A. L. Chistov, Subexponential-time computation of isolated primary components of a polynomial ideal, *Zap. Nauchn. Sem. POMI*, 2020, Volume 498, 64–74

Записки научных
семинаров ПОМИ
Том 498, 2020 г.

А. Л. Чистов

ВЫЧИСЛЕНИЕ ИЗОЛИРОВАННЫХ ПРИМАРНЫХ КОМПОНЕНТ ПОЛИНОМИАЛЬНОГО ИДЕАЛА ЗА СУБЭКСПОНЕНЦИАЛЬНОЕ ВРЕМЯ

Введение

Примарное разложение является важной конструкцией коммутативной алгебры. Оно было введено Э. Ласкером [11] для колец многочленов и сходящихся степенных рядов и в полной общности Э. Нётер [14]. Каноническое примарное разложение было предложено В. Ортизом [15]. Даже сейчас эта тематика является актуальной. Например, некоторые интересные результаты о примарных разложениях были получены Ю. Яо [18].

Первый алгоритм для вычисления примарных разложений для колец многочленов над полем характеристики нуль был опубликован Г. Герман [10], она была ученицей Э. Нётер. С тех пор многие авторы предлагали свои алгоритмы для примарного разложения. Литература на эту тему весьма обширна. Вероятно, одной из наиболее важных здесь является статья А. Зайденберга [16]. В скором времени было понято, что в общем случае данная проблема является трудной. Все верхние оценки для сложности примарного разложения были дважды экспоненциальными от числа переменных.

Хорошая оценка для сложности может быть здесь получена лишь в частных случаях, например для идеалов, задающих нульмерные многообразия. Нульмерный случай является более или менее простым согласно [12].

В других статьях, см., например, [9, 13, 17], авторы интересовались главным образом практической реализацией примарного разложения без оценок сложности.

Удивительно, что во всех этих статьях нет нижних оценок для примарных разложений. Фактически в настоящее время можно получить дважды экспоненциальную нижнюю оценку для примарного разложения только при помощи наших результатов, см. [8]. Точнее, из [8]

Ключевые слова: полиномиальные идеалы, примарные разложения, изолированные примарные компоненты, субэкспоненциальный алгоритм.

можно вывести, что существует идеал, заданный однородными многочленами от n переменных степени D^n, такой, что его примарной компонентой является простой идеал $\mathfrak{p}$ и всякая система образующих идеала $\mathfrak{p}$ содержит многочлен степени не меньше $D^{2^{cn}}$ для абсолютной константы $c > 0$. Из [8] можно также легко получить дважды экспоненциальную нижнюю оценку на степени некоторых вложенных компонент некоторых идеалов.

По нашему мнению, все построенные до настоящего времени алгоритмы для примарного разложения далеки от своей окончательной совершенной формы. Мы полагаем, что можно построить канонический алгоритм для канонического примарного разложения однородного полиномиального идеала. Это было бы весьма интересно с теоретической точки зрения. Однако в настоящей статье у нас скромная цель. Мы хотели бы предложить алгоритм для построения всех изолированных примарных компонент полиномиального идеала так, что они задаются с точностью до вложенных компонент, см. (i) и (ii) ниже. Преимущество нашего подхода состоит в том, что сложность данной конструкции субэкспоненциальна от длины записи входных данных. Для обоснования нашего алгоритма мы используем нетривиальный факт – оценку степени изолированного примарного идеала, см. лемму 1 в [7] и ниже доказательство теоремы 1. Теперь мы переходим к подробностям.

Пусть k – поле произвольной характеристики $p \geqslant 0$ с алгебраическим замыканием $\overline{k}$. Пусть H – примитивное подполе поля k и $H(t_1, \ldots, t_l)$ – поле рациональных функций от алгебраически независимых над H переменных $t_1, \ldots, t_l$. Мы предполагаем, что поле k является конечным сепарабельным расширением поля $H(t_1, \ldots, t_l)$, заданным своим примитивным элементом θ. Минимальный многочлен $\Phi \in H(t_1, \ldots, t_l)[Z]$ элемента θ дан, и старший коэффициент $\mathrm{lc}_Z\Phi$ равен 1.

