Subexponential–time computation of isolated primary components of a polynomial ideal

Alexander L. Chistov

St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia,
e-mail: alch@pdmi.ras.ru

Primary decomposition is an important construction in commutative algebra. It was introduced by E. Lasker [11] for polynomial rings and convergent power series rings, and in full generality by E. Noether [14].

[11] **Lasker E.:**, *“Zur Theorie der Moduln und Ideale”*, Mathematische Annalen, 60 (1905) p. 19–116

[14] **Noether E.:**, *“Idealtheorie in Ringbereichen”*, Mathematische Annalen, 83 (1921) No. 1, p. 24-66.

A canonical primary decomposition was suggested by V. Ortiz [15].

[15] **Ortiz V.:** *“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), p. 3385–3387.

Even now this subject is actual. For example, some interesting results about primary decomposition have been obtained by Y. Yao [18].

[18] **Yao Y.:** *"Primary decomposition: compatibility, independence and linear growth"*, Proc. Amer. Math. Soc. 130 (2002), no. 6, p. 1629–1637.

The first algorithm for computing primary decompositions for polynomial rings over a field of characteristic zero was published by Noether's student G. Hermann [10].

[10] **Hermann G.:**, *"Die Frage der endlich vielen Schritte in der Theorie der Polynomideale"*, Mathematische Annalen, 95 (1926) p. 736-788

Since that time many authors suggested algorithms for primary decomposition. The literature on this subject is vast. Probably one of the most important here is the paper of A. Seidenberg [16].

[16] **Seidenberg A.:** *“Constructions in algebra”*, Transactions of the American Mathematical Society 197 (1974) p. 273–313

Soon it was understood that in general case this problem is hard. All upper bounds for the complexity of primary decomposition were double exponential in the number of variable.

A good estimation for the complexity can be obtained here only in particular cases, for example, for ideals, determining zero–dimensional algebraic varieties. The zero–dimensional case is more or less easy by [12].

[12] **Lazard D.:** *“Résolution des systèmes d’équations algébriques”*, Theor. Comput. Sci. v.15 (1981), p. 77–110.

In other papers, see, e.g., [9], [17], [13], the authors interested mainly in practical implementation of primary decomposition without estimations of the complexity.

[9] **Decker W., Greuel G.M., Pfister G.:** *"Primary Decomposition: Algorithms and Comparisons"*, In: Matzat B.H., Greuel G.M., Hiss G. (eds.) Algorithmic Algebra and Number Theory (1999). p. 187–220 Springer, Berlin, Heidelberg.

[17] **Shimoyama T., Yokoyama K.:** *"Localization and Primary Decomposition of Polynomial Ideals"*, J. Symbolic Computation 22 (1996), p. 247–277

[13] **Masayuki N.:** *"New Algorithms for Computing Primary Decomposition of Polynomial Ideals"*, In: Fukuda K., van der Hoeven J., Joswig M., Takayama N. (eds.) - Mathematical Software - ICMS 2010, p. 233–244, LNCS 6327 (2010) Springer, Berlin, Heidelberg.

Surprisingly in all these papers one can not find lower bounds for primary decompositions. Actually at present one can obtain double–exponential lower bounds for primary decomposition only from our results, see [8]. More precisely, one can deduce from [8] that there is an ideal given by homogeneous polynomials n–variables of degrees D^n such that its primary component is a prime ideal $\mathfrak{p}$ and any system of generators of $\mathfrak{p}$ contains a polynomial of degree at least $d^{2^{cn}}$ for an absolute constant $c > 0$. From [8] one can also easily obtain a double–exponential lower bound for the degrees of some embedded components of an ideal.

[8] **Chistov A. L.:**, *“Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal”*, Algebra i Analiz, 20 (2008) No.6, p. 186–213 (in Russian) [English transl.: St. Petersburg Math. J., 20:6 (2009), p. 983–1001].

