_{\alpha,r,i}(a^*,Z) = \delta_{a^*,r,i}$$

для всех i,r. Обозначим через $\delta_{\alpha,r}$ дискриминант многочлена $g_{\alpha,r}$ относительно Z. Тогда $\delta_{\alpha,r}(a^*) = \delta_{a^*,r} \neq 0$ для всех $a^* \in \mathcal{W}_\alpha$ и $0 \leqslant r \leqslant \rho_0$.

Пусть $d'_r = \deg_Z g_{\alpha,r}$. Положим $\Phi_{\alpha,0,r} = Y_0^{d'_r} g_{\alpha,r}(a_1,\dots,a_\nu,Y_1/Y_0)$. Положим $J_{\alpha,0,r}$ равным одноэлементному множеству при $\deg_Z g_{\alpha,r} > 0$ и пустому множеству при $\deg_Z g_{\alpha,r} = 0$. Мы будем предполагать без ограничения общности, что для всякого α множества $J_{\alpha,0,r}$, $0 \leqslant r \leqslant \rho_0$, являются попарно непересекающимися. Далее, мы будем предполагать, не умаляя общности, что $J_{\alpha,0,r} = J_{a^*,r}$ для всякого $a^* \in \mathcal{W}_\alpha$.

Положим $H_j = g_{\alpha,r}$, $\lambda_{\alpha,0,r,1} = \mathrm{lc}_Z g_{\alpha,r}$, $\lambda_{\alpha,0,r,0} = 1$ и $\Phi_{\alpha,0,j} = Y_1 - ZY_0$ для всякого $j \in J_{\alpha,r}$, $0 \leqslant r \leqslant \rho_0$, см. пп. (v) и (vi) из введения.

Теперь мы имеем $\Xi_{j,a^*} = \Xi_{a^*,r}$ и $W_{j,a^*,\xi} = W_{a^*,r,\xi}$ для всякого $j \in J_{\alpha,0,r}$, $a^* \in \mathcal{W}_\alpha$, см. п. (vii) из введения.

Положим $G_j = \delta_{\alpha,r}$ и $G_{j,i} = \delta_{\alpha,r,i}$ для $j \in J_{\alpha,0,r}$, $0 \leqslant r \leqslant \rho_0$, $0 \leqslant i \leqslant n$, см. п. (ix) из введения.

Из данных определений и описанной конструкции следует модифицированная версия ослабленной теоремы 1 для $c = 0$, если выполнено условие $(\mathfrak{g})$.

Следовательно, по теореме 3 ослабленная модифицированная версия теоремы 1 справедлива для $c = 0$ для произвольных $a_1,\dots,a_\nu$ и любой степени d' (когда условие $(\mathfrak{g})$ не обязательно выполняется).

Предположим, что условие $(\mathfrak{g})$ не обязательно выполнено. Обозначим через f семейство коэффициентов из $k[a_1,\dots,a_\nu]$ многочленов $f_0,\dots,f_{m-1}$. Тогда по теореме 3, применённой к дереву $T_{0,d_0,\dots,f_{m-1}}(f)$ (см. определение этого дерева в разделе 2), мы получаем ослабленную теорему 1 для $c = 0$.

§4. Общий случай. Предварительные результаты

Пусть s – целое число, $0 \leqslant s \leqslant n-1$. Напомним, что конечные множества $\mathcal{M}_\varkappa$, $\mathcal{M}'_{s,\varkappa}$ определены во введении, см. (5). Пусть D – целое число, $D \geqslant 2$, и $\varkappa_3 = 2(n-s)D + s$, $\varkappa_4 = (n-s)D(D-1)/2$. Предположим, что $\mathcal{M}_{\varkappa_3}$, $\mathcal{M}'_{s,\varkappa_4}$ существуют (т.е. поле k содержит достаточно много элементов). Прежде всего, нам необходим следующий общий результат.

