Journal of Complexity 31 (2015) 206–236

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

On the complexity of computing with planar algebraic curves

Alexander Kobel[a,b,c], Michael Sagraloff[a,*]

[a] Max-Planck-Institut für Informatik, Saarbrücken, Germany

[b] International Max Planck Research School for Computer Science, Saarbrücken, Germany

[c] Universität des Saarlandes, Saarbrücken, Germany

ARTICLE INFO

Article history:
Received 24 February 2014
Accepted 30 July 2014
Available online 12 August 2014

Keywords:
Bivariate systems
Separating form
Topology analysis
Arrangement computation
Complexity analysis
Approximate multipoint evaluation

ABSTRACT

In this paper, we give improved bounds for the computational complexity of computing with planar algebraic curves. More specifically, for arbitrary coprime polynomials $f, g \in \mathbb{Z}[x, y]$ and an arbitrary polynomial $h \in \mathbb{Z}[x, y]$, each of total degree less than n and with integer coefficients of absolute value less than 2^τ, we show that each of the following problems can be solved in a deterministic way with a number of bit operations bounded by $\tilde{O}(n^6 + n^5\tau)$, where we ignore polylogarithmic factors in n and τ:

- *The computation of isolating regions in* $\mathbb{C}^2$ *for all complex solutions* of the system $f = g = 0$,
- *the computation of a separating form* for the solutions of $f = g = 0$,
- *the computation of the sign of* h at all real valued solutions of $f = g = 0$, and
- *the computation of the topology* of the planar algebraic curve $\mathcal{C}$ defined as the real valued vanishing set of the polynomial f.

Our bound improves upon the best currently known bounds for the first three problems by a factor of n^2 or more and closes the gap to the state-of-the-art randomized complexity for the last problem.

* Correspondence to: Max-Planck-Institut für Informatik, Department 1: Algorithms and Complexity, Campus E1 4, 66123 Saarbrücken, Germany.

E-mail addresses: alexander.kobel@mpi-inf.mpg.de (A. Kobel), michael.sagraloff@mpi-inf.mpg.de (M. Sagraloff).

http://dx.doi.org/10.1016/j.jco.2014.08.002
0885-064X/

1. Introduction

In this paper, we derive record bounds for the computational complexity of the following problems, which are related to the arrangement computation of planar algebraic curves:

(P1) Given two coprime polynomials $f, g \in \mathbb{Z}[x, y]$ of degree n or less, compute isolating regions in $\mathbb{C}^2$ for *all distinct complex* solutions $(x_i, y_i) \in \mathbb{C}^2$ of the system

$$f(x, y) = g(x, y) = 0, \tag{1}$$

with $i = 1, \ldots, r$ and some integer r with $r \le \deg f \cdot \deg g \le n^2$, which is the upper bound of the number of solutions of the zero-dimensional system due to Bézout's Theorem.

(P2) Compute a *separating form* $x + s \cdot y$, with $s \in \{0, 1, \ldots, n^4\}$, for (1) such that $x_i + s \cdot y_i \ne x_j + s \cdot y_j$ for all i, j with $i \ne j$.

(P3) Given an arbitrary polynomial $h \in \mathbb{Z}[x, y]$, evaluate the sign of h at all *real valued* solutions (x_i, y_i) of (1).

(P4) Given an arbitrary polynomial $f \in \mathbb{Z}[x, y]$, compute the topology of the real planar algebraic curve

$$\mathcal{C} := \{(x, y) \in \mathbb{R}^2 : f(x, y) = 0\} \tag{2}$$

in terms of a planar straight line graph that is isotopic[1] to $\mathcal{C}$.

We remark that a solution to the above problems allows us to answer all necessary queries for arrangement computations with planar algebraic curves [8,6,21,25,30]. Namely, for a set of planar algebraic curves, we can compute the topology of each of these curves from (P4), we can compute the intersection points of two curves from (P1), and, from (P3), we can decide whether two intersection points from two distinct pairs of curves are equal or not.

The main contribution of this paper is a *deterministic* algorithm that solves all of the above problems (P1)–(P4) in a number of bit operations bounded by $\tilde{O}(n^6 + n^5\tau)$, where n is an upper bound for the total degree of the polynomials f, g and h, and τ is an upper bound for the bitsize of their coefficients. For the first two problems, we also give more general bounds that take into account the case of unbalanced input. That is, if f and g are polynomials of total degree m and n and with integer coefficients of bitsize bounded by τ_f and τ_g, respectively, then (P1) and (P2) can be solved in time $\tilde{O}\big(\max^2\{m, n\} \cdot (m^2n^2 + mn(m\tau_g + n\tau_f))\big)$.

We briefly outline our approach: For (P1), we first extend (and modify) an algorithm from Berberich et al. [6,7], denoted BiSolve, that isolates only the *real valued* solutions of (1). The so-obtained algorithm $\mathbb{C}$BiSolve computes isolating polydisks in $\mathbb{C}^2$ for all complex solutions and further refines these disks to an arbitrarily small size if necessary. From a high-level perspective, the algorithm decomposes into two steps: In the first step, the *projection step*, we project all solutions onto their x- and y-coordinates using resultant computation and univariate root finding. This induces a grid consisting of $O(n^4)$ candidates that have to be checked for solutions in the second step, the *validation step*: For processing the candidates, we combine approximate evaluation of the input polynomials at the candidates and adaptive evaluation bounds derived from the co-factor representations of the resultant polynomials; see Section 2.3 for details. We further remark that $\mathbb{C}$BiSolve does not need any coordinate transformation and returns isolating polydisks in the initial coordinate system.

From the solutions of the system (1), we derive a corresponding separating form $x + s \cdot y$ for (1) by approximating all "bad" values for s (to an error of 1/2), for which a pair of distinct solutions is mapped to the same value via $x + s \cdot y$. Since there are at most r, with $r \le n^2$, many distinct solutions, there exist at most $\binom{r}{2} < n^4$ bad values for s. Hence, we can determine a separating form with an $s \in \{0, 1, \ldots, n^4\}$. This solves Problem (P2).

[1] We consider the stronger notion of an *ambient isotopy*, but omit the word "ambient". A graph $\mathcal{G}_C$, embedded in $\mathbb{R}^2$, is ambient isotopic to C if there exists a continuous mapping $\phi : [0, 1] \times \mathbb{R}^2 \mapsto \mathbb{R}^2$ with $\phi(0, \cdot) = \mathrm{id}_{\mathbb{R}^2}$, $\phi(1, C) = \mathcal{G}_C$, and $\phi(t_0, \cdot) : \mathbb{R}^2 \mapsto \mathbb{R}^2$ is a homeomorphism for each $t_0 \in [0, 1]$.