POLYNOMIAL MAPS ON VECTOR SPACES OVER A FINITE FIELD

MICHIEL KOSTERS

Abstract. Let $l$ be a finite field of cardinality $q$ and let $n$ be in $\mathbb{Z}_{\geq 1}$. 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

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

This improves previous known bounds.

1. Introduction

The main result of [MWW12] is the following theorem.

Theorem 1.1. Let $l$ be a finite field of cardinality $q$ and let $n$ be in $\mathbb{Z}_{\geq 1}$. 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 $\deg(f) = \max_i \deg(f_i)$. Assume that $l^n \setminus f(l^n)$ is not empty. Then we have

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

We refer to [MWW12] for a nice introduction to this problem including references and historical remarks. The proof in [MWW12] 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

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

We deduce the result 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 [Tur95].

2. Degrees

Let $l$ be a finite field of cardinality $q$ and let $V$ be a finite dimensional $l$-vector space. By $V^\vee = \text{Hom}(V, l)$ we denote the dual of $V$. Let $v_1, \ldots, v_f$ be a basis of $V$. By $x_1, \ldots, x_f$ we denote its dual basis in $V^\vee$, that is, $x_i$ is the map which sends $v_j$ to $\delta_{ij}$. Denote by $\text{Sym}_l(V^\vee)$ the symmetric algebra of $V^\vee$ over $l$. We have an isomorphism $l[x_1, \ldots, x_f] \to \text{Sym}_l(V^\vee)$ mapping $x_i$ to $x_i$. Note that $\text{Map}(V, l) = l^V$.

Date: April 29, 2014.

2010 Mathematics Subject Classification. 11T06.

This article is part of my PhD thesis written under the supervision of Hendrik Lenstra.
is a commutative ring under the coordinate wise addition and multiplication and it is a $l$-algebra. The linear map $V^\lor \to \text{Map}(V,l)$ induces by the universal property of $\text{Sym}_l(V^\lor)$ a ring morphism $\varphi : \text{Sym}_l(V^\lor) \to \text{Map}(V,l)$. 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:

$$\begin{array}{ccc}
\text{Sym}(V^\lor) & \longrightarrow & \text{Map}(V,l) \\
\downarrow & & \downarrow \\
l[x_1, \ldots, x_n] & \longrightarrow & \text{Map}(l^n,l).
\end{array}$$

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

*Proof.* After choosing a basis, we just consider the map $l[x_1, \ldots, x_f] \to \text{Map}(l^n,l)$.

For $c = (c_1, \ldots, c_f) \in l^f$ set

$$f_c = \prod_i (1 - (x_i - c_i)^q).$$

For $c' \in l^f$ we have $f_c(c') = \delta_{cc'}$. With these building blocks one easily shows that $\varphi$ is surjective.

For $i \in \{1,2,\ldots,f\}$ the element $x_i^q - x_i$ is in the kernel of $\varphi$. This shows that modulo the kernel any $g \in l[x_1, \ldots, x_f]$ has a representative

$$f = \sum_{m=(m_1, \ldots, m_n) : 0 \leq m_i \leq q-1} c_{m} x_1^{m_1} \cdots x_r^{m_n}.$$  

The set of such elements has cardinality $q^{rf}$. As $\# \text{Map}(V,l) = q^{rf}$, we see that the kernel is $(x_i^q - x_i : i = 1, \ldots, r)$. Furthermore, any element has a unique representative as described above. \hfill $\Box$

Note that $\text{Sym}_l(V^\lor)$ is a graded $l$-algebra where we say that 0 has degree $-\infty$. For $f \in \text{Map}(V,l)$ we set

$$\deg_l(f) = \min \{ \deg(g) : \varphi(g) = f \}.$$ 

Note that $\deg_l(f_1 + f_2) \leq \max(\deg_l(f_1), \deg_l(f_2))$, with equality if the degrees are different. In practice, if $f \in l[x_1, \ldots, x_n]$, then $\deg_l(f)$ is calculated as follows: for all $i$ replace $x_i^q$ by $x_i$ until $\deg_{x_i}(f) < q$. Then the degree is the total degree of the remaining polynomial.