Лемма 7. *Пусть $V \subset \mathbb{P}^n(\overline{k})$ – непустое проективное алгебраическое многообразие, такое, что размерность каждой его неприводимой компоненты равна s и $\deg V \leqslant D$. Тогда существует элемент $(Y_0, \dots, Y_{s+1}) \in \mathcal{M}_{\varkappa_3}^{s+1} \times \mathcal{M}'_{s,\varkappa_4}$, удовлетворяющий следующим свойствам.*

(a) *$V \cap \mathcal{Z}(Y_0, \dots, Y_s) = \varnothing$ в $\mathbb{P}^n(\overline{k})$, и существуют $\lambda_1, \dots, \lambda_s \in \overline{k}$, такие, что пересечение $V \cap \mathcal{Z}(Y_1 - \lambda_1 Y_0, \dots, Y_s - \lambda_s Y_0)$ трансверсально в каждой его точке. Отсюда следует, что морфизм*

$$\pi_s : V \to \mathbb{P}^s(\overline{k}), \quad (X_0 : \dots : X_n) \mapsto (Y_0 : \dots : Y_s),$$

является конечным доминантным сепарабельным (или, что эквивалентно по определению, ограничение морфизма π_s на каждую неприводимую компоненту многообразия V является конечным доминантным сепарабельным морфизмом). Более того,

$$\deg \pi_s = \deg V = \#(V \cap \mathcal{Z}(Y_1, \dots, Y_s)) = \#\pi_s^{-1}((1 : \lambda_1 : \dots : \lambda_s)).$$

(b) *Пусть $\Phi_s \in \overline{k}[Y_0, \dots, Y_s, Z]$ – ненулевой многочлен минимальной степени, такой, что полином $\Phi_s(Y_0, \dots, Y_{s+1})$ обращается в нуль тождественно на V. Обозначим через $\Delta_s \in \overline{k}[Y_0, \dots, Y_s]$ дискриминант многочлена Φ_s относительно Z. Тогда $\deg_{Y_0,\dots,Y_s,Z} \Phi_s = \deg_Z \Phi_s = \deg V$ и $\Delta_s \neq 0$.*

Доказательство. (a) Используем индукцию по s. База $s = 0$ тривиальна. Пусть $s \geqslant 1$. Существует линейная форма $Y_0 \in \mathcal{M}_{\varkappa_3}$, такая, что $\dim V \cap \mathcal{Z}(Y_0) = s - 1$. Заметим, что для произвольных $\mu_1, \dots, \mu_n \in \overline{k}$ для любых попарно различных линейных форм $L_1, \dots, L_n \in \mathcal{M}_{\varkappa_3} \setminus \{Y_0\}$ линейные формы $L_1 - \mu_1 Y_0, \dots, L_n - \mu_n Y_0$ линейно независимы над $\overline{k}$. Для всякой неприводимой над $\overline{k}$ компоненты E многообразия V выберем гладкую точку ξ_E алгебраического многообразия V, такую, что

$\xi_E \in E \setminus \mathcal{Z}(Y_0)$. Тогда число всех выбранных точек ξ_E не больше D по теореме Безу. Для всякой формы $L \in \mathcal{M}_{\varkappa_3}$ для всякой точки ξ_E существует элемент $\lambda_{L,E} \in \overline{k}$, такой, что $(L - \lambda_{L,E} Y_0)(\xi_E) = 0$.

Для всякой точки ξ_E существует не более $n - s$ попарно различных линейных форм $L \in \mathcal{M}_{\varkappa_3} \setminus \{Y_0\}$, таких, что $L - \lambda_{L,E} Y_0$ обращается в нуль тождественно на касательном пространстве алгебраического многообразия V в точке ξ_E. Далее, для всякой неприводимой над $\overline{k}$ компоненты E' алгебраического многообразия $V \cap \mathcal{Z}(Y_0)$ существует не более $(n-1) - (s-1)$ линейных форм $L \in \mathcal{M}_{\varkappa_3}$, таких, что L обращается в нуль тождественно на E'.

Следовательно, существует линейная форма $Y_s \in \mathcal{M}_{\varkappa_3} \setminus \{Y_0\}$, такая, что $Y_s - \lambda_{Y_s,E} Y_0$ не обращается в нуль тождественно на касательном пространстве каждой выбранной точки ξ_E и Y_s не обращается в нуль тождественно ни на одной из неприводимых компонент E' алгебраического многообразия $V \cap \mathcal{Z}(Y_0)$. Так что $\dim V \cap \mathcal{Z}(Y_0, Y_s) = s - 2$.

