Journal of Symbolic Computation 82 (2017) 123–133

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Bivariate triangular decompositions in the presence of asymptotes

Sylvain Lazard [a], Marc Pouget [a], Fabrice Rouillier [b]

[a] Inria, LORIA laboratory (Inria, CNRS, Université de Lorraine), Nancy, France
[b] Inria, Institut de Mathématiques de Jussieu, Paris, France

ARTICLE INFO

Article history:
Received 17 September 2015
Accepted 12 January 2017
Available online 31 January 2017

Keywords:
Polynomial system solving
Bivariate system
Triangular decomposition
Asymptotes

ABSTRACT

Given two coprime polynomials P and Q in $\mathbb{Z}[x, y]$ of degree at most d and coefficients of bitsize at most τ, we address the problem of computing a triangular decomposition $\{(U_i(x), V_i(x, y))\}_{i\in\mathcal{I}}$ of the system $\{P, Q\}$.

The state-of-the-art worst-case complexities for computing such triangular decompositions when the curves defined by the input polynomials do not have common vertical asymptotes are $\widetilde{O}(d^4)$ for the arithmetic complexity and $\widetilde{O}_B(d^6 + d^5\tau)$ for the bit complexity, where $\widetilde{O}$ refers to the complexity where polylogarithmic factors are omitted and O_B refers to the bit complexity.

We show that the same worst-case complexities can be achieved even when the curves defined by the input polynomials may have common vertical asymptotes. We actually present refined complexities, $\widetilde{O}(d_x d_y^3 + d_x^2 d_y^2)$ for the arithmetic complexity and $\widetilde{O}_B(d_x^3 d_y^3 + (d_x^2 d_y^3 + d_x d_y^4)\tau)$ for the bit complexity, where d_x and d_y bound the degrees of P and Q in x and y, respectively. We also prove that the total bitsize of the decomposition is in $\widetilde{O}((d_x^2 d_y^3 + d_x d_y^4)\tau)$.

1. Introduction

Computing triangular decompositions of algebraic systems is a well-known problem. In the special case of bivariate systems, given two coprime polynomials P and Q in $\mathbb{Z}[x, y]$, the triangular decomposition of the system $\{P, Q\}$ is a set of regular triangular systems, each of the form $\{U(x), V(x, y)\}$

E-mail addresses: Sylvain.Lazard@inria.fr (S. Lazard), Marc.Pouget@inria.fr (M. Pouget), Fabrice.Rouillier@inria.fr (F. Rouillier).

http://dx.doi.org/10.1016/j.jsc.2017.01.004
0747-7171/

with coefficients in $\mathbb{Z}$, whose sets of solutions are disjoint and are exactly those of $\{P, Q\}$. Recall that a triangular system $\{U(x), V(x, y)\}$ is said regular if U and the leading coefficient of V with respect to y are coprime.

For computing triangular decompositions of bivariate systems, a classical algorithm using subresultant sequences was first introduced by González-Vega and El Kahoui in the context of computing the topology of curves (González-Vega and El Kahoui, 1996). This algorithm is based on a direct consequence of the specialization property of subresultants and of the gap structure theorem, which implies the following (see Theorem 3): given two polynomials $P = \sum_{i=0}^{p} a_i(x)y^i$ and $Q = \sum_{i=0}^{q} b_i(x)y^i$ in $\mathbb{Z}[x, y]$ and $\alpha \in \mathbb{R}$ such that the leading coefficients $a_p(\alpha)$ and $b_q(\alpha)$ do not both vanish, then the first (with respect to increasing i) nonzero subresultant $\mathrm{Sres}_{y,i}(P, Q)(\alpha, y)$ is of degree i and is equal to the gcd of $P(\alpha, y)$ and $Q(\alpha, y)$. Note that values α such that $a_p(\alpha)$ and $b_q(\alpha)$ both vanish are exactly the x-coordinates of the common vertical asymptotes of the curves defined by P and Q, which we refer to as the common vertical asymptotes of the polynomials, for simplicity. Hence, when P and Q do not have common vertical asymptotes, the gap structure theorem induces a decomposition of the system $\{P, Q\}$ into triangular subsystems $\{U_i(x), \mathrm{Sres}_{y,i}(P, Q)(x, y)\}$ where the product of the U_i is the (squarefree part of the) resultant of P and Q with respect to y.