Положим $H_0 = \mathbb{Z}$, если $H = \mathbb{Q}$, и $H_0 = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, если $\mathrm{char}(k) = p > 0$. По определению длина записи $l(a)$ элемента $a \in H_0$ равна $[\log_2 |a|] + 2$, если $H_0 = \mathbb{Z}$ и $a \neq 0$, равна 1, если $H_0 = \mathbb{Z}$ и $a = 0$, и равна $[\log_2 p] + 1$, если $H_0 = \mathbb{F}_p$. Дополнительно мы будем предполагать, что $\Phi \in H_0[t_1, \ldots, t_l, Z]$ (здесь нет потери общности).

Пусть $X_1, \ldots, X_n$ – переменные. Каждый многочлен $g \in H_0[t_1, \ldots, t_l, X_1, \ldots, X_n]$ представляется в виде

$$g = \sum_{i_1,\ldots,i_l,\, j_1,\ldots,j_n} g_{i_1,\ldots,i_l,j_1,\ldots,j_n} t_1^{i_1} \ldots t^{i_l} X_1^{i_1} \ldots X_n^{i_n},$$

где $g_{i_1,\dots,i_l,j_1,\dots,j_n} \in H_0$. Степени $\deg_{t_1,\dots,t_l} g$ и $\deg_{X_1,\dots,X_n} g$ определяются естественным образом. Далее, по определению длина записи коэффициентов равна

$$l(g) = \max_{i_1,\dots,i_l,\, j_1,\dots,j_n} l(g_{i_1,\dots,i_l,j_1,\dots,j_n}).$$

Мы представляем многочлен Φ в виде $\Phi = \sum\limits_{0\leqslant i\leqslant N} \Phi_i Z^i$, где $\Phi_i \in H_0[t_1,\dots,t_l]$ и $N = \deg_Z(\Phi) - 1$. По определению $l(\Phi) = \max\limits_{0\leqslant i\leqslant N} l(\Phi_i)$. Далее мы будем предполагать, что $l(\Phi) \leqslant M_1$ и $\deg_{t_1,\dots,t_l,Z} \Phi \leqslant d_1$, где $d_1 \geqslant 2$.

Каждый элемент $z \in H(t_1,\dots,t_l)[\theta][X_1,\dots,X_n]$ представляется в виде $z = \sum_{0\leqslant i\leqslant N} z_i/z'$, где $z', z_i \in H_0[t_1,\dots,t_l,X_1,\dots,X_n]$, $z' \neq 0$ и наибольший общий делитель всех элементов $z', z_0,\dots,z_N$ равен 1 в кольце $H_0[t_1,\dots,t_l,X_1,\dots,X_n]$. Такое представление однозначно определено с точностью до знака в случае нулевой характеристики и с точностью до ненулевого множителя из $\mathbb{F}_p$, если $\mathrm{char}(k) = p > 0$. По определению

$$\deg_{t_1,\dots,t_l} z = \max_{0\leqslant i\leqslant N}\{\deg_{t_1,\dots,t_l} z_i, \deg_{t_1,\dots,t_l} z'\},$$
$$\deg_{X_1,\dots,X_n} z = \max_{0\leqslant i\leqslant N}\{\deg_{X_1,\dots,X_n} z_i, \deg_{X_1,\dots,X_n} z'\}$$

и длина записи коэффициентов равна $l(z) = \max_{0\leqslant i\leqslant N}\{l(z_i), l(z')\}$.

Пусть $f_1,\dots,f_m \in k[X_1,\dots,X_n]$ – многочлены. Эти многочлены заданы, и мы предполагаем, что

$$\deg_{X_1,\dots,X_n} f_i \leqslant d, \text{ где } \deg_{t_1,\dots,t_l} f_i \leqslant d_2$$

и $l(f_i) \leqslant M$ для всех i, $0 \leqslant i \leqslant m$, и некоторых $d, d_2 \geqslant 2$.

Обозначим через $I \subset \overline{k}[X_1,\dots,X_n] = A$ полиномиальный идеал, порождённый многочленами $f_1,\dots,f_m$. Мы предлагаем простой алгоритм для вычисления всех изолированных примарных компонент идеала I и доказываем теорему 1, см. ниже.