Далее, пересечение $E \cap \mathcal{Z}(Y_s - \lambda_{Y_s,E} Y_0)$ трансверсально в каждой точке ξ_E. Рассмотрим морфизм $\pi' : V \to \mathbb{P}^1(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (Y_0 : Y_s)$. Обозначим через V' множество точек $\xi \in V$, таких, что дифференциал $d_\xi \pi'$ равен нулю или ξ не является гладкой точкой многообразия V. Теперь дифференциал $d_{\xi_E} \pi'$ не равен нулю для всякой точки ξ_E. Поэтому $\dim V' \leqslant s - 1$.

Пусть E'' – произвольная неприводимая над $\overline{k}$ компонента многообразия V', такая, что $\dim E'' = s-1$. Мы утверждаем, что существует не более одного элемента $\mu \in \overline{k}$, такого, что E'' является неприводимой компонентой пересечения $V \cap \mathcal{Z}(Y_s - \mu Y_0)$. В самом деле, иначе $E'' \subset V \cap \mathcal{Z}(Y_0, Y_s)$. Поскольку $\dim V \cap \mathcal{Z}(Y_0, Y_s) \leqslant s - 2$, мы получаем противоречие.

Таким образом, существует $\lambda_s \in \overline{k}$, такое, что каждая неприводимая компонента алгебраического многообразия $V \cap \mathcal{Z}(Y_s - \lambda_s Y_0)$ не является неприводимой компонентой многообразия V'. Отсюда следует, что пересечение $V \cap \mathcal{Z}(Y_s - \lambda_s Y_0)$ трансверсально, т.е. для всякой неприводимой над $\overline{k}$ компоненты E''' последнего алгебраического многообразия существует гладкая точка $\xi \in E'''$, такая, что ξ является гладкой точкой многообразия V и пересечение касательных пространств многообразий V и $\mathcal{Z}(Y_s - \lambda_s Y_0)$ в точке ξ трансверсально. Также отсюда следует, что $\deg V = \deg V \cap \mathcal{Z}(Y_s - \lambda_s Y_0)$. Отождествим $\mathcal{Z}(Y_s - \lambda_s Y_0)$ с $\mathbb{P}^{n-1}(\overline{k})$. Теперь, заменяя $(\mathbb{P}^n(\overline{k}), V, Y_0, \mathcal{M}_{\varkappa_3})$ на

$(\mathbb{P}^{n-1}(\overline{k}), V \cap \mathcal{Z}(Y_s - \lambda_s Y_0), Y_0, \mathcal{M}_{\varkappa_3} \setminus \{Y_s\})$, мы доказываем утверждение (a), применяя индукционное предположение.

(b) Существует линейная форма $Y_{s+1} \in \mathcal{M}'_{s,\varkappa_4}$, такая, что число элементов $\#(Y_{s+1}/Y_0)(V \cap \mathcal{Z}(Y_1 - \lambda_1 Y_0, \ldots, Y_s - \lambda_s Y_0))$ равно $\deg V$. По теореме Безу для этой линейной формы Y_{s+1} справедливо утверждение (b) (мы оставляем подробности читателю). Лемма доказана. $\square$

Замечание 7. Пусть V – проективное алгебраическое многообразие из формулировки леммы 7 и $Y_0, \ldots, Y_s \in \overline{k}[X_0, \ldots, X_n]$ – произвольные линейные формы. Тогда $V \cap \mathcal{Z}(Y_0, \ldots, Y_s) = \varnothing$ в $\mathbb{P}^n(\overline{k})$ в том и только в том случае, если морфизм π_s является конечным доминантным (это хорошо известно). Мы хотели бы снова подчеркнуть, что если морфизм π_s является конечным доминантным сепарабельным, то автоматически справедливо утверждение (a) леммы 7. Доказательство последнего факта получается немедленно при помощи теоремы Безу.

