ON THE GRAPH OF A FUNCTION OVER A PRIME FIELD WHOSE SMALL POWERS HAVE BOUNDED DEGREE

SIMEON BALL AND ANDRÁS GÁCS

Abstract. Let f be a function from a finite field $\mathbb{F}_p$ with a prime number p of elements, to $\mathbb{F}_p$. In this article we consider those functions $f(X)$ for which there is a positive integer $n > 2\sqrt{p-1} - \frac{11}{4}$ with the property that $f(X)^i$, when considered as an element of $\mathbb{F}_p[X]/(X^p - X)$, has degree at most $p-2-n+i$, for all $i = 1, \ldots, n$. We prove that every line is incident with at most $t-1$ points of the graph of f, or at least $n+4-t$ points, where t is a positive integer satisfying $n > (p-1)/t + t - 3$ if n is even and $n > (p-3)/t + t - 2$ if n is odd. With the additional hypothesis that there are $t-1$ lines that are incident with at least t points of the graph of f, we prove that the graph of f is contained in these $t-1$ lines. We conjecture that the graph of f is contained in an algebraic curve of degree $t-1$ and prove the conjecture for $t=2$ and $t=3$. These results apply to functions that determine less than $p - 2\sqrt{p-1} + \frac{11}{4}$ directions. In particular, the proof of the conjecture for $t=2$ and $t=3$ gives new proofs of the result of Lovász and Schrijver [7] and the result in [5] respectively, which classify all functions which determine at most $2(p-1)/3$ directions.

1. Introduction

Let p be a prime power and let f be a function from $\mathbb{F}_p$, the finite field with p elements, to $\mathbb{F}_p$. Any such function has a unique representation as a polynomial of degree at most $p-1$ and, conversely, each polynomial $\phi(X)$ of degree at most $p-1$ defines a distinct function $x \mapsto \phi(x)$. The function $x \mapsto f(x)^i$ is understood to be the i-th power of the image of $f(x)$, will sometimes be abbreviated as f^i, and should not be confused with the i-fold composition of f.

This article is concerned with functions $f(x)$ for which there is an $n > 2\sqrt{p-1} - \frac{11}{4}$ with the property that, for all $i = 1, \ldots, n$, the function $f(x)^i$ has degree at most $p-2-n+i$. By degree we mean the degree of the polynomial of degree at most $p-1$ which represents the function $x \mapsto f(x)^i$, that is the degree of the residue of $f(x)^i$ in the quotient ring $\mathbb{F}_p[x]/(x^p - x)$.

We define $I(f)$ to be the maximum such n plus one. An alternative definition is given by

$$I(f) = \min\{i + j \mid \sum_{x \in \mathbb{F}_q} x^j f(x)^i \neq 0\}.$$

Date: 19 November 2007.

This work was carried out in part under the "Hungarian-Spanish Intergovernmental S and T co-operation programme". The first author also acknowledges the support of the Ramon y Cajal programme and the project MTM2005-08990-C02-01 of the Spanish Ministry of Science and Education and the project 2005SGR00256 of the Catalan Research Council. The second author was supported by OTKA grants T 67867, T 049662, TÉT grant E-16/04 and Bolyai scholarship.

To see this note that the sum $-\sum_{x\in\mathbb{F}_p} g(x)$ is equal to the coefficient of x^{p-1} in g, for any polynomial $g(X)$ of degree at most $p-1$. Thus, for all $n \leq I(f)-1$, the sum $\sum_{x\in\mathbb{F}_p} x^{n-i} f(x)^i = 0$ implies that $f(x)^i$ has degree at most $p-2-n+i$.

Let $M(f)$ be the number of elements c of $\mathbb{F}_p$ for which $x \mapsto f(x)+cx$ is a permutation of $\mathbb{F}_p$, in other words $f(X)+cX$ is a permutation polynomial. Alternatively, $-c$ does not occur as a direction determined by the function f, i.e. $-c \neq (f(y)-f(x))/(y-x)$ for all $x, y \in \mathbb{F}_p$, $x \neq y$. Indeed, the motivation to look at the properties of functions f for which $I(f)$ is large, stems from the desire to classify those functions that determine few directions.