By our opinion at present all the constructed algorithms for primary decomposition are far from the final perfect form. We think that one can find a canonical algorithm for canonical primary decomposition of a homogeneous polynomial ideal. It would be of great interest from theoretical point of view. But in this paper our aim is modest. We would like to suggest an algorithm for constructing all the isolated primary components of a polynomial ideal such that they are given up to embedded components, see below 1) and 2). The advantage of our approach is that the complexity of this construction is subexponential in the size of the input data. To substantiate our algorithm we use a non–trivial fact: estimation of the degree of the isolated primary ideal, see Lemma 1 [7] and below the proof of Theorem 1. Now we proceed to the details.

Let k be a field of arbitrary characteristic $p \geqslant 0$ with an algebraic closure $\overline{k}$. Let H be a primitive subfield of the field k and $H(t_1, \dots, t_l)$ be the field of rational functions in algebraically independent over H variables $t_1, \dots, t_l$. We assume that the field k is a finite separable extention $H(t_1, \dots, t_l)$ given by its primitive element θ. The minimal polynomial $\Phi \in H(t_1, \dots, t_l)[Z]$ of the element θ is given and the leading coefficient $\mathrm{lc}_Z \Phi = 1$.

Put $H_0 = \mathbb{Z}$ if $H = \mathbb{Q}$ and $H_0 = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ if $\mathrm{char}(k) = p > 0$. By definition the length $l(a)$ of an element $a \in H_0$ is equal to $[\log_2 |a|] + 2$ if $H_0 = \mathbb{Z}$ and $[\log_2 p] + 1$ if $H_0 = \mathbb{F}_p$. Additionally we suppose that $\Phi \in H_0[t_1, \dots, t_l, Z]$ (there is no loss of generality here).

Let $X_1, \dots, X_n$ be variables. Each polynomial $g \in H_0[t_1, \dots, t_l, X_1, \dots, X_n]$ is represented in the form $g = \sum_{i_1, \dots, i_l, j_1, \dots, j_n} g_{i_1, \dots, i_l, j_1, \dots, j_n} t_1^{i_1} \dots t^{i_l} X_1^{i_1} \dots X_n^{i_n}$ where all the coefficients $g_{i_1, \dots, i_l, j_1, \dots, j_n} \in H_0$. The degrees $\deg_{i_1, \dots, i_l} g$ and $\deg_{X_1, \dots, X_n} g$ are defined in a natural way. Further by definition the length of coefficients $l(g) = \max_{i_1,\ldots,i_l,\, j_1,\ldots,j_n} l(g_{i_1,\ldots,i_l,j_1,\ldots,j_n})$.

We represent $\Phi = \sum_{0 \leqslant i \leqslant N} \Phi_i Z^i$ where all $\Phi_i \in H_0[t_1, \ldots, t_l]$ and $N = \deg_Z(\Phi) - 1$. By definition $l(\Phi) = \max_{0 \leqslant i \leqslant N} l(\Phi_i)$. We shall assume in what follows that $l(\Phi) \leqslant M_1$ and the degree $\deg_{t_1,\ldots,t_l,Z} \Phi \leqslant d_1$ where $d_1 \geqslant 2$.

Each element $z \in H(t_1, \ldots, t_l)[\theta][X_1, \ldots, X_n]$ is represented in the form $z = \sum_{0 \leqslant i \leqslant N} z_i / z'$ where all $z', z_i \in H_0[t_1, \ldots, t_l, X_1, \ldots, X_n]$, $z' \neq 0$ and the the greatest common divisor of all the elements $z', z_0, \ldots, z_N$ is equal to 1 in the ring $H_0[t_1, \ldots, t_l, X_1, \ldots, X_n]$. Such a representation is uniquely defined up to a sign in the case of zero–characteristic and up to a nonzero factor from $\mathbb{F}_p$ if $\mathrm{char}(k) = p > 0$. By definition the degrees

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

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

and the length of coefficients $l(z) = \max_{0 \leqslant i \leqslant N} \{l(z_i), l(z')\}$.

