Записки научных
семинаров ПОМИ
Том 481, 2019 г.

А. Л. Чистов

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

Введение к третьей части

Настоящая статья продолжает работы [8, 9] и является третьей частью в серии из трёх. Во всех частях нумерация теорем (соответственно лемм, разделов и т.д.) единая. Она продолжается из [8] и [9] в этой заключительной части. Например, в этой статье ссылка на лемму 6 означает ссылку на лемму 6 из работы [8]. Аналогично раздел 3 означает здесь раздел 3 из работы [8]. Список литературы в данной статье (за исключением ссылок на [8, 9], которые здесь добавлены) совпадает со списком литературы из [8]. В [9] мы доказываем теорему 1. В этой последней третьей части мы докажем исправленную версию теоремы 2, см. введение статьи [8] и раздел 9. Основная работа проделана в [8, 9]. Фактически здесь мы суммируем результаты из [8, 9] и делаем некоторые общие замечания. Доказательство теоремы 2 дано в разделе 12. Оно подобно анализу сложности описанного алгоритма. В других наших статьях в аналогичных ситуациях мы опускали подобный анализ (или оставляли его читателю). Но здесь всё сложнее. Поэтому мы развиваем некоторую общую теорию, см. раздел 11. После этого мы резюмируем всю нашу конструкцию, для того чтобы доказать теорему 2.

Но сначала мы хотели бы исправить некоторые неточности. Первая относится к лемме 5 из работы [6]. Мы приводим корректную версию этой леммы в разделе 10, но она немного слабее. Следует удалить лемму 5 из работы [6] и лемму 3 из работы [8] (которая является ее следствием) и заменить все ссылки на эти леммы в [6, 8, 9] ссылками на лемму 17. Поскольку последняя лемма немного слабее, мы имеем следующие изменения в [6, 8, 9].

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

В теореме 1(a) из [6] должно стоять "число элементов $\#A$ ограничено сверху величиной $(d'd^{O(1)})^{\nu(\nu+1)/2}$" вместо "число элементов $\#A$ ограничено сверху величиной $(d'd^{O(1)})^{\nu}$".

В теореме 1(a) из [8] должно стоять "число элементов $\#A$ ограничено сверху величиной $(d'D_{n-c'}^{O(1)})^{\nu(\nu+1)/2}$" вместо "число элементов $\#A$ ограничено сверху величиной $(d'D_{n-c'}^{O(1)})^{\nu}$".

В теореме 2(c) из [8] изменяется оценка на время работы. Именно, теперь время работы полиномиально от D, $(d'D_{n-c'})^{\nu(\nu+l)}$, $(d'')^{l+1}$, $(d''')^{l+1}$, M_1, M_2 и m. Доказательство этой теоремы будет дано в разделе 12.

Так что изменения относятся к оценке на число стратов стратификаций в этих теоремах и также на время работы алгоритма из теоремы 2 статьи [8]. Это непринципиально для нас в настоящее время, поскольку в любом случае мы получаем алгоритмы субэкспоненциальной сложности для факторизации на абсолютно неприводимые множители многочленов с параметрическими коэффициентами и решения полиномиальных систем с такими коэффициентами. Таким образом, мы решили давно стоящие проблемы в этой области. До сих пор многие специалисты не верили, что такое вообще возможно.

Для удобства читателя и учитывая важность полученных результатов, мы приводим формулировки исправленных версий этих теорем в разделе 8 и разделе 9.

§8. Формулировка теоремы о факторизации многочленов с параметрическими коэффициентами на абсолютно неприводимые множители

Следующая теорема является исправленной версией теоремы 1 из работы [6]. Здесь имеется только одно отличие по сравнению с ней: оценка на $\#A$ в утверждении (a). Для удобства читателя мы дадим полную формулировку этой теоремы, повторив все условия из введения работы [6].

Пусть k – произвольное поле. Пусть p – характеристическая экспонента поля k, т.е. $p = 1$, если $\mathrm{char}(k) = 0$, и $p = \mathrm{char}(k)$, если $\mathrm{char}(k) > 0$. 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 $a_1, \dots, a_\nu$ (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 $\mathcal{V} = \mathbb{A}^\nu(\overline{k})$).

Пусть $f \in k[a_1, \dots, a_\nu, X_1, \dots, X_n]$ – многочлен и

$$\deg_{X_1,\dots,X_n} f \leqslant d, \quad \deg_{a_1,\dots,a_\nu} f \leqslant d' \tag{1}$$

для некоторых целых чисел $d \geqslant 2$ и $d' \geqslant 2$. В настоящей статье мы рассматриваем проблему, состоящую в том, чтобы представить пространство параметров как объединение

$$\mathbb{A}^\nu(\overline{k}) = \bigcup_{\alpha \in A} \mathcal{W}_\alpha \tag{2}$$

конечного числа ($\#A < +\infty$) квазипроективных алгебраических многообразий $\mathcal{W}_\alpha$, удовлетворяющих следующим свойствам. Для всякого $\alpha \in A$ для всех $a^* = (a_1^*, \dots, a_\nu^*) \in \mathcal{W}_\alpha$ существует разложение

$$f(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n) = \lambda_{a^*} \prod_{\gamma \in \Gamma_\alpha} F_{\gamma,a^*}^{e_\gamma}(X_1^{p^{i_\gamma}}, \dots, X_n^{p^{i_\gamma}}), \tag{3}$$

где $f_{\gamma,a^*} \in \overline{k}[X_1, \dots, X_n]$ – неприводимые многочлены над полем $\overline{k}$, $\lambda_{a^*} \in k$, $1 \leqslant e_\gamma \in \mathbb{Z}$, $1 \leqslant i_\gamma \in \mathbb{Z}$, $\#\Gamma_\alpha < +\infty$. Разложение (3) задано равномерно, т.е. некоторыми алгебраическими формулами (см. подробности ниже), определёнными везде на $\mathcal{W}_\alpha$ и зависящими от $a_1^*, \dots, a_\nu^*$ как от параметров. Отметим здесь, что все целые числа e_γ, i_γ и множества индексов Γ_α не зависят от $a^* \in \mathcal{W}_\alpha$.

Теперь мы собираемся придать точный смысл этой равномерности. Именно, разложение (2) удовлетворяет следующим свойствам.

(i) Для всякого $\alpha \in A$ многообразие $\mathcal{W}_\alpha$ непусто. Для произвольных $\alpha_1, \alpha_2 \in A$ если $\alpha_1 \neq \alpha_2$, то $\mathcal{W}_{\alpha_1} \cap \mathcal{W}_{\alpha_2} = \varnothing$, т.е. эти многообразия $\mathcal{W}_\alpha$ являются попарно непересекающимися; так что мы будем называть их стратами, а объединение (2) – 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 $\mathcal{W}_\alpha^{(\beta)} = \mathcal{Z}(\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)})$, $1 \leqslant \beta \leqslant \mu_\alpha$, является множеством всех общих нулей многочленов $\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)} \in k[a_1, \dots, a_\nu]$ в аффинном пространстве $\mathbb{A}^\nu(\overline{k})$, а $m_{\alpha,\beta} \geqslant 1$ – целое число.

Для всякого $\alpha \in A$ обозначим через $\overline{\mathcal{W}}_\alpha$ замыкание относительно топологии Зарисского алгебраического многообразия $\mathcal{W}_\alpha$ в $\mathbb{A}^\nu(\overline{k})$. Обозначим через $\mathcal{I}_\alpha$ идеал аффинного алгебраического многообразия $\overline{\mathcal{W}}_\alpha$.

(iii) Существуют множество индексов J_α, многочлены $\lambda_{\alpha,0}, \lambda_{\alpha,1} \in k[a_1, \dots, a_\nu]$, многочлены $f_j \in k[a_1, \dots, a_\nu, X_1, \dots, X_n]$, целые числа e_j, взаимно простые с p, целые числа $i_j \geqslant 0$ для $j \in J_\alpha$, такие, что каждый из многочленов $\lambda_{\alpha,0}, \lambda_{\alpha,1}$ не обращается в нуль ни в какой точке алгебраического многообразия $\mathcal{W}_\alpha$,

$$f = \frac{\lambda_{\alpha,1}}{\lambda_{\alpha,0}} \prod_{j \in J_\alpha} f_j^{e_j}(a_1, \dots, a_\nu, X_1^{p^{i_j}}, \dots, X_n^{p^{i_j}}) \tag{4}$$

на алгебраическом многообразии $\overline{\mathcal{W}}_\alpha$ (это означает, что многочлен

$$\lambda_{\alpha,0} f - \lambda_{\alpha,1} \prod_{j \in J_\alpha} f_j^{e_j}(a_1, \dots, a_\nu, X_1^{p^{i_j}}, \dots, X_n^{p^{i_j}})$$

лежит в $\mathcal{I}_\alpha$) и $J_{\alpha_1} \cap J_{\alpha_2} = \varnothing$ при $\alpha_1 \neq \alpha_2$. Кроме того, если $p = 1$, то $i_j = 0$ для всякого $j \in J_\alpha$.

(iv) Для всякого $i = -1, 0$ существует не более одного $\alpha \in A$, такого, что $\deg f_j = i$ для некоторого $j \in J_\alpha$. В этом случае $\# J_\alpha = 1$, $e_j = 1$, $\lambda_{\alpha,0} = \lambda_{\alpha,1} = 1$ и если $i = -1$, то $f_j = 0$, если $i = 0$, то $0 \neq f_j = f(a_1, \dots, a_\nu, 0, \dots, 0) \in k[a_1, \dots, a_\nu]$.

(v) Для всякого $\alpha \in A$ для всякого $j \in J_\alpha$ для всякого $a^* \in \mathcal{W}_\alpha$

$$\deg_{X_1,\dots,X_n} f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n) = \deg_{X_1,\dots,X_n} f_j.$$

Если $\deg_{X_1,\dots,X_n} f_j \geqslant 0$, то многочлен $f_j(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ сепарабелен (т.е. не имеет кратных множителей в $\overline{k}[X_1, \dots, X_n]$). Для всех попарно различных $j_1, j_2 \in J_\alpha$ многочлены $f_{j_1}(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ и $f_{j_2}(a_1^*, \dots, a_\nu^*, X_1, \dots, X_n)$ взаимно просты в кольце $\overline{k}[X_1, \dots, X_n]$.

Обозначим через A' подмножество таких элементов $\alpha \in A$, что $\deg f_j \geqslant 1$ для всех $j \in J_\alpha$. Для всех $\alpha \in A'$, $j \in J_\alpha$ существует многочлен $H_j \in k[a_1, \dots, a_\nu][Z]$, удовлетворяющий следующим свойствам.

(vi) Пусть $\alpha \in A'$, $j \in J_\alpha$. Обозначим через $\Delta_j \in k[a_1, \dots, a_\nu]$ дискриминант многочлена H_j относительно Z. Тогда Δ_j не обращается в нуль ни в какой точке алгебраического многообразия $\mathcal{W}_\alpha$.

В условиях п. (vi) для всякого $a^* \in \mathcal{W}_\alpha$ обозначим через Ξ_{j,a^*} множество всех корней многочлена $H_{\alpha,j}(a_1^*, \dots, a_\nu^*, Z) \in \overline{k}[Z]$. Тогда согласно п. (vi) для всякого $a^* \in \mathcal{W}_\alpha$ число корней $\#\Xi_{j,a^*}$ равно $\deg_Z H_j$ и старший коэффициент $\mathrm{lc}_Z H_j$ не обращается в нуль ни в какой точке a^*.

Теорема 1. *Пусть $f \in k[a_1, \dots, a_\nu, X_1, \dots, X_n]$ – многочлен, такой, как выше. Тогда при сформулированных выше условиях существует стратификация $\{\mathcal{W}_\alpha\}_{\alpha \in A}$ пространства параметров $\mathbb{A}^\nu(\overline{k})$, удовлетворяющая свойствам* (i)–(viii) *и такая, что*

(a) *число элементов $\#A$ ограничено сверху величиной $(d' d^{O(1)})^{\nu(\nu+1)/2}$, все целые числа μ_α ограничены сверху величиной $(d' d^{O(1)})^\nu$; здесь константы в $O(1)$ являются абсолютными;*

(b) *степени относительно $a_1, \dots, a_\nu$ всех многочленов $\psi_{\alpha,1}^{(\beta)}, \dots, \psi_{\alpha,m_{\alpha,\beta}}^{(\beta)}$, $\lambda_{\alpha,0}, \lambda_{\alpha,1}$, H_j, F_j, f_j ограничены сверху величиной $d' d^{O(1)}$ с абсолютной константой в $O(1)$.*

Все утверждения в случае покрытия пространства параметров остаются теми же самыми, что и в [6], см. замечание сразу после формулировки теоремы 1 в [6]. В частности, число элементов рассматриваемого покрытия ограничено сверху величиной $(d' d^{O(1)})^\nu$.

