ARTICLE IN PRESS YJSCO:1810

Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Bit complexity for multi-homogeneous polynomial system solving—Application to polynomial minimization ☆

Mohab Safey El Din [a], Éric Schost [b]

[a] Sorbonne Universités, UPMC Univ Paris 06, Inria Paris, PolSys Project, CNRS, LIP6 UMR 7606, France
[b] University of Waterloo, David R. Cheriton School of Computer Science, Canada

ARTICLE INFO

Article history:
Received 24 May 2016
Accepted 27 July 2017
Available online xxxx

Keywords:
Polynomial system solving
Multi-homogeneous systems
Polynomial optimization

ABSTRACT

Multi-homogeneous polynomial systems arise in many applications. We provide bit complexity estimates for solving them which, up to a few extra other factors, are quadratic in the number of solutions and linear in the height of the input system, under some genericity assumptions. The assumptions essentially imply that the Jacobian matrix of the system under study has maximal rank at the solution set and that this solution set is finite. The algorithm is probabilistic and a probability analysis is provided.

Next, we apply these results to the problem of optimizing a linear map on the real trace of an algebraic set. Under some genericity assumptions, we provide bit complexity estimates for solving this polynomial minimization problem.

1. Introduction

1.1. Motivation and problem statement

In this paper, we are interested in exact algorithms solving systems of polynomial equations with a multi-homogeneous structure (the polynomials we consider are actually affine, but can be seen

☆ The first author is member of and supported by Institut Universitaire de France. The second author is supported by an NSERC Discovery Grant.

E-mail addresses: Mohab.Safey@lip6.fr (M. Safey El Din), eschost@uwaterloo.ca (É. Schost).

http://dx.doi.org/10.1016/j.jsc.2017.08.001
0747-7171/© 2017 Elsevier Ltd. All rights reserved.

as the dehomogenization of multi-homogeneous ones); we focus in particular on the bit complexity aspects of this question. The main application we have in mind is the solution of some constrained optimization problems. This is used in many algorithms for studying real solutions to polynomial systems (see e.g. Bank et al., 1997, 2001; Safey El Din and Schost, 2003; Bank et al., 2014; Safey El Din and Schost, 2017, and references therein). We will also pay particular attention to the situation when the constraints are given as quadratic equations.

We work with polynomials in m groups of variables. Let thus $\boldsymbol{n} = (n_1, \ldots, n_m)$ be positive integers, and consider variables $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_m)$, with $\mathbf{X}_1 = (X_{1,1}, \ldots, X_{1,n_1})$, ..., $\mathbf{X}_m = (X_{m,1}, \ldots, X_{m,n_m})$. We write $N = n_1 + \cdots + n_m$ for the total number of variables.

Let $\mathbb{K}$ be a field and $\boldsymbol{f} = (f_1, \ldots, f_M)$ in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$, for some $M \leq N$ (we will sometimes write $\boldsymbol{f}_M$ instead of $\boldsymbol{f}$, in order to highlight the length of the sequence). We associate to $\boldsymbol{f}$ the algebraic set $Z(\boldsymbol{f})$, defined as the set of all $\boldsymbol{x}$ in $\overline{\mathbb{K}}^N$ such that $\boldsymbol{f}(\boldsymbol{x}) = 0$ and such that the Jacobian matrix of $\boldsymbol{f}$ has rank M at $\boldsymbol{x}$. By the Jacobian criterion (Eisenbud, 1995, Chapter 16), $Z(\boldsymbol{f})$ is either empty, or equidimensional of dimension $N - M$, and it is defined over $\mathbb{K}$.

Suppose that $M = N$. It is known that using the multi-degree structure of $\boldsymbol{f}$, that is, the partial degrees of these equations in $\mathbf{X}_1, \ldots, \mathbf{X}_m$, together with a multi-homogeneous Bézout bound, we can obtain finer estimates on the cardinality of $Z(\boldsymbol{f})$ than through the direct application of Bézout's theorem in many cases.