Although the results in the first section relate to functions over a field with a prime number of elements they more or less extend to all finite fields, some care having to be taken with the parity of the characteristic in a few places. However, the motivation to study functions with the above property is the fact that if the field is a prime field then $I(f)$ is greater than $M(f)$. Let us check this first.

Let

$$\pi_k(Y) = \sum_{x\in\mathbb{F}_p} (f(x)+xY)^k = \sum_{i+j=k} \sum_{x\in\mathbb{F}_p} \binom{i+j}{i} x^j f(x)^i Y^j.$$

By [6, Lemma 7.3], if $x \mapsto f(x)+cx$ is a permutation, then $\pi_k(c) = 0$ for all $0 < k < p-1$. For $k < p-1$ the polynomial $\pi_k(Y)$ has degree at most $k-1$, since the coefficient of Y^k is $\sum_{x\in\mathbb{F}_p} x^k = 0$. Therefore it is identically zero for all $0 \leq k-1 < M(f)$, unless $M(f) = p-1$ in which case f is linear. The binomial coefficient occurring in the coefficent of Y^j, $\binom{i+j}{i}$ is non-zero since $i+j < p$. Hence, if f is not linear then $I(f)-1 \geq M(f)$.

The purpose of this note is to say something about the graph of the function f given that $I(f) > 2\sqrt{p-1} - \frac{7}{4}$. We shall then apply these results to functions for which $M(f)$ is large. Previously, in [7], [5] and [2], although the proofs centered on functions for which $I(f)$ is large, all assumed that $M(f)$ was reasonably large too. Here we eliminate this necessity. Moreover, in previous articles $I(f)$ was required to be much larger, at least $(p+4)/3$, to be able to draw conclusions.

Other articles that are relevant here are [4] and [1] which deal with functions f over a finite field $\mathbb{F}_q$, where q is a prime power, for which $M(f) \geq (q-1)/2$ and [10] which bounds $M(f)$ in terms of the degree of f.

2. Properties of functions for which $I(f)$ is more than $2\sqrt{p-1} - \frac{7}{4}$

Write $I(f) = 2s+1+\epsilon$ where s is some integer satisfying $s > \sqrt{p-1} - \frac{11}{8}$ and $\epsilon = 0$ if $I(f)$ is odd and $\epsilon = 1$ if $I(f)$ is even. This implies $I(f) > 2\sqrt{p-1} - \frac{7}{4}$.

By definition

$$\sum_{x\in\mathbb{F}_p} f(x)^i x^j = 0,$$

for all $0 < i+j \leq 2s+\epsilon$, and the degree of f, which we write as f°, satisfies $f^\circ \leq p-2s-1-\epsilon$ and more generally $(f^i)^\circ \leq p-2s-2+i-\epsilon$, for all $i = 1, \ldots, 2s+\epsilon$.

Let
$$V = \{(F_1, F_2, \dots, F_s) \mid F_i \in \mathbb{F}_p[X],\ F_i^\circ \le s - i\}.$$
The set V consists of s-tuples of polynomials and is a vector space over $\mathbb{F}_p$ of dimension $s(s+1)/2$.

Consider the linear map ψ_1 from V to $\mathbb{F}_p[X]$ defined by
$$\psi_1((F_1, F_2, \dots, F_s)) = F_1 f + F_2 f^2 + \dots + F_s f^s.$$

We want to bound the dimension of the subspace $Im(\psi_1)$, the image of ψ_1. Note that the dimension of a subspace U of a vector space of polynomials is equal to the number of distinct degrees of polynomials that appear in U.

Lemma 2.1. *At most $(p-3)/2 - s - \epsilon$ of the numbers in the interval $[s+1, \dots, p-1]$ occur as degrees of polynomials in $Im(\psi_1)$.*

Proof. The maximum degree of a polynomial in $Im(\psi_1)$ is $p - s - 2 - \epsilon$ so we are only concerned with the interval $[s+1, \dots, p-s-2-\epsilon]$. Given any two polynomials g and h in $Im(\psi_1)$, the product gh can be written as a $\sum_{i=1}^{2s} G_i f^i$, where $G_i^\circ \le 2s - i$ for some G_i. Thus, since $I(f) \ge 2s+1$, it follows that $(gh)^\circ \ne p-1$ and if $\epsilon = 1$ then $(gh)^\circ \ne p-2$, since Xgh cannot have degree $p-1$ in this case.