§9. Формулировки теорем о решении систем полиномиальных уравнений с параметрическими коэффициентами

Следующая теорема является исправленной версией теоремы 1 из работы [8]. В её формулировке используются обозначения (а также ссылки на формулы (4) и (2), свойства (i)–(xiii) и т.д.) из введения статьи [8]. В частности, "как и выше" означает "как во введении из [8]". Имеется только одно отличие этой теоремы от теоремы 1 в [8]: оценка на $\#A$ в утверждении (a).

Теорема 1. *Пусть многочлены*

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

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 $\#A$ ограничено сверху величиной $(d'D_{n-c'}^{O(1)})^{\nu(\nu+1)/2}$; все целые числа μ_α, $m_{\alpha,\beta}$ ограничены сверху величиной $(d'D_{n-c'}^{O(1)})^{\nu}$; здесь константы в $O(1)$ являются абсолютными;*

(b) *степени относительно $a_1,\dots,a_\nu$ всех многочленов $\psi_{\alpha,1}^{(\beta)},\dots,\psi_{\alpha,m_{\alpha,\beta}}^{(\beta)}$ 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 следующее условие.

(l) *Поле k есть $\mathbb{Q}$, и в* (2) *для всякого i, где $0\leqslant i\leqslant m-1$, 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 $M\geqslant 1$.*

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

Тогда дополнительно выполняется следующее свойство.

(d) *При условии* (l) *коэффициенты из k всех многочленов из* (b) *и* (c) *фактически принадлежат $\mathbb{Z}$. Длины записи целых коэффициентов многочленов из* (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 (c) *ограничены сверху величиной*

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

с абсолютной константой в $O(1)$.

Все утверждения в случае покрытия пространства параметров остаются теми же самыми, что и в [6], см. замечание 2 после формулировки теоремы 1 в [8]. В частности, число элементов рассматриваемого покрытия ограничено сверху величиной $(d'D_{n-c'}^{O(1)})^{\nu}$.

Следующая теорема является исправленной версией теоремы 2 из работы [8]. В её формулировке используются обозначения (и ссылки на формулы (4) и (2), свойства (i)–(xiii), теорему 1, замечание 2 и т.д.) из введения статьи [8]. В частности, "при введенных ранее условиях" означает здесь "при условиях из введения статьи [8]". Имеется только одно отличие этой теоремы от теоремы 2 в [8]: оценка на время работы в утверждении (c) (и мы даём более подробную формулировку утверждения (c)). Эта теорема доказывается в разделе 12.

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

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

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

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

$$(M_1+M_2d''+c^2+\nu\log_2 d'+(l+1)\log_2(d''d'''))D_{n-c'}^{O(1)}. \tag{12}$$

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

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

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

$$(M_1+M_2d''+c^2+\nu\log_2 d'+(l+1)\log_2(d''d'''))D_{n-s}^{O(1)}. \tag{14}$$

(c) *Длина записи выходных данных для представления каждого страта* $\mathcal{W}_\alpha$, $\alpha \in A$ (*при фиксированном* α), *ограничена сверху многочленом от* D, $(d')^\nu$, $(d'')^{l+1}$, $(d''')^{l+1}$, M_1, M_2.

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

Отметим также, что формулировка теоремы 3 остаётся без изменений, поскольку в ней рассматривается случай покрытия (но в её доказательстве следует ссылаться на лемму 17 вместо леммы 5 из [6]).

§10. Лемма о покрытии и стратификации

Пусть пространство $\mathbb{A}^\mu(\overline{k})$ имеет координатные функции $b_1, \dots, b_\mu$. Пусть $V \subset \mathbb{A}^\mu(\overline{k})$ – квазипроективное алгебраическое многообразие и $\tilde{V}$ – замыкание относительно топологии Зарисского многообразия V в аффинном пространстве $\mathbb{A}^\mu(\overline{k})$. Предположим, что $\tilde{V} = \bigcup_{0 \leqslant a \leqslant \mu} V_a$ – разложение многообразия $\tilde{V}$ в объединение равноразмерностных алгебраических многообразий V_a, т.е. для всякого целого числа a, где $0 \leqslant a \leqslant \mu$, размерность каждой неприводимой компоненты E алгебраического многообразия V_a равна a и E является неприводимой компонентой многообразия $\tilde{V}$. Пусть $\deg V_a = D_a$ (степень аффинного алгебраического многообразия равна степени его замыкания относительно топологии Зарисского в соответствующем проективном пространстве). По определению $D_a(V) = D_a$. Для всякого целого числа $D \geqslant 2$ положим

$$\begin{aligned}
\deg V &= \sum_{0 \leqslant a \leqslant \mu} D_a, \\
\delta_1(V, D) &= \sum_{0 \leqslant a \leqslant \mu} D_a(V) D^a, \\
\delta(V, D) &= \sum_{0 \leqslant a \leqslant \mu} D_a(V)(D^{a+1} - 1)/(D - 1), \\
\delta^{(r)}(V, D) &= \sum_{r \leqslant a \leqslant \mu} D_a(V) D^{r-a}, \quad 0 \leqslant r \leqslant \mu.
\end{aligned}$$

Положим $\omega(-1, V, D) = 0$ и рекурсивно определим

$$\omega(r, V, D) = \delta^{(r)}(V, D)(1 + 2\omega(r - 1, V, D)), \quad 0 \leqslant r \leqslant \mu.$$

Лемма 17. *Пусть V – квазипроективное алгебраическое многообразие 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 $\deg_{b_1,\dots,b_\mu}\psi_{\gamma,i} \leqslant D$ при $\mu_{\gamma,1}+1 \leqslant i \leqslant \mu_{\gamma,2}$ для некоторого целого числа $D\geqslant 2$. Предположим, что $\bigcup\limits_{\gamma\in\Gamma}\mathcal{W}_\gamma \supset V$. Тогда

(∗) *существует подмножество $\Gamma_0 \subset \Gamma$, такое, что $V\subset\bigcup_{\gamma\in\Gamma_0}\mathcal{W}_\gamma$ и $\#\Gamma_0\leqslant\delta(V,D)$.*

Предположим дополнительно, что $\deg_{b_1,\dots,b_\mu}\psi_{\gamma,i}\leqslant D$ при $1\leqslant i\leqslant\mu_{\gamma,2}$. Тогда существует семейство квазипроективных алгебраических многообразий $\{\mathcal{W}_\beta\}_{\beta\in B}$, удовлетворяющее следующим свойствам.

(a) *Для всякого $\beta\in B$*

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

для некоторого целого числа $m_\beta\geqslant 2$ и некоторых полиномов $\psi^{(j)}_{\beta,i}\in\overline{k}[b_1,\dots,b_\mu]$, таких, что $\deg_{b_1,\dots,b_\mu}\psi_{\beta,i}\leqslant D$ для всех i,j.

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

(c) *$\{V\cap\mathcal{W}_\beta\}_{\beta\in B}$ 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 $\gamma\in\Gamma$, такое, что $\mathcal{W}_\beta\subset\mathcal{W}_\gamma$.*

(e) *$\#B\leqslant\omega(\dim V,V,D)$.*

Доказательство. Для всякого $\gamma\in\Gamma$ положим

$$\mathcal{W}^{(1)}_\gamma = \mathcal{Z}(\psi_{\gamma,1},\dots,\psi_{\gamma,\mu_{\gamma,1}}),\quad \mathcal{W}^{(2)}_\gamma = \mathcal{Z}(\psi_{\gamma,\mu_{\gamma,1}+1},\dots,\psi_{\gamma,\mu_{\gamma,2}}).$$

Докажем утверждение (*). Доказательство использует рекурсию по $\delta(V,D)$. База рекурсии $V=\varnothing$ тривиальна. Пусть $V=\bigcup\limits_{i\in I}E_i$, где E_i, $i\in I$, – семейство всех попарно различных неприводимых над $\overline{k}$ компонент многообразия V. Имеем $\delta(V,D)=\sum_{i\in I}\delta(V,E_i)$. Поэтому достаточно доказать требуемое утверждение для каждого E_i вместо V. Более точно, достаточно доказать для всякого $i\in I$ существование

подмножества $\Gamma_{0,i} \subset \Gamma$, такого, что $E_i \subset \bigcup\limits_{\gamma\in\Gamma_{0,i}} \mathcal{W}_\gamma$ и $\#\Gamma_{0,i} \leqslant \delta(E_i, D)$. После этого можно положить $\Gamma_0 = \bigcup\limits_{i\in I} \Gamma_{0,i}$.

Существует индекс $\gamma_i \in \Gamma$, такой, что $\mathcal{W}_{\gamma_i}$ содержит открытое относительно топологии Зарисского подмножество в E_i. Тогда $E_i \subset \mathcal{W}^{(1)}_{\gamma_i}$ и $\dim E_i \cap \mathcal{W}^{(2)}_{\gamma_i} < \dim E_i = a_i$. Следовательно, по теореме Безу имеем $D^{a_i} \deg E_i + \delta(E_i \cap \mathcal{W}^{(2)}_{\gamma_i}, D) \leqslant \delta(E_i, D)$ (мы оставляем подробности читателю). Теперь $E_i = (E_i \cap \mathcal{W}_{\gamma_i}) \cup (E_i \cap \mathcal{W}^{(2)}_{\gamma_i})$.

По рекурсивному предположению существует подмножество $\Gamma'_i \subset \Gamma$, такое, что $E_i \cap \mathcal{W}^{(2)}_{\gamma_i} \subset \bigcup_{\gamma\in\Gamma'_i} \mathcal{W}_\gamma$ и $\#\Gamma'_i \leqslant \delta(E_i \cap \mathcal{W}^{(2)}_{\gamma_i}, D)$. Положим $\Gamma_{0,i} = \{\gamma_i\} \cup \Gamma'_i$. Тогда $E_i \subset \bigcup_{\gamma\in\Gamma_{0,i}} \mathcal{W}_\gamma$ и $\#\Gamma_{0,i} \leqslant \delta(E_i, D)$ для всякого $i \in I$. Таким образом, существование подмножества Γ_0 доказано.

Теперь обозначим через $\widetilde{B}$ множество всех троек $(\gamma, \Gamma_1, \Gamma_2)$, таких, что $\gamma \in \Gamma$, $\Gamma_1 \subset \Gamma \setminus \{\gamma\}$, $\Gamma_2 \subset \Gamma \setminus \{\gamma\}$ и $\Gamma_1 \cap \Gamma_2 = \varnothing$. Мы будем писать $\widetilde{B} = \widetilde{B}(\Gamma, V)$, если важна зависимость от Γ и V. Для всякого $\beta = (\gamma, \Gamma_1, \Gamma_2) \in \widetilde{B}$ положим

$$\mathcal{W}_\beta = \mathcal{W}_\gamma \cap \bigcap_{\gamma''\in\Gamma_2} \mathcal{W}^{(2)}_{\gamma''} \setminus \bigcup_{\gamma'\in\Gamma_1} \mathcal{W}^{(1)}_{\gamma'}. \tag{54}$$

Здесь если $\Gamma_1 = \varnothing$, то $\bigcup_{\gamma\in\Gamma_1} \mathcal{W}^{(1)}_\gamma = \varnothing$, и если $\Gamma_2 = \varnothing$, то мы предполагаем, что $\mathcal{W}_\gamma \cap \bigcap_{\gamma\in\Gamma_2} \mathcal{W}^{(2)}_\gamma = \mathcal{W}_\gamma$. Заметим, что $\#\Gamma_1 \leqslant -1 + \#\Gamma$.

Докажем, что существует подмножество $B \subset \widetilde{B}$, такое, что справедливы утверждения (a)–(e). Сначала мы собираемся доказать, что существует подмножество $B \subset \widetilde{B}$, такое, что выполняется утверждение (c).

Пусть V_1 и V_2 – два квазипроективных алгебраических многообразия в $\mathbb{A}^\mu(\overline{k})$. Положим $V_1 < V_2$ в том и только в том случае, если $\dim V_1 < \dim V_2$ или $\dim V_1 = \dim V_2 = r$ (для некоторого r), но $\delta^{(r)}(V_1, D) < \delta^{(r)}(V_2, D)$.

Случай $V = \varnothing$ тривиален. Мы будем использовать рекурсию по V. Именно, предположим, что лемма доказана для всех квазипроективных алгебраических многообразий $V' < V$.

