Записки научных
семинаров ПОМИ
Том 436, 2015 г.

А. Л. Чистов

ВЫЧИСЛЕНИЯ С ПАРАМЕТРАМИ: ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ

Введение

Пусть k – поле произвольной характеристики и $a_1, \ldots, a_\nu$ – семейство независимых параметров (или переменных) над k. Обозначим через $\mathbb{A}^\nu(\overline{k})$ аффинное пространство параметров над алгебраическим замыканием $\overline{k}$ основного поля k с координатными функциями $a_1, \ldots, a_\nu$. Рассмотрим кольцо многочленов $R = k[a_1, \ldots, a_\nu]$.

Когда решают вычислительную алгебраическую задачу с входными данными, зависящими от параметров, целью является получить стратификацию пространства параметров на конечное число квазипроективных алгебраических многообразий $\mathcal{W}_\alpha$, $\alpha \in A$, удовлетворяющую следующему условию. Для произвольных значений параметров из любого страта $\mathcal{W}_\alpha$ выходные данные (или решение задачи для этих значений параметров) вычисляется одними и теми же многочленами из кольца R, зависящими только от α. Это, конечно, не совсем формальное объяснение.

Имеются статьи на данную тему, см., например, [1,2]. Однако до сих пор алгоритмы из этих статей были громоздкими и имели по крайней мере дважды экспоненциальные оценки на сложность.

Достаточно сложно формализовать всё это в форме удобной для приложений. Здесь требуется свежий взгляд на вещи. В настоящее время наша цель – дать теоретическое обоснование. Именно, для вычислений с параметрами (таких, как выше) мы предлагаем модель, основанную на семействах деревьев вычислений или, что то же самое, лесах вычислений. Мы доказываем фундаментальный результат, теорему 1 параграфа 4, относящийся к этой модели. В последующих работах мы надеемся применить результаты этой статьи на практике: для разложения на абсолютно неприводимые множители многочленов с параметрическими коэффициентами, и после этого – для решения

Ключевые слова: вычисления с параметрами, стратификации, деревья вычислений, леса вычислений.

систем полиномиальных уравнений с параметрическими коэффициентами. Конечно, основная цель – избежать дважды экспоненциальных верхних оценок на сложность.

В настоящей статье наш основной инструмент – дерево вычислений, см. §1. Оказывается, что для практических целей неудобно рассматривать только одно дерево вычислений. Так что нам требуется ввести сначала полные сигнатуры, метки и сигнатуры, относящиеся к вершинам дерева вычислений (см. §2), а затем леса вычислений и алгоритмы, соответствующие им (см. § 3). Эти леса вычислений являются гораздо более функциональными и предоставляют требуемую свободу для решения задач со входными данными, зависящими от параметров.

§1. Деревья вычислений

В этом разделе мы вводим наш основной инструмент – деревья вычислений. Пусть $a_1, \ldots, a_\nu$ – параметры, такие же, как и выше. Напомним, что $R = k[a_1, \ldots, a_\nu]$. Положим K равным полю частных кольца R.

Дерево вычислений T со входными параметрами $a_1, \ldots, a_\nu$ над основным полем k определяется следующим образом. Это корневое дерево с корнем $v_0 = v_0(T)$; так что v_0 – фиксированная вершина дерева T. Каждая вершина v уровня $\varkappa$ дерева T имеет вид $v = v_{i_0,\ldots,i_\varkappa}$, где $i_0 = 0$, для всякого j, $0 \leqslant j \leqslant \varkappa$, также $v_{i_0,\ldots,i_j}$ является вершиной дерева T и для всякого j, $1 \leqslant j \leqslant \varkappa$, вершина $v_{i_0,\ldots,i_j}$ является сыном вершины $v_{i_0,\ldots,i_{j-1}}$ (последовательность $i_0, \ldots, i_\varkappa$ однозначно определена вершиной v, поскольку T – дерево). По определению уровень вершины v равен $\varkappa$. В этом случае мы будем писать $l(v) = \varkappa$.

Обозначим через $I_{i_0,\ldots,i_\varkappa}$ множество всех i, таких, что $v_{i_0,\ldots,i_\varkappa,i}$ является потомком вершины $v = v_{i_0,\ldots,i_\varkappa}$. Следовательно, $I_{i_0,\ldots,i_\varkappa}$ – множество всех потомков уровня 1 (или сыновей) вершины v. Если $v = v_{i_0,\ldots,i_\varkappa}$, то положим $I_v = I_{i_0,\ldots,i_\varkappa}$. Если $I_v = \varnothing$, то v является листом дерева T. Обозначим через $L(T)$ множество всех листьев дерева T. Положим $l(T) = \max_{v \in L(T)} l(v)$. По определению целое число $l(T)$ есть уровень дерева T. По определению дерево вычислений равномерно тогда и только тогда, когда $l(v) = l(T)$ для всех $v \in L(T)$.

По определению условие $\mathcal{A}_v = \mathcal{A}_{i_0,\ldots,i_\varkappa}$ соответствует каждой вершине v. Оно имеет вид

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

где $\wedge$, $\vee$ обозначают логические конъюнкцию и дизъюнкцию, а все $\varphi_{v,\beta} \in k[a_1, \ldots, a_\nu]$, $1 \leqslant \beta \leqslant \mu_{v,2}$, являются полиномами, для некоторых целых чисел $\mu_{v,2} \geqslant \mu_{v,1} \geqslant 0$. Мы имеем по определению $\mu_{v_0,2} = 0$ и, следовательно, $\mathcal{A}_{v_0} = \mathrm{true}$. Мы будем рассматривать условие (1) как булеву функцию на $\mathbb{A}^\nu(\overline{k})$. Именно, для всякого $(a_1^*, \ldots, a_\nu^*) \in \mathbb{A}^\nu(\overline{k})$ значение $\mathcal{A}_v(a_1^*, \ldots, a_\nu^*) \in \{\mathrm{true}, \mathrm{false}\}$ определяется естественным образом (чтобы получить это значение, следует подставить $(a_1^*, \ldots, a_\nu^*)$ в (1)).

Далее, семейство многочленов $\mathcal{C}_v = \mathcal{C}_{i_0,\ldots,i_\varkappa} = \{c_{v,j}\}_{1 \leqslant j \leqslant m_v}$ из кольца R соответствует вершине v, где $m_v \geqslant 0$ – целое число (так, что все $c_{v,j} \in R$; если $m_v = 0$, то $\mathcal{C}_v$ пусто). Это семейство $\mathcal{C}_v$ является выходом вычисления, соответствующего вершине v (может быть, здесь лучше сказать “вычисления, предшествующего вершине v с выходом в вершине v”, но в дальнейшем мы не будем использовать эту терминологию).

По определению имеем $\mathcal{C}_{v_0} = \{a_i\}_{1 \leqslant i \leqslant \nu}$, т.е. $c_{v_0,i} = a_i$ для всех i, $1 \leqslant i \leqslant \nu = m_{v_0}$.

Обозначим через $J_v = \{v_{i_0}, v_{i_0,i_1}, \ldots, v_{i_0,\ldots,i_{\varkappa-1}}\}$ множество всех предков различных уровеней $\geqslant 1$ вершины v. Входные данные вычисления, соответствующего вершине v, – это семейство $\{c_{w,i}\}_{1 \leqslant i \leqslant m_w, w \in J_v}$.

Пусть $\mathcal{Z}_v = \{Z_{w,i}\}_{1 \leqslant i \leqslant m_w, w \in J_v}$ – семейство новых переменных и $R[\mathcal{Z}_v]$ – кольцо многочленов от всех переменных из последнего семейства. Тогда для всякого j, $1 \leqslant j \leqslant m_v$, задан многочлен $C_{v,j} \in R[\mathcal{Z}_v]$, такой, что

$$c_{v,j} = C_{v,j}|_{Z_{w,i} = c_{w,i}\ \forall (w,i)}, \tag{2}$$

т.е. $c_{v,j}$ получается подстановкой $Z_{w,i} = c_{w,i}$ в многочлен $C_{v,j}$ для всех $w \in J_v$, $1 \leqslant i \leqslant m_w$. Другими словами, чтобы получить выход в вершине v, следует вычислить полиномы $C_{v,j}$, $1 \leqslant j \leqslant m_v$, беря значения аргументов из семейства входных данных, соответствующих вершине v.

Если $v \in L(T)$, то семейство $\mathcal{C}_v$ является выходом, соответствующим листу v.