Пусть V – проективное алгебраическое многообразие из утверждения леммы 7. Предположим, что $Y_0, \ldots, Y_s \in k[X_0, \ldots, X_n]$ – линейные формы, такие, что $V \cap \mathcal{Z}(Y_0, \ldots, Y_s) = \varnothing$ в $\mathbb{P}^n(\overline{k})$ и $Y_0, \ldots, Y_s$, $X_{s+1}, \ldots, X_n$ линейно независимы над k. Пусть t – трансцендентный элемент над k.

Предположим, что $s \leqslant n-1$. Пусть $Y \in k[X_0, \ldots, X_n]$ – линейная форма, такая, что $Y_0, \ldots, Y_s, Y$ линейно независимы над k. Обозначим через $\Phi_Y \in \overline{k}[Y_0, \ldots, Y_s, Z]$ ненулевой многочлен минимальной степени (относительно $Y_0, \ldots, Y_s, Z$), такой, что $\mathrm{lc}_Z \Phi_Y = 1$ и многочлен $\Phi_Y(Y_0, \ldots, Y_s, Y)$ обращается в нуль тождественно на алгебраическом многообразии V. Если $s = n-1$, то, очевидно, $V = \mathcal{Z}(\Phi_Y(Y_0, \ldots, Y_s, Y))$ в $\mathbb{P}^n(\overline{k})$.

Пусть $s \leqslant n-2$. Пусть $Y \in \mathcal{M}'_{s,\varkappa_4}$ и i – целое число, такое, что $s+2 \leqslant i \leqslant n$. Обозначим через $\Phi_{Y,i} \in \overline{k}[t, Y_0, \ldots, Y_s, Z]$ ненулевой многочлен минимальной степени (относительно $t, Y_0, \ldots, Y_s, Z$), такой, что $\mathrm{lc}_Z \Phi_{Y,i} = 1$ (см. замечание 7) и многочлен $\Phi_{Y,i}(t, Y_0, \ldots, Y_s, Y + tX_i)$ обращается в нуль тождественно на алгебраическом многообразии V. Пусть $\widetilde{\Phi} \in \overline{k}[t, Y_0, \ldots, Y_s, Z]$ – многочлен, такой, что $\mathrm{lc}_Z \widetilde{\Phi} \in \overline{k}$ и бесквадратные части многочленов $\widetilde{\Phi}$ и $\Phi_{Y,i}$ совпадают (т.е. эти многочлены имеют одно и то же множество неприводимых над $\overline{k}$ множителей). Тогда для краткости мы будем говорить, что многочлен $\widetilde{\Phi}$ удовлетворяет

свойству минимальности бесквадратной части для основного поля k, алгебраического многообразия V и линейных форм $Y_0, \dots, Y_s, Y, X_i$.

Пусть $\widetilde{\Phi}_{Y,i} \in \overline{k}[t, Y_0, \dots, Y_s, Z]$ – многочлен, удовлетворяющий свойству минимальности бесквадратной части для основного поля k, алгебраического многообразия V и линейных форм $Y_0, \dots, Y_s, Y, X_i$. Предположим дополнительно, что $\mathrm{lc}_Z \widetilde{\Phi}_{Y,i} = 1$. Представим этот многочлен в виде

$$\widetilde{\Phi}_{Y,i}(t, Y_0, \dots, Y_s, Y + tX_i) = \sum_{0 \leqslant j \leqslant \deg_Z \widetilde{\Phi}_{Y,i}} \widetilde{\Phi}_{Y,i,j} t^j,$$

где $\widetilde{\Phi}_{Y,i,j} \in \overline{k}[Y_0, \dots, Y_s, Y, X_i]$ (заметим, что сейчас линейные формы $Y_0, \dots, Y_s, Y, X_i$ линейно независимы над $\overline{k}$).