Для произвольного квазипроективного алгебраического многообразия V существует индекс $\gamma_0 \in \Gamma$, такой, что $\dim V \cap \mathcal{W}_{\gamma_0} = \dim V = r$. Тогда

$$V = (V \cap \mathcal{W}_{\gamma_0}) \cup (V \setminus \mathcal{W}^{(1)}_{\gamma_0}) \cup (V \cap \mathcal{W}^{(1)}_{\gamma_0} \cap \mathcal{W}^{(2)}_{\gamma_0})$$

и это объединение трёх попарно непересекающихся алгебраических многообразий. Положим $V_1 = V \setminus \mathcal{W}_{\gamma_0}^{(1)}$ и $V_2 = V \cap \mathcal{W}_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)}$. Мы имеем $V_1 < V$ и $V_2 < V$ по теореме Безу. Более точно,

$$1 + \delta^{(r)}(V_1, D) + \delta^{(r)}(V_2, D) \leqslant \delta^{(r)}(V, D).$$

Применяя теорему Безу несколько раз, мы выводим, что

$$\delta^{(j)}(V_2, D) \leqslant \delta^{(j)}(V, D), \quad 0 \leqslant j \leqslant r-1,$$

и, очевидно,

$$\delta^{(j)}(V_1, D) < \delta^{(j)}(V, D), \quad 0 \leqslant j \leqslant r-1.$$

Поэтому

$$\begin{aligned} \omega(j, V_1, D) &< \omega(j, V, D), \quad 0 \leqslant j \leqslant r-1, \\ \omega(j, V_2, D) &\leqslant \omega(j, V, D), \quad 0 \leqslant j \leqslant r-1. \end{aligned}$$

Заметим, что если $\Gamma = \{\gamma_0\}$, то $V \setminus \mathcal{W}_{\gamma_0}^{(1)} = \varnothing$ и $V \cap \mathcal{W}_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)} = \varnothing$.

Следовательно, по рекурсивному предположению существует подмножество $B' \subset \widetilde{B}(\Gamma \setminus \{\gamma_0\}, V \setminus \mathcal{W}_{\gamma_0}^{(1)})$, такое, что выполняется утверждение (c) для $(V \setminus \mathcal{W}_{\gamma_0}^{(1)}, B')$ вместо (V, B).

Аналогично по рекурсивному предположению существует подмножество $B'' \subset \widetilde{B}(\Gamma \setminus \{\gamma_0\}, V \cap \mathcal{W}_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)})$, такое, что выполняется утверждение (c) для $(V \cap \mathcal{W}_{\gamma_0}^{(1)} \cap \mathcal{W}_{\gamma_0}^{(2)}, B'')$ вместо (V, B).

Положим

$$\begin{aligned} B^{(1)} &= \{(\gamma, \Gamma_1 \cup \{\gamma_0\}, \gamma_2) \,:\, (\gamma, \Gamma_1, \Gamma_2) \in B'\}, \\ B^{(2)} &= \{(\gamma, \Gamma_1, \Gamma_2 \cup \{\gamma_0\}) \,:\, (\gamma, \Gamma_1, \Gamma_2) \in B''\}. \end{aligned}$$

Положим $B = \{(\gamma_0, \varnothing, \varnothing)\} \cup B^{(1)} \cup B^{(2)}$. Теперь, очевидно, справедливо утверждение (c).

В дальнейшем мы будем предполагать без ограничения общности, что $V \cap \mathcal{W}_\beta \neq \varnothing$ для всякого $\beta \in B$. По рекурсивному предположению $\#B^{(1)} \leqslant \omega(\dim V_1, V_1, D)$ и $\#B^{(2)} \leqslant \omega(\dim V_2, V_2, D)$. Предположим,

что $\dim V_1 = \dim V_2 = \dim V = r$. Тогда

$$\begin{aligned}
&\#B \leqslant 1 + \omega(\dim V_1, V_1, D) + \omega(\dim V_2, V_2, D)\\
&= 1 + \delta^{(r)}(V_1, D)(1 + 2\omega(r-1, V_1, D))\\
&+\delta^{(r)}(V_2, D)(1 + 2\omega(r-1, V_2, D))\\
&\leqslant 1 + \delta^{(r)}(V_1, D)(1 + 2\omega(r-1, V, D))\\
&+\delta^{(r)}(V_2, D)(1 + 2\omega(r-1, V, D))\\
&\leqslant \delta^{(r)}(V, D)(1 + 2\omega(r-1, V, D)) = \omega(\dim V, V, D).
\end{aligned}$$

Предположим, что $\dim V_1 < r$ и $\dim V_2 = \dim V = r$. Тогда

$$\begin{aligned}
&\#B \leqslant 1 + \omega(\dim V_1, V_1, D) + \omega(\dim V_2, V_2, D)\\
&= 1 + \omega(\dim V_1, V, D) + \delta^{(r)}(V_2, D)(1 + 2\omega(r-1, V_2, D))\\
&\leqslant 1 + \omega(r-1, V, D) + \delta^{(r)}(V_2, D)(1 + 2\omega(r-1, V, D))\\
&\leqslant \delta^{(r)}(V, D)(1 + 2\omega(r-1, V, D)) = \omega(\dim V, V, D).
\end{aligned}$$

Предположим, что $\dim V_2 < r$ и $\dim V_1 = \dim V = r$. Тогда аналогично предыдущему случаю мы получаем, что $\#B \leqslant \omega(\dim V, V, D)$.

Наконец, предположим, что $\dim V_1 < r$, $\dim V_2 < r$ и $\dim V = r$. Тогда

$$\begin{aligned}
&\#B \leqslant 1 + \omega(\dim V_1, V_1, D) + \omega(\dim V_2, V_2, D)\\
&= 1 + \omega(\dim V_1, V, D) + \omega(\dim V_2, V, D)\\
&\leqslant 1 + 2\omega(r-1, V, D)\\
&\leqslant \delta^{(r)}(V, D)(1 + 2\omega(r-1, V, D)) = \omega(\dim V, V, D).
\end{aligned}$$

Утверждение (e) доказано.

Теперь утверждения (a) и (d) немедленно следуют из (c) и (4). Докажем утверждение (b). Мы снова предполагаем, что утверждение (b) доказано для всех алгебраических многообразий $V' < V$. Положим $m(V) = \max_{\beta \in B} m_\beta$. Мы считаем, что $V \neq \varnothing$. Тогда, согласно описанной конструкции и рекурсивному предположению,

$$\begin{aligned}
&m(V) \leqslant \max\{m(V_1) + 1, m(V_2), 1\} \max\{\delta_1(V_1, D) + 1, \delta_1(V_2, D), 1\}\\
&\leqslant \max\{\delta_1(V, D), 1\} \leqslant \delta_1(V, D).
\end{aligned}$$

Утверждение (b) доказано. □

Следствие 3. *Предположим, что выполняются все условия леммы* 17 *за исключением, может быть, условия* $\bigcup\limits_{\gamma\in\Gamma}\mathcal{W}_\gamma \supset V$. *Предположим, что для всякой тройки* $(\gamma,\Gamma_1,\Gamma_2)\in\widetilde{B}$ *можно выяснить, верно ли, что*

$$\dim\Big(V\cap\bigcap_{\gamma''\in\Gamma_2}\mathcal{W}^{(2)}_{\gamma''}\setminus\bigcup_{\gamma'\in\Gamma_1}\mathcal{W}^{(1)}_{\gamma'}\Big)=\dim\Big(V\cap\mathcal{W}_\gamma\cap\bigcap_{\gamma''\in\Gamma_2}\mathcal{W}^{(2)}_{\gamma''}\setminus\bigcup_{\gamma'\in\Gamma_1}\mathcal{W}^{(1)}_{\gamma'}\Big). \tag{55}$$

Тогда все же можно применить рекурсию для построения стратификации из доказательства леммы. Эта рекурсия останавливается (*т.е. требуемая стратификация не может быть построена*) *в том и только в том случае, если* $\bigcup\limits_{\gamma\in\Gamma}\mathcal{W}_\gamma\not\supset V$. *Следовательно, можно выяснить, верно ли, что* $\bigcup\limits_{\gamma\in\Gamma}\mathcal{W}_\gamma\supset V$, *проверяя истинность или ложность не более* $\omega(\dim V,V,D)\#\Gamma$ *равенств* (55). *Если* $\bigcup\limits_{\gamma\in\Gamma}\mathcal{W}_\gamma\supset V$, *то таким образом можно построить семейство* $\{\mathcal{W}_\beta\}_{\beta\in B}$ *из формулировки леммы* 17 *такое, что* $\{V\cap\mathcal{W}_\beta\}_{\beta\in B}$ *является стратификацией многообразия* V.

Доказательство. Следует из доказательства леммы. □

Следствие 4. *Предположим, что справедливы все условия леммы* 17 *за исключением, может быть, условия* $\bigcup_{\gamma\in\Gamma}\mathcal{W}_\gamma\supset V$. *Предположим, что имеется алгоритм* $\mathfrak{H}$, *который для заданных подмножеств* $\Gamma_1,\Gamma_2\subset\Gamma$ *находит индекс* $\gamma\in\Gamma$ (*если он существует*), *такой, что выполняется равенство* (55), *или устанавливает, что такого* γ *не существует. Тогда всё же можно применить рекурсию для построения стратификации из доказательства леммы. Эта рекурсия останавливается* (*т.е. требуемая стратификация не может быть построена*) *в том и только в том случае, если* $\bigcup\limits_{\gamma\in\Gamma}\mathcal{W}_\gamma\not\supset V$. *Следовательно, можно выяснить, верно ли, что* $\bigcup_{\gamma\in\Gamma}\mathcal{W}_\gamma\supset V$, *применяя алгоритм* $\mathfrak{H}$ *не более* $\omega(\dim V,V,D)$ *раз. Если* $\bigcup\limits_{\gamma\in\Gamma}\mathcal{W}_\gamma\supset V$, *то тем самым можно построить семейство* $\{\mathcal{W}_\beta\}_{\beta\in B}$ *из утверждения леммы* 17, *такое, что* $\{V\cap\mathcal{W}_\beta\}_{\beta\in B}$ *является стратификацией многообразия* V.

Доказательство. Следует из доказательства леммы. □

Следствие 5. *Предположим, что для всякого* $\gamma_1 \in \Gamma$ *выполняются условия следствия* 3 *для* $V \cap \mathcal{W}_{\gamma_1}$ *вместо* V. *Тогда можно выяснить, верно ли, что* $V \subset \bigcup_{\gamma\in\Gamma,\gamma\neq\gamma_1} \mathcal{W}_\gamma$, *проверяя истинность или ложность не более* $\omega(\dim V \cap \mathcal{W}_{\gamma_1}, V \cap \mathcal{W}_{\gamma_1}, D)(\#\Gamma - 1)$ *равенств* (55) (*с* $V \cap \mathcal{W}_{\gamma_1}$ *вместо* V). *Следовательно, итерируя эту конструкцию* (*мы оставляем подробности читателю*), *можно найти подмножество* Γ_0 *из формулировки леммы* 17.

Доказательство. Вытекает из следствия 3. □

Следствие 6. *В условиях леммы* 6 *предположим, что*

$$V = \mathcal{Z}(\varphi_1^{(1)}, \dots, \varphi_{\nu_1}^{(1)}) \setminus \bigcup_{2\leqslant j\leqslant m'} \mathcal{Z}(\varphi_1^{(j)}, \dots, \varphi_{\nu_j}^{(j)}) \tag{56}$$

для некоторых полиномов $\varphi_j^{(i)} \in \overline{k}[b_1, \dots, b_\mu]$, *таких, что* $\deg_{b_1,\dots,b_\mu} \varphi_i \leqslant D$ *при* $1 \leqslant i \leqslant m_2$ *для целых чисел* $D \geqslant 2$, $\nu_i \geqslant 0$, $m' \geqslant 1$. *Предположим, что* $\dim V = c$. *Тогда* $\#\Gamma_0 \leqslant (\mu+1)D^\mu$ *и* $\#B < 2^{c+1}D^{(2\mu-c)(c+1)/2}$.

В частности, если $V = \mathbb{A}^\mu(\overline{k})$, *то мы имеем* $\#\Gamma_0 \leqslant (\mu+1)D^\mu$ *и* $\#B < 2^{\mu+1}D^{\mu(\mu+1)/2}$.