Мы требуем дополнительно, чтобы для всякого $(a_1^*, \ldots, a_\nu^*) \in \overline{k}^\nu$ если $\varkappa \geqslant 1$ и

$$\bigwedge_{0 \leqslant \beta \leqslant \varkappa - 1} \mathcal{A}_{i_0,\ldots,i_\beta}(a_1^*, \ldots, a_\nu^*) = \mathrm{true}, \tag{3}$$

то существует не более одного индекса $i_\varkappa \in I_{i_0,\ldots,i_{\varkappa-1}}$, такого, что $\mathcal{A}_{i_0,\ldots,i_\varkappa}(a_1^*, \ldots, a_\nu^*) = \mathrm{true}$.

Далее, мы вводим квазипроективное алгебраическое многообразие $\mathcal{W}_v = \mathcal{W}_{i_0,\dots,i_\varkappa}$, соответствующее вершине v. Положим

$$\overline{\mathcal{A}}_v = \overline{\mathcal{A}}_{i_0,\dots,i_\varkappa} = \bigwedge_{0\leqslant\beta\leqslant\varkappa} \mathcal{A}_{i_0,\dots,i_\beta}.$$

По определению

$$\begin{aligned}\mathcal{W}_v = \mathcal{W}_{i_0,\dots,i_\varkappa} &= \Big\{(a_1^*,\dots,a_\nu^*)\in\overline{k}^\nu \ : \bigwedge_{0\leqslant\beta\leqslant\varkappa} \mathcal{A}_{i_0,\dots,i_\beta}(a_1^*,\dots,a_\nu^*) = \mathrm{true}\Big\}\\ &= \Big\{(a_1^*,\dots,a_\nu^*)\in\overline{k}^\nu \ : \overline{\mathcal{A}}_v(a_1^*,\dots,a_\nu^*) = \mathrm{true}\Big\}\end{aligned}$$

(эти многообразия необязательно неприводимы над k). Очевидно,

$$\begin{aligned}\mathcal{W}_v = \mathcal{W}_{i_0,\dots,i_\varkappa} &= \mathcal{Z}(\varphi_{w,i},\ w\in J_v\cup\{v\}, 1\leqslant i\leqslant\mu_{w,1})\\ &\quad\setminus \bigcup_{w\in J_v\cup\{v\}} \mathcal{Z}(\varphi_{w,i},\ \mu_{w,1}+1\leqslant i\leqslant\mu_{w,2}) \subset \mathbb{A}^\nu(\overline{k}),\end{aligned} \tag{4}$$

где $\mathcal{Z}(\dots)$ – множество нулей соответствующего семейства многочленов в $\mathbb{A}^\nu(\overline{k})$.

Для всякого дерева вычислений T и его вершины v положим

$$\mathcal{W}_v' = \mathcal{Z}(\varphi_{v,1},\dots,\varphi_{v,\mu_{v,1}}),\quad \mathcal{W}_v'' = \mathcal{Z}(\varphi_{v,\mu_{v,1}+1},\dots,\varphi_{v,\mu_{v,2}}).$$

Таким образом, $\mathcal{W}_v', \mathcal{W}_v''$ являются аффинными алгебраическими многообразиями в $\mathbb{A}^\nu(\overline{k})$. В этих обозначениях

$$\mathcal{W}_v = \bigcap_{w\in J_v\cup\{v\}} \mathcal{W}_w' \setminus \bigcup_{w\in J_v\cup\{v\}} \mathcal{W}_w''.$$

Обозначим через $L(T)$ множество всех листьев дерева T. Положим

$$\mathcal{S}(T) = \bigcup_{v\in L(T)} \mathcal{W}_v. \tag{5}$$

Тогда $\mathcal{S}(T)$ – конструктивное подмножество в аффинном пространстве $\mathbb{A}^\nu(\overline{k})$, и (5) – стратификация множества $\mathcal{S}(T)$ в объединение квазипроективных алгебраических многообразий $\mathcal{W}_v$, $v\in L(T)$.

Теперь равенство $\mathcal{S}(T) = \mathbb{A}^\nu(\overline{k})$ эквивалентно следующему условию. Для всякого $(a_1^*,\dots,a_\nu^*)\in\overline{k}^\nu$ для всякой вершины $v = v_{i_0,\dots,i_{\varkappa-1}} \notin L(T)$ дерева T если $\varkappa\geqslant 1$ и справедливо (3), то существует один и только один индекс $i\in I_{i_0,\dots,i_{\varkappa-1}}$, такой, что $\mathcal{A}_{i_0,\dots,i_{\varkappa-1},i}(a_1^*,\dots,a_\nu^*) = \mathrm{true}$.

По определению дерево T называется общим в том и только в том случае, если $\mathcal{S}(T)$ является непустым открытым в топологии Зарисского подмножеством пространства $\mathbb{A}^{\nu}(\overline{k})$.

Для завершения определения дерева вычислений нам необходимо ввести полные сигнатуры, метки и сигнатуры.

§2. Полные сигнатуры, метки и сигнатуры

Пусть Ω' – наименьшее множество, удовлетворяющее следующим свойствам:

(i) $\Omega' \supset \mathbb{Z}$,

(ii) если $\sigma_1, \dots, \sigma_N \in \Omega'$, $N \geqslant 1$, то $(\sigma_1, \dots, \sigma_N) \in \Omega'$.

Множество Ω' счётно, поскольку его можно рассматривать как подмножество множества всех конечных последовательностей $q_1, \dots, q_N$, где $q_j \in \mathbb{Z} \cup \{)\} \cup \{(\} \cup \{,\}$. Заметим здесь, что $\mathbb{Z}^N \subset \Omega'$ для всякого $N \geqslant 1$ и $\mathbb{Z}^{N_1} \times \mathbb{Z}^{N_2}$ не отождествляется с $\mathbb{Z}^{N_1+N_2}$, т.е. если $\sigma_1 \in \mathbb{Z}^{N_1}$, $\sigma_2 \in \mathbb{Z}^{N_2}$, то $(\sigma_1, \sigma_2) \in \mathbb{Z}^{N_1} \times \mathbb{Z}^{N_2}$, но $(\sigma_1, \sigma_2) \notin \mathbb{Z}^{N_1+N_2}$.

Обозначим через Ω подмножество всех элементов $\omega \in \Omega'$, таких, что $\omega = (\omega_1, \dots, \omega_N)$, где $1 \leqslant N \in \mathbb{Z}$ (если $N = 1$, то $\omega = \omega_1$), все $\omega_i \in \Omega$, $1 \leqslant i \leqslant N$, и $0 \leqslant \omega_1 \in \mathbb{Z}$.

Если $\omega = (\omega_1, \dots, \omega_N) \in \Omega$, то положим $\mathrm{j}(\omega) = \omega_1$.

Пусть T – дерево вычислений. Каждой вершине v дерева T сопоставляется полная сигнатура $r(v) \in \Omega$. Она удовлетворяет следующему свойству:

- $\mathrm{j}(r(v)) = m_v$.

Пусть v_0 – корень дерева T. Положим $r(T) = r(v_0)$. По определению $r(T)$ – полная сигнатура дерева вычислений T.

Неформально говоря, полная сигнатура $r(v)$ описывает природу математических объектов, которые представляются семействами $\{c_{v,j}(a^*)\}_{1 \leqslant j \leqslant m_v}$ для $a^* \in \mathcal{W}_v$ (например, они могут быть матрицами фиксированного размера с элементами из поля $\overline{k}$, или полиномами с некоторыми ограничениями на степени и число переменных с коэффициентами из поля $\overline{k}$, или другими математическими объектами). Фактически полные сигнатуры играют вспомогательную роль, но они упрощают изложение. Кодирование математических объектов элементами из Ω, конечно, не является каноническим, однако оно существует и должно быть фиксировано заранее. Мы выбираем такое

большое множество Ω, чтобы иметь достаточную свободу для полных сигнатур.

На практике, для того чтобы сделать изложение менее формальным, мы будем использовать метки вместо сигнатур. Например, если семейства $\{c_{v,j}(a^*)\}_{1\leqslant j\leqslant m_v}$ для $a^* \in \mathcal{W}_v$ представляют полиномы от X с коэффициентами из $\overline{k}$ степени не выше d, то можно приписать метку "многочлены от X степени не выше d" вершине v вместо полной сигнатуры $r(v)$. Так что здесь "многочлены от X степени не выше d" – просто описание полной сигнатуры $r(v)$. Это будет удобно и не приведёт к двусмысленности. Отметим, что для всякого элемента $\omega \in \Omega$ должно быть не более одного такого неформального описания.