Более точно, пусть $\mathfrak{p}$ – изолированный ассоциированный простой идеал идеала I. Пусть $V_\mathfrak{p} = \mathcal{Z}(\mathfrak{p})$ – алгебраическое многообразие всех общих нулей многочленов из идеала $\mathfrak{p}$ в $\mathbb{A}^n(\overline{k})$. Пусть $\dim V_\mathfrak{p} = n - s$. Обозначим через $k_\mathfrak{p}$ конечное расширение поля k, которое является полем определения многообразия $V_\mathfrak{p}$. Пусть $I_\mathfrak{p}$ является $\mathfrak{p}$-примарной компонентой идеала I. Тогда для всякого $\mathfrak{p}$ мы строим поле $k_\mathfrak{p}$, поле частных $K'_\mathfrak{p}$ кольца определённых над $k_\mathfrak{p}$ регулярных функций $k_\mathfrak{p}[V_\mathfrak{p}]$

алгебраического многообразия $V_{\mathfrak{p}}$. Следовательно, поле частных $K_{\mathfrak{p}}$ кольца $A/\mathfrak{p}$ изоморфно $\overline{k}\otimes_{k_{\mathfrak{p}}} K'_{\mathfrak{p}}$. Далее, строятся следующие объекты.

(i) Полиномиальный идеал $J \subset \overline{k}[X_1,\dots,X_n]$, такой, что $I_{\mathfrak{p}}$ является единственной изолированной примарной компонентой идеала J. Идеал J задаётся системой образующих $g_{\mathfrak{p},1},\dots,g_{\mathfrak{p},m_{\mathfrak{p}}} \in k_{\mathfrak{p}}[X_1,\dots,X_n]$. Все степени удовлетворяют неравенствам $\deg_{X_1,\dots,X_n} g_{\mathfrak{p},i} \leqslant d^{2s}$, $1 \leqslant i \leqslant m_{\mathfrak{p}}$.

(ii) Конечномерную $K_{\mathfrak{p}}$-алгебру $K_{\mathfrak{p}} \otimes_A (A/I_{\mathfrak{p}})$. Эта алгебра задаётся её базисом над $K_{\mathfrak{p}}$ с таблицей умножения. Следовательно, $I_{\mathfrak{p}}$ совпадает с ядром естественного гомоморфизма $A \to K_{\mathfrak{p}} \otimes_A (A/I_{\mathfrak{p}})$. Фактически эти объекты заданы над полем $K'_{\mathfrak{p}}$ естественным образом.

Обозначим через $V = \mathcal{Z}(f_1,\dots,f_m)$ алгебраическое многообразие всех общих нулей многочленов $f_1,\dots,f_m$ в $\mathbb{A}^n(\overline{k})$. Отметим, что гомоморфизм $A/I \to K_{\mathfrak{p}} \otimes_A (A/I_{\mathfrak{p}})$ для примарного идеала $I_{\mathfrak{p}}$ является аналогом общей точки $\overline{k}[V] \to K_{\mathfrak{p}}$ неприводимой компоненты $\mathcal{Z}(\mathfrak{p})$ алгебраического многообразия V.

Теорема 1. *Время работы предложенного алгоритма для построения всех объектов из пунктов* (i) и (ii) *полиномиально от* $(d^n d_1 d_2)^{l+1}$, d^{n^2}, M_1, M_2, m *и* p. *Аналогично, например, работе* [3] *можно привести подробные эффективные оценки на степени и длины записи коэффициентов всех объектов, встречающихся в этом алгоритме* (*здесь мы оставляем подробности заинтересованному читателю*).

Таким образом, время работы алгоритма из теоремы 1 по существу то же самое, что и время работы алгоритма для решения системы полиномиальных уравнений $f_1 = \dots = f_m = 0$, см. [2–6].

§1. Доказательство теоремы 1

Прежде всего, мы сведём проблему к однородному случаю. Положим ${}^hA = \overline{k}[X_0,\dots,X_n]$. Для всякого многочлена $f \in A$ обозначим через

$$ {}^hf = X_0^{\deg_{X_1,\dots,X_n} f}(X_1/X_0,\dots,X_n/X_0) \in {}^hA $$

гомогенизацию многочлена f. Для всякого идеала $\mathfrak{a} \subset A$ определим

$$ {}^h\mathfrak{a} = \{z \in {}^hA : \exists N\, \exists a\, (0 \leqslant N \in \mathbb{Z} \,\&\, a \in \mathfrak{a} \,\&\, X_0^N z = {}^ha)\}. $$

По определению ${}^h\mathfrak{a}$ является гомогенизацией идеала $\mathfrak{a}$, так что ${}^h\mathfrak{a}$ – однородный идеал.