Доказательство. Оценка на $\#\Gamma_0$ получается непосредственно. Мы имеем

$$\begin{aligned}
&\#B \leqslant \omega(c, V, D) \leqslant D^{\mu-c}(1 + 2D^{\mu-c+1}(1 + 2D^{\mu-c+2}(\dots(1 + 2D^\mu)\dots)))\\
&= D^{\mu-c} + 2D^{2\mu-2c+1} + 4D^{3\mu-3c+3} + \dots + 2^c D^{(2\mu-c)(c+1)/2}\\
&< 2^{c+1}D^{(2\mu-c)(c+1)/2}.
\end{aligned}$$

Следствие доказано. □

§11. Ещё немного общей теории

Предположим, что дано многозначное дерево вычислений T с входными параметрами $a_1, \dots, a_\nu$ над полем k. Таким образом, пространство параметров $\mathbb{A}^\nu(\overline{k})$ имеет координатные функции $a_1, \dots, a_\nu$. Обозначим через $\mathcal{S}(T) \in \mathbb{A}^\nu(\overline{k})$ область определения дерева T. Далее, пусть $\mathfrak{Q} = \mathfrak{F}(T)$ – алгоритм, соответствующий многозначному дереву вычислений T. Следовательно, $\mathfrak{Q} \subset \mathcal{S}(T) \times \mathcal{K}$ является бинарным отношением. Предположим также, что задан алгоритм с перечислениями $\widetilde{\mathfrak{Q}}$, вычисляющий функцию $\mathfrak{Q}' : \mathcal{S}(T) \to \mathcal{K}$ (это отображение в обычном

смысле) и соответствующий дереву T. Таким образом, $\mathfrak{Q}'$ является ограничением бинарного отношения $\mathfrak{Q}$. Определения и подробности см. в разделе 2. В частности, для всякой вершины w дерева T определены квазипроективные алгебраические многообразия $\mathcal{W}_w \subset \mathbb{A}^\nu(\overline{k})$.

Для доказательства теоремы 2 из раздела 9 удобно предполагать, что для всякой точки $a^* \in \mathcal{S}(T)$ алгоритм $\widetilde{\mathfrak{Q}}$ вычисляет не только $\mathfrak{Q}'(a^*)$, но также и некоторые другие объекты из конструкции, описанной в [8, 9]. Подробности будут даны ниже в этом разделе.

Напомним, что для всякой вершины v многозначного дерева вычислений T определены булевы условия $\mathcal{A}_v$, $\overline{\mathcal{A}}_v$ и квазипроективное алгебраическое многообразие $\mathcal{W}_v$, см. раздел 1 в [5] и раздел 2 в [8]. Именно, $\mathcal{A}_v$ имеет вид

$$(\varphi_{v,1} = 0) \wedge \ldots \wedge (\varphi_{v,\mu_{v,1}} = 0) \wedge ((\varphi_{v,\mu_{v,1}+1} \neq 0) \vee \ldots \vee (\varphi_{v,\mu_{v,2}} \neq 0)) \quad (57)$$

для некоторых многочленов $\varphi_{i,j} \in k[a_1, \ldots, a_\nu]$.

Напомним, как мы представляем многообразия $\mathcal{W}_w$, соответствующие вершинам w многозначного дерева вычислений. Согласно формуле (4) из раздела 1 работы [5] (сейчас эта формула относится к многозначному дереву вычислений; также мы теперь заменяем обозначение $\mu_{w,i}$ из [5] на $\mu'_{w,i}$, для того чтобы избежать двусмысленности),

$$\mathcal{W}_v = \mathcal{W}_{i_0,\ldots,i_\varkappa} = \mathcal{W}_v^{(1)} \setminus \mathcal{W}_v^{(2)} \subset \mathbb{A}^\nu(\overline{k}),$$

где

$$\mathcal{W}_v^{(1)} = \mathcal{Z}(\varphi_{w,i},\, w \in J_v \cup \{v\}, 1 \leqslant i \leqslant \mu'_{w,1}), \quad (58)$$

$$\mathcal{W}_v^{(2)} = \bigcup_{w \in J_v \cup \{v\}} \mathcal{Z}(\varphi_{w,i},\, \mu'_{w,1} + 1 \leqslant i \leqslant \mu'_{w,2}) \quad (59)$$

для некоторых многочленов $\varphi_{w,i} \in k[a_1, \ldots, a_\nu]$ (здесь J_v – множество всех предков вершины v в рассматриваемом дереве).

Пусть v_0 – корень дерева T. В дальнейшем мы будем предполагать, что $\mathcal{W}_{v_0} = \mathbb{A}^\nu(\overline{k})$ (фактически, здесь нет ограничения общности).

Пусть $\psi_v^{(1)} = \{\psi_{v,i}^{(1)}\}_{1 \leqslant i \leqslant m_{v,1}}$ – максимальное линейно независимое над k подсемейство семейства полиномов $\varphi_{w,i}$, где $w \in J_v \cup \{v\}$, $1 \leqslant i \leqslant \mu'_{w,1}$. Предположим, что известно представление (58) для вершины v дерева T. Тогда можно выбрать и зафиксировать такое подсемейство $\psi_v^{(1)}$ для этой вершины v, так что $\mathcal{W}_v^{(1)} = \mathcal{Z}(\psi_{v,i}^{(1)},\, 1 \leqslant i \leqslant m_{v,1})$.

Предположим, что известно представление (59) для всякой вершины v и всех её предков в дереве T. Тогда для всякой вершины v дерева

T мы рекурсивно определяем семейство полиномов

$$\psi_v^{(2)} = \{\psi_{v,i}^{(2)}\}_{1\leqslant i\leqslant m_{v,2}},$$

такое, что $\mathcal{W}_v^{(2)} = \mathcal{Z}(\psi_{v,i}^{(2)},\ 1 \leqslant i \leqslant m_{v,2})$, следующим образом. База рекурсии соответствует корню v_0 дерева. В этом случае $m_{v_0,1} = m_{v_0,2} = 0$ и $\psi_v^{(2)}$ – пустое семейство. Теперь предположим, что v является сыном вершины v_1 и семейство $\psi_{v_1}^{(2)}$ определено. Тогда положим $\psi_v^{(2)}$ равным максимальному линейно независимому над k подсемейству семейства

$$\psi_{v_1,i}^{(2)}\varphi_{v,j}, \quad 1 \leqslant i \leqslant m_{v_1,2},\ \mu'_{v,1} + 1 \leqslant j \leqslant \mu'_{v,2} \tag{60}$$

(можно выбрать и зафиксировать такое подсемейство). Таким образом,

$$\mathcal{W}_v = \mathcal{W}_v^{(1)} \setminus \mathcal{W}_v^{(2)}, \quad \mathcal{W}_v^{(i)} = \mathcal{Z}(\psi_{v,j}^{(i)},\ 1 \leqslant i \leqslant m_{v,i}), \quad i = 1, 2. \tag{61}$$

Напомним, что $\mathcal{S}(T) = \bigcup_{v\in L(T)} \mathcal{W}_v$, где $L(T)$ – множество всех листьев дерева T. Положим $\Gamma = L(T)$. В дальнейшем в этом разделе мы предполагаем, что $\mu = \nu$ и $a_i = b_i$ для $1 \leqslant i \leqslant \mu$. Теперь каждое алгебраическое многообразие $\mathcal{W}_\gamma$ задано как в лемме 17. Предположим также, что выполняются все другие условия леммы 17. Следовательно, теперь $V \subset \mathcal{S}(T)$. Предположим дополнительно, что V удовлетворяет условиям из следствия 6, см. (56).

Напомним, что во введении статьи [8] определена функция $\mathrm{l}(\ldots)$ длины записи (или битового размера) коэффициентов из поля k многочленов (из различных колец) в случае, когда $k = k_0(\tau_1, \ldots, \tau_l)[\tau_{l+1}]$.

Лемма 18. *Предположим, что поле $k = k_0(\tau_1, \ldots, \tau_l)[\tau_{l+1}]$ – из введения. Пусть V – алгебраическое многообразие из следствия 6. Обозначим через $\overline{V}$ замыкание многообразия V в проективном пространстве $\mathbb{P}^\nu(\overline{k})$ (это проективное пространство имеет координатные функции $a_0, \ldots, a_\nu$). Положим $\dim \overline{V} = \overline{c}$ (так что $c \leqslant \overline{c} \leqslant \nu$). Предположим дополнительно, что для всех u, j длины записи коэффициентов $\mathrm{l}(\varphi_j^{(u)})$ ограничены сверху числом M, см. (56). Тогда можно построить представление $V = \bigcup\limits_{i\in I} V_i$, где все V_i являются объединениями неприводимых компонент многообразия V одной и той же размерности, зависящей только от i, и каждая неприводимая компонента многообразия V является неприводимой компонентой только одного из V_i. Каждое многообразие V_i задаётся его общей точкой из некоторой конечно порождённой сепарабельной алгебры над полем $k^{p^{-r}}$, где*

p – характеристическая экспонента поля k и $0 \leqslant r \in \mathbb{Z}$ (оно зависит от i). Более точно, можно построить гомоморфизм k-алгебр

$$\xi_i : (k^{p^{-r}}[V_i])^{p^r} \to k(t_1, \dots, t_{\nu-s})[Z]/(\Phi_i) = k(t_1, \dots, t_{\nu-s})[\eta_i], \quad (62)$$

индуцирующий изоморфизм между полным кольцом частных $(k^{p^{-r}}[V_i])^{p^r}$ и $k(t_1, \dots, t_{\nu-s})[\eta_i]$. Здесь $t_1, \dots, t_{\nu-s}$ алгебраически независимы над k, многочлен $\Phi_i \in k(t_1, \dots, t_{\nu-s})[Z]$ сепарабелен относительно Z и имеет степень не меньше единицы, $\eta_i = Z \bmod \Phi_i$. Обозначим через $\overline{a}_u \in k^{p^{-r}}[V_i]$ координатную функцию на V_i (она является вычетом элемента a_u), $1 \leqslant u \leqslant \nu$. Тогда $\dim V_i = \nu - s$ (где s зависит от i). Многочлен Φ_i и все элементы $\xi_i(\overline{a}_u^{p^r}) \in k(t_1, \dots, t_{\nu-s})[\eta_i]$, $1 \leqslant u \leqslant \nu$, также могут быть построены.

Время работы алгоритма для построения такого представления $V = \bigcup\limits_{i \in I} V_i$ и всех гомоморфизмов (62) *полиномиально от M, M_1, d_1^{l+1} и $D^{\nu(\overline{c}+l+1)}$.*

Доказательство. Положим $V^{(j)} = \mathcal{Z}(\varphi_1^{(j)}, \dots, \varphi_{\nu_j}^{(j)})$ для всякого j. Можно вычислить разложение $V^{(1)} = \cup_{i \in I'} E_i$, где E_i являются равноразмерностными квазипроективными алгебраическими многообразиями. Они задаются их общими точками ξ_i', аналогичными (62). Мы используем рекурсию по $j \geqslant 0$. Для $0 \leqslant j \leqslant m'$ положим $E_{i,j}$ равным объединению всех неприводимых компонент E многообразия E_i, таких, что $E \setminus \bigcup\limits_{2 \leqslant u \leqslant j} V^{(u)} \neq \varnothing$. Предположим, что объединение $E_{i,j-1} \neq \varnothing$ уже построено для некоторого j, где $1 \leqslant j \leqslant m' - 1$, и задано его общей точкой $\xi_{i,j-1}$, аналогичной (62). Пусть t – новая переменная. Можно вычислить $\sum\limits_{1 \leqslant u \leqslant \mu_j} t^u \xi_{i,j-1}((\varphi_u^{(j)})^{p^r}) = \sum\limits_{0 \leqslant u \leqslant \deg_Z \Phi} c_u \eta_{i,j-1}^u$, где $c_i \in k(t, t_1, \dots, t_{\nu-s})$. После этого можно построить многочлен

$$\Phi'_{i,j-1} = \mathrm{G\,C\,D}(\Phi_{i,j-1}, \sum_{0 \leqslant u \leqslant \deg_Z \Phi_{i,j-1}} c_u Z^u) \in k(t_1, \dots, t_{\nu-s})[Z],$$

ср. разделы 6 и 7. Тогда $\Phi'_{i,j-1}$ соответствует общей точке $\xi'_{i,j-1}$ (аналогичной (62)) объединения $E'_{i,j-1}$ всех неприводимых компонент E многообразия $E_{i,j-1}$, таких, что $E \subset W^{(j)}$. Положим

$$\Phi_{i,j} = \Phi_{i,j-1}/\Phi'_{i,j-1}.$$

Теперь если $\deg_Z \Phi_{i,j} \geqslant 1$, то многочлен $\Phi_{i,j}$ соответствует общей точке $\xi_{i,j}$ многообразия $E_{i,j}$, аналогичной (62). Если $\deg_Z \Phi_{i,j} = 0$, то устанавливаем, что $E_{i,j} = \varnothing$ (здесь мы оставляем подробности читателю). Если $E_{i,j} = \varnothing$, то также $E_{i,j_1} = \varnothing$ для всех $j_1 > j$.