If $\epsilon = 0$ then only half of the numbers in the interval $[s+1, \dots, p-s-2]$ can occur as degrees of polynomials in $Im(\psi_1)$, that is at most $(p-3)/2 - s$.

If $\epsilon = 1$ and m a number in the interval $[(p+1)/2, \dots, p-s-3]$ occurs as a degree of a polynomial in $Im(\psi_1)$, then neither $p-1-m$, nor $p-2-m$ occur as degrees of a polynomial in $Im(\psi_1)$. Thus, if a positive number d of the numbers in the interval $[(p+1)/2, \dots, p-s-3]$ occur as a degree of a polynomial in $Im(\psi_1)$, then at most $(p-3)/2 - s - d - 1$ of the numbers in the interval $[s+1, \dots, (p-3)/2]$ occur as a degree of a polynomial in $Im(\psi_1)$. If $g \in Im(\psi_1)$ then $g^\circ \ne (p-1)/2$, since $(g^2)^\circ \ne p-1$. Thus, overall at most $(p-5)/2 - s$ of the numbers in the interval $[s+1, \dots, p-s-3]$ can occur as degrees of polynomials in $Im(\psi_1)$. The case $d = 0$ does not occur since $f, f^2, \dots, f^s \in Im(\psi_1)$ and it is not possible that all these polynomials have degree less than $(p-1)/2$. □

Let t be a positive integer with the property that $I(f) - 1 - \epsilon = 2s > (p-1-2\epsilon)/t + t - 3$ and $2 \le t \le \sqrt{p-1}$. Note that $t < s+2$, so the following lemma is not trivial.

Lemma 2.2. *Either the polynomial f has less than t distinct zeros or it has more than $s+2$ distinct zeros.*

Proof. Let r be the number of distinct zeros of f and suppose that $t \le r \le s$. We will deal with the cases $r = s+1$ and $r = s+2$ at the end of the proof.

A zero of f is a zero of any polynomial in $Im(\psi_1)$, so all non-zero polynomials in $Im(\psi_1)$ have degree at least r. Thus, applying Lemma 2.1,
$$dim\ Im(\psi_1) \le (p-3)/2 - s - \epsilon + s - r + 1 = (p-1)/2 - r - \epsilon,$$
and so $Ker(\psi_1)$, the kernel of ψ_1 satisfies
$$dim\ Ker(\psi_1) \ge s(s+1)/2 - (p-1)/2 + r + \epsilon.$$

Let $(F_1,\dots,F_s)\in Ker(\psi_1)$. Then $F_1f+F_2f^2+\ldots+F_sf^s=0$ and for all x such that $f(x)\neq 0$

$$-F_1=F_2f+\ldots+F_sf^{s-1}.$$

The degree of this equation is at most $p-s-3$ and it holds for all elements that are not zeros of f, of which there are at least $p-s-2$ by assumption, so it holds for all elements of $\mathbb{F}_p$. Therefore a zero of f is a zero of the polynomial F_1, which implies, if F_1 is not zero then it has degree at least r. By definition it has degree at most $s-1$.

Define a linear map ψ_2 from $Ker(\psi_1)$ to $\mathbb{F}_p[X]$ by

$$\psi_2((F_1,F_2,\dots,F_s))=F_2f+F_3f^2+\ldots+F_sf^{s-1}.$$

A non-zero polynomial in the $Im(\psi_2)$ has degree at least r and at most $s-1$ and so

$$dim\ Ker(\psi_2)\geq s(s+1)/2-(p-1)/2+r+\epsilon-(s-r).$$

Let $(F_1,\dots,F_s)\in Ker(\psi_2)$. Then $F_2f+F_3f^2+\ldots+F_sf^{s-1}=0$ and for all x such that $f(x)\neq 0$

$$-F_2=F_3f+\ldots+F_sf^{s-2}.$$

The degree of this equation is at most $p-s-4$ and since it holds for at least $p-s-2$ elements of $\mathbb{F}_p$, it holds for all elements of $\mathbb{F}_p$. Therefore a zero of f is a zero of the polynomial F_2, which implies, if F_2 is not zero then it has degree at least r, and by definition it has degree at most $s-2$.