Let $W$ be a finite dimensional $l$-vector space. Then we have $\text{Map}(V,W) = W \otimes_l \text{Map}(V,l)$. For $f \in \text{Map}(V,W)$ we set

$$\deg_l(f) = \max \{ \deg_l(g \circ f) : g \in W^\lor \}.$$ 

If $g_1, \ldots, g_n$ is a basis of $W^\lor$, then $\deg_l(f) = \max (\deg_l(g_i \circ f) : i = 1, \ldots, n)$. This follows from the identity $\deg_l(\sum_i c_i g_i) \leq \max_i (\deg_l(g_i))$ for $c_i \in l$. Note that the degree is bounded above by $(q-1) \cdot \dim_l(V)$.

For $i \in \mathbb{Z}_{\geq 0}$ and a subset $S$ of $\text{Sym}_l(V^\lor)$ we set

$$S_i^l = \text{Span}(s_1 \circ \cdots \circ s_i : s_i \in S) \in \text{Sym}_l(V^\lor).$$
Lemma 2.2. Let $f \in \text{Map}(V,W)$. For $i \in \mathbb{Z}_{\geq 0}$ one has: $\deg_f \leq i \iff f \in W \otimes_l (l + V^i)_l$.

Proof. Suppose first that $W = l$. The proof comes down to showing the following identity for $i \in \mathbb{Z}_{\geq 0}$:

$$l + V^i + \ldots + (V^i)_l = (l + V^i)_l.$$ 

The general case follows easily. □

3. Relations between degrees

Let $k$ be a finite field and let $l$ be a subfield of cardinality $q$. Set $h = [k : l]$. Let $V$ and $W$ be finite dimension $k$-vector spaces. Let $f \in \text{Map}(V,W)$. In this section we will describe the relation between the $k$-degree and the $l$-degree.

Let us first assume that $W = k$. Let $v_1, \ldots, v_r$ be a basis of $V$ over $k$. Let $R = k[x_1, \ldots, x_r]/(x_1^h - x_1, \ldots, x_r^h - x_r)$. We have the following diagram where all morphisms are ring morphisms. Here $\psi$ is the map discussed before, $\tau$ is the natural isomorphism, $\varphi$ is the isomorphism discussed before, and $\sigma$ is the isomorphism, depending on the basis, discussed above.

$$k \otimes_l \text{Map}(V,l) \xrightarrow{\tau} \text{Map}(V,k) \xrightarrow{\psi} \text{Sym}_l(\text{Hom}_l(V,l)) \xrightarrow{\varphi} \text{Sym}_k(\text{Hom}_k(V,k))/\ker(\varphi) \stackrel{\rho}{\longrightarrow} R.$$ 

Consider the ring morphism $\rho = \sigma \circ \varphi^{-1} \circ \tau \circ \psi: k \otimes_l \text{Sym}_l(\text{Hom}_l(V,l)) \rightarrow R$. Lemma 2.2 suggest that to compare degrees, we need to find $\rho(k \otimes_l (l + \text{Hom}_l(V,l))_l^i)$.

The following lemma says that it is enough to find $k + k \otimes_l \text{Hom}_l(V,l)$.

Lemma 3.1. For $i \in \mathbb{Z}_{\geq 0}$ we have the following equality in $k \otimes_l \text{Sym}_l(V)$:

$$k \otimes_l (l + \text{Hom}_l(V,l))_l^i = (k + k \otimes_l \text{Hom}_l(V,l))_k^i.$$ 

Proof. Both are $k$-vector spaces and the inclusions are not hard to see. □

The following lemma identifies $k + k \otimes_l \text{Hom}_l(V,l)$.