Таким образом, в конечном счёте можно построить общие точки $\xi_{i,m'}$ всех непустых многообразий из семейства $E_{i,m'}$, $i \in I$. Мы имеем $\dim V = \max\{\dim E_i \,:\, E_{i,m'} \neq \varnothing\}$. Положим $I = \{i \in I' \,:\, E_{i,m'} \neq \varnothing\}$, $V_i = E_{i,m'} \setminus \bigcup\limits_{2 \leqslant j \leqslant m'} V^{(j)}$ и $\xi_i = \xi_{i,m'}$.

Время работы $\mathcal{T}$ алгоритма для построения представления $V = \bigcup_{i \in I} V_i$ и всех гомоморфизмов ξ_i по существу то же самое, что и время работы для решения систем однородных полиномиальных уравнений относительно $a_0, \ldots, a_\nu$ или, более точно, для разложения алгебраического многообразия в объединение равноразмерностных алгебраических многообразий. Верхняя оценка на последнее время работы может быть легко получена из конструкции, описанной в разделах 6 и 7 (или даже из статьи [3]; фактически, эта оценка была известна, когда появилась статья [3]). Именно, в разделах 6 и 7 следует рассмотреть частный случай систем с коэффициентами из k (без параметров) и после этого заменить переменные $X_0, \ldots, X_n$ на $a_0, \ldots, a_\nu$ (сейчас a_i не рассматриваются как параметры; они являются переменными). В разделах 6 и 7 осуществляются лишь некоторые переборы и вычисляются некоторые определители. Таким образом, мы получаем, что $\mathcal{T}$ ограничено сверху полиномом от M, M_1, d_1^{l+1}, $D^{\nu(\overline{c}+l+1)}$. Лемма доказана. $\square$

Для всякой вершины v многозначного дерева вычислений T определены булево условие $\mathcal{A}_v$ и семейство $\mathcal{C}_v = \{c_{v,j}\}_{1 \leqslant j \leqslant m_v}$ полиномов $c_{v,j} \in k[a_1, \ldots, a_\nu]$, см. [5, раздел 1] и [8, раздел 2]. Обозначим через S_v множество сыновей вершины v в многозначном дереве T.

Для всякой точки $a^* = (a_1^*, \ldots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$ естественным образом определено значение $\mathcal{A}_v(a^*) \in \{\text{true}, \text{false}\}$, см. (57). Рассмотрим семейство $\mathcal{C}_v(a^*) = \{c_{v,j}(a^*)\}_{1 \leqslant j \leqslant m_v}$.

Мы будем предполагать, что вершина v дерева T построена алгоритмом $\widetilde{\Omega}$ (для некоторого входа a^* на некотором шаге этого алгоритма), если построены $\mathcal{A}_v, \mathcal{C}_v$ и (рекурсивно, может быть, на предыдущих шагах) построены все предки вершины v в этом дереве T.

Для всякой точки $a^* = (a_1^*, \dots, a_\nu^*) \in \mathcal{S}(T)$ алгоритм $\widetilde{\mathfrak{Q}}$ вычисляет лист $\gamma \in \Gamma$, такой, что $a^* \in \mathcal{W}_\gamma$, и выход $\mathfrak{Q}'(a^*)$, соответствующий листу a^*.

Более того, мы будем предполагать, что для произвольной точки $a^* \in \mathbb{A}^\nu(\overline{k})$ алгоритм с перечислениями $\widetilde{\mathfrak{Q}}$ строит последовательно вершины $v_0, v_1, \dots, v_N$, зависящие от a^*, и для всякой вершины v_i вычисляет $\mathcal{A}_{v_i}(a^*), \mathcal{C}_{v_i}(a^*)$. Причём выполняются следующие условия (эти условия описывают также рекурсивные шаги алгоритма $\widetilde{\mathfrak{Q}}$).

(i) Вершина v_0 является корнем дерева T, и $v_i \notin L(T)$ при любом i, где $0 \leqslant i \leqslant N-1$.

(ii) $\mathcal{A}_{v_i}(a^*) = \text{true}$ при $0 \leqslant i \leqslant N$.

(iii) Вершина $v_N \in L(T)$ является листом дерева T в том и только в том случае, если $a^* \in \mathcal{S}(T)$, и в этом случае $\mathfrak{Q}'(a^*) = \mathcal{C}_{v_N}(a^*)$.

(iv) Предположим, что $v_0, \dots, v_i$ построены для некоторого $i \geqslant 0$ и $v_i \notin L(T)$. Тогда для того, чтобы найти v_{i+1} или выяснить, что $i = N$ (конечно, в этом случае $a^* \notin \mathcal{S}(T)$), алгоритм $\widetilde{\mathfrak{Q}}$ строит последовательность $w_{i,1}, w_{i,2}, \dots, w_{i,M_i}$ вершин из множества $S_{v_0} \cup \ldots \cup S_{v_i}$ для некоторого целого числа $M_i \geqslant 0$.

Пусть $0 \leqslant j \leqslant M_i$. Положим

$$J_{i,j} = \{(u,v) \in \mathbb{Z}^2 : (1 \leqslant u \leqslant i-1 \,\&\, 1 \leqslant v \leqslant M_u) \vee (u = i \,\&\, 1 \leqslant v \leqslant j)\}$$

и $\beta_{u,v} = \mathcal{A}_{w_{u,v}}(a^*)$, $(u,v) \in J_{i,j}$.

(v) Пусть $0 \leqslant j \leqslant M_i$. Предположим, что $w_{i,1}, \dots, w_{i,j}$ уже построены и $\mathcal{A}_{w_{i,u}}(a^*) = \text{false}$ для $1 \leqslant u \leqslant j$. Тогда вершина $w_{i,j+1}$ (если она существует) однозначно определена булевыми значениями $\beta_{u,v}$, $(u,v) \in J_{i,j}$. Более того, используя эти булевы значения, можно выяснить, верно ли, что $j = M_i$.

(vi) Предположим, что мы выяснили, что $j = M_i$, и $\mathcal{A}_{w_{i,u}}(a^*) = \text{false}$ для $1 \leqslant u \leqslant j$. Тогда $N = i$ и $a^* \notin \mathcal{S}(T)$.

(vii) Предположим, что мы выяснили, что $j < M_i$. Тогда алгоритм $\widetilde{\mathfrak{Q}}$ строит $w_{i,j+1}$, используя только $\mathcal{A}_{w_{u,v}}, \mathcal{C}_{w_{u,v}}$ и $\beta_{u,v}$ для $(u,v) \in J_{i,j}$ (так что точка a^* требуется только для вычисления всех $\beta_{u,v}$; все $\mathcal{A}_{w_{u,v}}, \mathcal{C}_{w_{u,v}}$ строятся на предыдущих шагах).

(viii) Булево значение $\mathcal{A}_{w_{i,j+1}}(a^*)$ вычисляется алгоритмом $\widetilde{\mathfrak{Q}}$ после того, как построена вершина $w_{i,j+1}$.

(ix) Если $\mathcal{A}_{w_{i,j+1}}(a^*) = \text{false}$, то мы возвращаемся к п. (v) с $j+1$ вместо j.

(x) Если $\mathcal{A}_{w_{i,j+1}}(a^*) = \text{true}$, то $j+1 = M_i$. В этом случае мы имеем $w_{i,j+1} = v_{i+1}$. Если $v_{i+1} \notin L(T)$, то мы возвращаемся к (iv) с $i+1$ вместо i. Если $v_{i+1} \in L(T)$, то $i+1 = N$, алгоритм $\widetilde{\Omega}$ заканчивает свою работу и требуемая последовательность $v_1, \ldots, v_N$ построена.

(xi) Для всякого i, где $0 \leqslant i \leqslant N-1$, вершина v_{i+1} не является сыном вершины v_i в том и только в том случае, если $\mathcal{A}_w(a^*) = \text{false}$ для всех $w \in S_{v_i}$.

Эти условия являются естественными. По крайней мере, они выполняются для алгоритмов с перечислениями в наших статьях, посвящённых задачам с параметрическими коэффициентами. Из этих условий следует, что

(xii) существует подпоследовательность $v_{i_0}, v_{i_1}, \ldots, v_{i_M}$ последовательности $v_0, v_1, \ldots, v_N$, такая, что $0 = i_0 < i_1 < \ldots < i_M = N$,

(xiii) вершина $v_{i_{j+1}}$ является сыном вершины v_{i_j} при $0 \leqslant j \leqslant M-1$.

Обозначим через $\mathcal{M}_{i,j}$ число битовых операций, необходимых для того, чтобы вычислить $w_{i,j+1}$ или выяснить, что $M_i = j$, при условии, что все вершины $w_{u,v}$ и константы $\beta_{u,v}$, $(u,v) \in J_{i,j}$, известны, см. п. (vi), (vii). Предположим, что для любой точки $a^* \in \mathbb{A}^\nu(\overline{k})$ и любых i, j, где $1 \leqslant i \leqslant N$, $0 \leqslant j \leqslant M_i$, мы имеем

$$\sum_{1 \leqslant i \leqslant N} M_i \leqslant \mathcal{N} \quad \text{и} \quad \mathcal{M}_{i,j} \leqslant \mathcal{M} \tag{63}$$

для некоторых целых чисел $\mathcal{N}, \mathcal{M} \geqslant 1$.

Алгоритм $\widetilde{\Omega}$ определён на $\mathbb{A}^\nu(\overline{k})$ и $v_N \in L(T)$ тогда и только тогда, когда $a^* \in \mathcal{S}(T)$. Напомним, что $\mathcal{S}(T) \subset \mathbb{A}^\nu(\overline{k})$ является конструктивным множеством. Пусть $K \supset k$ – произвольное поле. Тогда при помощи расширения скаляров можно определить алгоритм $\widetilde{\Omega}$ на $\mathbb{A}^\nu(\overline{K})$ естественным образом (мы оставляем подробности читателю). Это расширение алгоритма $\widetilde{\Omega}$ будет обозначаться снова через $\widetilde{\Omega}$. Конечно, многозначное дерево вычислений T при этом расширении скаляров остаётся тем же самым. Еще отметим, что, используя рекурсию по (i,j), легко доказать, что для всякой точки $b^* \in \mathbb{A}^\nu(\overline{K})$ существует точка $a^* \in \mathbb{A}^\nu(\overline{k})$, такая, что последовательности $v_1, \ldots, v_N$, все вершины $w_{u,v}$ и булевы значения $\beta_{u,v}$ $(u,v) \in J_{N,M_N}$, соответствующие b^*

и a^*, совпадают. Это следует из того, что для всякой пары (i,j) конструктивное множество, заданное условием $\bigwedge_{(u,v)\in J_{i,j}}(\mathcal{A}_{w_{u,v}} = \beta_{u,v})$ (см. выше), определено над полем $\overline{k}$.

Для этого расширения алгоритма $\widetilde{\Omega}$ мы имеем $v_N \in L(T)$ в том и только в том случае, если $b^* \in \mathcal{S}(T)(\overline{K})$.

Пусть V_i (для некоторого $i \in I$) – равноразмерностное алгебраическое многообразие из леммы 18. Положим $K_i = k(t_1,\dots,t_{\nu-s})[\eta_i]$, см. (62). Сейчас K_i является конечномерной сепарабельной алгеброй над полем $k(t_1,\dots,t_{\nu-s})$.

Для всякого ненулевого элемента $z \in K_i$ можно выяснить, верно ли, что z является делителем нуля в K_i, вычисляя норму $N_{K_i/k(t_1,\dots,t_{\nu-s})}(z)$ как определитель матрицы $k(t_1,\dots,t_{\nu-s})$-линейного отображения $K_i \to K_i$, $a \mapsto za$, в базисе η_i^j, $0 \leqslant j < \deg\Phi_i$, алгебры K_i над $k(t_1,\dots,t_{\nu-s})$.

Для всякого полинома $\varphi_{v,j}$ (см. (57)) существует единственный полином $\phi_{v,j} \in k[a_1,\dots,a_\nu]$, такой, что $\phi_{v,j}(a_1^{p^r},\dots,a_\nu^{p^r}) = \varphi_{v,j}^{p^r}$.

Пусть $c = (c_1,\dots,c_\nu) \in \mathbb{A}^\nu(K_i^{1/p^r})$ – произвольная точка. Пусть v – вершина дерева T.