Введём также сигнатуры вершин деревьев вычислений. Мы не даём их формальное определение. Сигнатуры будут определяться каждый раз, когда это будет необходимо для рассматриваемых деревьев и их вершин. Здесь мы дадим только следующее пояснение. Метка вершины v зависит от некоторых параметров, скажем $n_1, \ldots, n_\alpha$ (обычно они принимают целые значения; не следует путать их с параметрами $a_1, \ldots, a_\nu$, которые принимают значения из $\overline{k}$). Тогда набор из α элементов $(n_1, \ldots, n_\alpha)$ этих параметров является сигнатурой вершины v. Положим $\rho(v) = (n_1, \ldots, n_\alpha)$.

Обозначим через $\lambda(v)$ метку вершины v. Пусть $\lambda(v)$ зависит от значений $n_1, \ldots, n_\alpha$ параметров, см. выше. Напомним, что $\lambda(v)$ является строкой символов. Выберем символ, который не содержится в строке никакой метки, скажем $\bullet$. Строка $\lambda(v)$ содержит $n_1, \ldots, n_\alpha$ (здесь мы отождествляем целые числа со строками символов, их представляющими; это не приведёт к двусмысленности). Заменим n_i на $\bullet$ для всякого i, $1 \leqslant i \leqslant \alpha$, в строке $\lambda(v)$. Мы получаем новую строку $\overline{\lambda}(v)$. Строка $\overline{\lambda}(v)$ будет называться основой метки $\lambda(v)$. Две вершины v_1, v_2 дерева T эквивалентны в том и только в том случае, если $\overline{\lambda}(v_1) = \overline{\lambda}(v_2)$, т.е. в том и только в том случае, если их метки совпадают с точностью до значений параметров. Таким образом, определены классы эквивалентности вершин дерева T.

Мы предполагаем дополнительно, что для всякого класса эквивалентности $\mathcal{V}$ вершин дерева T существует функция $\mathrm{i} : \rho(\mathcal{V}) \to \mathbb{Z}$, определённая на множестве сигнатур $\rho(v)$, $v \in \mathcal{V}$, удовлетворяющая следующему свойству. Для всякой вершины $v \in \mathcal{V}$ мы имеем $m_v = \mathrm{i}(\rho(v))$, или, что то же самое, $\mathrm{i}(\rho(v)) = \mathrm{j}(r(v))$. Заметим, что функция i зависит от класса эквивалентности $\mathcal{V}$.

В рассмотренном случае метка “многочлены от X степени не выше d” содержит целочисленный параметр d. Этот параметр d является сигнатурой вершины v. Основа этой метки – “многочлены от X степени не выше $\bullet$”. Мы имеем $m_v = \mathfrak{i}(d) = d + 1$.

Другой пример: если вершина v имеет метку “матрицы размера $n \times m$”, то сигнатура вершины v равна (n, m). Основа рассматриваемой метки в этом случае есть “матрицы размера $\bullet \times \bullet$”. Мы имеем $m_v = \mathfrak{i}(n, m) = n\,m$.

Для того чтобы сделать изложение более кратким, во многих случаях, описывая деревья вычислений, удобно использовать сигнатуры вершин вместо полных сигнатур и меток, если вся другая информация о математических объектах, соответствующих вершинам этих деревьев, известна из контекста. Это не приведёт к двусмысленности, поскольку в данной ситуации полные сигнатуры вершин однозначно определены.

Вернёмся к полным сигнатурам. Пусть $\sigma_i \in \Omega$, $1 \leqslant i \leqslant N$. Рассмотрим вложение

$$\pi^{(N)} : \Omega^N \to \Omega, \quad (\sigma_1, \ldots, \sigma_N) \mapsto \left(\sum_{1 \leqslant i \leqslant N} \mathfrak{j}(\sigma_i),\ (\sigma_1, \ldots, \sigma_N) \right).$$

Пусть теперь $T_1, \ldots, T_N$ – деревья вычислений с входными параметрами $a_1, \ldots, a_\nu$ над основным полем k, такие, что $r(T_i) = r(T_j)$ для всех i,j, $1 \leqslant i, j \leqslant N$ (т.е. полные сигнатуры этих деревьев совпадают). Мы собираемся определить набор из N деревьев $\langle T_1, \ldots, T_N \rangle$. Этот набор также является деревом вычислений со входными параметрами $a_1, \ldots, a_\nu$ над основным полем k с той же самой полной сигнатурой, т.е. $r(\langle T_1, \ldots, T_N \rangle) = r(T_1)$. Пусть $v_{i,0}$ – корень дерева T_i, $1 \leqslant i \leqslant N$. Каждая вершина дерева $\langle T_1, \ldots, T_N \rangle$ имеет вид $(v_1, \ldots, v_N)$, где v_i является вершиной дерева T_i, $1 \leqslant i \leqslant N$, и $(v_1, \ldots, v_N)$ удовлетворяет следующему свойству.

(*) Существует целое число j, $1 \leqslant j \leqslant N + 1$, такое, что
- $v_i \in L(T_i)$ при $1 \leqslant i \leqslant j - 1$,
- если $j < N + 1$, то $v_j \notin L(T_j)$,
- $v_i = v_{i,0}$ при $j + 1 \leqslant i \leqslant N$.

Корень дерева $\langle T_1, \ldots, T_N \rangle$ есть $(v_{1,0}, \ldots, v_{N,0})$. Если $(v_1, \ldots, v_N)$ удовлетворяет условию (*) и $1 \leqslant j \leqslant N$, то

$$I_{(v_1, \ldots, v_N)} = \{v_1\} \times \ldots \times \{v_{j-1}\} \times I_{v_j} \times \{v_{j+1,0}\} \times \ldots \times \{v_{N,0}\}.$$

Если $j = N+1$, то $I_{(v_1,\dots,v_N)} = \varnothing$, т.е. $(v_1,\dots,v_N) \in L(\langle T_1,\dots,T_N\rangle)$.

Если $w = (v_1,\dots,v_N)$ удовлетворяет условию (*) с произвольным j, то положим

$$m_w = \sum_{1\leqslant u\leqslant \min\{j,N\}} m_{v_u}.$$

Если $1 \leqslant i \leqslant m_w$, то $c_{w,i} = c_{v_\alpha,\beta}$, где $i = \beta + \sum_{1\leqslant u\leqslant \alpha-1} m_{v_u}$ для однозначно определённых целых чисел α,β, таких, что $1 \leqslant \alpha \leqslant \min\{j,N\}$, $1 \leqslant \beta \leqslant m_\alpha$. Иными словами, семейство выходных данных $\{c_{w,i}\}_{1\leqslant i\leqslant m_w}$ совпадает с объединением семейств $\{c_{v_\alpha,\beta}\}_{1\leqslant\beta\leqslant m_{v_\alpha}}$ по всем α, $1 \leqslant \alpha \leqslant \min\{j,N\}$. Положим $\mathcal{A}_w = \mathcal{A}_{v_j}$, $j' = \min\{j,N\}$ и

$$r(w) = \pi^{(j')}(r(v_1),\dots,r(v_{j'})).$$

Теперь многочлены $C_{w,i}$, $m_w - m_{v_j} + 1 \leqslant i \leqslant m_w$, определяются естественным образом при помощи многочленов $C_{v_j,\alpha}$, $1 \leqslant \alpha \leqslant m_{v_j}$. Многочлены $C_{w,i}$ с $1 \leqslant i \leqslant m_w - m_{v_j}$ являются просто некоторыми переменными. Здесь мы оставляем подробности читателю.

Таким образом, мы определили дерево вычислений $\langle T_1,\dots,T_N\rangle$. Мы вернёмся к этой конструкции в следующем разделе.

Дерево вычислений T_1 со входными параметрами $a_1,\dots,a_\nu$ над основным полем k является поддеревом дерева вычислений T_2 со входными парами $a_1,\dots,a_\nu$ над основным полем k в том и только в том случае, если существует вложение ι множества вершин дерева T_1 в множество вершин дерева T_2, удовлетворяющее следующим свойствам (a)–(d).

(a) Для всякой вершины v дерева T_1 мы имеем $\mathcal{C}_v = \mathcal{C}_{\iota(v)}$ и $r(v) = r(\iota(v))$. Следовательно, $m_v = m_{\iota(v)}$.

(b) Для всякой вершины v дерева T_1 мы имеем $\iota(I_v) \subset I_{\iota(v)}$. Следовательно, для всякой вершины v дерева T_1 справедливо равенство $\iota(J_v) = J_{\iota(v)}$ и $\mathcal{Z}_v$ находится во взаимно однозначном соответствии с $\mathcal{Z}_{\iota(v)}$. Мы будем отождествлять $\mathcal{Z}_v$ с $\mathcal{Z}_{\iota(v)}$.