Lemma 3.2. One has

$$\rho(k + k \otimes_l \text{Hom}_l(V,l)) = \text{Span}_k \left( \{ x_j^q : 1 \leq j \leq r, \ 0 \leq s < h \} \cup \{ 1 \} \right).$$ 

Proof. Note that $\tau \circ \psi(k + k \otimes_l \text{Hom}_l(V,l)) = k \oplus \text{Hom}_l(V,k) \subseteq \text{Map}(V,k)$. Note that

$$\sigma^{-1} \left( \text{Span}_k \left( \{ x_j^q : 1 \leq j \leq r, \ 0 \leq s < h \} \right) \right) \subseteq \text{Hom}_l(V,k).$$ 

As both sets have dimension $\dim(V) = r \cdot h$ over $k$, the result follows. □

For $m, n \in \mathbb{Z}_{\geq 1}$ we set $s_m(n)$ to be the sum of the digits of $n$ in base $m$.

Lemma 3.3. Let $m \in \mathbb{Z}_{\geq 2}$ and $n, n' \in \mathbb{Z}_{\geq 0}$. Then the following hold:

i. $s_m(n + n') \leq s_m(n) + s_m(n')$;

ii. Suppose $n = \sum_i c_i m^i, c_i \geq 0$. Then we have $\sum_i c_i \geq s_m(n)$ with equality iff for all $i$ we have $c_i < m$. 

Proof. i. This is well-known and left to the reader.

ii. We give a proof by induction on \( n \). For \( n = 0 \) the result is correct. Suppose first that \( n = c_m m^s \) and assume that \( c_s \geq m \). Then we have \( n = (c_s - m)m^s + m^{s+1} \).

By induction and ii we have

\[
c_s > c_s - m + 1 \geq s_m((c_s - m)m^s) + s_m(m^{s+1}) \geq s_m(c_s m^s).
\]

In general, using i, we find

\[
\sum_i c_i \geq \sum_i s_m(c_i m^i) \geq s_m(n).
\]

Also, one easily sees that one has equality iff all \( c_i \) are smaller than \( m \). \( \square \)

**Proposition 3.4.** Let \( f \in k[x_1, \ldots, x_r] \) nonzero with the degree in all \( x_i \) of all the monomials less than \( q^h \). Write \( f = \sum_{s=(s_1, \ldots, s_r)} c_s x_1^{s_1} \cdots x_r^{s_r} \). Then the \( l \)-degree of \( \tau^{-1} \circ \varphi(f) \in k \otimes_l \operatorname{Map}(V,l) \) is equal to

\[
\max\{s_q(s_1) + \cdots + s_q(s_r) : s = (s_1, \ldots, s_r) \text{ s.t. } c_s \neq 0\}.
\]

**Proof.** Put \( g = \tau^{-1} \circ \varphi \circ \sigma^{-1}(f) \). From Lemma 2.2, Lemma 3.1 and Lemma 3.2 we obtain the following. Let \( i \in \mathbb{Z}_{\geq 0} \). Then \( \deg_i(g) \leq i \) iff

\[
g \in \rho(k \otimes_l (l + \operatorname{Hom}(V,l))^i_l) = \rho((k + k \otimes_l \operatorname{Hom}(V,l))^i_k)
\]

\[
= \left(\operatorname{Span}_k \left\{ x_j^{q^r} : 1 \leq j \leq r, \ 0 \leq s < h \cup \{1\} \right\} \right)^i_k.
\]

The result follows from Lemma 3.3. \( \square \)

The case for a general \( W \) just follows by decomposing \( W \) into a direct sum of copies of \( k \) and then taking the maximum of the corresponding degrees.

### 4. Proof of main theorem

**Lemma 4.1.** Let \( m, q, h \in \mathbb{Z}_{>0} \) and suppose that \( q^h - 1 \mid m \). Then we have: \( s_q(m) \geq h(q - 1) \).