Let $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ be polynomials. These polynomials are given and we assume that the degrees $\deg_{X_1,\ldots,X_n} f_i \leqslant d$ where $\deg_{t_1,\ldots,t_l} f_i \leqslant d_2$ and the lengths of coefficients $l(f_i) \leqslant M$ for all $0 \leqslant i \leqslant m$ and some $d, d_2 \geqslant 2$.

Denote by $I \subset \overline{k}[X_1, \ldots, X_n] = A$ the polynomial ideal generated by the polynomials $f_1, \ldots, f_m$. We suggest a simple algorithm for computing all the isolated primary components of the ideal I and prove Theorem 1, see below.

More precisely, let $\mathfrak{p}$ be an arbitrary isolated associated prime ideal of the ideal I. Let $V_{\mathfrak{p}} = \mathcal{Z}(\mathfrak{p})$ be the algebraic variety of all common zeroes of the polynomials from the ideal $\mathfrak{p}$ in $\mathbb{A}^n(\overline{k})$. Let the dimension $\dim V_{\mathfrak{p}} = n - s$. Denote by $k_{\mathfrak{p}}$ a finite extension of the field k which is a field of definition of the variety $V_{\mathfrak{p}}$. Let $I_{\mathfrak{p}}$ be the $\mathfrak{p}$–primary component of the ideal I.

Then for each $\mathfrak{p}$ we construct the field $k_{\mathfrak{p}}$, the field of fractions $K'_{\mathfrak{p}}$ of the ring of defined over $k_{\mathfrak{p}}$ regular functions $k_{\mathfrak{p}}[V_{\mathfrak{p}}]$ of the algebraic variety $V_{\mathfrak{p}}$. Hence the field of fractions $K_{\mathfrak{p}}$ of the ring $A/\mathfrak{p}$ is isomorphic to $\overline{k} \otimes_{k_{\mathfrak{p}}} K'_{\mathfrak{p}}$. Furthermore, the following objects are constructed.

1) A polynomial ideal $J \subset \overline{k}[X_1, \ldots, X_n]$ such that $I_{\mathfrak{p}}$ is a unique isolated primary component of J. The ideal J is given by its system of generators $g_{\mathfrak{p},1}, \ldots, g_{\mathfrak{p},m_{\mathfrak{p}}} \in k_{\mathfrak{p}}[X_1, \ldots, X_n]$. All the degrees $\deg_{X_1,\ldots,X_n} g_{\mathfrak{p},i} \leqslant d^{2s}$, $1 \leqslant i \leqslant m_{\mathfrak{p}}$.

2) A finite dimensional $K_{\mathfrak{p}}$–algebra $K_{\mathfrak{p}} \otimes_A (A/I_{\mathfrak{p}})$. This algebra is given by its basis over $K_{\mathfrak{p}}$ and the multiplication table. Hence $I_{\mathfrak{p}}$ coincides with the kernel of the natural homomorphism $A \to K_{\mathfrak{p}} \otimes_A (A/I_{\mathfrak{p}})$. Actually these objects are defined over the field $K'_{\mathfrak{p}}$ in a natural sense.

Denote by $V = \mathcal{Z}(f_1, \ldots, f_m)$ the algebraic variety of all common zeroes of the polynomials $f_1, \ldots, f_m$ in $\mathbb{A}^n(\overline{k})$. Notice that the homomorphism $A/I \to K_{\mathfrak{p}} \otimes_A (A/I_{\mathfrak{p}})$ for a primary ideal $I_{\mathfrak{p}}$ is an analog of the generic point $\overline{k}[V] \to K_{\mathfrak{p}}$ of the irreducible component $\mathcal{Z}(\mathfrak{p})$ of the algebraic variety V.

THEOREM 1 *The working time of the suggested algorithm for constructing all the objects from the items 1) and 2) is polynomial in d^{n^2}, $(d^n d_1 d_2)^{l+1}$, M_1, M_2, m and p. Similarly to, e.g., [3] one can give also detailed efficient estimates for degrees and lengths of coefficients of all the objects involved in this algorithm (here we leave the details to the interested reader).*

So the working time of the algorithm Theorem 1 is essentially the same as the working time of the algorithm for solving system of polynomial equations $f_1 = \ldots = f_m = 0$, see [2]–[6].