(c) Для всякой вершины v дерева T_1 мы имеем $C_{v,j} = C_{\iota(v),j}$ при $1 \leqslant m \leqslant v$.

(d) Для всякой вершины v дерева T_1 мы имеем $\mu_{v,1} = \mu_{\iota(v),1}$, $\mu_{v,2} = \mu_{\iota(v),2}$ и $\varphi_{v,j} = \varphi_{\iota(v),j}$ при $1 \leqslant j \leqslant \mu_{v,2}$. Следовательно, $\mathcal{A}_v = \mathcal{A}_{\iota(v)}$, $\overline{\mathcal{A}}_v = \overline{\mathcal{A}}_{\iota(v)}$.

При описанных условиях если $\iota(L(T_1)) \subset L(T_2)$, то $\mathcal{S}(T_1) \subset \mathcal{S}(T_2)$. Если для всякого листа $v \in L(T_2)$ существует такой лист $w \in L(T_1)$,

что $\iota(w) \in J_v$ (т.е. вершина $\iota(w)$ является предком вершины v), то $\mathcal{S}(T_1) \supset \mathcal{S}(T_2)$.

В дальнейшем, при условии, что не оговорено противное, если T_1 является поддеревом дерева T_2, то для всех вершин v дерева T_1 мы будем отождествлять вершины v и $\iota(v)$ деревьев T_1 и T_2 соответственно.

Дерево вычислений T' называется несократимым тогда и только тогда, когда для всякого листа $v \in L(T')$ алгебраическое многообразие $\mathcal{W}_v$ непусто. Очевидно, для всякого дерева вычислений T существует единственное несократимое дерево вычислений $\mathrm{IRD}(T)$, которое является поддеревом в T, таким, что $L(\mathrm{IRD}(T)) = \{v \in L(T) : \mathcal{W}_v \neq \varnothing\}$. Мы имеем $\mathcal{S}(T) = \mathcal{S}(\mathrm{IRD}(T))$.

Пусть $k^{p^{-\infty}}$ – совершенное замыкание поля k. Пусть v – вершина дерева вычислений T и I_v – семейство всех его потомков уровня 1. Мы будем говорить, что *вычисление в вершине v* (не следует путать: здесь это не вычисление, соответствующее вершине v, введённое выше) *является разложением алгебраического многообразия $\mathcal{W}_v$ на неприводимые над $k^{p^{-\infty}}$ компоненты*, в том и только в том случае, если выполняются следующие условия.

- Для всякой вершины $w \in I_v$ алгебраическое многообразие $\mathcal{W}_w$ является открытым в топологии Зарисского подмножеством неприводимой над $k^{p^{-\infty}}$ компоненты алгебраического многообразия $\mathcal{W}_v$. Более точно, существует линейный порядок $<$ на множестве вершин I_v и разложение $\mathcal{W}_v = \bigcup_{w \in I_v} \mathcal{W}_{v,w}$ алгебраического многообразия $\mathcal{W}_v$ на неприводимые над $k^{p^{-\infty}}$ компоненты $\mathcal{W}_{v,w}$, такие, что $\mathcal{W}_w = \mathcal{W}_{v,w} \setminus \bigcup_{w' < w} \mathcal{W}_{v,w'}$.
- Для всякой вершины $w \in I_v$ мы имеем $m_w = m_v$ и $\mathcal{C}_w = \mathcal{C}_v$, т.е. $\mathcal{C}_w = \mathcal{C}_v = \{c_{v,j}\}_{1 \leqslant j \leqslant m_v}$.

Следовательно, для всякого дерева вычислений T существует дерево вычислений T', такое, что T является поддеревом в T', множество листьев $L(T')$ есть $\bigcup_{v \in L(T)} I_v$ (здесь I_v является множеством всех потомков уровня 1 вершины v в дереве T') и вычисление в каждой вершине $v \in L(T)$ (рассматриваемой как вершина дерева T') является разложением алгебраического многообразия $\mathcal{W}_v$ на неприводимые над $k^{p^{-\infty}}$ компоненты. Теперь для всякого листа w дерева T' квазипроективное алгебраическое многообразие $\mathcal{W}_w$ определено и неприводимо над полем $k^{p^{-\infty}}$.

В конце раздела мы опишем ещё одну конструкцию, относящуюся к деревьям вычислений. Пусть $a'_1, \dots, a'_\mu$ – некоторые алгебраически независимые над k параметры и $b_1, \dots, b_\nu \in k[a'_1, \dots, a'_\mu]$. Пусть T – дерево вычислений, введённое выше. Тогда мы определяем дерево $T(b)$ со входными параметрами $a'_1, \dots, a'_\mu$ над основным полем k следующим образом. Заменим везде в определении дерева T элементы $a_1, \dots, a_\nu$ на $b_1, \dots, b_\nu$. Мы получим объекты

$$v, r(v), c_{b,v,j}, \varphi_{b,v,j}, \mathcal{A}_{b,v}, \overline{\mathcal{A}}_{b,v},$$

соответствующие объектам $v, r(v), c_{v,j}, \varphi_{v,j}, \mathcal{A}_v, \overline{\mathcal{A}}_v$. Мы имеем

$$c_{b,v,j}, \varphi_{b,v,j} \in k[a'_1, \dots, a'_\mu]$$

и многообразия

$$\mathcal{W}_{b,v} = \left\{ (a'_1, \dots, a'_\mu) \in \overline{k}^\mu \ : \ \overline{\mathcal{A}}_{b,v}(a'_1, \dots, a'_\mu) \right\}.$$

В целом мы получаем модифицированное неполное дерево (вообще говоря, оно не удовлетворяет определению деревьев вычислений, поскольку $b_1, \dots, b_\nu$ могут быть алгебраически зависимы над k). Обозначим его через $T'(b)$. Добавим к этому неполному дереву $T'(b)$ новый корень $v_{0,0}$, положим $c_{v_{0,0},i} = a'_i$, $1 \leqslant i \leqslant \mu = m_{v_{0,0}}$, и положим $r(v_{0,0})$ равным полной сигнатуре вектора $(a'_1, \dots, a'_\mu) \in R^\mu$. Единственный сын корня $v_{0,0}$ есть корень v_0 дерева $T'(b)$. Таким образом, мы получаем дерево $T(b)$ со входными параметрами $a'_1, \dots, a'_\mu$ над основным полем k, а также неполное дерево $T'(b)$.

§3. Леса вычислений и соответствующие им алгоритмы

Пусть Σ – подмножество в Ω, см. предыдущий параграф. По определению лес вычислений – это семейство деревьев вычислений

$$T = \{T_\sigma\}_{\sigma \in \Sigma},$$

таких, что $r(T_\sigma) = \sigma$ для всякого $\sigma \in \Sigma$. Пусть $\sigma = (\sigma_1, \dots, \sigma_{m'}) \in \Sigma$. Тогда T_σ является деревом вычислений с σ_1 входными параметрами над основным полем k. Обозначим эти параметры через $a_1, \dots, a_{\sigma_1}$.

По определению лес вычислений $T = \{T_\sigma\}_{\sigma \in \Sigma}$ является общим в том и только в том случае, если для всякого $\sigma \in \Sigma$, такого, что $\mathcal{S}(T_\sigma) \neq \varnothing$, дерево вычислений T_σ является общим.

По определению лес вычислений $T = \{T_\sigma\}_{\sigma\in\Sigma}$ является равномерным в том и только в том случае, если дерево вычислений T_σ является равномерным для всякого $\sigma \in \Sigma$.

Положим $\mathcal{K} = \coprod_{\omega\in\Omega} \overline{k}^{\mathrm{j}(\omega)}$. Это копроизведение в категории множеств. Мы будем использовать отождествление

$$\mathcal{K} = \bigcup_{\omega\in\Omega} \left(\overline{k}^{\mathrm{j}(\omega)} \times \{\omega\}\right) \tag{6}$$

и аналогичные отождествления для других копроизведений в категории множеств. Положим $\mathcal{S}(T) = \coprod_{\sigma\in\Sigma} \mathcal{S}(T_\sigma)$. Имеем $\mathcal{S}(T) \subset \mathcal{K}$.