Положим $\mathcal{A}_{K_i,v}(c) = \mathrm{true}$ в том и только в том случае, если $\mathcal{A}_v(c) = \mathrm{true}$ и для всякого j, где $1 \leqslant j \leqslant \mu_{v,2}$, либо $\phi_{v,j}(c_1^{p^r},\dots,c_\nu^{p^r}) = 0$, либо $\phi_{v,j}(c_1^{p^r},\dots,c_\nu^{p^r})$ не является делителем нуля в K_i.

Положим $\mathcal{A}_{K_i,v}(c) = \mathrm{false}$ в том и только в том случае, если $\mathcal{A}_v(c) = \mathrm{false}$ и для всякого j, где $1 \leqslant j \leqslant \mu_{v,2}$, либо $\phi_{v,j}(c_1^{p^r},\dots,c_\nu^{p^r}) = 0$, либо $\phi_{v,j}(c_1^{p^r},\dots,c_\nu^{p^r})$ не является делителем нуля в K_i.

Положим $\mathcal{A}_{K_i,v}(c) = \mathrm{undefined}$ в том и только в том случае, если существует целое число j, такое, что $1 \leqslant j \leqslant \mu_{v,2}$ и $\phi_{v,j}(c_1^{p^r},\dots,c_\nu^{p^r}) \neq 0$ является делителем нуля в K_i.

Теперь мы собираемся описать модифицированную версию $\widetilde{\Omega}_{K_i}$ алгоритма $\widetilde{\Omega}$. Алгоритм $\widetilde{\Omega}_{K_i}$ имеет область входных данных $\mathbb{A}^\nu(K_i^{p^{-r}})$. Пусть $c \in \mathbb{A}^\nu(K_i^{p^{-r}})$. Заменим в условиях (i)–(xi), относящихся к $\widetilde{\Omega}$, для всякой вершины w дерева T, появляющейся в этих условиях (это может быть $v_1,\dots,v_N$, $w_{u,v}$ и т.д.), булевы значения $\mathcal{A}_w(a^*)$ на $\mathcal{A}_{K_i,w}(c)$. Обозначим через (i)′–(x)′ вновь полученные утверждения. Например, в этих новых утверждениях (i)′–(xi)′ имеем $\beta_{u,v} = \mathcal{A}_{K_i,w_{u,v}}(c)$.

Для входа c алгоритм $\widetilde{\Omega}_{K_i}$ строит вершины $v_1, v_2, \ldots, v_i$ и $w_{u,v}$ дерева T согласно п. (i)′–(xi)′ до тех пор, пока $\beta_{u,v} \in \{\text{true}, \text{false}\}$. Если получится, что $\beta_{u,v} = \text{undefined}$, то алгоритм находит многочлен $\phi_{w_{u,v},j}$, такой, что $\phi_{w_{u,v},j}(c_1^{p^r}, \ldots, c_\nu^{p^r}) \neq 0$ является делителем нуля в K_i, и заканчивает свою работу. Таким образом, для входа c алгоритм $\widetilde{\Omega}_{K_i}$ имеет один из следующих выходов:

(a) построена требуемая последовательность вершин $v_1, \ldots, v_N$ согласно (i)′–(x)′,

(b) найден делитель нуля $\phi_{w_{u,v},j}(c_1^{p^r}, \ldots, c_\nu^{p^r}) \neq 0$ в K_i для некоторых u, v, j.

Сепарабельная алгебра K_i является прямым произведением полей. Пусть L – произвольный множитель из этого произведения, и пусть $\pi : K_i \to L$ – естественная проекция на этот множитель. Положим $\pi(c) = (\pi(c_1), \ldots, \pi(c_\nu)) \in \mathbb{A}^\nu(\overline{L})$. Предположим, что последовательность $v_1, \ldots, v_N$ вершин дерева T является выходом (см. (a)) алгоритма $\widetilde{\Omega}_{K_i}$ для входа c. Тогда, очевидно, та же самая последовательность $v_1, \ldots, v_N$ является выходом алгоритма $\widetilde{\Omega}$ для входа $\pi(c)$.

Предположим, что получен выход (b). Тогда (ср. с доказательством леммы 18) можно получить представление

$$\phi_{w_{u,v},j}(c_1^{p^r}, \ldots, c_\nu^{p^r}) = \sum_{0 \leqslant u < \deg \Phi_i} c_u \eta_i^u,$$

где $c_u \in k(t_1, \ldots, t_{\nu-s})$, и вычислить полиномы

$$\Phi_i' = \mathrm{G\,C\,D}\,(\Phi_i, \sum_{0 \leqslant u < \deg \Phi_i} c_u Z^i) \quad \text{и} \quad \Phi_i'' = \Phi_i / \Phi_i'.$$

Мы имеем $\deg_Z \Phi_i' \geqslant 1$ и $\deg_Z \Phi_i'' \geqslant 1$. Следовательно, можно получить представление $V_i = V_i' \cup V_i''$, где V_i' и V_i'' являются объединениями неприводимых компонент алгебраического многообразия V_i, для всякой неприводимой компоненты E многообразия V_i мы имеем $E \not\subset V' \cap V''$ и (ср. (62)) существуют гомоморфизмы сепарабельных алгебр

$$\xi_i' : (k^{p^{-r}}[V_i'])^{p^r} \to k(t_1, \ldots, t_{\nu-s})[Z]/(\Phi_i') = k(t_1, \ldots, t_{\nu-s})[\eta_i'] = K_i',$$

$$\xi_i'' : (k^{p^{-r}}[V_i''])^{p^r} \to k(t_1, \ldots, t_{\nu-s})[Z]/(\Phi_i'') = k(t_1, \ldots, t_{\nu-s})[\eta_i''] = K_i''.$$

Здесь $\eta_i' = Z \bmod \Phi_i'$ (соответственно $\eta_i'' = Z \bmod \Phi_i''$). Мы имеем $\xi'(\overline{a}_u^{p^r}) = \xi(\overline{a}_u^{p^r}) \bmod \Phi_i'$ (соответственно $\xi''(\overline{a}_u^{p^r}) = \xi(\overline{a}_u^{p^r}) \bmod \Phi_i''$) для

$1 \leqslant i \leqslant \nu$. В правой части последнего равенства $\overline{a}_u \in k^{p^{-r}}[V_i]$, а в левой части $\overline{a}_u \in k^{p^{-r}}[V_i']$ (соответственно $\overline{a}_u \in k^{p^{-r}}[V_i']$), см. формулировку леммы 18. Гомоморфизм ξ_i' (соответственно ξ_i'') индуцирует изоморфизм полного кольца частных алгебры $(k^{p^{-r}}[V_i'])^{p^r}$ и $k(t_1, \ldots, t_{\nu-s})[\eta_i']$ (соответственно полного кольца частных алгебры $(k^{p^{-r}}[V_i''])^{p^r}$ и $k(t_1, \ldots, t_{\nu-s})[\eta_i'']$). Мы имеем $K_i = K_i' \times K_i''$. Обозначим через $\pi' : K_i \to K_i'$ и $\pi'' : K_i \to K_i'$ естественные проекции. Положим $\pi'(c) = (\pi'(c_1), \ldots, \pi'(c_\nu))$ и $\pi''(c) = (\pi''(c_1), \ldots, \pi''(c_\nu))$.

Мы собираемся описать алгоритм $\overline{\Omega}_{K_i}$ с областью входных данных $\mathbb{A}^\nu(K_i^{p^{-r}})$. Для всякой точки $c \in \mathbb{A}^\nu(K_i^{p^{-r}})$ на выходе алгоритма $\overline{\Omega}_{K_i}$ мы получаем семейство подалгебр $K_{i,j}$, $j \in J_i$, алгебры K_i, такое, что $K_i = \prod_{j \in J_i} K_{i,j}$. Каждая подалгебра имеет вид

$$K_{i,j} = k(t_1, \ldots, t_{\nu-s})[Z]/(\Phi_{i,j}) = k(t_1, \ldots, t_{\nu-s})[\eta_{i,j}],$$

где многочлен $\Phi_{i,j}$ делит Φ_i и $\eta_{i,j} = Z \bmod \Phi_{i,j}$. Обозначим через $\pi_{i,j} : K_i \to K_{i,j}$ естественные проекции. Положим

$$\pi_{i,j}(c) = (\pi_{i,j}(c_1), \ldots, \pi_{i,j}(c_\nu))$$

для всякого $j \in J_i$. Далее, для всякого $j \in J_i$ на выходе алгоритма $\overline{\Omega}_{K_i}$ мы получаем дополнительно последовательность вершин $v_{j,1}, \ldots, v_{j,N_j}$, такую, что она является выходом алгоритма $\widetilde{\Omega}_{K_{i,j}}$ для входа $\pi_{i,j}(c)$. Помимо этого, можно представить v_i в виде $V_i = \bigcup_{j \in J_i} V_{i,j}$, где $V_{i,j}$ является объединением неприводимых компонент алгебраического многообразия V_i и для всякого $j \in J_i$ строится гомоморфизм k-алгебр

$$\xi_{i,j} : (k^{p^{-r}}[V_{i,j}])^{p^r} \to k(t_1, \ldots, t_{\nu-s})[\eta_{i,j}], \tag{64}$$

индуцирующий изоморфизм полного кольца частных алгебры $(k^{p^{-r}}[V_{i,j}])^{p^r}$ и $k(t_1, \ldots, t_{\nu-s})[\eta_{i,j}]$ и такой, что

$$\xi_{i,j}(\overline{a}_u^{p^r}) = \xi_i(\overline{a}_u^{p^r}) \bmod \Phi_i$$

для $1 \leqslant i \leqslant \nu$. В правой части последнего равенства $\overline{a}_u \in k^{p^{-r}}[V_i]$, а в левой части $\overline{a}_u \in k^{p^{-r}}[V_{i,j}]$, см. формулировку леммы 18.

Алгоритм $\overline{\Omega}_{K_i}$ рекурсивен по размерности $\dim K_i$ над полем $k(t_1, \ldots, t_{\nu-s})$. Опишем шаг рекурсии. Пусть $c \in \mathbb{A}^\nu(K_i^{p^{-r}})$. Тогда мы применяем алгоритм $\widetilde{\Omega}_{K_i}$ к этому входу c. Если получается выход (а), т.е., построена последовательность $v_1, \ldots, v_N$ вершин дерева T, то положим $J_i = \{j^*\}$ (здесь можно выбрать или создать элемент

$j^* = j(K_i)$, зависящий от K_i; например, можно положить $j^* = \{K_i\}$), $N_i = N$, $v_{j^*,j} = v_j$, $1 \leqslant j \leqslant N_i$.

Если K_i является полем, то обязательно получается выход (a), так что для базы рекурсии алгоритм описан.

Предположим, что получается выход (b). Тогда мы получаем представления $K_i = K_i' \times K_i''$, $V_i = V_i' \cup V_i''$, см. выше. Мы рекурсивно применяем алгоритм $\widetilde{\Omega}_{K_i'}$ к $\pi'(c)$. На выходе алгоритма $\overline{\Omega}_{K_i'}$ получаем семейство подалгебр $K_{i,j}'$, $j \in J_i'$, алгебры K_i', такое, что $K_i' = \prod_{j \in J_i} K_{i,j}'$. Далее, для всякого $j \in J_i'$ на выходе алгоритма $\overline{\Omega}_{K_i'}$ мы получаем дополнительно последовательность вершин $v_{j,1}, \ldots, v_{j,N_j}$, такую, что она является выходом алгоритма $\widetilde{\Omega}_{K_{i,j}'}$ для входа $\pi_{i,j}'(c)$. Кроме того, можно получить представление $V_i' = \bigcup_{j \in J_i'} V_{i,j}$ и построить гомоморфизмы $\xi_{i,j}$, $j \in J_i'$, такие, что рекурсивно выполняются требуемые свойства для V_i', J_i' (вместо V_i, J_i).

Аналогично мы рекурсивно применяем алгоритм $\widetilde{\Omega}_{K_i''}$ к $\pi''(c)$. На выходе алгоритма $\overline{\Omega}_{K_i''}$ мы получаем семейство подалгебр $K_{i,j}''$, $j \in J_i''$, алгебры K_i'', такое, что $K_i'' = \prod_{j \in J_i} K_{i,j}''$. Далее, для всякого $j \in J_i''$ на выходе алгоритма $\overline{\Omega}_{K_i''}$ мы получаем дополнительно последовательность вершин $v_{j,1}, \ldots, v_{j,N_j}$, такую, что она является выходом алгоритма $\widetilde{\Omega}_{K_{i,j}''}$ для входа $\pi_{i,j}''(c)$. Кроме того, можно получить представление $V_i'' = \bigcup_{j \in J_i''} V_{i,j}$ и построить гомоморфизмы $\xi_{i,j}$, $j \in J_i''$, такие, что рекурсивно выполняются требуемые свойства для V_i'', J_i'' (вместо V_i, J_i).

