Theoretical Computer Science 657 (2017) 73–85

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Solving systems of diagonal polynomial equations over finite fields

Gábor Ivanyos [a,*], Miklos Santha [b,c]

[a] Institute for Computer Science and Control, Hungarian Academy of Sciences, Kende u. 13-17, 1111 Budapest, Hungary
[b] CNRS, LIAFA, Université Paris Diderot, 75205 Paris, France
[c] Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore

ARTICLE INFO

Article history:
Received 7 September 2015
Received in revised form 14 April 2016
Accepted 20 April 2016
Available online 7 June 2016

Keywords:
Algorithm
Polynomial equations
Finite fields
Chevalley–Warning theorem
Quantum computing

ABSTRACT

We present an algorithm to solve a system of diagonal polynomial equations over finite fields when the number of variables is greater than some fixed polynomial of the number of equations whose degree depends only on the degree of the polynomial equations. Our algorithm works in time polynomial in the number of equations and the logarithm of the size of the field, whenever the degree of the polynomial equations is constant. As a consequence we design polynomial time quantum algorithms for two algebraic hidden structure problems: for the hidden subgroup problem in certain semidirect product p-groups of constant nilpotency class, and for the multi-dimensional univariate hidden polynomial graph problem when the degree of the polynomials is constant.[1]

1. Introduction

Finding small solutions in some well defined sense for a system of integer linear equations is an important, well studied, and computationally hard problem. *Subset Sum*, which asks the solvability of a single equation in the binary domain is one of Karp's original 21 NP-complete problems [18].

The guarantees of many lattice based cryptographic systems come from the average case hardness of *Short Integer Solution*, dating back to Ajtai's breakthrough work [2], where we try to find short nonzero vectors in a random integer lattice. Indeed, this problem has a remarkable worst case versus average case hardness property: solving it on the average is at least as hard as solving various lattice problems in the worst case, such as the decision version of the shortest vector problem, and finding short linearly independent vectors.

Turning back to binary solutions, deciding if there exists a nontrivial zero-one solution of the system of linear equations

$$\begin{array}{rcl} a_{11}y_1+\ldots+a_{1n}y_n & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}y_1+\ldots+a_{mn}y_n & = & 0 \end{array} \tag{1}$$

[*] Corresponding author.
E-mail addresses: Gabor.Ivanyos@sztaki.mta.hu (G. Ivanyos), miklos.santha@gmail.com (M. Santha).

[1] An extended abstract reporting on preliminary versions of the results of this paper has appeared in [16].

http://dx.doi.org/10.1016/j.tcs.2016.04.045
0304-3975/© 2016 Elsevier B.V. All rights reserved.

in the finite field $\mathbb{F}_q$, where q is a power of some prime number p, is easy when $q = p = 2$. However, by modifying the standard reduction of *Satisfiability* to *Subset Sum* [27] it can be shown that it is an NP-hard problem for $q \geq 3$.

The system (1) is equivalent to the system of equations

$$\begin{array}{rcl} a_{11}x_1^{q-1} + \ldots + a_{1n}x_n^{q-1} & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}x_1^{q-1} + \ldots + a_{mn}x_n^{q-1} & = & 0 \end{array} \tag{2}$$

where we look for a nontrivial solution in the whole $\mathbb{F}_q^n$.

In this paper we will consider finding a nonzero solution for a system of diagonal polynomial equations similar to (2), but where more generally, the variables are raised to some power $d \geq 2$. We state formally this problem.

Definition 1. The *System of Diagonal Equations* problem SDE is parametrized by a finite field $\mathbb{F}_q$ and three positive integers n, m and d.

SDE($\mathbb{F}_q, n, m, d$)
Input: A system of polynomial equations over $\mathbb{F}_q$:

$$\begin{array}{rcl} a_{11}x_1^{d} + \ldots + a_{1n}x_n^{d} & = & 0 \\ \vdots & \vdots & \vdots \\ a_{m1}x_1^{d} + \ldots + a_{mn}x_n^{d} & = & 0 \end{array} \tag{3}$$

Output: A nonzero solution $(x_1, \ldots, x_n) \neq \overrightarrow{0}$.

Here $\overrightarrow{0}$ stands for the zero vector of length n. (We will use this notation where we want to stress the distinction between the zero element of a field and the zero vector of a vector space.)

For $j = 1, \ldots, n$, let us denote by v_j the column vector $(a_{1j}, \ldots, a_{mj})^T \in \mathbb{F}_q^m$. Then the system of equations (3) is the same as

$$\sum_{j=1}^{n} x_j^d v_j = \overrightarrow{0}. \tag{4}$$

That is, solving SDE($\mathbb{F}_q, n, m, d$) is equivalent to the task of representing the zero vector as a nontrivial linear combination of a subset of $\{v_1, \ldots, v_n\}$ with dth power coefficients. We present our algorithm actually as solving this vector problem. The special case $d = q - 1$ is the vector zero sum problem where the goal is to find a non-empty subset of the given vectors with zero sum.

Under which conditions can we be sure that for system (3) there exists a nonzero solution? The elegant result of Chevalley [6] and Warning [29] states that the number of solutions of a general (not necessary diagonal) system of polynomial equations is a multiple of the characteristic p of $\mathbb{F}_q$, whenever the number of variables is greater than the sum of the degrees of the polynomials. For diagonal systems (3) this means that when $n > dm$, the existence of a nonzero solution is assured.

In general little is known about the complexity of finding another solution, given a solution of a system which satisfies the Chevalley–Warning condition. When $q = 2$, Papadimitriou has shown [22] that this problem is in the complexity class Polynomial Parity Argument (PPA), the class of NP search problems where the existence of the solution is guaranteed by the fact that in every finite graph the number of vertices with odd degree is even. This implies that it cannot be NP-hard unless NP = co-NP. It is also unlikely that the problem is in P since Alon has shown [3] that this would imply that there are no one-way permutations.

Let us come back to our special system of equations (3). In the case $m = 1$, a nonzero solution can be found in polynomial time for a single equation which satisfies the Chevalley condition due to the remarkable work of van de Woestijne [28] where he proves the following.

Fact 2. *In deterministic polynomial time in d and $\log q$ we can find a nontrivial solution for*

$$a_1x_1^d + \ldots + a_{d+1}x_{d+1}^d = 0.$$

In the case of more than one equation we don't know how to find a nonzero solution for system (3) under just the Chevalley condition. However, if we relax the problem, and take much more variables than are required for the existence of a nonzero solution, we are able to give a polynomial time solution. Using van de Woestijne's result for the one dimensional case, a simple recursion based on reducing one big system with m equations into $d + 1$ subsystems with $m - 1$ equations