Finite Fields and Their Applications 54 (2018) 288–296

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Finding roots of a multivariate polynomial in a linear subspace

Ming-Deh A. Huang

Computer Science Department, University of Southern California, USA

ARTICLE INFO

Article history:
Received 21 June 2017
Accepted 14 August 2018
Available online xxxx
Communicated by Gary L. Mullen

MSC:
13P10
13P15

Keywords:
Polynomial system
Zero-dimensional
Weil descent

ABSTRACT

Suppose F is a polynomial of total degree d in t variables over a finite field $k = \mathbb{F}_{q^n}$. We are interested in finding roots of F that lie in a $\mathbb{F}_q$-linear subspace of k^t. For $m \leq n$, we characterize a large class of m-dimensional $\mathbb{F}_q$-subspaces U of k^t such that the set of roots of F that lie in U can be bounded by d^m in cardinality, independent of q, and constructed in expected time polynomial in n, t and d^m.

1. Introduction

Let k be a field and let $\mathcal{F}$ be a finite set of polynomials in $k[x_1, \ldots, x_t]$. The algebraic set $V_{\overline{k}}(\mathcal{F})$ consists of $(\alpha_1, \ldots, \alpha_t) \in \overline{k}^t$ such that $f(\alpha_1, \ldots, \alpha_t) = 0$ for all $f \in \mathcal{F}$, where $\overline{k}$ denotes the algebraic closure of k. If $\mathcal{F}$ has only one polynomial F, we simply write $V_{\overline{k}}(F)$ for $V_{\overline{k}}(\mathcal{F})$.

Let $F \in k[x_1, \ldots, x_t]$ where $k = \mathbb{F}_{q^n}$ is a finite field. We are interested in finding the roots of F which lie in a $\mathbb{F}_q$-linear subspace of k^t. In this paper, we characterize a large

E-mail address: mdhuang@usc.edu.

https://doi.org/10.1016/j.ffa.2018.08.002

class of $\mathbb{F}_q$-linear subspaces U of k^t such that $|V_{\overline{k}}(F) \cap U|$ can be bounded in terms of the degree of F and the dimension of U, independent of q.

Throughout the paper we fix a $\mathbb{F}_q$-linear basis $\theta_1, \ldots, \theta_n$ of $k = \mathbb{F}_{q^n}$. With respect to the basis, $k = \mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$ are isomorphic as $\mathbb{F}_q$-linear spaces. Similarly, we have an isomorphism between k^t and $\mathbb{F}_q^{tn}$ as $\mathbb{F}_q$-linear spaces, under which $(x_i)_{i=1}^t \in k^t$ is identified with $(y_{ij})_{\substack{i=1,\ldots,t \\ j=1,\ldots,n}} \in \mathbb{F}_q^{tn}$, where $x_i = \sum_{j=1}^n y_{ij}\theta_j$ with $y_{ij} \in \mathbb{F}_q$.

To illustrate the problem and our approach consider the case where F is linear, and we look for solutions of F in an m-dimensional $\mathbb{F}_q$-linear subspace U of k^t. Substituting x_i using the identity $x_i = \sum_{j=1}^n y_{ij}\theta_j$, we get $F(x_1, \ldots, x_t) = \sum_{i=1}^n F_i\theta_i$ where F_i is a linear polynomial in the nt variables y_{ij}. Observe that $x_i \in \mathbb{F}_{q^n}$ if and only if $y_{ij} \in \mathbb{F}_q$ for $j = 1, \ldots, n$. It follows that an $\mathbb{F}_{q^n}$-solution to F in t variables corresponds to an $\mathbb{F}_q$-solution to the system of polynomials $F_1, \ldots, F_n$ in nt variables.

The subspace U can be expressed as the image of an $\mathbb{F}_q$-linear map $\lambda = (\lambda_{ij})_{\substack{i=1,\ldots,t \\ j=1,\ldots,n}}$ from $\mathbb{F}_q^m$ to $\mathbb{F}_q^{nt}$ where each λ_{ij} is an $\mathbb{F}_q$-linear function in m variables $z_1, \ldots, z_m$.

For $i = 1, \ldots, n$, let G_i be the linear polynomials obtained from F_i by substituting y_{ij} using the identity $y_{ij} = \lambda_{ij}(z_1, \ldots, z_m)$. Then the solutions we are looking for is the set of $\mathbb{F}_q$-solutions to the system of n linear polynomials $G_1, \ldots, G_n \in \mathbb{F}_q[z_1, \ldots, z_m]$.

If $n < m$, the rank of the linear system determined by $G_1, \ldots, G_n$ is at most n, so there are at least q^{m-n} solutions from U. If $n \geq m$ and U is chosen at random, then heuristically the linear system is likely of rank m, in which case there is at most one solution. It will follow as a special case of our main result that for a random choice of U in a large collection of subspaces of dimension $m \leq n$ this is indeed the case.

In general when the degree of F is bounded by d, we show that the number of solutions that lie a subspace of dimension $m \leq n$ is typically bounded by d^m.

To state our main result precisely, we need to introduce some notation.

As before we fix a $\mathbb{F}_q$-linear basis $\theta_1, \ldots, \theta_n$ of $k = \mathbb{F}_{q^n}$, and with respect to the basis an isomorphism between k^t and $\mathbb{F}_q^{tn}$ as $\mathbb{F}_q$-linear spaces so that $(x_i)_{i=1}^t \in k^t$ is identified with $(y_{ij})_{\substack{i=1,\ldots,t \\ j=1,\ldots,n}} \in \mathbb{F}_q^{tn}$, where $x_i = \sum_{j=1}^n y_{ij}\theta_j$ with $y_{ij} \in \mathbb{F}_q$.

We fix an ordering of the set of indices $\Delta = \{(i,j) : i = 1, \ldots, t; j = 1, \ldots, n\}$. Let $\omega_1, \ldots, \omega_{tn}$ be the enumeration of the elements of Δ under the ordering.

In general a linear map from $\mathbb{F}_q^m$ to $\mathbb{F}_q$ sends $z = (z_1, \ldots, z_m) \in \mathbb{F}_q^m$ to $\sum_{i=1}^m a_i z_i \in \mathbb{F}_q$ where $a_i \in \mathbb{F}_q$ for $i = 1, \ldots, m$. A linear map λ from $\mathbb{F}_q^m$ to $k^t \cong \mathbb{F}_q^{tn}$ can be defined by tn linear maps λ_{ω_i} from $\mathbb{F}_q^m$ to $\mathbb{F}_q$, for $i = 1, \ldots, tn$. Thus, $\lambda(z) = (y_{\omega_i})_{i=1}^{tn}$ where $y_{\omega_i} = \lambda_{\omega_i}(z)$ for $i = 1, \ldots, tn$, and we write $\lambda = (\lambda_{\omega_i})_{i=1}^{tn}$.

We will restrict our attention to those λ such that $\lambda_{\omega_i}(z) = z_i$ for $i = 1, \ldots, m$. Let Λ_m denote the collection of such $\mathbb{F}_q$-linear maps.

We note that the image of $\lambda \in \Lambda_m$ is an m-dimensional $\mathbb{F}_q$-subspace of $k^t \cong \mathbb{F}_q^{tn}$ consisting of $(y_{\omega_i})_{i=1}^{tn}$ where

$$y_{\omega_i} = \lambda_{\omega_i}(y_{\omega_1}, \ldots, y_{\omega_m})$$

for $i = m+1, \ldots, tn$.