Лемма 8. *Пусть V – непустое проективное алгебраическое многообразие из формулировки леммы 7. Предположим, что $Y_0, \dots, Y_s \in k[X_0, \dots, X_n]$ – линейные формы, такие, что $V \cap \mathcal{Z}(Y_0, \dots, Y_s) = \varnothing$ в $\mathbb{P}^n(\overline{k})$ и $Y_0, \dots, Y_s, X_{s+1}, \dots, X_n$ линейно независимы над k. Пусть $\deg_Z \widetilde{\Phi}_{Y,i} \leqslant \widetilde{D}$. Пусть $0 \leqslant s \leqslant n-2$. Тогда во введённых обозначениях*

$$V = \mathcal{Z}(\widetilde{\Phi}_{Y,i,j},\ Y \in \mathcal{M}'_{\varkappa_4},\ s+2 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant \deg_Z \widetilde{\Phi}_{Y,i}), \tag{25}$$

т.е. многообразие V является множеством всех общих нулей в $\mathbb{P}^n(\overline{k})$ системы однородных полиномиальных уравнений $\widetilde{\Phi}_{Y,i,j} = 0$ для всех Y, i, j. Число уравнений этой системы ограничено сверху числом $(n-s-1)\widetilde{D}(1+(n-s)D(D-1)/2)$. Степени этих уравнений ограничены сверху числом $\widetilde{D}$.

Доказательство. Пусть V_1 – проективное алгебраическое многообразие из правой части равенства (25). Очевидно, $V \subset V_1$. Нам требуется доказать, что $V \supset V_1$. Пусть $\xi = (\xi_0 : \dots : \xi_n) \in V_1$ и $\xi_i \in \overline{k}$ для всех i. Осуществляя при необходимости перестановку линейных форм $Y_0, \dots, Y_s$, мы будем предполагать без ограничения общности, что $Y_0(\xi) \neq 0$. Положим $\xi' = (1 : (Y_1/Y_0)(\xi) : \dots : (Y_s/Y_0)(\xi)) \in \mathbb{P}^s(\overline{k})$ и $\Xi = \pi_s^{-1}(\xi')$. Так что число элементов $\#\Xi$ не превосходит D. Существует линейная форма $Y_\xi \in \mathcal{M}'_{\varkappa_4}$, такая, что $\#(Y_\xi/Y_0)(\Xi) = \#\Xi$.

По замечанию 7 и свойствам многочленов $\Phi_{Y,i}$ и $\widetilde{\Phi}_{Y,i}$ существует точка $\xi^{(i)} \in \Xi$, такая, что $(Y_\xi/Y_0)(\xi^{(i)}) + t(X_i/Y_0)(\xi^{(i)}) = (Y_\xi/Y_0)(\xi) + t(X_i/Y_0)(\xi)$ при $s+2 \leqslant i \leqslant n$. Отсюда следует, что $(Y_\xi/Y_0)(\xi^{(i)}) = (Y_\xi/Y_0)(\xi)$ и $(X_i/Y_0)(\xi^{(i)}) = (X_i/Y_0)(\xi)$ при $s+2 \leqslant i \leqslant n$. Согласно выбору Y_ξ мы имеем $\xi^{(i_1)} = \xi^{(i_2)}$ при $s+2 \leqslant i_1, i_2 \leqslant n$. Положим $\xi'' =$

$\xi^{(s+2)} \in V$. Тогда мы имеем $(Y_i/Y_0)(\xi) = (Y_i/Y_0)(\xi'')$ при $1 \leqslant i \leqslant s$, $(Y_\xi/Y_0)(\xi) = (Y_\xi/Y_0)(\xi'')$ и $(X_i/Y_0)(\xi) = (X_i/Y_0)(\xi'')$ при $s+2 \leqslant i \leqslant n$. Но линейные формы $Y_0, \ldots, Y_s, Y_\xi, X_{s+2}, \ldots, X_n$ линейно независимы над k. Отсюда следует, что $\xi = \xi'' \in V$. Последние два утверждения леммы об оценках на число уравнений и степени очевидны. Лемма доказана. $\square$

