Finite Fields and Their Applications 41 (2016) 174–192

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

An improvement over the GVW algorithm for inhomogeneous polynomial systems ☆

Yao Sun [a], Zhenyu Huang [a,*], Dingkang Wang [b], Dongdai Lin [a]

[a] *SKLOIS, Institute of Information Engineering, CAS, Beijing 100093, China*
[b] *KLMM, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China*

ARTICLE INFO

Article history:
Received 18 August 2015
Received in revised form 2 March 2016
Accepted 14 June 2016
Communicated by S. Gao

MSC:
13P10
13P15
11T55
68W30

Keywords:
Gröbner basis
The GVW algorithm
Signature-based algorithm
Linear algebra
Boolean polynomial ring

ABSTRACT

The GVW algorithm provides a new framework for computing Gröbner bases efficiently. If the input system is not homogeneous, some J-pairs with larger signatures but lower degrees may be rejected by GVW's criteria, and instead, GVW has to compute some J-pairs with smaller signatures but higher degrees. Consequently, degrees of polynomials appearing during the computations may unnecessarily grow up higher, and hence, the total computations become more expensive. This phenomenon happens more frequently when the coefficient field is a finite field and the field polynomials are involved in the computations. In this paper, a variant of the GVW algorithm, called M-GVW, is proposed. The concept of *mutant pairs* is introduced to overcome the inconveniences brought by inhomogeneous inputs. In aspects of implementations, to obtain efficient implementations of GVW/M-GVW over boolean polynomial rings, we take advantages of the famous library M4RI. We propose a new *rotating swap* method of adapting efficient routines in M4RI to deal with the one-direction reductions in GVW/M-GVW. Our implementations are tested with many examples from Boolean polynomial rings, and the timings show M-GVW usually

☆ The authors are supported by National Key Basic Research Program of China (No. 2013CB834203), National Natural Science Foundation of China (No. 11301523 and No. 61502485), the Strategic Priority Research Program of the Chinese Academy of Sciences (No. XDA06010701), and IEE's Research Project on Cryptography (No. Y4Z0061A02).

* Corresponding author.
E-mail addresses: sunyao@iie.ac.cn (Y. Sun), huangzhenyu@iie.ac.cn (Z. Huang), dwang@mmrc.iss.ac.cn (D. Wang), ddlin@iie.ac.cn (D. Lin).

http://dx.doi.org/10.1016/j.ffa.2016.06.002

performs much better than the original GVW algorithm if mutant pairs are found.

1. Introduction

Gröbner bases, proposed by Buchberger in 1965 [5], have been proven to be very useful in many aspects of algebra. In the past forty years, many efficient algorithms have been proposed to compute Gröbner bases. One important improvement is that Lazard pointed out the strong relation between Gröbner bases and linear algebra [23]. This idea has been implemented in F4 by Faugère [15], and also as XL type algorithms by Courtois et al. [7] and Ding et al. [9].

Faugère introduced the concept of signatures for polynomials and presented the famous F5 algorithm [16]. Since then, signature-based algorithms have been widely investigated, and several variants of F5 have been presented, including F5C [11], extended F5 [22], F5 with revised criterion (the AP algorithm) [4], and RB [13]. Gao et al. proposed another signature-based algorithm G2V [19] in a different way from F5, and GVW [20,21] is an extended version of G2V. The authors studied generalized criteria and signature-based algorithms in solvable polynomial algebra in [26,27]. For an overview of all signature-based algorithms, readers are referred to the survey by Eder and Faugère [14].

For implementations of signature-based algorithms, Roune and Stillman efficiently implemented GVW and AP without using linear algebra [24]. Faugère gave the matrix-F5 algorithm in [18]. An F5 in F4-style was described in more details by Albrecht and Perry [1].

In GVW, criteria always reject J-pairs with larger signatures, and process J-pairs with smaller signatures instead. Unfortunately, when the input systems are inhomogeneous, J-pairs with larger signatures probably have relatively lower degrees, where by saying degrees of polynomials, we mean the total degrees of polynomials. This phenomenon happens more frequently when the coefficient field is a finite field and the field polynomials are involved in the computations. This is not good for efficient Gröbner basis computations, because rejecting polynomials of lower degrees and reducing those of higher degrees will take more computing time. The case may be even worse if linear algebra is used for reductions. As suggested by Faugère in [15,16], a good strategy of dealing with critical pairs (equivalent to J-pairs in GVW) in a batch is to select all critical pairs with the minimal degree. So if polynomials with larger signatures and lower degrees are rejected by criteria, matrices with higher degrees may be constructed instead, which definitely leads to more computations. In fact, this case really happens when we are computing Gröbner bases for the HFE systems by using GVW. Some other influences of inhomogeneous input systems were discussed by Eder [12].