Now we define recursively maps ψ_j, for $j=3,4,\dots,s-t+1$, from the $Ker(\psi_{j-1})$ to $\mathbb{F}_p[X]$ by

$$\psi_j((F_1,F_2,\dots,F_s))=F_jf+F_{j+1}f^2+\ldots+F_sf^{s-j+1}.$$

Arguing as before, non-zero polynomials in the $Im(\psi_j)$ have degree at least r and at most $s-j+1$ and so the dimension of $Im(\psi_j)$ is at most $s-j-r+2$. Therefore

$$dim\ Ker(\psi_j)\geq s(s+1)/2-(p-1)/2+r+\epsilon-(s-r)-(s-r-1)-\ldots-(s-j-r+2).$$

In particular

$$dim\ Ker(\psi_{s-r+1})\geq(2rs-p+1-r(r-3)+2\epsilon)/2,$$

which is greater than zero since $2rs-r(r-3)$ is minimised while r ranges between t and $s+2$ when $r=t$, and $2ts-t(t-3)>p-1-2\epsilon$.

Let $(F_1,F_2,\dots,F_s)$ be a non-zero element of $Ker(\psi_{s-r+1})$. The fact that $F_{s-r+1}f+\ldots+F_sf^r=0$ implies that for all x that are not zeros of f

$$-F_{s-r+1}=F_{s-r+2}f+\ldots+F_sf^{r-1}.$$

However, the degree of this equation is at most $p-2s+r-3\leq p-s-3$ and, since it holds for at least $p-s-2$ elements, it holds for all elements of $\mathbb{F}_p$. Therefore a zero of f is a zero of the polynomial F_{s-r+1}, which implies that F_{s-r+1} is zero since it has degree at most $r-1$. Similarly $F_{s-r+2},F_{s-r+3},\dots,F_s$ are zero. Now $(F_1,F_2,\dots,F_s)=(F_1,F_2,\dots,F_{s-r},0,\dots,0)\in Ker(\psi_{s-r+1})\subseteq Ker(\psi_{s-r})\subseteq\ldots\subseteq Ker(\psi_1)$. Recursively $(F_1,F_2,\dots,F_{s-r-j},0,\dots,0)\in Ker(\psi_{s-r-j})$ implies $F_{s-r-j}=0$ for $j=0,1,\dots,s-r-1$, and hence $(F_1,F_2,\dots,F_s)=0$. We have shown that if $(F_1,\dots,F_s)\in Ker(\psi_{s-r+1})$ then $(F_1,F_2,\dots,F_s)=0$. Thus the dimension of $Ker(\psi_{s-r+1})$ is zero, which is not the case.

Let us finally deal with the cases $r = s+1$ and $r = s+2$. In these cases, since the zeros of f are zeros of any polynomial in $Im(\psi_1)$, every polynomial in $Im(\psi_1)$ has degree at least $s+1$. Lemma 2.1 implies

$$dim\ Im(\psi_1) \leq (p-3)/2 - s - \epsilon,$$

and so

$$dim\ Ker(\psi_1) \geq s(s+1)/2 - (p-3)/2 + s + \epsilon,$$

which is greater than zero since $s > \sqrt{p-1} - \frac{11}{8}$ and $p \geq 5$.

Let $(F_1, \ldots, F_s) \in Ker(\psi_1)$. Then $F_1 f + F_2 f^2 + \ldots + F_s f^s = 0$ and for all x such that $f(x) \neq 0$,

$$-F_1 = F_2 f + \ldots + F_s f^{s-1}.$$

The degree of this equation is at most $p-s-3$ and it holds for all elements that are not zeros of f, of which there are at least $p-s-2$ by assumption, so it holds for all elements of $\mathbb{F}_p$. The degree of F_1 is at most $s-1$ and has at least $s+1$ zeros, since it is zero whenever f is zero. Therefore $F_1 = 0$ and arguing as before $F_2 = \ldots = F_s = 0$, and we have shown that the dimension of $Ker(\psi_1)$ is zero, which is not the case. □

Lemma 2.3. *If f has more than $s+2$ distinct zeros then it has at least $I(f)+3-t$ distinct zeros.*

Proof. Since f has more than $s+2$ distinct zeros, the image of ψ_1 contains no polynomials of degree less than $s+3$. Thus, by Lemma 2.1, the dimension of $Im(\psi_1) \leq (p-3)/2 - s - \epsilon$.