In this paper, we focus on the case $\mathbb{K} = \mathbb{Q}$, and show how the same phenomenon holds in terms of bit complexity. Indeed, our goal is to obtain an algorithm for solving such systems whose bit complexity is, up to some extra factors, quadratic in the multi-homogeneous bound and linear in the *heights* of the polynomials in the input system (which is a measure of their bit size).

In the following paragraphs, we recall the notion of height and the data structure we use to represent $Z(\boldsymbol{f})$. We will also use these notions to describe related works on solving multi-homogeneous systems.

Let us first however describe how such results can be applied to the problem of minimizing the map $\pi_1 : (x_1, \ldots, x_n) \mapsto x_1$ subject to the constraints $h_1 = \cdots = h_p = 0$, with $\mathbf{h} = (h_1, \ldots, h_p) \subset \mathbb{Z}[X_1, \ldots, X_n]$. Assuming that $\mathbf{h}$ is a reduced regular sequence, that the minimizer exists and that the set of minimizers is finite, it is well-known that this problem can be tackled by solving the so-called Lagrange system

$$h_1 = \cdots = h_p = 0, \ [L_1, \ldots, L_p] \begin{bmatrix} \frac{\partial h_1}{\partial X_2} & \cdots & \frac{\partial h_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial h_p}{\partial X_2} & \cdots & \frac{\partial h_p}{\partial X_n} \end{bmatrix} = [0 \ \cdots \ 0], u_1 L_1 + \cdots + u_p L_p = 1,$$

where $\mathbf{L} = (L_1, \ldots, L_p)$ are new variables (called Lagrange multipliers) and $(u_1, \ldots, u_p)$ are randomly chosen integers. Hence, using the notation introduced above, we have for this system $m = 2$, $\boldsymbol{n} = (n, p)$, $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2)$ with $\mathbf{X}_1 = (X_1, \ldots, X_n)$ and $\mathbf{X}_2 = \mathbf{L}$.

1.2. *Bit size and data structures*

1.2.1. *Multi-degree, height and bit size*

Let $\mathbb{K}$ be a field as above. To a polynomial f in $\mathbb{K}[\mathbf{X}_1, \ldots, \mathbf{X}_m]$ we associate its *multi-degree* $\mathrm{mdeg}(f) = (d_1, \ldots, d_m) \in \mathbb{N}^m$, with $d_i = \deg(f, \mathbf{X}_i)$ for all i. When comparing multi-degrees, we use the (partial) componentwise order, so that saying that f has multi-degree at most $\underline{d} = (d_1, \ldots, d_m)$ means that $\deg(f, \mathbf{X}_i) \leq d_i$ holds for all i. Similarly, to a sequence of polynomials $\boldsymbol{f}_M$, we associate its multi-degree $\mathrm{mdeg}(\boldsymbol{f}_M) = (\mathrm{mdeg}(f_1), \ldots, \mathrm{mdeg}(f_M))$. Saying that $\boldsymbol{f}_M$ has multi-degree at most $\boldsymbol{d} = (\underline{d}_1, \ldots, \underline{d}_M)$, with now all $\underline{d}_i = (d_{i,1}, \ldots, d_{i,m})$ in $\mathbb{N}^m$, means that $\deg(f_i, \mathbf{X}_j) \leq d_{i,j}$ holds for all i, j.

Consider a polynomial f with coefficients in $\mathbb{Q}$. To measure its bit size, we will use its *height*, defined as follows. First, for $a = u/v$ in $\mathbb{Q} - \{0\}$, define the height of a, $\mathrm{ht}(a)$, as $\max(\log(|u|), \log(v))$, with $u \in \mathbb{Z}$ and $v \in \mathbb{N}$ coprime. For a non-zero univariate or multivariate polynomial f with rational coefficients, we let $v \in \mathbb{N}$ be the minimal common denominator of all its non-zero coefficients; then