Заметим, что $\mathcal{K}$ можно рассматривать как подмножество прямого произведения $\left(\bigcup_{j\geqslant 0} \overline{k}^j\right) \times \Omega$. Поэтому мы имеем естественные проекции на прямые множители: $p_1 : \mathcal{K} \to \bigcup_{j\geqslant 0} \overline{k}^j$ и $p_2 : \mathcal{K} \to \Omega$. Аналогичным образом канонические проекции p_1 и p_2 будут определяться для других копроизведений семейств множеств (мы будем использовать для них те же самые обозначения).

Пусть v – вершина дерева T_σ и $a^* = (a^*, \dots, a^*_{\sigma_1}) \in \overline{k}^{\sigma_1}$. Тогда положим

$$\begin{aligned} c_v &= (c_{v,1}, \dots, c_{v,m_v}), \\ c_v(a^*) &= (c_{v,1}(a^*_1, \dots, a^*_{\sigma_1}), \dots, c_{v,m_v}(a^*_1, \dots, a^*_{\sigma_1})) \end{aligned}$$

(фактически c_v совпадает с $\mathcal{C}_v$, см. §1).

Теперь мы определим функцию $\mathfrak{F} : \mathcal{S}(T) \to \mathcal{K}$, соответствующую лесу вычислений T, следующим образом. Пусть $(a^*, \sigma) \in \mathcal{S}(T)$. Следовательно, $\sigma \in \Sigma$, $a^* = (a^*, \dots, a^*_{\sigma_1}) \in \mathcal{S}(T_\sigma)$. Так что существует однозначно определённый лист $v \in L(T_\sigma)$, такой, что $a^* \in \mathcal{W}_v$. Тогда по определению

$$\mathfrak{F}(a^*, \sigma) = (c_v(a^*), r(v)) \in \mathcal{K}.$$

Мы будем обозначать через $\mathfrak{F}(T)$ функцию $\mathfrak{F}$, чтобы уточнить зависимость от леса T.

По определению функция $\mathfrak{F}$ есть алгоритм, соответствующий лесу вычислений T. Каждый вход этого алгоритма является элементом из $\mathcal{S}(T)$, каждый его выход принадлежит множеству $\mathfrak{F}(\mathcal{S}(T)) \subset \mathcal{K}$.

Произвольная функция $\mathfrak{Q}$ является алгоритмом, соответствующим лесу вычислений, в том и только в том случае, если существует лес вычислений T, такой, что

$$\mathfrak{Q} = \mathfrak{F}(T). \tag{7}$$

Положим
$$\mathfrak{f}(T) = p_1 \circ \mathfrak{F}(T), \quad \mathfrak{r}(T) = p_2 \circ \mathfrak{F}(T).$$

Теперь мы собираемся определить композицию лесов вычислений. Она также является лесом вычислений. Пусть T_1 и T_2 – два леса вычислений. Тогда композиция $T_2 \circ T_1$ определена в том и только в том случае, если
$$\mathfrak{F}(T_1)(\mathcal{S}(T_1)) \subset \mathcal{S}(T_2) \tag{8}$$
т.е. в том и только в том случае, если определена композиция функций $\mathfrak{F}(T_2) \circ \mathfrak{F}(T_1)$. Более того,
$$\mathfrak{F}(T_2 \circ T_1) = \mathfrak{F}(T_2) \circ \mathfrak{F}(T_1).$$

Дадим точное определение. Для краткости мы будем обозначать $T = T_2 \circ T_1$. Предположим, что выполняется условие (8). Пусть $T_1 = \{T_{1,\sigma}\}_{\sigma\in\Sigma_1}$. Тогда $T = \{T_\sigma\}_{\sigma\in\Sigma_1}$ и для всякого $\sigma \in \Sigma_1$ дерево вычислений T_σ определяется следующим образом. Пусть $v \in L(T_{1,\sigma})$ – произвольный лист дерева $T_{1,\sigma}$. Следовательно, определены выходные данные $c_v = (c_{v,1}, \dots, c_{v,m_v})$ и полная сигнатура $r(v)$, см. §1. Рассмотрим дерево вычислений $T_{2,r(v)}(c_v)$, см. конец §1 (деревья $T_{2,r(v)}$ и $T_{2,r(v)}(c_v)$ определены согласно (8)). Мы удаляем корень этого дерева $T_{2,r(v)}(c_v)$ и получаем неполное дерево $T'_{2,r(v)}(c_v)$. Для всякого $v \in L(T_{1,\sigma})$ мы склеиваем корень неполного дерева $T'_{2,r(v)}(c_v)$ и вершину v. После склеивания этой вновь полученной вершине соответствуют следующие объекты: выходные данные c_v, условие $\mathcal{A}_v$ и полная сигнатура $r(v)$. Они уже определены для дерева $T_{1,\sigma}$. В результате мы получаем для всякого $\sigma \in \Sigma_1$ дерево вычислений T_σ и, следовательно, требуемый лес вычислений T. Мы имеем $l(T_\sigma) = \max_{v\in L(T_{1,\sigma})}(l(v) + l(T_{2,r(v)})$.

Пусть
$$T_i = \{T_{i,\sigma}\}_{\sigma\in\Sigma}, \quad 1 \leqslant i \leqslant N,$$
– N лесов вычислений. Положим
$$\langle T_1, \dots, T_N\rangle = \{\langle T_{1,\sigma}, \dots, T_{N,\sigma}\rangle\}_{\sigma\in\Sigma},$$
где $\langle T_{1,\sigma}, \dots, T_{N,\sigma}\rangle$ – набор из N деревьев вычислений $T_{1,\sigma}, \dots, T_{N,\sigma}$, см. §1. Так что $\langle T_1, \dots, T_N\rangle$ – лес вычислений. Он называется набором N лесов вычислений $T_1, \dots, T_N$.

Заметим, что $\mathcal{S}(\langle T_{1,\sigma}, \dots, T_{N,\sigma}\rangle_\sigma) = \bigcap_{1\leqslant i\leqslant N} \mathcal{S}(T_{i,\sigma})$ для всякого элемента $\sigma \in \Sigma$ и, следовательно, $\mathcal{S}(\langle T_{1,\sigma}, \dots, T_{N,\sigma}\rangle) = \bigcap_{1\leqslant i\leqslant N} \mathcal{S}(T_i)$. Далее, функция $\mathfrak{F}(\langle T_{1,\sigma}, \dots, T_{N,\sigma}\rangle)$ описывается следующим образом.

Пусть $(a^*,\sigma)\in\mathcal{S}(\langle T_{1,\sigma},\,\ldots,T_{N,\sigma}\rangle)$ и $\mathfrak{f}_j=\mathfrak{f}(T_j)$, $\mathfrak{r}_j=\mathfrak{r}(T_j)$ при $1\leqslant j\leqslant N$. Тогда

$$\mathfrak{F}(\langle T_{1,\sigma},\ldots,T_{N,\sigma}\rangle)(a^*,\sigma)=((\mathfrak{f}_1(a^*,\sigma),\ldots,\mathfrak{f}_N(a^*,\sigma)),\pi^{(N)}(\sigma_1,\ldots,\sigma_N)),$$

причём мы отождествляем здесь $\overline{k}^{\sigma_{1,1}}\times\ldots\times\overline{k}^{\sigma_{N,1}}$ с $\overline{k}^{\sigma_{1,1}+\ldots+\sigma_{N,1}}$.

На практике, для того чтобы сделать изложение более кратким, определяя алгоритмы, соответствующие лесам вычислений (и другие объекты, введённые в этом разделе), мы часто будем использовать сигнатуры вместо полных сигнатур, особенно когда другая информация об этих лесах известна из контекста.

Именно, пусть $T=\{T_\sigma\}_{\sigma\in\Sigma}$ – лес вычислений, такой, как и выше. Напомним, что в предыдущем разделе мы ввели метки вершин деревьев вычислений и их основы. Пусть $\mathcal{V}(T)$ – множество всех вершин всех деревьев из семейства T. Как и в §2, две вершины $v_1,v_2\in\mathcal{V}(T)$ эквивалентны в том и только в том случае, если $\overline{\lambda}(v_1)=\overline{\lambda}(v_2)$, т.е. тогда и только тогда, когда они имеют одну и ту же основу меток. Поэтому определено отношение эквивалентности $\mathcal{L}$ на множестве $\mathcal{V}(T)$.

Далее, как в §2, мы предполагаем, что для всякого класса $\mathcal{V}$ эквивалентности $\mathcal{L}$ существует функция $\mathfrak{i}\,:\,\rho(\mathcal{V})\to\mathbb{Z}$, определённая на множестве сигнатур $\rho(v)$, $v\in\mathcal{V}$, удовлетворяющая следующему свойству. Для всякой вершины $v\in\mathcal{V}$ мы имеем $m_v=\mathfrak{i}(\rho(v))$, или, что то же самое, $\mathfrak{i}(\rho(v))=\mathfrak{j}(r(v))$. Отметим, что эта функция $\mathfrak{i}$ зависит от класса эквивалентности $\mathcal{V}$.