Пусть c – целое число, $-1 \leqslant c \leqslant n$. Теперь мы собираемся описать некоторый предварительный алгоритм (с переборами, см. раздел 2). Для краткости обозначим $f_{a^*,i} = f_i(a^*, X_0, \ldots, X_n)$, $0 \leqslant i \leqslant m-1$. Применяя лемму 3 из раздела 1 к семейству многочленов $X_j^{d_0-d_i} f_{a^*,i}$, $0 \leqslant j \leqslant n$, $0 \leqslant i \leqslant m-1$, мы находим максимальное линейно независимое над k подсемейство $\{X_{j_\gamma}^{d_0-d_{i_\gamma}} f_{a^*,i_\gamma}\}$, $1 \leqslant \gamma \leqslant N$, этого семейства. Следовательно, $N \leqslant \binom{n+d}{n}$. Положим $I_{a^*} = \{i_\gamma : 1 \leqslant \gamma \leqslant N\}$. Тогда, очевидно, $\mathcal{Z}(f_{a^*,0}, \ldots, f_{a^*,m-1}) = \mathcal{Z}(f_{a^*,i},\, i \in I_{a^*})$. Так что, заменяя при необходимости семейство многочленов $f_{a^*,0}, \ldots, f_{a^*,m-1}$ на $\{f_{a^*,i}\}_{i \in I_{a^*}}$, в дальнейшем мы будем предполагать, не умаляя общности, что $m \leqslant \binom{n+d}{n}$. Если $a^* \in \mathcal{U}_c$, то, очевидно, $m \geqslant n-c$.

Если $c = n$, то тривиально выполняются свойства (α_{n-c}) и (β_{n-c}), см. ниже. В дальнейшем в этом разделе мы предполагаем, что $c < n$.

Предположим, что $c = -1$. Тогда положим $Y_i = X_i$ при $0 \leqslant i \leqslant n$.

Предположим, что $0 \leqslant c \leqslant n-1$. Мы считаем, что поле k содержит достаточно много элементов, и поэтому существует множество линейных форм $\mathcal{L}_c$ (определённое во введении).

Пусть $a^* \in \mathcal{U}_c$. Используя перебор и конструкцию из раздела 3, мы находим элемент $(Y_0, \ldots, Y_c) \in \mathcal{L}_c^{c+1}$ (он зависит от a^*), такой, что $V_{a^*} \cap \mathcal{Z}(Y_0, \ldots, Y_c) = \varnothing$, см. лемму 7 (а). Положим $Y_i = X_i$ при $c+1 \leqslant i \leqslant n$. Следовательно, линейные формы $Y_0, \ldots, Y_n$ линейно независимы над k.

Теперь вернёмся к случаю $-1 \leqslant c \leqslant n-1$. Наша цель состоит в том, чтобы построить многочлены $h_{a^*,1}, \ldots, h_{a^*,n-c}$, удовлетворяющие следующим свойствам.

(α_{n-c}) Для всякого i, $1 \leqslant i \leqslant n-c$,

$$h_{a^*,i} = f_{a^*,i-1} + \sum_{i \leqslant w \leqslant m-1} q_{a^*,i,w}\, f_{a^*,w},$$

где $q_{a^*,i,w} \in k[X_0, \ldots, X_n]$ – однородные многочлены степени $\deg_{X_0,\ldots,X_n} q_{a^*,i,w} = d_w - d_{i-1}$.

(β_{n-c}) $\dim \mathcal{Z}(h_{a^*,1},\dots,h_{a^*,n-c}) = c$.

Тогда $V_{a^*,c}$ является объединением некоторых неприводимых компонент алгебраического многообразия $\mathcal{Z}(h_{a^*,1},\dots,h_{a^*,n-c})$.

Замечание 8. Пусть $\nu = 0$ (так что в обозначениях a^* можно опустить). В [2, гл. 2, §3] конструкция многочленов $h_1,\dots,h_{n-c}$ (там используется обозначение m вместо $n-c$) с "несущественными компонентами" (см. лемму 2.11 в [2]) является неаккуратной. Следует совсем удалить эту лемму. Но требуемое исправление является коротким и простым. Оно приведено в нашей диссертации [7, стр. 221] (отметим, что в [7] и [2] рассматривается случай, когда $d_i = d$ для всех i, и тогда имеют место упрощения). В настоящей статье мы следуем диссертации [7] с небольшими модификациями в этом вопросе.