Обратно, если $\mathfrak{b} \subset {}^hA$ – однородный идеал, то положим $\mathfrak{b}' = \{b|_{X_0=1} : b \in \mathfrak{b}\}$. Тогда $\mathfrak{b}' \subset A$ является идеалом. Далее, для всякого идеала $\mathfrak{a} \subset A$ мы имеем $({}^h\mathfrak{a})' = \mathfrak{a}$.

Следующие утверждения получаются непосредственно, и мы оставляем их доказательства читателю. Здесь достаточно использовать стандартные факты, например, из [1].

Пусть $\mathfrak{p} \subset A$ – простой идеал. Тогда ${}^h\mathfrak{p} \subset {}^hA$ также является простым идеалом. Далее, если $\mathfrak{q}$ является $\mathfrak{p}$-примарным идеалом, то ${}^h\mathfrak{q}$ является ${}^h\mathfrak{p}$-примарным идеалом.

Пусть $\mathfrak{a} \subset A$ – произвольный идеал и $\mathfrak{a} = \bigcap\limits_{\mathfrak{p}\in \mathrm{Ass}(\mathfrak{a})} \mathfrak{a}_\mathfrak{p}$ является несократимым примарным разложением идеала $\mathfrak{a}$, где $\mathfrak{a}_\mathfrak{p}$ – $\mathfrak{p}$-примарная компонента идеала $\mathfrak{a}$ для всякого $\mathfrak{p} \in \mathrm{Ass}(\mathfrak{a})$. Тогда множество ассоциированных простых идеалов идеала ${}^h\mathfrak{a}$ равно $\{{}^h\mathfrak{p} : \mathfrak{p} \in \mathrm{Ass}(\mathfrak{a})\}$ и ${}^h\mathfrak{a} = \bigcap\limits_{\mathfrak{p}\in \mathrm{Ass}(\mathfrak{a})} {}^h\mathfrak{a}_\mathfrak{p}$ является несократимым примарным разложением идеала ${}^h\mathfrak{a} \subset {}^hA$.

Пусть $\mathfrak{a} \subset A$ – произвольный идеал. Положим $\overline{\mathfrak{a}}$ равным однородному идеалу кольца ${}^hA$, порождённому всеми многочленами $\{{}^ha : a \in \mathfrak{a}\}$. Тогда $\overline{\mathfrak{a}}' = \mathfrak{a}$. Далее, для всякого простого идеала $\mathfrak{p} \in \mathrm{Ass}(\overline{\mathfrak{a}}) \setminus \mathrm{Ass}({}^h\mathfrak{a})$ имеем $X_0 \in \mathfrak{p}$, и через $\overline{\mathfrak{a}}_\mathfrak{p}$ мы обозначаем $\mathfrak{p}$-примарную компоненту идеала $\overline{\mathfrak{a}}$ (в некотором фиксированном примарном разложении идеала $\overline{\mathfrak{a}}$). Тогда $\overline{\mathfrak{a}} = \bigcap\limits_{\mathfrak{p}\in \mathrm{Ass}(\mathfrak{a})} {}^h\mathfrak{q}_\mathfrak{p} \cap \bigcap\limits_{\mathfrak{p}\in \mathrm{Ass}(\overline{\mathfrak{a}})\setminus \mathrm{Ass}({}^h\mathfrak{a})} \overline{\mathfrak{a}}_\mathfrak{p}$ является несократимым примарным разложением идеала $\overline{\mathfrak{a}}$ (подсказка для доказательства: для достаточно большого целого числа $N \geqslant 0$ мы имеем ${}^h\mathfrak{a} = \overline{\mathfrak{a}} : X_0^N$). Положим ${}^\infty\mathfrak{a} = \bigcap\limits_{\mathfrak{p}\in \mathrm{Ass}(\overline{\mathfrak{a}})\setminus \mathrm{Ass}({}^h\mathfrak{a})} \mathfrak{q}_\mathfrak{p}$. Тогда $\overline{\mathfrak{a}} = {}^h\mathfrak{a} \cap {}^\infty\mathfrak{a}$ и $X_0^N \in {}^\infty\mathfrak{a}$ для достаточно большого целого числа $N \geqslant 0$.

