Journal of Computational and Applied Mathematics 234 (2010) 3344–3355

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

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

A bivariate preprocessing paradigm for the Buchberger–Möller algorithm☆

Xiaoying Wang, Shugong Zhang, Tian Dong*

School of Mathemathics, Key Lab. of Symbolic Computation and Knowledge Engineering (Ministry of Education), Jilin University, Changchun 130012, PR China

ARTICLE INFO

Article history:
Received 30 October 2009
Received in revised form 20 April 2010

MSC:
13P10
65D05
12Y05

Keywords:
Buchberger–Möller algorithm
Bivariate Lagrange interpolation
Degree reducing interpolation space
Cartesian set

ABSTRACT

For the last almost three decades, since the famous Buchberger–Möller (BM) algorithm emerged, there has been wide interest in vanishing ideals of points and associated interpolation polynomials. Our paradigm is based on the theory of bivariate polynomial interpolation on cartesian point sets that gives us a related degree reducing interpolation monomial and Newton bases directly. Since the bases are involved in the computation process as well as contained in the final output of the BM algorithm, our paradigm obviously simplifies the computation and accelerates the BM process. The experiments show that the paradigm is best suited for the computation over finite prime fields that have many applications.

1. Introduction

For an arbitrary field $\mathbb{F}$, we let $\mathbb{F}_q$ a finite prime field of size q and $\Pi^d := \mathbb{F}[x_1, \ldots, x_d]$ the d-variate polynomial ring over $\mathbb{F}$. Given a preassigned set of distinct affine points $\Xi \subset \mathbb{F}^d$, the d-dimensional affine space over $\mathbb{F}$, it is well-known that the set of all polynomials in Π^d vanishing at Ξ constitutes a radical zero-dimensional ideal, denoted by $\mathcal{I}(\Xi)$, which is called the *vanishing ideal* of Ξ.

In recent years, there has been considerable interest in vanishing ideals of points in many branches of mathematics such as algebraic geometry [1], multivariate interpolation [2,3], coding theory [4,5], statistics [6], and even computational molecular biology [7,8]. As is well known, the most significant milestone of the computation of vanishing ideals is the algorithm presented in [9] by Hans Michael Möller and Bruno Buchberger known as the Buchberger–Möller algorithm (BM algorithm for short). For any point set $\Xi \subset \mathbb{F}^d$ and fixed term order $\prec$, the BM algorithm yields the reduced Gröbner basis for $\mathcal{I}(\Xi)$ w.r.t. $\prec$ and a $\prec$-degree reducing interpolation Newton basis for a d-variate Lagrange interpolation on Ξ. The algorithm also produces the Gröbner escalier of $\mathcal{I}(\Xi)$ w.r.t. $\prec$ as a byproduct. Afterwards, in 1993, the BM algorithm was applied in [10] in order to solve the renowned FGLM-problem. In the same year, [11] merged the BM and FGLM algorithms into four variations that can solve more general zero-dimensional ideals and therefore related ideal interpolation problems [3]. The algorithms are referred as MMM algorithms.

Although very important, the BM algorithm (and MMM algorithms) has a very poor complexity that limits its applications. In this decade, many authors have proposed new algorithms that can reduce the complexity but are mostly suitable for special cases. [12] presented a modular version of the BM algorithm that is best suited to the computation over $\mathbb{Q}$. [13–15]

☆ This work was supported in part by the National Grand Fundamental Research 973 Program of China (No. 2004CB318000).
* Corresponding author.
E-mail address: dongtian@jlu.edu.cn (T. Dong).

0377-0427/$ – see front matter
doi:10.1016/j.cam.2010.04.035

presented algorithms for obtaining, with relatively little effort, the Gröbner éscalier of a vanishing ideal w.r.t. the (inverse) lexicographic order that can lead to an interpolation Newton basis or the reduced Gröbner basis for the vanishing ideal after solving a linear system.

For a fixed point set Ξ in $\mathbb{F}^d$ and a term order $\prec$, it is well known that there are *two* factors that determine the Gröbner éscalier of $\mathcal{I}(\Xi)$ w.r.t. $\prec$ thereby the reduced Gröbner basis for $\mathcal{I}(\Xi)$ and related degree reducing interpolation Newton bases (up to coefficients). One is apparently the cardinal of Ξ. It is the unique determinate factor in univariate cases. Another one is the geometry (the distribution of the points) of Ξ that is dominating in multivariate cases but not taken into consideration by the BM and MMM algorithms. In recent years, [16–18] studied multivariate Lagrange interpolation on a special kind of point sets, cartesian point sets (aka lower point sets), and constructed the associated Gröbner éscalier and degree reducing interpolation Newton bases theoretically. We know from [9,11] that, for a cartesian subset of Ξ (it always exists!), certain associated degree reducing interpolation Newton basis forms part of the output of the BM algorithm w.r.t. some reordering of Ξ. Therefore, finding a large enough cartesian subset of Ξ with little enough effort will reduce the complexity of the BM algorithm.

Following this idea, the paper proposes a preprocessing paradigm for the BM algorithm with the organization as follows. The next section is devoted as a preparation for the paper. And then, our main results are presented in two sections. Section 3 will pursue the paradigm for two special term orders while Section 4 will set forth our solution for other more general cases. In the last section, Section 5, some implementation issues and experimental results will be illustrated.