References

[1] **Bourbaki N.:**, *“Algèbre commutative”, Chap. 1–7* Actualités Sci. Indust., nos. 1290, 1293, 1308, 1314, Paris 1961, 1964, 1965.

[2] **Chistov A. L.:** *“Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time”*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 137 (1984), p. 124–188 (in Russian) [English transl.: J. Sov. Math. 34, (4), (1986) p. 1838–1882].

[3] **Chistov A. L.:** *“An improvement of the complexity bound for solving systems of polynomial equations”*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 390 (2011), p. 299–306.

[4] **Chistov A. L.:** *“Systems with Parameters, or Efficiently Solving Sys-*

tems of Polynomial Equations 33 Years Later. I", Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 462 (2017), p. 122–166 (in Russian) [English transl.: Journal of Mathematical Sciences, v. 232 (2018) Issue 2, p. 177-203].

[5] **Chistov A. L.:** *"Systems with Parameters or Efficiently Solving Systems of Polynomial Equations, 33 Years Later. II"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 468 (2018), p. 138–176 (in Russian) [English transl.: Journal of Mathematical Sciences, v. 240 (2019) Issue 5, p. 594-616].

[6] **Chistov A. L.:** *"Systems with Parameters or Efficiently Solving Systems of Polynomial Equations, 33 Years Later. III"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 481 (2018), p. 146–177 (in Russian) [English transl.: Journal of Mathematical Sciences v.247 Issue 5, p. 738–757].

[7] **Chistov A. L.:** *“Inequalities for Hilbert functions and Primary Decompositions”*, Algebra i Analiz, 19 (2007) No.6 p. 143-172 (in Russian) [English transl.: St. Petersburg Math. Journal, Vol. 19 (2008), No. 6, p. 975–994].

[8] **Chistov A. L.:**, *“Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal”*, Algebra i Analiz, 20 (2008) No.6, p. 186–213 (in Russian) [English transl.: St. Petersburg Math. J., 20:6 (2009), p. 983–1001].

[9] **Decker W., Greuel G.M., Pfister G.:** *“Primary Decomposition: Algorithms and Comparisons”*, In: Matzat B.H., Greuel G.M., Hiss G. (eds.) Algorithmic Algebra and Number Theory (1999). p. 187–220 Springer, Berlin, Heidelberg.

[10] **Hermann G.:**, *"Die Frage der endlich vielen Schritte in der Theorie der Polynomideale"*, Mathematische Annalen, 95 (1926) p. 736-788

[11] **Lasker E.:**, *"Zur Theorie der Moduln und Ideale"*, Mathematische Annalen, 60 (1905) p. 19–116

[12] **Lazard D.:** *"Résolution des systèmes d'équations algébriques"*, Theor. Comput. Sci. v.15 (1981), p. 77–110.

[13] **Masayuki N.:** *"New Algorithms for Computing Primary Decomposition of Polynomial Ideals"*, In: Fukuda K., van der Hoeven J., Joswig M., Takayama N. (eds.) - Mathematical Software - ICMS 2010, p. 233–244, LNCS 6327 (2010) Springer, Berlin, Heidelberg.

[14] **Noether E.:**, *"Idealtheorie in Ringbereichen"*, Mathematische Annalen, 83 (1921) No. 1, p. 24-66.

[15] **Ortiz V.:** *"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), p. 3385–3387.

[16] **Seidenberg A.:** *"Constructions in algebra"*, Transactions of the American Mathematical Society 197 (1974) p. 273–313

[17] **Shimoyama T., Yokoyama K.:** *"Localization and Primary Decomposition of Polynomial Ideals"*, J. Symbolic Computation 22 (1996), p. 247–277

[18] **Yao Y.:** *"Primary decomposition: compatibility, independence and linear growth"*, Proc. Amer. Math. Soc. 130 (2002), no. 6, p. 1629–1637.