Пусть $\mathfrak{b} \subset {}^hA$ – однородный идеал. Тогда ${}^hA/\mathfrak{b}$ является градуированным ${}^hA$-модулем. Для всякого целого числа $m \geqslant 0$ через $({}^hA/\mathfrak{b})_m$ обозначим m-ю однородную компоненту модуля ${}^hA/\mathfrak{b}$. Тогда $({}^hA/\mathfrak{b})_m$ является конечномерным векторным пространством над полем $\overline{k}$. Характеристическая функция χ идеала $\mathfrak{b}$ определяется по формуле $\chi(m) = \dim_{\overline{k}}({}^hA/\mathfrak{b})_m$. Существует многочлен $P \in \mathbb{Q}[Z]$ (это многочлен Гильберта модуля ${}^hA/\mathfrak{b}$), такой, что для всех достаточно больших

$m \geqslant 0$ мы имеем $\chi(m) = P(m)$. Мы будем обозначать $\chi(m) = \chi_{\mathfrak{b}}(m)$ и $P = P_{\mathfrak{b}}$, если важна зависимость от $\mathfrak{b}$.

Пусть $V_{\mathfrak{b}}$ – многообразие всех общих нулей в $\mathbb{P}^n(\overline{k})$ многочленов из идеала $\mathfrak{b}$. Степень $\deg_Z P$ совпадает с размерностью $\dim V_{\mathfrak{p}}$. Пусть $\deg_Z P \geqslant 0$. Тогда степень $\deg \mathfrak{b}$ идеала $\mathfrak{b}$ по определению равна $\deg \mathfrak{b} = (\deg_Z P)!\mathrm{lc}_Z P$, где $\mathrm{lc}_Z P$ – старший коэффициент многочлена P. Если $\deg_Z P = -1$, т.е. $P = 0$ (или, что то же самое, $V_{\mathfrak{b}} = \varnothing$), то по определению $\deg \mathfrak{b} = 0$. Мы имеем $\deg \mathfrak{b} \in \mathbb{Z}$ для всех однородных идеалов $\mathfrak{b}$.

В [7, лемма 1], мы доказали следующий факт. Пусть $f_1, \ldots, f_s \in {}^hA$, $1 \leqslant s \leqslant n$, являются однородными многочленами. Положим $\mathfrak{b} \subset {}^hA$ равным идеалу, порождённому многочленами $f_1, \ldots, f_s$. Пусть $\mathfrak{b} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(b)} \mathfrak{b}_{\mathfrak{p}}$ – примарное разложение идеала $\mathfrak{b}$. Обозначим через $\mathrm{Assi}(\mathfrak{b})$ множество всех изолированных простых идеалов идеала $\mathfrak{a}$. Положим $\mathfrak{b}^{(s)} = \bigcap_{\mathfrak{p} \in \mathrm{Assi}(\mathfrak{b}),\, \mathrm{ht}(\mathfrak{p}) = s} \mathfrak{b}_{\mathfrak{p}}$, где $\mathrm{ht}(\mathfrak{p})$ – высота простого идеала $\mathfrak{p}$ (здесь $\mathrm{ht}(\mathfrak{p})$ равна коразмерности многообразия $\mathcal{Z}(\mathfrak{p})$ в $\mathbb{P}^n(\overline{k})$). Тогда

$$\chi_{\mathfrak{b}^{(s)}}(m) \leqslant \binom{m+n-s}{n-s} \prod_{1 \leqslant i \leqslant s} d_i$$

и, следовательно, $\deg \mathfrak{b}^{(s)} \leqslant d_1 d_2 \ldots d_s$. Это обобщает неравенство Безу на случай примарных идеалов (последнее неравенство для $\deg \mathfrak{b}^{(s)}$ нетривиально, поскольку размерность $\dim V_{\mathfrak{b}}$ может быть больше $n - s$).