Мы будем предполагать без ограничения общности, что $J_i' \cap J_i'' = \varnothing$. Теперь достаточно положить $J_i = J_i' \cup J_i''$. Алгоритм $\overline{\Omega}_{K_i}$ описан.

Положим

$$c^{(i)} = (c_1^{(i)}, \ldots, c_\nu^{(i)}) = (\xi_i(\overline{a}_1^{p^r})^{1/p^r}, \ldots, \xi_i(\overline{a}_\mu^{p^r})^{1/p^r}) \in \mathbb{A}^\nu(K_i^{p^{-r}}))$$

для всякого $i \in I$, см. лемму 18 (здесь r зависит от i).

Лемма 19. *В условиях леммы* 18 *предположим, что* $V \subset \mathcal{S}(T)$. *Тогда, применяя лемму* 18 *и после этого алгоритм* $\overline{\Omega}_{K_i}$ *к точке* $c^{(i)}$, *можно построить разложение* $V_i = \bigcup\limits_{j \in J_i} V_{i,j}$. *Для всякого* $j \in J_i$ *можно построить гомоморфизм* (64) *и вершину* $\gamma(i,j) \in \Gamma = L(T)$ *(зависящую от* i *и* j*) со всеми её предками в* T, *такую, что*

$$\dim V_{i,j} \setminus \mathcal{W}_{\gamma(i,j)} < \dim V_{i,j}$$

и, следовательно, $\dim V_{i,j}\cap\mathcal{W}_{\gamma(i,j)} = \dim V_{i,j}$ *и* $\dim V_i\cap\mathcal{W}_{\gamma(i,j)} = \dim V_i$.

Выберем такое i, *что* $\dim V_i = \dim V$. *Тогда, таким образом, можно построить вершину* $\gamma_0 \in \Gamma$, *для которой* $\dim V \cap \mathcal{W}_{\gamma_0} = \dim V$.

Время работы алгоритма для построения всех $\gamma(i,j)$ *с соответствующими гомоморфизмами* (64) (*и, следовательно,* γ_0) *полиномиально от* $\mathcal{N}$, $\mathcal{M}$, M, M_1, d_1^{l+1}, $D^{\nu(\overline{c}+l+1)}$.

Доказательство. Это уже доказано. □

Лемма 20. *В условиях леммы* 19 *предположим, что для всякого* $\gamma \in \Gamma = L(T)$ *мы имеем* $\deg_{a_1,\dots,a_\nu} \psi_{\gamma,j}^{(i)} \leqslant D$ *при* $1 \leqslant j \leqslant m_{\gamma,i}$, $i = 1,2$ (*см.* (61)), *где* D – *из утверждения леммы* 18. *Тогда, применяя леммы* 19 *и* 18 *к многообразиям* $V \cap \bigcap\limits_{\gamma''\in\Gamma_2} \mathcal{W}_{\gamma''}^{(2)} \setminus \bigcup\limits_{\gamma'\in\Gamma_1} \mathcal{W}_{\gamma'}^{(1)}$ *для некоторых* $\gamma', \gamma'' \in \Gamma$ *и затем следствия* 3–6, *можно построить покрытие* $\bigcup\limits_{\gamma\in\Gamma_0} \mathcal{W}_\gamma \supset V$ *и стратификацию* $\{V \cap \mathcal{W}_\beta\}_{\beta\in B}$ *алгебраического многообразия* V, *такие, что* $\#\Gamma_0 \leqslant \delta(V,D)$ *и* $\#B < 2^{c+1}D^{(2\nu-c)(c+1)/2}$, *см. лемму* 17. *Более того, для всякой вершины* $\beta \in B$ *можно построить вершину* $\gamma(\beta) \in \Gamma_0$, *такую, что* $\mathcal{W}_\beta \subset \mathcal{W}_{\gamma(\beta)}$, *и для всякой вершины* $\gamma \in \Gamma_0$ *построить всех её предков* J_γ *в дереве* T. *Очевидно, поддерево* T' *многозначного дерева вычислений* T *с множеством вершин* $\Gamma_0 \cup \bigcup\limits_{\gamma\in\Gamma_0} J_\gamma$ *является несократимым.*

Время работы алгоритма для построения множества Γ_0 *и семейства* $\{\mathcal{W}_\beta\}_{\beta\in B}$ *полиномиально от* $\mathcal{N}$, $\mathcal{M}$, M, M_1, d_1^{l+1}, $D^{\nu(\overline{c}+l+1)}$.

Доказательство. По лемме 19 мы можем применить следствие 4 и построить семейство $\{\mathcal{W}_\beta\}_{\beta\in B'}$, такое, что $\{V\cap\mathcal{W}_\beta\}_{\beta\in B'}$ является стратификацией многообразия V (здесь мы меняем обозначение B из следствия 4 на B'). Более того, для всякого $\beta \in B'$ мы находим вершину $\gamma'(\beta) \in \Gamma$, такую, что $\mathcal{W}_{\gamma'(\beta)} \supset \mathcal{W}_\beta$. Положим $\Gamma' = \{\gamma'(\beta) : \beta \in B'\}$. По следствию 6 мы имеем $\#\Gamma' \leqslant \#B' < 2^{c+1}D^{(2\nu-c)(c+1)/2}$. Сверх того, для всякой вершины $\gamma \in \Gamma'$ мы строим множество всех ее предков в дереве T.

Затем, применяя следствие 5, мы строим подмножество $\Gamma_0 \subset \Gamma'$, такое, что $\#\Gamma_0 \leqslant \delta(V,D)$. Наконец, применяя следствие 3 к Γ_0 вместо Γ, мы строим семейство $\{\mathcal{W}_\beta\}_{\beta\in B}$ с числом элементов

$\#B < 2^{c+1}D^{(2\nu-c)(c+1)/2}$, такое, что $\{V \cap \mathcal{W}_\beta\}_{\beta\in B}$ является стратификацией алгебраического многообразия V, и для всякого $\beta \in B$ строим вершину $\gamma(\beta) \in \Gamma_0$, такую, что $\mathcal{W}_{\gamma(\beta)} \supset \mathcal{W}_\beta$. Лемма доказана. □

§12. Доказательство теоремы 2

Пусть f – семейство коэффициентов из $k[a_1, \dots, a_\nu]$ всех многочленов $f_0, \dots, f_{m-1}$. Напомним, что для доказательства модифицированной теоремы 1 (для покрытия пространства параметров) мы вводим многозначный лес вычислений $T_1 = \{T_{1,n,d_0,\dots,d_{m-1}}\}$, после этого рассматриваем многозначное дерево вычислений $T_{1,n,d_0,\dots,d_{m-1}}(f)$ и, наконец, несократимое многозначное дерево вычислений $T'_{1,n,d_0,\dots,d_{m-1}}(f)$, см. конец раздела 7. В настоящей статье для упрощения обозначений мы изменим их. Именно, мы будем обозначать $T_{1,n,d_0,\dots,d_{m-1}}$ и $T'_{1,n,d_0,\dots,d_{m-1}}(f)$ через $T_{n,d_0,\dots,d_{m-1}}$ и $T'_{n,d_0,\dots,d_{m-1}}(f)$ соответственно[1]. Но обозначение $T_1 = \{T_{n,d_0,\dots,d_{m-1}}\}_{\forall n,d_0,\dots,d_{m-1}}$ для леса вычислений остаётся тем же самым.

Более точно (в новых обозначениях), пусть $\alpha \in L(T_{n,d_0,\dots,d_{m-1}})$ – произвольный лист. Тогда семёрка $\mathcal{Q}_\alpha$ (или выход) соответствует α (напомним, что сейчас $m_\alpha = 2$), см. раздел 7. Листья деревьев $T_{n,d_0,\dots,d_{m-1}}$ и $T_{n,d_0,\dots,d_{m-1}}(f)$ находятся во взаимно однозначном соответствии. Таким образом, мы отождествляем

$$L(T_{n,d_0,\dots,d_{m-1}}) \quad \text{и} \quad L(T_{n,d_0,\dots,d_{m-1}}(f)).$$

Обозначим через $\mathcal{Q}_\alpha(f)$ семёрку (или выход), соответствующую листу $\alpha \in L(T_{n,d_0,\dots,d_{m-1}}(f))$. Очевидно,

$$L(T'_{n,d_0,\dots,d_{m-1}}(f)) \subset L(T_{n,d_0,\dots,d_{m-1}}(f)).$$

Если $\alpha \in L(T'_{n,d_0,\dots,d_{m-1}}(f))$, то выход $\mathcal{Q}_\alpha(f)$ соответствует листу α в дереве $T'_{n,d_0,\dots,d_{m-1}}(f)$.

Далее, для всякой точки $a^* \in \mathcal{W}_\alpha$ мы имеем

$$\mathcal{Q}_{a^*} = \mathcal{Q}_\alpha(f)|_{a_1=a_1^*,\dots,a_\nu=a_\nu^*}$$

в обозначениях из раздела 7 работы [9]. Рассматривая дерево $T'_{n,d_0,\dots,d_{m-1}}(f)$, мы доказываем модифицированную теорему 1 (для

[1]Предпоследний абзац раздела 7 в [9] сразу перед списком литературы содержит небольшие очевидные опечатки, относящиеся к этим первоначальным обозначениям. Там мы забыли три закрывающие скобки.

случая покрытия множества $\mathcal{U}_c$; мы имеем $\mu_\alpha = 2$ для всякого α). После этого теорема 1 (для случая стратификации множества $\mathcal{U}_c$) немедленно выводится из модифицированной теоремы 1 с использованием леммы 17 (теперь каждое μ_α ограничено сверху величиной $(d' D_{n-c'}^{O(1)})^\nu$ и α не является листом дерева $T'_{n,d_0,\dots,d_{m-1}}(f)$; оно получается согласно лемме 17).

Пусть s – целое число, такое, что $c' \leqslant s \leqslant \min\{c, n-1\}$, см. введение. Также обозначим через $T^{(s)}_{n,d_0,\dots,d_{m-1}}$ некоторое минимальное многозначное дерево вычислений $T_{n,d_0,\dots,d_{m-1}}$, удовлетворяющее следующему свойству. Для всякого листа $\alpha \in L(T_{n,d_0,\dots,d_{m-1}})$ существует лист $v \in L(T^{(s)}_{n,d_0,\dots,d_{m-1}})$, такой, что α является потомком листа v и все объекты из пятёрки $\mathcal{Q}_{\alpha,s}$ (см. конец раздела 7) вычисляются в вершинах дерева $T^{(s)}_{n,d_0,\dots,d_{m-1}}$. Уровень дерева $T^{(s)}_{n,d_0,\dots,d_{m-1}}$ ограничен величиной $D_{n-s}^{O(1)}$, см. раздел 7. Пусть $N_s = l(T^{(s)}_{n,d_0,\dots,d_{m-1}})$ – уровень дерева $T^{(s)}_{n,d_0,\dots,d_{m-1}}$. Мы будем предполагать без ограничения общности, что для всякого листа $v \in T^{(s)}_{n,d_0,\dots,d_{m-1}}$ его уровень $\mathrm{l}(v)$ равен N_s.

В вершинах дерева $T_{n,d_0,\dots,d_{m-1}}(f)$ (а значит, и $T'_{n,d_0,\dots,d_{m-1}}(f)$) вычисляются некоторые определители. Теперь утверждение (b) теоремы 2 следует непосредственно из конструкции из работы [9], см. также замечание из введения работы [9] об оценках длин записи целых коэффициентов определителей (мы оставляем подробности читателю). Таким образом, утверждение (b) доказано.