2. Preliminary

In this section, we will introduce some notation and recall some basic facts for the reader's convenience. For more details, we refer the reader to [19,20].

We let $\mathbb{N}_0$ denote the monoid of nonnegative integers. A *polynomial* $f \in \Pi^2$ is of the form

$$f = \sum_{\boldsymbol{\alpha}\in\mathbb{N}_0^2} f_{\boldsymbol{\alpha}} X^{\boldsymbol{\alpha}}, \quad \#\{\boldsymbol{\alpha} \in \mathbb{N}_0^2 : 0 \neq f_{\boldsymbol{\alpha}} \in \mathbb{F}\} < \infty,$$

where *monomial* $X^{\boldsymbol{\alpha}} = x^{\alpha_1} y^{\alpha_2}$ with $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$. The set of bivariate monomials in Π^2 is denoted by $\mathbb{T}^2$.

Fix a term order $\prec$ on Π^2 that may be of lexicographical order $\prec_{\text{lex}}$, inverse lexicographical order $\prec_{\text{inlex}}$, or total degree inverse lexicographical order $\prec_{\text{tdinlex}}$ etc. For all $f \in \Pi^2$, with $f \neq 0$, we may write

$$f = f_{\boldsymbol{\gamma_1}} X^{\boldsymbol{\gamma_1}} + f_{\boldsymbol{\gamma_2}} X^{\boldsymbol{\gamma_2}} + \cdots + f_{\boldsymbol{\gamma_r}} X^{\boldsymbol{\gamma_r}},$$

where $0 \neq f_{\boldsymbol{\gamma_i}} \in \mathbb{F}$, $\boldsymbol{\gamma_i} \in \mathbb{N}_0^2$, $i = 1, \ldots, r$, and $X^{\boldsymbol{\gamma_1}} \succ X^{\boldsymbol{\gamma_2}} \succ \cdots \succ X^{\boldsymbol{\gamma_r}}$. We shall call $\mathrm{LT}(f) := f_{\boldsymbol{\gamma_1}} X^{\boldsymbol{\gamma_1}}$ the *leading term* and $\mathrm{LM}(f) := X^{\boldsymbol{\gamma_1}}$ the *leading monomial* of f. Furthermore, for a non-empty subset $F \subset \Pi^2$, put

$$\mathrm{LT}(F) := \{\mathrm{LT}(f) : f \in F\}.$$

As in [21], we define the $\prec$-*degree* of a polynomial $f \in \Pi^2$ to be the leading bidegree w.r.t. $\prec$

$$\delta(f) := \boldsymbol{\gamma}, \qquad X^{\boldsymbol{\gamma}} = \mathrm{LM}(f),$$

with $\delta(0)$ undefined. Further, for any finite dimensional subset $F \subset \Pi^2$, define

$$\delta(F) := \max_{f\in F} \delta(f).$$

Finally, for any $f, g \in \Pi^2$, if $\delta(f) \prec \delta(g)$ then we say that f is of *lower degree* than g and use the abbreviation

$$f \prec g := \delta(f) \prec \delta(g).$$

In addition, $f \preceq g$ is interpreted as the degree of f is lower than or equal to that of g.

Let $\mathcal{A}$ be a finite subset of $\mathbb{N}_0^2$. $\mathcal{A}$ is called a *lower* set if, for any $\boldsymbol{\alpha} = (\alpha_1, \alpha_2) \in \mathcal{A}$, we always have

$$\mathrm{R}(\boldsymbol{\alpha}) := \{(\alpha_1', \alpha_2') \in \mathbb{N}_0^2 : 0 \leq \alpha_i' \leq \alpha_i, i = 1, 2\} \subset \mathcal{A}.$$

Especially, $\mathbf{0} \in \mathcal{A}$. Moreover, we set $m_j = \max_{(h,j)\in\mathcal{A}} h$, $0 \leq j \leq \nu$, with $\nu = \max_{(0,k)\in\mathcal{A}} k$. Clearly, $\mathcal{A}$ can be determined uniquely by the ordered $(\nu+1)$-tuple $(m_0, m_1, \ldots, m_\nu)$ hence represented as $\mathrm{L}_x(m_0, m_1, \ldots, m_\nu)$. Swapping the roles of x and y, we can also represent $\mathcal{A}$ as $\mathrm{L}_y(n_0, n_1, \ldots, n_{m_0})$ with $n_i = \max_{(i,k)\in\mathcal{A}} k$, $0 \leq i \leq m_0$. It should be noticed that $\nu = n_0$.

Given a set $\Xi = \{\xi^{(1)}, \ldots, \xi^{(\mu)}\} \subset \mathbb{F}^2$ of μ distinct points. For prescribed values $f_i \in \mathbb{F}$, $i = 1, \ldots, \mu$, find all polynomials $p \in \Pi^2$ satisfying

$$p(\xi^{(i)}) = f_i, \quad i = 1, \ldots, \mu. \tag{1}$$

We call it the problem of *bivariate Lagrange interpolation*. Note that in most cases, especially from a numerical point of view, we are not interested in all such p's but a "degree reducing" one, as in the univariate cases.

Definition 1 (*[2]*). Fix term order $\prec$. We call a subspace $\mathcal{P} \subset \Pi^2$ a *degree reducing interpolation space* w.r.t. $\prec$ for the bivariate Lagrange interpolation (1) if