Лемма 1. *Пусть $\mathfrak{p} \subset {}^hA$ – однородный простой идеал и $\mathfrak{q}$ является $\mathfrak{p}$-примарным идеалом степени $\deg \mathfrak{q} = \nu \deg \mathfrak{p} \geqslant 1$ для некоторого $\nu > 0$. Тогда ν – целое число и $\mathfrak{p}^\nu \subset \mathfrak{q}$.*

Доказательство. Действительно, существует ненулевой однородный многочлен $a \in {}^hA \setminus \mathfrak{q}$, такой, что $\mathfrak{p}a \subset \mathfrak{q}$. Положим $\mathfrak{q}_1 = {}^hAa + \mathfrak{q}$. Тогда для всякого $\mathfrak{P} \in \mathrm{Ass}(\mathfrak{q}_1)$ имеем $\mathfrak{P} \supset \mathfrak{p}$. Положим $\mathfrak{q}_{1,\mathfrak{P}}$ равным $\mathfrak{P}$-примарной компоненте идеала $\mathfrak{q}_1$ в некотором фиксированном примарном разложении идеала $\mathfrak{q}_1$. Если $\mathfrak{p} \notin \mathrm{Ass}(\mathfrak{q}_1)$, то положим $\mathfrak{q}_{1,\mathfrak{p}} = {}^hA$. Рассматривая эпиморфизм ${}^hA/\mathfrak{q}_1 \to {}^hA/\mathfrak{q}_{1,\mathfrak{p}}$ и мономорфизм ${}^hA/\mathfrak{q}_1 \to \prod_{\mathfrak{P} \in \mathrm{Ass}(\mathfrak{q}_1)} {}^hA/\mathfrak{P}$, мы получаем, что в любом случае $\chi_{\mathfrak{q}_{1,\mathfrak{p}}}(m) \leqslant \chi_{\mathfrak{q}_1}(m) \leqslant \sum_{\mathfrak{P} \in \mathrm{Ass}(\mathfrak{q}_1)} \chi_{\mathfrak{q}_{1,\mathfrak{P}}}(m)$ для всякого целого числа $m \geqslant 0$. Но если $\mathfrak{P} \neq \mathfrak{p}$, то $\deg P_{\mathfrak{q}_{1\mathfrak{P}}} < \deg P_{\mathfrak{p}}$, и если $\mathfrak{p} \in \mathrm{Ass}(\mathfrak{q}_1)$, то $\deg P_{\mathfrak{q}_{1\mathfrak{P}}} < \deg P_{\mathfrak{q}_{1,\mathfrak{p}}}$. Теперь из точной последовательности $0 \to A/\mathfrak{p} \to A/\mathfrak{q} \to A/\mathfrak{q}_1 \to 0$ мы

получаем, что $\deg \mathfrak{q} = \deg \mathfrak{p} + \deg \mathfrak{q}_{1,\mathfrak{p}}$. Положим $\nu_1 = \deg \mathfrak{q}_1 / \deg \mathfrak{p}$, если $\mathfrak{q}_{1,\mathfrak{p}} \neq {}^hA$, и $\nu_1 = 0$, если $\mathfrak{q}_{1,\mathfrak{p}} = {}^hA$. По индукции $\nu_1 \in \mathbb{Z}$ и $\mathfrak{p}^{\nu_1} \subset \mathfrak{q}_{1,\mathfrak{p}}$. Следовательно, $\nu = \nu_1 + 1 \in \mathbb{Z}$ и $\mathfrak{p}^{\nu_1} \subset {}^hAa + \mathfrak{q}$. Таким образом, $\mathfrak{p}^{\nu} \subset \mathfrak{q}$. Лемма доказана. □

Лемма 2. *Пусть многочлены $f_1, \ldots, f_m$ – такие же, как во введении. Положим $\mathfrak{f} = \sum\limits_{1 \leqslant i \leqslant m} Af_i$ равным идеалу кольца A. Пусть $\mathfrak{p} \in \operatorname{Assi}(\mathfrak{f})$ и $\operatorname{ht}(\mathfrak{p}) = s$, где $0 \leqslant s \leqslant n$. Обозначим через $\mathfrak{b}$ идеал, порождённый всеми полиномами b^{p^s}, где $b \in \mathfrak{p}$ и $\deg_{X_1,\ldots,X_n} b \leqslant d^s$. Положим $\mathfrak{q} = \mathfrak{f} + \mathfrak{b}$. Тогда $\operatorname{Assi}(\mathfrak{q}) = \{\mathfrak{p}\}$ и $\mathfrak{p}$-примарная компонента $\mathfrak{q}_{\mathfrak{p}}$ идеала $\mathfrak{q}$ совпадает с $\mathfrak{p}$-примарной компонентой $\mathfrak{f}_{\mathfrak{p}}$ идеала $\mathfrak{f}$.*