If the input polynomials have degree at most d and coefficients of bitsize at most τ, the worst-case bit complexity of this algorithm was initially analyzed in $\widetilde{O}_B(d^{16} + d^{14}\tau^2)$ (González-Vega and El Kahoui, 1996). The complexity analysis was later improved to $\widetilde{O}_B(d^7 + d^6\tau)$ (Diochnos et al., 2009, §4.2) and more recently to $\widetilde{O}_B(d^6 + d^5\tau)$ by considering amortized bounds on the degrees and bitsizes of factors of the resultant (Bouzidi et al., 2016, Proposition 16). No better complexity is known for computing triangular decompositions, even in the expected Las Vegas or Monte Carlo settings and even in the absence of common vertical asymptotes.

In the general case when P and Q (may) admit common vertical asymptotes, the natural solution for computing a (full) triangular decomposition is to first use González-Vega and El Kahoui algorithm to compute the triangular decomposition of the solutions of $\{P, Q\}$ that do not lie on common vertical asymptotes (this can be done by removing from the resultant of P and Q the solutions corresponding to these asymptotes, i.e., $\gcd(a_p, b_q)$). Then, the triangular decomposition algorithm is called recursively on P and Q reduced modulo $\gcd(a_p, b_q)$. The drawback of this approach is that the number of recursive calls may be linear in the minimum of the degrees in x and y of the input polynomials (it may happen that only one vertical asymptote is "handled" at each recursive call) and that the bitsize of the coefficients of the reduction of P and Q increases at each recursive call.

Li et al. (2011) proposed a simple variation on this natural algorithm where, instead of considering P and Q modulo $\gcd(a_p, b_q)$ at the first recursive call (and similarly for the other calls), they simply remove the leading terms $a_p y^p$ and $b_q y^q$ of P and Q.[1] However, they did not provide a complexity analysis of their algorithm.

Here, we present and analyze a variation on this algorithm. First, we solve some issues in Li et al.'s algorithm in which, during the recursion, the reduced versions of P and Q may not define a zero-dimensional system (and also that they may be both univariate). Second, we carefully arrange our computations in a way that is critical for the analysis of our complexity bounds. In particular, (i) we only compute the principal subresultant sequence (instead of the full polynomial sequence) in order to compute only the relevant subresultant polynomials and (ii) in the recursion, we only compute the decomposition above the roots that define asymptotes for all the preceding polynomials.

In our modified algorithm, the number of recursive calls may still be linear in d but we show that the complexity of the overall recursive algorithm is the same as the complexity of the non-recursive algorithm (with no vertical asymptotes), that is $\widetilde{O}(d^4)$ for the arithmetic complexity and $\widetilde{O}_B(d^6 + d^5\tau)$ for the bit complexity (see Lemma 9 and Proposition 10). More precisely, we prove an arithmetic complexity in $\widetilde{O}(d_x d_y^3 + d_x^2 d_y^2)$ and a bit complexity in $\widetilde{O}_B(d_x^3 d_y^3 + (d_x^2 d_y^3 + d_x d_y^4)\tau)$ in the worst case where d_x and d_y bound the degrees of P and Q in x and y, respectively (see Proposition 10). We also prove that the total bitsize of the decomposition is in $\widetilde{O}((d_x^2 d_y^3 + d_x d_y^4)\tau)$. This implies in particular

[1] In Li et al. (2011), this reduction, called "reductum", is not actually defined but it is defined in other articles by these authors; see e.g. Boulier et al. (2010).