**Proof.** We do a proof by induction on \( m \).

Suppose that \( m < q^h \). Then \( m = q^h - 1 \) and we have \( s_q(m) = h(q - 1) \).

Suppose \( m \geq q^h \). Write \( m = m_0 q^h + m_1 \) with \( 0 \leq m_1 < q^h \) and \( m_0 \geq 1 \). We claim that \( q^h - 1 \mid m_0 + m_1 \). Note that \( m_0 + m_1 \equiv m_0 q^h + m_1 \equiv 0 \pmod{q^h - 1} \). Then by induction we find

\[
s_q(m) = s_q(m_0) + s_q(m_1) \geq s_q(m_0 + m_1) \geq h(q - 1).
\]

\( \square \)

**Lemma 4.2.** Let \( k \) be a finite field of cardinality \( q \). Let \( R = k[X_a : a \in k] \) and consider the action of \( k^* \) on \( R \) given by

\[
k^* \mapsto \operatorname{Aut}_{k-\text{alg}}(R)
\]

\[
c \mapsto (X_a \mapsto X_{ca}).
\]

Let \( F \in R \) fixed by the action of \( k^* \) with \( F(0, \ldots, 0) = 0 \) and such that the degree of no monomial of \( F \) is a multiple of \( q^r - 1 \). Then for \( w = (a)_a \in k^k \) we have \( F(w) = 0 \).
Proof. We may assume that $F$ is homogeneous with $d = \deg(F)$ which is not a multiple of $q' - 1$. Take $\lambda \in k^*$ a generator of the cyclic group. As $F$ is fixed by $k^*$ we find:

$$F(w) = F(\lambda w) = \lambda^d F(w).$$

As $\lambda^d \neq 1$, we have $F(w) = 0$ and the result follows. $\square$

Finally we can state and prove a stronger version of Theorem 1.2.

**Theorem 4.3.** Let $k$ be a finite field. Let $l \subseteq k$ be a subfield with $[k : l] = h$ and let $V$ be a finite dimensional $k$-vector space. Let $f \in \text{Map}(V, V)$ be a non-constant and non-surjective map. Then $f$ misses at least

$$\frac{\dim_k(V) \cdot h \cdot (\#l - 1)}{\deg_l(f)}$$

values.

Proof. Set $\#l = q$. Put a $k$-linear multiplication on $V$ such that it becomes a field. This allows us reduce to the case where $V = k$. Assume $V = k$. After shifting we may assume $f(0) = 0$. Put an ordering $\leq$ on $k$. In $k[T]$ we have

$$\prod_{a \in k} (1 - f(a)T) = 1 - \sum_a f(a)T + \sum_{a < b} f(a)f(b)T^2 - \ldots = \sum_i a_i T^i.$$

For $1 \leq i < \frac{h(q-1)}{\deg_l(f)}$ we claim that $a_i = 0$. Put $f_0 \in k[x]$ a polynomial of degree at most $q^h - 1$ inducing $f : k \to k$. Consider $g_i = \prod_{a_1 < \ldots < a_i} f_0(X_{a_1}) \cdots f_0(X_{a_i})$ in $k[X_a : a \in k]$, which is fixed by $k^*$. We have a map

$$\varphi : k[X_a : a \in k] \to \text{Map}(k^k, k).$$

Proposition 3.4 gives us that $\deg_l(\varphi(g_i)) = i \cdot \deg_l(f) < h(q - 1)$. We claim that there is no monomial in $g_i$ with degree a multiple of $q^h - 1$. Indeed, suppose that there is a monomial $c X_{r_1} \cdot \ldots X_{r_i} \neq 0$ in $g_i$ (note that not all $r_i$ are zero) and suppose that $q^h - 1 | \sum_i r_i$. Then by Lemma 4.1 and Proposition 3.4 we have

$$h(q - 1) \leq s_q(\sum_j r_j) \leq \sum_j s_q(r_j) \leq i \cdot \deg_l(f) < h(q - 1),$$

contradiction. Hence we can apply Lemma 4.2 to conclude that $a_i = 0$.