Пусть v – вершина дерева $T^{(s)}_{n,d_0,\dots,d_{m-1}}(f)$. Положим

$$T = T^{(s)}_{n,d_0,\dots,d_{m-1}}(f).$$

Теперь мы используем обозначения из раздела 11. Напомним (см. [9, конец раздела 7]), что степени относительно $a_1, \dots, a_\nu$ всех многочленов из семейств $\psi_v^{(1)}$, $\psi_v^{(2)}$ (см. (61), (60)) ограничены сверху величиной $D_{n-s}^{O(1)}$. Обозначим через $(\mathrm{a}_{s,v})$ утверждение (a) теоремы 2 с (s, v) вместо (c', α). Таким образом, утверждение $(\mathrm{a}_{s,v})$ относится ко всем полиномам из семейств $\psi_v^{(1)}$ и $\psi_v^{(2)}$. Теперь из определений и конструкции,

описанной в [5,8,9], немедленно вытекает, что утверждение $(\mathrm{a}_{s,v})$ справедливо для полиномов $\varphi_{v,1},\dots,\varphi_{v,\mu'_{v,2}}$ вместо $\psi^{(\beta)}_{v,1},\dots,\psi^{(\beta)}_{v,m_{v,\beta}}$. Следовательно, согласно определению семейств $\psi^{(1)}_v$, $\psi^{(2)}_v$ и поскольку уровень дерева $T^{(s)}_{n,d_0,\dots,d_{m-1}}(f)$ ограничен величиной $D^{O(1)}_{n-s}$, справедливо утверждение $(\mathrm{a}_{s,v})$. Таким образом, утверждение (a) модифицированной теоремы 2 доказано. Утверждение (a) теоремы 2 немедленно следует из утверждения (a) модифицированной теоремы 2 и теоремы 3.

Остаётся доказать утверждение (c). Алгоритм $\widetilde{\Omega}$, удовлетворяющий условиям (i)–(xi) из раздела 11 для дерева $T = T_{n,d_0,\dots,d_{m-1}}(f)$, описан в [8, 9]. При этом $\mathcal{N}$ ограничено сверху величиной $D^{O(1)}_{n-c'}$ и $\mathcal{M}$ ограничено сверху полиномом от D, $(d')^\nu$, $(d'')^{l+1}$, $(d''')^{l+1}$, M_1, M_2 и m (напомним, что D определено во введении статьи [8]). Это немедленно следует из конструкции, описанной в [8,9]. Теперь, применяя лемму 20, мы доказываем утверждение (c). Теорема 2 и её модифицированная версия (для случая покрытия) доказаны.

§13. Проблемы и замечания, относящиеся к полученным результатам

1. Напомним, что $\omega(\mu, \mathbb{A}^\mu(\overline{k}), D) < 2^{\mu+1}D^{\mu(\mu+1)/2}$ по следствию 6. Интересно, можно ли доказать более сильную версию леммы 17 для $V = \mathbb{A}^\mu(\overline{k})$. Именно, верно ли, что в утверждении (e) леммы 17 можно заменить верхнюю границу $\omega(\mu, \mathbb{A}^\mu(\overline{k}), D)$ на $D^{O(\mu)}$.

2. Напомним, что в условиях леммы 17 с $V = \mathbb{A}^\mu(\overline{k})$ множество $\Gamma_0 \subset \Gamma$ определяет покрытие $\bigcup_{\gamma\in\Gamma_0}\mathcal{W}_\gamma = \mathbb{A}^\mu(\overline{k})$ с числом элементов $\#\Gamma_0 \leqslant (D^{\mu+1}-1)/(D-1)$. Если использовать вероятностные алгоритмы, то можно построить это подмножество $\Gamma_0 \subset \Gamma$ за время, полиномиальное от $D^{\mu(\mu+1)/2}$. Интересно, верно ли, что, используя вероятностные алгоритмы, можно построить такое подмножество Γ_0 за время, полиномиальное от длины записи входных данных и D^μ.

3. Алгоритм для факторизации многочленов с параметрическими коэффициентами использует деревья вычислений почти до самого конца. Именно (см. подробности в [6]), пространство $\mathbb{A}^1(\overline{k}) \times \mathbb{A}^\nu(\overline{k})$ стратифицируется, и эта стратификация возникает из дерева вычислений. Затем мы рассматриваем проекцию $\mathbb{A}^1(\overline{k}) \times \mathbb{A}^\nu(\overline{k}) \to \mathbb{A}^\nu(\overline{k})$ и получаем

покрытие пространства параметров $\mathbb{A}^\nu(\overline{k})$. Следовательно, это покрытие может быть построено с помощью многозначного дерева вычислений (хотя мы и не отмечаем это явно в [6]). И только после этого можно применить лемму 17, для того чтобы получить требуемую стратификацию пространства параметров $\mathbb{A}^\nu(\overline{k})$.

Интересно выяснить, верно ли, что можно разложить на множители многочлен с параметрическими коэффициентами, используя только обычные деревья вычислений в смысле [5] (конечно, не всякое многозначное дерево вычислений является обычным), и получить в теореме 1 раздела 8 лучшую оценку сверху $\#A = (d'd^{O(1)})^\nu$ на число стратов, применяя теорему 1 работы [5].

4. Та же самая проблема имеется в конструкции для решения систем полиномиальных уравнений с параметрическими коэффициентами. Возможно ли решать системы полиномиальных уравнений с параметрическими коэффициентами, используя только обычные деревья вычислений (по крайней мере, в случае разложения на равноразмерностные алгебраические многообразия)? Если это возможно, то можно надеяться получить в теореме 1 раздела 9 лучшую верхнюю оценку $\#A = (d' D_{n-c'}^{O(1)})^\nu$ на число стратов, применяя теорему 1 из работы [5].

5. Можно доказать некоторые версии теорем 1 и 2 раздела 9 с более тонкой стратификацией (соответственно покрытием). Мы будем обозначать её по-прежнему через $\mathcal{W}_\alpha$, $\alpha \in A$. Теперь дополнительно выполняется следующее условие.

(xiv) Для всякого $\alpha \in A$, для всех целых чисел s, r, удовлетворяющих неравенствам $c' \leqslant s \leqslant \min\{c, n-1\}$, $0 \leqslant r \leqslant \rho_s$, для всякого $j \in J_{\alpha,s,r}$ строятся индексы $i_{j,0}, \ldots, i_{j,s}$ и линейная форма $L_j \in \mathcal{L}'_s$, такие, что $0 \leqslant i_{j,0} < \ldots < i_{j,s} \leqslant n$ и для всякой точки $a^* \in \mathcal{W}_\alpha$, для всякого $\xi \in \Xi_{j,a^*}$ морфизм

$$W_{j,a^*,\xi} \to \mathbb{P}^s(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (X_{i_{j,0}} : \ldots : X_{i_{j,s}}),$$

является конечным доминантным сепарабельным (см. определения в разделе 4). Далее, обозначим через $\Phi'_{j,a^*,\xi} \in \overline{k}[X_{i_{j,0}}, \ldots, X_{i_{j,s}}, Z]$ неприводимый над k многочлен, такой, что $\Phi'_{j,a^*,\xi}(X_{i_{j,0}}, \ldots, X_{i_{j,s}}, L_j)$ обращается в нуль тождественно на алгебраическом многообразии $W_{j,a^*,\xi}$. Тогда

$$\deg_Z \Phi'_{j,a^*,\xi} = \deg W_{j,a^*,\xi} = \deg \Phi_j.$$

Для того чтобы получить формулировки новых версий теорем 1 и 2 раздела 9, следует заменить в формулировках этих теорем “(i)–(xiii)” на “(i)–(xiv)” и “(ii)–(xiii)” на “(ii)–(xiv)”. При этом в замечании 2 (см. введение в [8]) следует также заменить “(i)–(xiii)” на “(i)–(xiv)” и “(ii)–(xiii)” на “(ii)–(xiv)”. Доказательства этих новых версий рассматриваемых теорем аналогичны доказательствам исходных версий и оставляются заинтересованному читателю.

6. Напомним, что в замечании 3 из введения статьи [8] мы описали, как изменить (8), (9), (11)–(14). Сейчас мы хотели бы уточнить это замечание. Можно изменить определения множеств линейных форм $\mathcal{M}_\varkappa$ и $\mathcal{M}'_{s,\varkappa}$ следующим образом.

Если $\mathrm{char}(k) = 0$, то мы выбираем простое число q, удовлетворяющее условию $q = D_{n-s}^{O(1)}$ с подходящей константой в $O(...)$, которая может быть вычислена явно. Пусть $\{0, 1, \dots, q-1\} \subset \mathbb{Z}$. Для всякого целого числа a положим $\overline{a} \in \{0, 1, \dots, q-1\}$ равным представителю вычета a по модулю q. В определениях множеств $\mathcal{M}_\varkappa$ и $\mathcal{M}'_{s,\varkappa}$ (см. формулу (5) из введения работы [8]) мы заменяем везде γ на $\overline{\gamma}$. Обозначим полученные множества линейных форм вновь через $\mathcal{M}_\varkappa$ и $\mathcal{M}'_{s,\varkappa}$.

Если $\mathrm{char}(k) = p > 1$ и $l > 0$, то мы выбираем неприводимый многочлен $q \in k_0[\tau_1]$ степени $\deg_{\tau_1} q = O(\log_p(D_{n-s})/\varepsilon$ (напомним, что $\#k_0 = p^\varepsilon$) с подходящей константой в $O(...)$, которая может быть вычислена явно. Для всякого многочлена $a \in k_0[\tau_1]$ положим $\overline{a} \in \sum_{0 \leqslant j < \deg q} k_0 \tau_1^j \subset k_0[\tau_1]$ равным представителю вычета a по модулю q. Мы выбираем все подмножества $\mathcal{I}_\varkappa \subset k_0[\tau_1] \setminus \{0\}$. В определениях множеств $\mathcal{M}_\varkappa$ и $\mathcal{M}'_{s,\varkappa}$ (см. формулу (5) из введения работы [8]) мы заменяем везде γ на $\overline{\gamma}$. Мы обозначаем полученные множества линейных форм вновь через $\mathcal{M}_\varkappa$ и $\mathcal{M}'_{s,\varkappa}$.

С такими модифицированными множествами линейных форм $\mathcal{M}_\varkappa$ и $\mathcal{M}'_{s,\varkappa}$ (и, следовательно, модифицированными $\mathcal{L}_s$, $\mathcal{L}'_s$) теоремы 1 и 2 раздела 9 справедливы с c вместо c^2 в (8), (9), (11)–(14). То же самое справедливо для версий этих теорем из замечания 5 этого раздела, см. выше. Доказательства получаются непосредственно и оставляются читателю.

7. Пусть $\nu = 0$. Тогда A является одноэлементным множеством и мы обозначаем $J_{\alpha,s,r} = J_{s,r}$, $V_{a^*,s,r} = V_{s,r}$, где $a^* = 0 \in \mathbb{A}^0(\overline{k}) = \{0\}$ для всех s, r.

Пусть поле $k = k_0(\tau_1, \dots, \tau_l)[\tau_{l+1}]$ – из введения. Из конструкции, описанной в [8,9], можно получить алгоритм, который для всяких s, r,

таких, что $c' \leqslant s \leqslant \min\{c, n-1\}$, $0 \leqslant r \leqslant \rho_s$, строит разложение многообразия $V_{s,r}$ в объединение неприводимых над полем $k^{p^{-r}}$ компонент. Именно, множество неприводимых над $k^{p^{-r}}$ компонент многообразия $V_{s,r}$ находится в естественном взаимно однозначном соответствии с множеством всех неприводимых над k множителей многочленов H_j, $j \in J_{s,r}$ (мы оставляем подробности читателю). Время работы этого алгоритма полиномиально от D, $(d')^\nu$, $(d'')^{l+1}$, $(d''')^{l+1}$, M_1, M_2, m и p (напомним, что D определено во введении из [8]).

Следовательно, в этом алгоритме раскладываются на неприводимые множители над полем k только многочлены от одной переменной, ср. со свойством 8 в начале введения из [8].

Список литературы

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 учёной степени д.ф.-м.н., Ленинград, 1987.
8. А. Л. Чистов, *Системы с параметрами, или эффективное решение систем полиномиальных уравнений* 33 *года спустя.* I. — Зап. научн. семин. ПОМИ **462** (2017), 122–166.
9. А. Л. Чистов, *Системы с параметрами, или эффективное решение систем полиномиальных уравнений* 33 *года спустя.* II. — Зап. научн. семин. ПОМИ **468** (2018), 138–176.
10. A. L. Chistov, *Алгоритмы полиномиальной сложности для новой модели представления алгебраических многообразий.* — Зап. научн. семин. ПОМИ **378** (2010), 133–170.

11. A. Chistov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde matrices, NP-completeness, and transversal subspaces.* — Found. Comput. Math. **3**, No. 4 (2003), 421–427.
12. D. Lazard, F. Rouillier, *Solving parametric polynomial systems.* — J. Symbolic Comput. **42**, No. 6 (2007), 636–667.
13. D. Lazard, *Résolution des systémes d'équations algébriques.* — Theoret. Comput. Sci. **15** (1981), 77–110.
14. 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.

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 union of strata. For values of 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 the 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. This solves a long standing problem to avoid double exponential growth of coefficients for this problem.

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

Поступило 10 сентября 2019 г.