Доказательство. Мы имеем $\mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\mathfrak{p})$ в $\mathbb{A}^n(\overline{k})$, см. [2–4], более точно, например, [4, лемма 7]. Аналогично $\mathcal{Z}({}^h\mathfrak{b}) = \mathcal{Z}({}^h\mathfrak{p})$. Поэтому также $\mathcal{Z}(\mathfrak{q}) = \mathcal{Z}(\mathfrak{p})$ и $\mathcal{Z}({}^h\mathfrak{q}) = \mathcal{Z}({}^h\mathfrak{p})$.

Существуют многочлены $g_1, \ldots, g_s \in \mathfrak{f}$, такие, что $\deg g_i \leqslant d$ для всех $1 \leqslant i \leqslant s$ и $\mathcal{Z}(\mathfrak{p})$ является неприводимой компонентой алгебраического многообразия $\mathcal{Z}(g_1, \ldots, g_s)$ в $\mathbb{A}^n(\overline{k})$. Положим $\mathfrak{g} = \sum_{1 \leqslant i \leqslant s} Ag_i \subset A$. Тогда $\mathfrak{p} \in \operatorname{Assi}(\mathfrak{g})$. Через $\mathfrak{g}_{\mathfrak{p}}$ обозначим $\mathfrak{p}$-примарную компоненту идеала $\mathfrak{g}$. Тогда, очевидно, $\mathfrak{g}_{\mathfrak{p}} \subset \mathfrak{f}_{\mathfrak{p}}$. Следовательно, также ${}^h\mathfrak{g}_{\mathfrak{p}} \subset {}^h\mathfrak{f}_{\mathfrak{p}}$. Мы имеем $\deg {}^h\mathfrak{g}_{\mathfrak{p}} \leqslant d^s$, см. [7, лемма 1]. Следовательно, $\deg {}^h\mathfrak{f}_{\mathfrak{p}} \leqslant d^s$. Согласно лемме 1, применённой к ${}^h\mathfrak{p}$ вместо $\mathfrak{p}$, имеем $({}^h\mathfrak{p})^{d^s} \subset {}^h\mathfrak{f}_{\mathfrak{p}}$. Следовательно, также ${}^h\mathfrak{b} \subset {}^h\mathfrak{f}_{\mathfrak{p}}$. Поэтому $\mathfrak{b} \subset \mathfrak{f}_{\mathfrak{p}}$. Отсюда вытекает, что $\mathfrak{q}_{\mathfrak{p}} = \mathfrak{f}_{\mathfrak{p}}$. Лемма доказана. □

Сейчас мы можем описать требуемый алгоритм и доказать теорему 1 (однако мы оставляем подробности читателю). Применяя алгоритм для решения систем полиномиальных уравнений, см. [2–6], мы находим все простые идеалы $\mathfrak{p} \in \operatorname{Assi}(\mathfrak{f})$. Более точно, положим $I = \mathfrak{f}$, см. лемму 2. Для всякого $\mathfrak{p} \in \operatorname{Assi}(\mathfrak{f})$ с $\operatorname{ht}(\mathfrak{p}) = s$ построим поля $k_{\mathfrak{p}}$, $K'_{\mathfrak{p}}$, $K_{\mathfrak{p}}$ и общую точку $A/I \to K_{\mathfrak{p}}$. Затем мы строим систему образующих идеала $\mathfrak{b}$ (линейно независимую над полем $k_{\mathfrak{p}}$), см. лемму 2, и полагаем $J = I + \mathfrak{b}$. После этого мы находим систему образующих $g_{\mathfrak{p},1}, \ldots, g_{\mathfrak{p},m_{\mathfrak{p}}} \in k_{\mathfrak{p}}[X_1, \ldots, X_n]$ идеала J.