Hence we conclude

$$\prod_{a \in k} (1 - f(a)T) \equiv 1 \pmod{T^{\frac{h(q-1)}{\deg_l(f)}}}.$$
Combining this gives:
\[
\prod_{a \in k \setminus f(k)} (1 - aT) = \frac{\prod_{a \in k}(1 - aT)}{\prod_{b \in f(k)}(1 - bT)} = \prod_{a \in k}(1 - aT) \prod_{c \in k}(1 - f(c)T) \pmod{T^{\frac{h(b-1)}{\deg(f)}}}
\]
\[
= \prod_{b \in f(k)} (1 - bT)^{\#f^{-1}(b)-1} \pmod{T^{\frac{h(b-1)}{\deg(f)}}}.
\]

Note that the polynomials \(\prod_{a \in k \setminus f(k)} (1 - aT)\) and \(\prod_{b \in f(k)} (1 - bT)^{\#f^{-1}(b)-1}\) have degree bounded by \(s = k \setminus f(k)\) and are different since \(s \geq 1\). But this implies that \(s \geq \frac{h(q-1)}{\deg(f)}\).

\[\square\]

**Remark 4.4.** Different \(l\) in Theorem 4.3 may give different lower bounds.

5. Examples

In this section we will give examples which meet the bound from Theorem 4.2.

**Example 5.1** \((n = \deg(f))\). Let \(l\) be a finite field of cardinality \(q\). In this example we will show that for \(n, d \in \mathbb{Z}_{\geq 2}\) there are functions \(f_1, \ldots, f_n \in l[x_1, \ldots, x_n]\) such that the maximum of the degrees is equal to \(d\) such that the induced map \(f : l^n \to l^n\) satisfies \(|l^n \setminus f(l^n)| = \frac{n(q-1)}{d} = q - 1\). For \(i = 1, \ldots, n - 1\) set \(f_i = x_i\). Let \(l_{n-1}\) be the unique extension of \(l\) of degree \(n - 1\). Let \(v_1, \ldots, v_{n-1}\) be a basis of \(l_{n-1}\) over \(l\). Then \(g = \text{Norm}_{l_{n-1}/l}(x_1 v_1 + \ldots + x_{n-1} v_{n-1})\) is a homogeneous polynomial of degree \(n - 1\) in \(x_1, \ldots, x_{n-1}\). Put \(f_n = x_n \cdot g\). As the norm of a nonzero element is nonzero, one easily sees that \(l^n \setminus f(l^n) = \{0\} \times \ldots \times \{0\} \times l^*\) has cardinality \(q - 1\).

**Example 5.2** \((n = \frac{\deg(f)}{q-1})\). Let \(l\) be a finite field and let \(n \in \mathbb{Z}_{\geq 1}\). Let \(f_1, \ldots, f_n \in l[x_1, \ldots, x_n]\) such that the combined map \(f : l^n \to l^n\) satisfies \(|l^n \setminus f(l^n)| = 1\) (Lemma 2.4). From Theorem 4.2 and the upper bound \(n(q - 1)\) for the degree we deduce that \(\deg(f) = n(q - 1)\).

**References**

[MWW12] Gary L. Mullen, Daqing Wan, and Qiang Wang. Value sets of polynomial maps over finite fields. [http://arxiv.org/abs/1210.8119](http://arxiv.org/abs/1210.8119) 2012. preprint.

[Tur95] Gerhard Turnwald. A new criterion for permutation polynomials. *Finite Fields Appl.*, 1(1):64–82, 1995.

**Mathematisch Instituut**

P.O. Box 9512
2300 RA Leiden
The Netherlands

E-mail address: mkosters@math.leidenuniv.nl

URL: www.math.leidenuniv.nl/~mkosters