Предположим дополнительно, что

(i) для всех $\sigma\in\Sigma$ корни $v_{\sigma,0}$ принадлежат одному и тому же классу $\mathcal{V}_0$ эквивалентности $\mathcal{L}$,

(ii) для всех $\sigma\in\Sigma$ и для всех $v\in L(T_\sigma)$ листья v принадлежат одному и тому же классу $\mathcal{V}_1$ эквивалентности $\mathcal{L}$.

Обозначим через $\mathfrak{i}_0$ (соответственно $\mathfrak{i}_1$) функцию $\mathfrak{i}$, соответствующую $\mathcal{V}_0$ (соответственно $\mathcal{V}_1$). Положим

$$R_0=\{\rho(v_{\sigma,0})\,:\,\sigma\in\Sigma\}\subset\mathcal{V}_0,\quad R_1=\{\rho(v)\,:\,v\in L(T_\sigma)\,\&\,\sigma\in\Sigma\}.$$

Напомним, что для всякой метки существует не более одной полной сигнатуры, соответствующей ей. Следовательно, для всякого $\rho_0\in R_0$ существует единственный элемент $\sigma\in\Sigma$, такой, что $\rho_0=\rho(v_{\sigma,0})$. Таким образом, мы получаем функцию $s_0\,:\,R_0\to\Sigma$, такую, что $\rho_0=\rho(v_{s_0(\rho_0),0})$ для всякого $\rho_0\in R_0$. Аналогично существует функция s_1 :

$R_1 \to \Omega$, такая, что для всякого $\rho_1 \in R_1$ имеем $s_1(\rho_1) \in \bigcup_{\sigma\in\Sigma} L(T_\sigma)$ и $\rho_1 = \rho(v_{s_1(\rho_1)})$.

При условиях (i) и (ii) алгоритм $\mathfrak{F}(T)$, соответствующий лесу вычислений T, может быть задан посредством отображения

$$\mathfrak{F}'(T) \,:\, \coprod_{q\in R_0} \overline{k}^{\mathfrak{i}_0(q)} \to \coprod_{q\in R_1} \overline{k}^{\mathfrak{i}_1(q)}, \tag{9}$$

такого, что для всякого $(a^*, \rho_0) \in \coprod_{q\in R_0} \overline{k}^{\mathfrak{i}_0(q)}$ мы имеем

$$\mathfrak{F}'(T)(a^*, \rho_0) = (c_v(a^*), \rho(v)),$$

где лист $v \in L(T_{s_0(\rho_0)})$ однозначно определён условием $a^* \in \mathcal{W}_v$, см. определение $\mathfrak{F}(T)$.

Легко видеть также, что для всякого $(a^*, \sigma) \in \coprod_{\sigma\in\Sigma} \overline{k}^{\mathfrak{j}(\sigma)}$

$$\mathfrak{F}(T)(a^*, \sigma) = (p_1(\mathfrak{F}'(a^*, \rho(v_{\sigma,0}))), r(s_1(p_2(\mathfrak{F}'(a^*, \rho(v_{\sigma,0})))))).$$

При условиях (i) и (ii) отображение (9) также будет называться алгоритмом, соответствующим лесу вычислений T. В этом случае мы будем обозначать также $T = \{T_q\}_{q\in R_0}$, где $T_{\rho(v_{\sigma,0})} = T_\sigma$ для всякого $\sigma \in \Sigma$. Это не приведёт к двусмысленности.

Предположим, что

(iii) ограничения $\mathfrak{i}_0|_{R_0}$ и $\mathfrak{i}_1|_{R_1}$ инъективны.

В этом случае, определяя $\mathfrak{F}'(T)$, мы будем использовать $\bigcup$ вместо $\coprod$ (это более естественно). Заметим, что тогда $\bigcup_{q\in R_1} \overline{k}^{\mathfrak{i}(q)} \subset \bigcup_{j\geqslant 0} \overline{k}^j$.

Следовательно, при условиях (i)–(iii) алгоритм $\mathfrak{F}(T)$, соответствующий лесу вычислений T, может быть задан отображением

$$\mathfrak{F}''(T) \,:\, \bigcup_{q\in R_0} \overline{k}^{\mathfrak{i}_0(q)} \to \bigcup_{j\geqslant 0} \overline{k}^j. \tag{10}$$

При условиях (i)–(iii) отображение $\mathfrak{F}''(T)$ также будет называться алгоритмом, соответствующим лесу вычислений T. Это не приведёт к двусмысленности.

Предположим, что мы используем $\mathfrak{F}'(T)$ (соответственно $\mathfrak{F}''(T)$) в качестве определения алгоритма, соответствующего лесу вычислений. Тогда произвольная функция $\mathfrak{Q}$ является алгоритмом, соответствующим лесу вычислений, в том и только в том случае, если существует лес вычислений T, такой, что $\mathfrak{Q} = \mathfrak{F}'(T)$ (соответственно $\mathfrak{Q} = \mathfrak{F}''(T)$). Это не приведёт к двусмысленности с определением, данным выше, см. (7), так как каждый раз всё будет ясно из контекста.

Мы хотели бы подчеркнуть здесь, что “алгоритм, соответствующий лесу вычислений T”, “его вход” и “его выход”, “алгоритм, соответствующий лесу вычислений”, являются нераздельными терминами из их определений (и ничем большим).

В следующих статьях (см. также примеры ниже в конце этого параграфа), мы будем строить функции, соответствующие лесам вычислений. Эти функции возникают из некоторых алгоритмов, так что этим оправдан термин “алгоритм, соответствующий лесу вычислений”. Как правило, мы не будем строить сами леса вычислений. Это можно сделать непосредственно, и мы будем оставлять данное построение заинтересованному читателю. Но, конечно, нам требуются эти леса вычислений, чтобы применять относящиеся к ним конструкции.

Пример 1. Многочлен $g = \sum_{0\leqslant j\leqslant d} g_j X^j \in \overline{k}[X]$, $d = \deg_X g$, задаётся вектором его коэффициентов $(g_0, \ldots, g_d) \in \overline{k}^{d+1}$ и сигнатурой $d \geqslant -1$ (если $g = 0$, то $\deg_X g = -1$ и $(g_0, \ldots, g_d) = ()$ является набором из 0 элементов). Обозначим через $P_d \subset \overline{k}[X]$ подмножество всех многочленов степени d. Положим $C(g, X) = (g_0, \ldots, g_d)$. Мы будем отождествлять P_d с подмножеством в $\overline{k}^{d+1}$, $g \mapsto C(g, X)$. Имеем $\overline{k}[X] = \bigcup_{d\geqslant -1} P_d \subset \bigcup_{d\geqslant -1} \overline{k}^{d+1}$.

Теперь пусть $f = (f_0, \ldots, f_d) \in \overline{k}^{d+1}$, $d \geqslant -1$. Это вектор сигнатуры d. Положим $\mathrm{RDP}_X(f) = \sum_{0\leqslant i\leqslant d} f_i X^i \in \overline{k}[X]$ и $d' = \deg_X f$. Тогда $-1 \leqslant d' \leqslant d$, и поэтому $\sum_{0\leqslant i\leqslant d} f_i X^i$ – многочлен степени не выше d. Таким образом, мы получаем функцию

$$\mathrm{RDP}_X : \bigcup_{d\geqslant -1} \overline{k}^{d+1} \to \bigcup_{d'\geqslant -1} P_{d'}.$$

Мы имеем $\mathrm{RDP}_X(f) = (f_0, \ldots, f_{d'})$ и $d' \geqslant 0$ в том и только в том случае, если $f_d = \ldots = f_{d'+1} = 0$ и $f_{d'} \neq 0$. Очевидно, $\mathrm{RDP}_X(f) = ()$ тогда и только тогда, когда $f_d = \ldots = f_0 = 0$. Следовательно, функция RDP_X является алгоритмом, соответствующим лесу вычислений $\{T_d\}_{d\geqslant -1}$. Каждое дерево из этого леса имеет уровень 1, т.е. каждый сын его корня является листом. Дерево T_d имеет $d + 2$ листьев. Они соответствуют значениям $-1 \leqslant d' \leqslant d$.

