Journal of Symbolic Computation 47 (2012) 655–679

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

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

Characteristic set algorithms for equation solving in finite fields☆

Xiao-Shan Gao, Zhenyu Huang

KLMM, Institute of Systems Science, AMSS, Chinese Academy of Sciences, Beijing, 100190, China

ARTICLE INFO

Article history:
Received 30 October 2009
Accepted 30 May 2010
Available online 22 December 2011

Keywords:
Characteristic set
Finite field
Boolean polynomial
Proper triangular set
Single exponential algorithm
Stream cipher

ABSTRACT

Efficient characteristic set methods for computing zeros of polynomial equation systems in a finite field are proposed. The concept of proper triangular sets is introduced and an explicit formula for the number of zeros of a proper and monic triangular set is given. An improved zero decomposition algorithm is proposed to reduce the zero set of an equation system to the union of zero sets of monic proper triangular sets. The bitsize complexity of this algorithm is shown to be $O(l^n)$ for Boolean polynomials, where n is the number of variables and $l \geq 2$ is the number of equations. We also give a multiplication free characteristic set method for Boolean polynomials, where the sizes of the polynomials occurred during the computation do not exceed the sizes of the input polynomials and the bitsize complexity of algorithm is $O(n^d)$ for input polynomials with n variables and degree d. The algorithms are implemented in the case of Boolean polynomials and extensive experiments show that they are quite efficient for solving certain classes of Boolean equations raising from stream ciphers.

1. Introduction

Solving polynomial equations in finite fields plays a fundamental role in many important fields such as coding theory, cryptology, and analysis of computer hardware. To find efficient algorithms to solve such equations is a central issue both in mathematics and in computer science (see Problem 3 in (Smale, 1998) and Section 8 of (Coron and de Weger, 2007)). Efficient algebraic algorithms for solving equations in finite fields have been developed, such as the Gröbner basis methods (Bardet et al., 2003;

☆ This paper is supported by a National Key Basic Research Project of China and a grant from NSFC.
E-mail addresses: xgao@mmrc.iss.ac.cn (X.-S. Gao), huangzhenyu@mmrc.iss.ac.cn (Z. Huang).

0747-7171/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2011.12.025

Brickenstein and Dreyer, 2007; Faugère, 1999, 2002; Faugère and Ars, 2003; Kapur and Narendran, 1985; Gerdt and Zinin, 2008; Sato and Inoue, 2005) and the XL algorithm and its improved versions (Courtois et al., 2000).

The **characteristic set (CS)** method is a tool for studying polynomial, algebraic differential, and algebraic difference equation systems (Aubry et al., 1999; Boulier et al., 1995; Bouziane et al., 2001; Chou, 1988; Chou and Gao, 1990; Dahan et al., 2005; Gallo and Mishra, 1991; Gao et al., 2009; Hubert, 2000; Kalkbrener, 1993; Kapur and Wan, 1990; Lazard, 1991; Lin and Liu, 1993; Maza, 2000; Möller, 1993; Szántó, 1999; Wang, 1993; Wu, 1986; Yang et al., 1996). The idea of the method is reducing equation systems in general form to equation systems in the form of triangular sets. With this method, solving an equation system can be reduced to solving univariate equations in cascaded form. In the case of finite fields, univariate equations can be solved with Berlekamp's algorithm (Menezes et al., 1996). The CS method can also be used to compute the dimension, the degree, and the order for an equation system, to solve the radical ideal membership problem, and to prove theorems from elementary and differential geometries (Wu, 2001).

In most existing work on CS methods, the zeros of the equations are taken in an algebraically closed field which is infinite. These methods can also be used to find zeros of the equations in finite fields. But, they do not take into the account of the special properties of the finite fields and thus are not efficient for solving equations in finite fields. In this paper, we propose efficient CS methods to solve equations in the general finite field $\mathbb{F}_q$ with q elements. More precisely, we will develop efficient CS algorithms for polynomial systems in the ring

$$\mathbb{R}_q = \mathbb{F}_q[x_1, \ldots, x_n]/(\mathbb{H})$$

where $\mathbb{H} = \{x_1^q - x_1, \ldots, x_n^q - x_n\}$. Due to the special property of $\mathbb{R}_q$, the proposed CS methods are more efficient and have better properties than the general CS method.

A triangular set may have no solutions in a finite field. For instance, $x^2 + 1 = 0$ has no solution in the finite field $\mathbb{F}_3$. To avoid this problem, we introduce the concept of proper triangular sets and prove that proper triangular sets are square-free and always have solutions. We also give an explicit formula for the number of solutions of a monic and proper triangular set. We modify the definition of regular triangular sets (Aubry et al., 1999; Bouziane et al., 2001; Yang et al., 1996) in $\mathbb{R}_q$ and give an exact upper bound for the number of solutions of a regular and proper triangular set.

We propose an improved zero decomposition algorithm which allows us to decompose the zero set of a polynomial equation system in $\mathbb{R}_q$ as the disjoint union of the zero sets of proper and monic triangular sets. As a consequence, we can give an explicit formula for the number of solutions of the equation system. We prove that our elimination procedure to compute a triangular set needs a polynomial number of polynomial multiplications, which is not valid for the general CS method.

An element in $\mathbb{R}_2$ is called a Boolean polynomial. Solving Boolean polynomial systems is especially important and more methods are available. This paper will focus on CS methods. We show that for Boolean polynomial equations, the CS method proposed in this paper and that proposed in (Chai et al., 2008) for Boolean polynomials could be further improved.

Firstly, we show that the bitsize complexity of the algorithm proposed in this paper is $O(l^n)$ for Boolean polynomials, where n is the number of variables and $l \geq 2$ is the number of equations. This is the first complexity analysis for the Ritt–Wu style zero decomposition algorithms. The results in (Gallo and Mishra, 1991) are only for the procedure to compute the CS of an ideal, which is similar to the well-ordering procedure in the Ritt–Wu style decomposition (Wu, 1986). In (Szántó, 1999), a zero decomposition algorithm based on the computation of resultants is given, whose complexity is also single exponential. It seems to us that although the algorithms proposed in (Gallo and Mishra, 1991; Szántó, 1999) have nice complexity bounds, they are practically very inefficient. On the other hand, the algorithm proposed in this paper is practically very efficient as shown by the experiments presented in Section 6.

We also present a multiplication-free CS algorithm in $\mathbb{R}_2$, where the size of the polynomials occurring in the well-ordering procedure is bounded by the size of the input polynomial system and the worst case bitsize complexity of the algorithm is roughly $O(n^d)$, where n is the number of indeterminates and d the degree of the input polynomials. This result is surprising, because repeated