Предположим, что $1 \leqslant j \leqslant n-c+1$. Рассмотрим следующее свойство:

(γ_{j-1}) $\mathcal{Z}(h_{a^*,1},\dots,h_{a^*,j-1}) \cap \mathcal{Z}(Y_0,Y_1,\dots,Y_{n-j+1}) = \varnothing$ в $\mathbb{P}^n(\overline{k})$.

(Если $j=1$, то последовательность $h_{a^*,1},\dots,h_{a^*,j-1}$ является пустой и $\mathcal{Z}(h_{a^*,1},\dots,h_{a^*,j-1}) = \mathbb{P}^n(\overline{k})$.) Заметим, что если выполняются свойства (α_{n-c}) и (γ_{n-c}), то также справедливы свойства (α_{n-c}) и (β_{n-c}).

Пусть $1 \leqslant j \leqslant n-c$. Предположим, что рекурсивно построены многочлены $h_{a^*,1},\dots,h_{a^*,j-1}$, удовлетворяющие свойствам (α_{j-1}) и (γ_{j-1}) (для базы рекурсии $j=1$ ничего не построено). Мы собираемся построить многочлен $h_{a^*,j}$, такой, что выполняются свойства (α_j), (γ_j).

Согласно (γ_{j-1}) мы имеем

$$\dim \mathcal{Z}(h_{a^*,1},\dots,h_{a^*,j-1},Y_0,Y_1,\dots,Y_{n-j}) = 0.$$

Следовательно, $E_{j-1} = \mathcal{Z}(h_{a^*,1},\dots,h_{a^*,j-1},Y_0,Y_1,\dots,Y_{n-j})$ является конечным множеством. Мы имеем $E_{j-1} \cap V_{a^*} = \varnothing$, поскольку $n-j \geqslant c$ и $V_{a^*} \cap \mathcal{Z}(Y_0,\dots,Y_c) = \varnothing$. Следовательно, по свойству (α_{j-1}) также

$$E_{j-1} \cap \mathcal{Z}(f_{a^*,j-1},\dots,f_{a^*,m-1}) = \varnothing.$$

Теперь рекурсивно найдём индексы $j-1 \leqslant j_1 < \dots < j_{m'} \leqslant m$, такие, что $m' \leqslant \#E_{j-1} \leqslant D'_{j-1}$ (целое число D'_{j-1} определено во введении) и

$$E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1},\dots,f_{a^*,j_{m'}}) = \varnothing.$$

Именно, пусть $1 \leqslant i \leqslant m-2$ и $E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1},\dots,f_{a^*,j_{i-1}}) \neq \varnothing$. Тогда положим

$$j_i = \sup\{w : E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1},\dots,f_{a^*,j_{i-1}},f_{a^*,w},f_{a^*,w+1},\dots,f_{a^*,m-1}) = \varnothing\}.$$

Мы используем конструкцию из раздела 3, для того чтобы найти индекс j_i. Очевидно,

$$E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_{i-1}}) \neq E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_i}).$$

Если $E_{j-1} \cap \mathcal{Z}(f_{a^*,j_1}, \dots, f_{a^*,j_i}) = \varnothing$, то положим $m' = i$ и требуемые индексы построены.

Пусть t – трансцендентный элемент над k. Положим $q_{j,i} = 0$, если $j \leqslant i \leqslant m-1$ и $i \notin \{j_1, \dots, j_{m'}\}$. Положим

$$q_{j,j_w} = \sum_{1 \leqslant u \leqslant j} t^{j(w-1)+u} Y_{n-j+u}^{d_{j-1}-d_{j_w}}, \quad 1 \leqslant w \leqslant m', \tag{26}$$

и

$$\widetilde{h}_{a^*,j} = \sum_{j \leqslant w \leqslant m-1} q_{j,w} f_{a^*,w} \in \overline{k}[t, X_0, \dots, X_n]. \tag{27}$$

Следовательно, $0 \neq \widetilde{h}_{a^*,j}(\eta) \in \overline{k}[t]$ для всякого $\eta \in E_{j-1}$. Мы имеем $\deg_t \widetilde{h}_{a^*,j} \leqslant jm' \leqslant jD'_{j-1}$.