Теперь $K_{\mathfrak{p}} \otimes_A (A/J)$ является конечномерной $K_{\mathfrak{p}}$-алгеброй. Мы строим её базис над полем $K_{\mathfrak{p}}$ с таблицей умножения (фактически эта алгебра определена над полем $K'_{\mathfrak{p}}$). Рассмотрим мультипликативно замкнутое множество $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$. Тогда можно отождествить $K \otimes_A J =$

$S_{\mathfrak{p}}^{-1}J = S_{\mathfrak{p}}^{-1}I_{\mathfrak{p}} = K \otimes_A I_{\mathfrak{p}}$. Следовательно, $K_{\mathfrak{p}} \otimes_A (A/J) = S_{\mathfrak{p}}^{-1}(A/J) = S_{\mathfrak{p}}^{-1}(A/I_{\mathfrak{p}}) = K_{\mathfrak{p}} \otimes_A (A/I_{\mathfrak{p}})$.

Оценка на время работы описанного алгоритма немедленно следует из [2–6]. Аналогично можно получить оценки на степени и длины записи коэффициентов всех объектов, встречающихся в алгоритме. Теорема доказана.

Список литературы

1. Н. Бурбаки, *Коммутативная алгебра,* М.: Мир, 1971.
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. А. Л. Чистов, *Улучшение оценки сложности для решения систем алгебраических уравнений.* — Зап. научн. семин. ПОМИ **390** (2011), 299–306.
4. А. Л. Чистов, *Системы с параметрами, или эффективное решение систем полиномиальных уравнений 33 года спустя. I.* — Зап. научн. семин. ПОМИ **462** (2017), 122–166.
5. А. Л. Чистов, *Системы с параметрами, или эффективное решение систем полиномиальных уравнений 33 года спустя. II.* — Зап. научн. семин. ПОМИ **468** (2018), 138–176.
6. А. Л. Чистов, *Системы с параметрами, или эффективное решение систем полиномиальных уравнений 33 года спустя. III.* — Зап. научн. семин. ПОМИ **481** (2018), 146–177.
7. А. Л. Чистов, *Неравенства для функций Гильберта и примарные разложения.* — Алгебра и анализ **19**, вып. 6 (2007), 143–172.
8. А. Л. Чистов, *Дважды экспоненциальная нижняя оценка на степень системы образующих полиномиального простого идеала.* — Алгебра и анализ **20**, вып. 6 (2008), 186–213.
9. W. Decker, G. M. Greuel, G. Pfister, *Primary decomposition: algorithms and comparisons.* In: B. H. Matzat, G. M. Greuel, G. Hiss (eds.), Algorithmic Algebra and Number Theory, Springer, Berlin–Heidelberg (1999), pp. 187–220.
10. G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.* — Math. Ann. **95** (1926), 736–788.
11. E. Lasker, *Zur Theorie der Moduln und Ideale.* — Math. Ann. **60** (1905), 19–116.
12. D. Lazard, *Résolution des systèmes d'équations algébriques.* — Theoret. Comput. Sci. **15** (1981), 77–110.
13. N. Masayuki, *New algorithms for computing primary decomposition of polynomial ideals.* In: K. Fukuda, J. van der Hoeven, M. Joswig, N. Takayama (eds.), Mathematical Software – ICMS 2010, Lect. Notes Comput. Sci. **6327**, Springer, Berlin–Heidelberg, 2010, pp. 233–244.
14. E. Noether, *Idealtheorie in Ringbereichen.* — Math. Ann. **83**, No. 1 (1921), 24–66.

15. V. Ortiz, *Sur une certaine décomposition canonique d'un idéal en intersection d'idéaux primaires dans un anneau noethérien commutatif.* — C. R. Acad. Sci. Paris **248** (1959), 3385–3387.
16. A. Seidenberg, *Constructions in algebra.* — Trans. Amer. Math. Soc. **197** (1974), 273–313.
17. T. Shimoyama, K. Yokoyama, *Localization and primary decomposition of polynomial ideals.* — J. Symbolic Comput. **22** (1996), 247–277.
18. Y. Yao, *Primary decomposition: compatibility, independence and linear growth.* — Proc. Amer. Math. Soc. **130**, No. 6 (2002), 1629–1637.

Chistov A. L. Subexponential-time computation of isolated primary components of a polynomial ideal.

We suggest an algorithm for constructing all the isolated primary components of a given polynomial ideal. At the output, they are determined by systems of generators up to embedded components, and also as kernels of some homomorphisms. The complexity of this algorithm is subexponential in the size of the input data.

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

Поступило 31 августа 2020 г.