Для произвольного многочлена $g = \sum_{0\leqslant i\leqslant d} g_i X^i \in k[X]$, $\deg_X g = d$, и целого числа $d' \geqslant -1$ удобно ввести обозначение $C(g, X, d') = (g_0, \ldots, g_{d'}) \in \overline{k}^{d'+1}$, где $g_\alpha = 0$ для $d < \alpha \leqslant d'$ (если $d' > d$).

Пример 2. Аналогичным образом пусть $g \in \overline{k}[X_1, \ldots, X_n]$ – произвольный многочлен степени $\deg_{X_1,\ldots,X_n} g = d$ для целого числа $d \geqslant -1$. Здесь мы рассматриваем n как фиксированную константу.

Следовательно, можно представить этот многочлен в виде

$$g = \sum_{\substack{i_1,\ldots,i_n \geqslant 0,\\ i_1+\ldots+i_n \leqslant d}} g_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n},$$

где все коэффициенты $g_{i_1,\ldots,i_n}$ лежат в $\overline{k}$. Так что здесь на входе многочлен g задан семейством $C(g; X_1, \ldots, X_n) = \{g_{i_1,\ldots,i_n}\}_{\substack{i_1,\ldots,i_n \geqslant 0,\\ i_1+\ldots+i_n \leqslant d}}$ его коэффициентов из $\overline{k}$ и сигнатурой d.

Положим $g_{i_1,\ldots,i_n} = 0$ для всех целых чисел $i_1, \ldots, i_n \geqslant 0$, таких, что $i_1 + \ldots + i_n > d$, и пусть для всякого $d' \geqslant -1$

$$C(g; X_1, \ldots, X_n, d') = \{g_{i_1,\ldots,i_n}\}_{\substack{i_1,\ldots,i_n \geqslant 0,\\ i_1+\ldots+i_n \leqslant d'.}}$$

В случае многих переменных обозначим через $P_{n,d} \subset \overline{k}[X_1, \ldots, X_n]$ подмножество многочленов степени d. Мы отождествляем $P_{n,d}$ с подмножеством в $\overline{k}^{N_d}$, $g \mapsto C(g, X_1, \ldots, X_n)$, где $N = \binom{n+d}{n}$. Теперь

$$\overline{k}[X_1, \ldots, X_n] = \bigcup_{d \geqslant -1} P_{n,d} \subset \bigcup_{d \geqslant -1} \overline{k}^{N_d} \subset \bigcup_{j \geqslant 0} \overline{k}^j.$$

Пусть $f = \{f_{i_1,\ldots,i_n}\}_{\substack{i_1,\ldots,i_n \geqslant 0,\\ i_1+\ldots+i_n \leqslant d.}}$ – произвольный элемент объединения $\bigcup_{d \geqslant -1} \overline{k}^{N_d}$. Тогда положим $\mathrm{RDP}_{X_1,\ldots,X_n}(f)$ равным многочлену из $\overline{k}[X_1, \ldots, X_n]$, такому, что $f = C(\mathrm{RDP}_{X_1,\ldots,X_n}(f); X_1, \ldots, X_n, d)$. Положим

$$\deg_{X_1,\ldots,X_n} \mathrm{RDP}_{X_1,\ldots,X_n}(f) = d'.$$

Следовательно, $-1 \leqslant d' \leqslant d$. Поэтому определена функция

$$\mathrm{RDP}_{X_1,\ldots,X_n} : \bigcup_{d \geqslant -1} \overline{k}^{N_d} \to \bigcup_{d' \geqslant -1} P_{n,d'}.$$

Можно легко доказать, что $\mathrm{RDP}_{X_1,\ldots,X_n}$ является алгоритмом, соответствующим некоторому лесу вычислений $\{T_d\}_{d \geqslant -1}$. Дерево T_d имеет уровень $l(T_d) = 1$ и $d + 2$ листьев (мы оставляем подробности читателю).

Пример 3. Пусть $g \in \overline{k}[X_1, \ldots, X_n]$ – многочлен из предыдущего примера. Пусть $\deg_{X_1} g = d''$, $\deg_{X_2,\ldots,X_n} g = d'''$. Положим

$$\mathrm{RDP}_{X_1}(g) = \{g_{i_1,\ldots,i_n}\}_{\substack{i_1,\ldots,i_n \geqslant 0,\, i_1 \leqslant d'' \\ i_2+\ldots+i_n \leqslant d'''}},$$

$$\mathrm{LC}_{X_1}(g) = \mathrm{RDP}_{X_2,\ldots,X_n}\left(\{g_{d'',i_2\ldots,i_n}\}_{\substack{i_2,\ldots,i_n \geqslant 0, \\ i_2+\ldots+i_n \leqslant d'''}}\right),$$

где $g_{i_1,\ldots,i_n}$ – элементы из $C(g; X_1, \ldots, X_n, d'' + d''')$.

Тогда RDP_{X_1} и LC_{X_1} – алгоритмы, соответствующие лесам вычислений. Все деревья этих лесов имеют уровень 2. Для степени (или сигнатуры) d они имеют не более $(d+2)^2$ листьев (мы оставляем подробности читателю).

§4. Лемма о покрытии и основной результат

В этом разделе мы докажем результат, который станет фундаментальным для всей теории вычислений с параметрами.

Пусть $\mathbb{A}^\nu(\overline{k})$ имеет координатные функции $a_1, \ldots, a_\nu$. Пусть $W \subset \mathbb{A}^\nu(\overline{k})$ является квазипроективным алгебраическим многообразием и $\overline{W}$ – замыкание относительно топологии Зарисского многообразия W в аффинном пространстве $\mathbb{A}^\nu(\overline{k})$. Предположим, что $\overline{W} = \bigcup_{0 \leqslant a \leqslant \nu} W_a$ – разложение многообразия $\overline{W}$ на равноразмерностные аффинные алгебраические многообразия, т.е. для всякого целого числа a, $0 \leqslant a \leqslant \nu$, размерность каждой неприводимой компоненты E алгебраического многообразия W_a равна a и E является неприводимой компонентой многообразия $\overline{W}$. Пусть $\deg W_a = D_a$ (степень аффинного алгебраического многообразия равна степени его замыкания относительно топологии Зарисского в соответствующем проективном пространстве). По определению $D_a(W) = D_a$. Для всякого целого числа $d \geqslant 2$ положим

$$\delta(W, d) = \sum_{0 \leqslant a \leqslant \nu} D_a(W) \frac{d^{a+1} - 1}{d - 1}.$$

В формулировке следующей леммы $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m_i}^{(i)})$ есть множество всех общих нулей многочленов $f_1^{(i)}, \ldots, f_{m_i}^{(i)} \in \overline{k}[a_1, \ldots, a_\nu]$, $m_i \geqslant 0$, в аффинном пространстве $\mathbb{A}^\nu(\overline{k})$; в дальнейшем мы используем также другие аналогичные обозначения.

Лемма. *Пусть $W \subset \mathbb{A}^\nu(\overline{k})$ – квазипроективное алгебраическое многообразие. Пусть $\mathcal{W}_i$, $i \in I$, – конечное семейство квазипроективных алгебраических многообразий в $\mathbb{A}^\nu(\overline{k})$. Предположим, что для всякого $i \in I$ можно представить $\mathcal{W}_i$ в виде*

$$\mathcal{W}_i = \mathcal{W}_i' \setminus \mathcal{Z}(f_1^{(i)}, \dots, f_{m_i}^{(i)}),$$

где $\mathcal{W}_i' \subset \mathbb{A}^\nu(\overline{k})$ – замкнутое алгебраическое многообразие и $f_1^{(i)}, \dots, f_{m_i}^{(i)} \in \overline{k}[a_1, \dots, a_\nu]$ – многочлены степени $\deg_{a_1,\dots,a_\nu} f_j^{(i)} \leqslant d$ при $1 \leqslant j \leqslant m_i$ и $d \geqslant 2$. Предположим, что

$$W \subset \bigcup_{i \in I} \mathcal{W}_i.$$

Тогда существует конечное множество индексов $I' \subset I$, такое, что

$$\#I' \leqslant \delta(W, d) \quad \text{и} \quad W \subset \bigcup_{i \in I'} \mathcal{W}_i.$$

Доказательство. Можно предполагать без ограничения общности, что W является неприводимым над $\overline{k}$. При этом дополнительном предположении мы используем индукцию по $\dim W$. База индукции $\dim W = 0$ очевидна.