Положим $\beta_j = jm' D'_{j-1}$. Напомним, что $\mathcal{I}_{\beta_j}$ – подмножество в $k \setminus \{0\}$ с числом элементов $\#\mathcal{I}_{\beta_j} = \beta_j + 1$. Следовательно, существует $t_{a^*,j} \in \mathcal{I}_{\beta_j}$, такое, что $\widetilde{h}_{a^*,j}(t_{a^*,j}, \eta_0, \dots, \eta_n) \neq 0$ для всякого $\eta = (\eta_0 : \dots : \eta_n) \in E_{j-1}$. Положим $h_{a^*,j} = \widetilde{h}_{a^*,j}(t_{a^*,j}, X_0, \dots, X_n)$ и $q_{a^*,j,w} = q_{j,w}|_{t=t_{a^*,j}}$ для всех w. Тогда выполняются свойства (α_j), (γ_j).

Можно найти требуемое $t_{a^*,j}$, перебирая элементы $t' \in \mathcal{I}_{\beta_j}$ и решая, верно ли, что

$$\mathcal{Z}(h_{a^*,1}, \dots, h_{a^*,j-1}, \widetilde{h}_{a^*,j}(t', X_0, \dots, X_n), Y_0, \dots, Y_{n-j}) = \varnothing,$$

при помощи конструкции из раздела 3. Рекурсия для построения многочленов $h_{a^*,1}, \dots, h_{a^*,n-c}$ описана полностью. Заметим, что одновременно мы получили многочлены $q_{a^*,j,w}$ и все элементы $t_{a^*,j} \in \mathcal{I}_{\beta_j}$.

Литература

1. A. Ayad, *Complexity of solving parametric polynomial systems.* — Zap. Nauchn. Semin. POMI **387** (2011), 5–52.
2. А. Л. Чистов, *Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время.* — Зап. научн. семин. ЛОМИ **137** (1984), 124–188.
3. A. L. Chistov, *An improvement of the complexity bound for solving systems of polynomial equations.* — Zap. Nauchn. Semin. POMI **390** (2011), 299–306.

4. А. Л. Чистов, *Оценка степени системы уравнений, задающей многообразие приводимых многочленов.* — Алгебра и анализ **24**, вып. 3 (2012), 199–222; *Исправление*: Алгебра и анализ **25**, вып. 2 (2013), 279.
5. А. Л. Чистов, *Вычисления с параметрами: теоретическое обоснование.* — Зап. научн. семин. ПОМИ **436** (2015), 219–239.
6. А. Л. Чистов, *Эффективное разложение многочленов с параметрическими коэффициентами на абсолютно неприводимые множители.* — Зап. научн. семин. ПОМИ **448** (2016), 286–325.
7. А. Л. Чистов, *Эффективные алгоритмы факторизации многочленов и их приложения.* Диссертация на соискание ученой степени доктора физико-математических наук, Ленинград, 1987.
8. A. Chistov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde matrices, NP-completeness, and transversal subspaces.* — Found. Comput. Math. **3**, No. 4 (2003), 421–427.
9. D. Lazard, F. Rouillier, *Solving parametric polynomial systems.* — J. Symbolic Comput. **42**, No. 6 (2007), 636–667.
10. D. Lazard, *Résolution des systèmes d'équations algébriques.* — Theoret. Comput. Sci. **15** (1981), 77–110.
11. D. Lazard, *Commutative algebra and computer algebra.* — Lect. Notes Comput. Sci. **144** (1983), 40–48.

Chistov A. L. Systems with parameters, or efficiently solving systems of polynomial equations: 33 years later. I.

Consider a system of polynomial equations with parametric coefficients over an arbitrary ground field. We show that the variety of parameters can be represented as a union of strata. For values of the parameters from each stratum, the solutions of the system are given by algebraic formulas depending only on this stratum. Each stratum is a quasiprojective algebraic variety with degree bounded from above by a subexponential function in the size of the input data. Also, the number of strata is subexponential in the size of the input data. Thus, here we avoid double exponential upper bounds on the degrees and solve a long-standing problem.

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

Поступило 15 августа 2017 г.