Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Symbolic Computation 39 (2005) 31–49
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Computing zero-dimensional schemes

J. Abbott[a,*], M. Kreuzer[b], L. Robbiano[a]

[a]*Department of Mathematics, University of Genova, 16146 Genova, Italy*
[b]*Fakultät für Mathematik, Universität Regensburg, 93040 Regensburg, Germany*

Received 29 March 2001; accepted 9 September 2004

Abstract

This paper is a natural continuation of Abbott et al. [Abbott, J., Bigatti, A., Kreuzer, M., Robbiano, L., 2000. Computing ideals of points. J. Symbolic Comput. 30, 341–356] further generalizing the Buchberger–Möller algorithm to zero-dimensional schemes in both affine and projective spaces. We also introduce a new, general way of viewing the problems which can be solved by the algorithm: an approach which looks to be readily applicable in several areas. Implementation issues are also addressed, especially for computations over $\mathbb{Q}$ where a trace-lifting paradigm is employed. We give a complexity analysis of the new algorithm for fat points in affine space over $\mathbb{Q}$. Tables of timings show the new algorithm to be efficient in practice.

Keywords: Gröbner basis algorithm; Fat points; Zero-dimensional schemes

1. Introduction

Nowadays it is common knowledge that Gröbner bases and Buchberger's Algorithm are key ingredients in computational commutative algebra, and are hence fundamental tools for applications in several fields both inside and outside mathematics (see Buchberger (1985)). It is also well known that the computation of a Gröbner basis can be time-consuming due to its intrinsic complexity. Therefore many attempts have been made in recent years to find

* Corresponding address: Dipartimento di Matematica, Universita‘ di Genova, Via Dodecaneso 35809, 16146 Genova, Italy. Tel.: +39 010 353 6890; fax: +39 010 353 6752.

E-mail addresses: abbott@dima.unige.it (J. Abbott), martin.kreuzer@mathematik.uni-regensburg.de (M. Kreuzer), robbiano@dima.unige.it (L. Robbiano).

doi:10.1016/j.jsc.2004.09.001

special situations in which the usual computational scheme of Buchberger's Algorithm can be improved.

For instance, in a recent paper (see Abbott et al. (2000)) we addressed the problem of computing the vanishing ideal of a set of reduced K-rational points, where K is a field. In particular, we studied the case $K = \mathbb{Q}$. Our investigation was based on the Buchberger–Möller Algorithm (BM-algorithm) which improves the traditional scheme for computing intersections of ideals of points considerably (see Buchberger and Möller (1982)).

The first question that we want to address now is the following. Is there a more general computational problem one of whose specializations is solved by the classical BM-algorithm? For this we let $P = K[x_1, \dots, x_n]$ be the polynomial ring in n indeterminates over a field K, we let M be a P-module, and we let $\varphi : P \longrightarrow M$ be a homomorphism of P-modules. The task is to compute $\mathrm{Ker}(\varphi)$ efficiently.

Let us see how this general setting specializes to the case treated by the classical BM-algorithm. Let $\mathbf{p}_1, \dots, \mathbf{p}_s \in \mathbb{A}^n_K$ and $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ be their associated maximal ideals. Let $M = \bigoplus_{i=1}^s P/\mathfrak{m}_i \cong K^s$, and let $\varphi : P \longrightarrow M$ be defined by $\varphi(f) = (f(p_1), \dots, f(p_s))$. Then the problem of computing $\mathrm{Ker}(\varphi)$ is exactly the problem of computing $\bigcap_{i=1}^s \mathfrak{m}_i$, and indeed a good solution is the BM-algorithm.

A more general instance of the above computational problem is the computation of the vanishing ideal of a zero-dimensional scheme. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ be maximal ideals in P, and for each i let $\mathfrak{q}_i$ be an $\mathfrak{m}_i$-primary ideal. Then $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ is the vanishing ideal of some zero-dimensional subscheme $\mathbb{X} \subseteq \mathbb{A}^n_K$. It is also the kernel of the canonical P-linear map $\pi : P \longrightarrow \bigoplus_{i=1}^s P/\mathfrak{q}_i$. In this case the methods based on Buchberger's Algorithm tend to be rather inefficient in practice and faster methods are needed.

If the ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ are described by the vanishing of certain "dual functionals", a suitable adaptation of the BM-algorithm was given in Marinari et al. (1993). But to find those functionals from systems of generators of $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ does not seem easy, especially if K has finite characteristic. A more direct approach was suggested in Lakshman (1991), but the cost of computing local normal form vectors and the problem of the growth of coefficients in the case $K = \mathbb{Q}$ were ignored. The related problem of computing minimal generators has been studied in Cioffi (1998) and Cioffi and Orecchia (2001).

To get a better grip on this situation, and in order to put it in a suitable general framework, we start in Section 2 by studying K-linear, surjective maps $\varphi : P \longrightarrow K^\mu$ where $\mu \geq 1$; this was partly inspired by some ideas given in Mourrain (1999), and is further extended in Robbiano (2001). We show that $\mathrm{Ker}(\varphi)$ is a zero-dimensional ideal in P if and only if φ maps a polynomial to its normal form vector with respect to a tuple of polynomials whose residue classes are a K-vector space basis of $P/\mathrm{Ker}(\varphi)$. The important case is when φ is explicitly computable. For instance, if $P/\mathrm{Ker}(\varphi)$ is generated by the residue classes of the terms in the complement of some leading term ideal and if φ is constructed using the normal form map, it is explicitly computable. But we shall also see that there are cases where φ is explicitly computable, but not of this type. The "change of basis" between two such maps having the same kernel is achieved by a generalization of the well-known FGLM-algorithm.

Then we present our first generalization of the BM-algorithm in Section 3. It computes the vanishing ideal of a zero-dimensional scheme $\mathbb{X} \subseteq \mathbb{A}^n_K$ as above. The zero-dimensional ideals whose intersection we want to compute are represented by normal form vector maps.