Finite Fields and Their Applications 31 (2015) 1–7

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Polynomial maps on vector spaces over a finite field ☆

Michiel Kosters

Mathematisch Instituut, P.O. Box 9512, 2300 RA Leiden, The Netherlands

ARTICLE INFO

Article history:
Received 12 June 2014
Received in revised form 12 August 2014
Accepted 13 August 2014
Available online 4 November 2014
Communicated by Rudolf Lidl

MSC:
11T06

Keywords:
Finite field
Map
Polynomial
Degree
Surjectivity

ABSTRACT

Let l be a finite field of cardinality q and let n be in $\mathbf{Z}_{\geq 1}$. Let $f_1, \ldots, f_n \in l[x_1, \ldots, x_n]$ not all constant and consider the evaluation map $f = (f_1, \ldots, f_n): l^n \to l^n$. Set $\deg(f) = \max_i \deg(f_i)$. Assume that $l^n \setminus f(l^n)$ is not empty. We will prove

$$\left|l^n \setminus f(l^n)\right| \geq \frac{n(q-1)}{\deg(f)}.$$

This improves previous known bounds.

1. Introduction

The main result of [1] is the following theorem.

Theorem 1.1. *Let l be a finite field of cardinality q and let n be in $\mathbf{Z}_{\geq 1}$. Let $f_1, \ldots, f_n \in l[x_1, \ldots, x_n]$ not all constant and consider the map $f = (f_1, \ldots, f_n): l^n \to l^n$. Set*

☆ This article is part of my PhD thesis written under the supervision of Hendrik Lenstra.
E-mail address: mkosters@math.leidenuniv.nl.
URL: http://www.math.leidenuniv.nl/mkosters.

http://dx.doi.org/10.1016/j.ffa.2014.08.001
1071-5797/

$\deg(f) = \max_i \deg(f_i)$. *Assume that* $l^n \setminus f(l^n)$ *is not empty. Then we have*

$$\left|l^n \setminus f\left(l^n\right)\right| \geq \min\left\{\frac{n(q-1)}{\deg(f)}, q\right\}.$$

We refer to [1] for a nice introduction to this problem including references and historical remarks. The proof in [1] relies on p-adic liftings of such polynomial maps. We give a proof of a stronger statement using different techniques.

Theorem 1.2. *Under the assumptions of Theorem 1.1 we have*

$$\left|l^n \setminus f\left(l^n\right)\right| \geq \frac{n(q-1)}{\deg(f)}.$$

We deduce the result (see Theorem 4.3) from the case $n = 1$ by putting a field structure k on l^n and relate the k-degree and the l-degree. We prove the result $n = 1$ in a similar way as in [2].

2. Degrees

Let l be a finite field of cardinality q and let V be a finite dimensional l-vector space. By $V^\vee = \operatorname{Hom}(V, l)$ we denote the dual of V. Let $v_1, \ldots, v_s$ be a basis of V. By $x_1, \ldots, x_s$ we denote its dual basis in $V^\vee$, that is, x_i is the map which sends v_j to δ_{ij}. Denote by $\operatorname{Sym}_l(V^\vee)$ the symmetric algebra of $V^\vee$ over l. We have an isomorphism $l[x_1, \ldots, x_s] \to \operatorname{Sym}_l(V^\vee)$ mapping x_i to x_i. Note that $\operatorname{Map}(V, l) = l^V$ is a commutative ring under the coordinate wise addition and multiplication and it is an l-algebra. The linear map $V^\vee \to \operatorname{Map}(V, l)$ induces by the universal property of $\operatorname{Sym}_l(V^\vee)$ a ring morphism $\varphi: \operatorname{Sym}_l(V^\vee) \to \operatorname{Map}(V, l)$. When choosing a basis, we have the following commutative diagram, where the second horizontal map is the evaluation map and the vertical maps are the natural isomorphisms:

$$\begin{array}{ccc} \operatorname{Sym}(V^\vee) & \xrightarrow{\varphi} & \operatorname{Map}(V, l) \\ \uparrow & & \uparrow \\ l[x_1, \ldots, x_s] & \longrightarrow & \operatorname{Map}(l^s, l). \end{array}$$

Lemma 2.1. *The map* φ *is surjective. After a choice of a basis as above the kernel is equal to* $(x_i^q - x_i : i = 1, \ldots, s)$ *and every* $f \in \operatorname{Map}(V, l)$ *has a unique representative* $\sum_{m=(m_1,\ldots,m_s):\ 0 \leq m_i \leq q-1} c_m x_1^{m_1} \cdots x_s^{m_s}$ *with* $c_m \in l$.

Proof. After choosing a basis, we just consider the map

$$l[x_1, \ldots, x_s] \to \operatorname{Map}\left(l^s, l\right).$$