Journal of Symbolic Computation 84 (2018) 147–171

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Certifying solutions to overdetermined and singular polynomial systems over $\mathbb{Q}$

Tulay Ayyildiz Akoglu [a,1], Jonathan D. Hauenstein [b,2], Agnes Szanto [a,3]

[a] Department of Mathematics, North Carolina State University, Campus Box 8205, Raleigh, NC, 27965, USA
[b] Department of Applied and Computational Mathematics and Statistics, University of Notre Dame, Notre Dame, IN, 46556, USA

ARTICLE INFO

Article history:
Received 19 November 2015
Accepted 3 November 2016
Available online 24 March 2017

Keywords:
Overdetermined
Polynomial system
Singular solutions
Certification
Rational univariate representation
Isosingular deflation

ABSTRACT

This paper is concerned with certifying that a given point is near an exact root of an overdetermined or singular polynomial system with rational coefficients. The difficulty lies in the fact that consistency of overdetermined systems is not a continuous property. Our certification is based on hybrid symbolic-numeric methods to compute an exact *rational univariate representation* (RUR) of a component of the input system from approximate roots. For overdetermined polynomial systems with simple roots, we compute an initial RUR from approximate roots. The accuracy of the RUR is increased via Newton iterations until the exact RUR is found, which we certify using exact arithmetic. Since the RUR is well-constrained, we can use it to certify the given approximate roots using α-theory. To certify isolated singular roots, we use a determinantal form of the *isosingular deflation*, which adds new polynomials to the original system without introducing new variables. The resulting polynomial system is overdetermined, but the roots are now simple, thereby reducing the problem to the overdetermined case. We prove that our algorithms have complexity that are polynomial in the input plus the output size upon successful convergence, and we use worst case upper bounds

E-mail addresses: hauenstein@nd.edu (J.D. Hauenstein), aszanto@ncsu.edu (A. Szanto).
[1] This research was partly supported by the Ministry of National Education of Turkey.
[2] This research was partly supported by DARPA grant YFA D14AP00052, Alfred P. Sloan Research Fellowship BR2014-110 TR14, and NSF grants DMS-1262428 and ACI-1440583.
[3] This research was partly supported by NSF grant CCF-1217557.

http://dx.doi.org/10.1016/j.jsc.2017.03.004
0747-7171/

for termination when our iteration does not converge to an exact RUR. Examples are included to demonstrate the approach.

1. Introduction

In their recent article Hauenstein and Sottile (2012), F. Sottile and the second author showed that one can get an efficient and practical root certification algorithm using α-theory (cf. Smale, 1986; Blum et al., 1998) for well-constrained polynomials systems. The same paper also considers overdetermined systems over the rationals and shows how to use α-theory to certify that a given point is *not* an approximation of any exact roots of the system. On the other hand, to certify that a point is near an exact root, one can use universal lower bounds for the minimum of positive polynomials on a disk. That paper concludes that all known bounds were “too small to be practical.”

A closer look at the literature on lower bounds for the minimum of positive polynomials over the roots of zero-dimensional rational polynomial systems reveals that they all reduce the problem to the univariate case and use univariate root separation bounds (see, for example, Canny, 1990; Jeronimo and Perrucci, 2010; Brownawell and Yap, 2009; Jeronimo et al., 2013). This led to the idea of directly using an exact univariate representation for the certification of the input system instead of using universal lower bounds that are often very pessimistic. For example, the overdetermined system

$$f_1 := x_1 - \frac{1}{2},\ f_2 := x_2 - x_1^2, \ldots, f_n := x_n - x_{n-1}^2,\ f_{n+1} := x_n$$

has no common roots, but the value of f_{n+1} on the common root of $f_1, \ldots, f_n$ is double exponentially small in n. While universal lower bounds cover these artificial cases, our approach, as we shall see, has the ability to terminate early in cases when the witness for our input instance is small.

In principle, one can compute such a univariate representation using purely algebraic techniques, for example, by solving large linear systems corresponding to resultant or subresultant matrices (see, for example, Szanto, 2008). However, this purely symbolic method would again lead to worst case complexity bounds. Instead, we propose a hybrid symbolic-numeric approach, using the approximate roots of the system, as well as exact univariate polynomial arithmetic over $\mathbb{Q}$. We expect that our method will make the certification of roots of overdetermined systems practical for cases when the universal lower bounds are too pessimistic, or when the actual size of our univariate representation is significantly smaller than in the worst case.

Consider an overdetermined system $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbb{Q}[x_1, \ldots, x_n]$ for some $m > n$, and assume that the ideal $\mathcal{I} := \langle f_1, \ldots, f_m \rangle$ is radical and zero dimensional. Under these assumptions, the so-called Rational Univariate Representation (RUR) for $V(\mathcal{I})$ exists (cf. Rouillier, 1999), as well as for any component of $V(\mathcal{I})$ over the rationals. Since the polynomials in the RUR have also rational coefficients, we can hope to compute them exactly, unlike the possibly irrational coordinates of the common roots of $V(\mathcal{I})$. With the exact RUR, which is a well-constrained system of polynomials, we can use α-theory as in Hauenstein and Sottile (2012) to certify that a given point is an approximate root for the RUR, and thus for our original system $\mathbf{f}$. Our symbolic-numeric method to compute a RUR for $V(\mathcal{I})$ or for a rational component of $V(\mathcal{I})$ consists of the following steps:

Initialization

(i) Compute approximations of all isolated roots to a given accuracy of a random well-constrained (square) set of linear combinations of the polynomials $f_1, \ldots, f_m$ using homotopy continuation (e.g., see Bates et al., 2013c; Sommese and Wampler, 2005);

(ii) Among the approximate roots computed in Step (i), choose the candidates which could be approximations to roots in $V(\mathcal{I})$ or a rational component of $V(\mathcal{I})$ – for this step, we can only give heuristics on how to proceed;

(iii) Chose a separating linear form (primitive element) for the approximate roots chosen in Step (ii);