Опишем индукционный переход. Предположим, что $\dim W = \alpha > 0$ и требуемое утверждение доказано для всех неприводимых над $\overline{k}$ квазипроективных алгебраических многообразий $W' \subset \mathbb{A}^\nu(\overline{k})$ с $\dim W' < \alpha$. Тогда существует $\iota \in I$, такое, что $W \cap \mathcal{W}_\iota$ содержит открытое в топологии Зарисского подмножество многообразия W. Очевидно, $W \subset \mathcal{W}_\iota'$, $\dim(W \cap \mathcal{Z}(f_1^{(\iota)}, \dots, f_{m_\iota}^{(\iota)})) < \alpha$ и

$$W = (W \cap \mathcal{W}_\iota) \cup (W \cap \mathcal{Z}(f_1^{(\iota)}, \dots, f_{m_\iota}^{(\iota)})).$$

Можно записать

$$W \cap \mathcal{Z}(f_1^{(\iota)}, \dots, f_{m_\iota}^{(\iota)}) = \bigcup_{j \in J} W_j,$$

где W_j, $j \in J$, – все неприводимые над $\overline{k}$ компоненты пересечения из левой части последнего равенства. Так что каждое W_j есть неприводимое над $\overline{k}$ квазипроективное алгебраическое многообразие в $\mathbb{A}^\nu(\overline{k})$ с $\dim W_j = \alpha_j < \alpha$. По индукционному предположению для всякого $j \in J$ существует подмножество I_j' с $\#I_j' \leqslant \delta(W_j, d)$, такое, что $W_j \subset \bigcup_{i \in I_j'} \mathcal{W}_i$. Положим $I' = \{\iota\} \cup \bigcup_{j \in J} I_j'$. Теперь достаточно доказать, что $\#I' \leqslant \delta(W, d)$.

Пусть $h_1, \ldots, h_\alpha$ – линейные комбинации многочленов $f_1^{(\iota)}, \ldots, f_{m_\iota}^{(\iota)}$ в общем положении (фактически здесь "общее положение" состоит в том, что выполняется условие (11) для $\beta = 1, 2, \ldots, \alpha$, см. ниже; мы оставляем подробности читателю). Тогда для всякого целого числа β, $1 \leqslant \beta \leqslant \alpha$,

$$W \cap \mathcal{Z}(h_1, \ldots, h_\beta) = \left(\bigcup_{\{j \in J \,:\, \alpha_j \geqslant \alpha - \beta\}} W_j \right) \cup \bigcup_{j \in J'_\beta} W'_j, \tag{11}$$

где W'_j, $j \in J'_\beta$, – конечное (может быть, пустое) семейство попарно различных неприводимых над $\overline{k}$ алгебраических многообразий, таких, что $\dim W'_j = \alpha - \beta$ для всякого $j \in J'_\beta$ и $W'_{j_1} \neq W_{j_2}$ для всех $j_1 \in J'_\beta$, $j_2 \in J$.

Положим $W'_\beta = \bigcup_{j \in J'_\beta} W'_j$. Обозначим $W'_0 = W$. Тогда из (11) следует, что для всякого β, $1 \leqslant \beta \leqslant \alpha$,

$$W'_{\beta-1} \cap \mathcal{Z}(h_\beta) = W'_\beta \cup \bigcup_{\{j \in J \,:\, \alpha_j = \alpha - \beta\}} W_j. \tag{12}$$

Поэтому по теореме Безу

$$d \deg W'_{\beta-1} \geqslant \deg W'_\beta + \sum_{\{j \in J \,:\, \alpha_j = \alpha - \beta\}} \deg W_j, \quad \beta = 1, 2, \ldots, \alpha. \tag{13}$$

Используя индукцию по β, мы получаем из (13), что

$$d^\beta \deg W \geqslant \sum_{1 \leqslant \gamma \leqslant \beta} \sum_{\{j \in J \,:\, \alpha_j = \alpha - \gamma\}} d^{\beta - \gamma} \deg W_j + \deg W'_\beta.$$

Суммируя эти неравенства по $\beta = 1, 2, \ldots, \alpha$, получаем

$$\delta(W, d) - \deg W \geqslant \sum_{j \in J} \delta(W_j, d) + \sum_{1 \leqslant \beta \leqslant \alpha} \deg W'_\beta.$$

Но $\deg W \geqslant 1$. Следовательно,

$$\delta(W, d) \geqslant 1 + \sum_{j \in J} \delta(W_j, d) \geqslant 1 + \sum_{j \in J} \# I'_j \geqslant \# I'.$$

Лемма доказана. □

Следствие 1. *Пусть $W \subset \mathbb{A}^\nu(\overline{k})$ – квазипроективное алгебраическое многообразие. Пусть $\mathcal{W}_i$, $i \in I$, – конечное семейство квазипроективных алгебраических многообразий в $\mathbb{A}^\nu(\overline{k})$. Предположим, что*

для всякого $i \in I$ можно представить $\mathcal{W}_i$ в виде

$$\mathcal{W}_i = \mathcal{W}_i' \setminus \bigcup_{1 \leqslant j \leqslant w_i} \mathcal{Z}(f_{i,j,1}, \ldots, f_{i,j,m_{i,j}}),$$

где $\mathcal{W}_i' \subset \mathbb{A}^\nu(\overline{k})$ – замкнутое аффинное алгебраическое многообразие и $f_{i,j,1}, \ldots, f_{i,j,m_{i,j}} \in \overline{k}[a_1, \ldots, a_\nu]$ – многочлены степени $\deg_{a_1,\ldots,a_\nu} f_{i,j,v} \leqslant d$ при $1 \leqslant j \leqslant w_i \in \mathbb{Z}$, $1 \leqslant v \leqslant m_{i,j} \in \mathbb{Z}$ и $2 \leqslant d \in \mathbb{Z}$. Пусть $w = \max\{w_i : i \in I\}$. Предположим, что

$$W \subset \bigcup_{i \in I} \mathcal{W}_i.$$

Тогда существует конечное подмножество индексов $I' \subset I$, такое, что

$$\#I' \leqslant \delta(W, wd) \quad \text{и} \quad W \subset \bigcup_{i \in I'} \mathcal{W}_i.$$

Доказательство. Действительно, можно записать

$$\bigcup_{1 \leqslant j \leqslant w_i} \mathcal{Z}(f_{i,j,1}, \ldots, f_{i,j,m_{i,j}}) = \mathcal{Z}(f_1^{(i)}, \ldots, f_{m_i}^{(i)}),$$

где $m_i \geqslant 0$ и $f_1^{(i)}, \ldots, f_{m_i}^{(i)} \in \overline{k}[a_1, \ldots, a_\nu]$ с $\deg f_j^{(i)} \leqslant wd$ при $1 \leqslant j \leqslant m_i$, $i \in I$. После этого следствие вытекает из леммы немедленно. □

Теперь мы готовы сформулировать наш основной результат.

Теорема 1. *Пусть T – 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* (1) *и $\deg_{a_1,\ldots,a_\nu} \varphi_{v,\beta} \leqslant d$ для всех β, $\mu_{1,v} < \beta \leqslant \mu_{2,v}$, см.* (1)*, для некоторого целого числа $d \geqslant 2$. Пусть $\mathcal{S}(T) = \bigcup_{1 \leqslant j \leqslant N} S_j$, где все S_j – квазипроективные алгебраические многообразия в $\mathbb{A}^\nu(\overline{k})$. Тогда число листьев несократимого дерева $\mathrm{IRD}(T)$ (или, что то же самое, число листьев v дерева T, таких, что $\mathcal{W}_v \neq \varnothing$) удовлетворяет неравенству*

$$\#L(\mathrm{IRD}(T)) \leqslant \sum_{1 \leqslant j \leqslant N} \delta(S_j, wd).$$

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

$$\#L(\mathrm{IRD}(T)) \leqslant \frac{(wd)^{\nu+1} - 1}{wd - 1}.$$

Доказательство. Это следует немедленно из следствия 1, определений и формулы (4). Теорема доказана. □

Литература

1. A. Ayad, *Complexity of solving parametric polynomial systems.* — Zap. Nauchn. Semin. POMI **387** (2011), 5–52.
2. D. Lazard, F. Rouillier, *Solving parametric polynomial systems.* — J. Symbolic Comput. **42**, No. 6 (2007), 636–667.

Chistov A. L. Computations with parameters: a theoretical background.

Consider a computational algebraic problem with the inputs depending on parameters. The aim of the computation is to stratify the variety of parameters such that for each stratum $\mathcal{W}_\alpha$ the solution of the problem for arbitrary values of parameters from each stratum as function of parameters is computed by the same algebraic formulas depending only on the stratum $\mathcal{W}_\alpha$.

We suggest a model for computations with parameters which is convenient for practical aims and prove a fundamental result for it.

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 3 августа 2015 г.