Therefore the dimension of $Ker(\psi_1)$ is at least $s(s+1)/2 - (p-3)/2 + s + \epsilon > 0$.

Again, let r be the number of distinct zeros of f, so $r \geq s+3$, and let

$$g(X) = (X^p - X)/((X^p - X), f(X)),$$

so the degree of g is $p - r$.

Define a linear map ϕ_2 from $Ker(\psi_1)$ to $\mathbb{F}_p[X]$ by

$$\phi_2((F_1, F_2, \ldots, F_s)) = F_1 + F_2 f + \ldots + F_s f^{s-1}.$$

Let $(F_1, F_2, \ldots, F_s) \in Ker(\psi_1)$. Since $F_1 f + F_2 f^2 + \ldots + F_s f^s = 0$ it follows that for all x such that $f(x) \neq 0$ we have $F_1 + F_2 f + \ldots + F_s f^{s-1} = 0$ and so there is a polynomial $k(X)$ with the property that

$$F_1 + F_2 f + \ldots + F_s f^{s-1} = g(X)k(X).$$

The degree of the left-hand side of this equality is at most $p - s - 3 - \epsilon$ so the degree of k is at most $r - s - 3 - \epsilon$. Thus, $dim\ Im(\phi_2) \leq r - s - 2 - \epsilon$ and therefore

$$dim\ Ker(\phi_2) \geq s(s+1)/2 - (p-3)/2 + s + \epsilon - (r - s - 2 - \epsilon).$$

Define recursively linear maps ϕ_j for $j = 3, 4, \ldots, s$, from the kernel of ϕ_{j-1} to $\mathbb{F}_p[X]$ by

$$\phi_j((F_1, F_2, \ldots, F_s)) = F_{j-1} + F_j f + \ldots + F_s f^{s-j+1}.$$

Let $(F_1, F_2, \ldots, F_s) \in Ker(\phi_{j-1})$. Then

$$F_{j-2} + F_{j-1} f + \ldots + F_s f^{s-j+2} = 0.$$

Every one of the r zeros of f is a zero of F_{j-2}, which has degree at most $s-j+2<r-1$. Thus $F_{j-2}=0$. Since $F_{j-1}f+F_jf^2+\ldots+F_sf^{s-j+2}=0$ it follows that for all x such that $f(x)\neq 0$ we have $F_{j-1}+F_jf+\ldots+F_sf^{s-j+1}=0$ and so there is a polynomial $k_j(X)$ with the property that

$$F_{j-1}+F_jf+\ldots+F_sf^{s-j+1}=g(X)k_j(X).$$

The degree of the left-hand side of this equality is at most $p-s-j-1-\epsilon$, so the degree of k_j is at most $r-s-j-1-\epsilon$. Thus, the dimension of $Im(\phi_j)\leq r-s-j-\epsilon$. Hence, for $j\leq r-s-1$, the dimension of the kernel of ϕ_j is at least

$$s(s+1)/2-(p-3)/2+s+\epsilon-[(r-s-2-\epsilon)+(r-s-3-\epsilon)+\ldots+(r-s-j-\epsilon)].$$

Let us suppose that $r\leq 2s+1$ and consider the above in the case $j=r-s-1$.

The dimension of the kernel of ϕ_{r-s-1} is at least

$$s(s+1)/2-(p-3)/2+s+\epsilon-(r-s-2-\epsilon)(r-s-1-\epsilon)/2.$$

Now if $(F_1,F_2,\ldots,F_s)\in Ker(\phi_{r-s-1})$ then $F_1=\ldots=F_{r-s-2}=0$ and

$$F_{r-s-1}+F_{r-s-2}f+\ldots+F_sf^{2s-r+1}=g(X)k_{r-s}(X).$$

The degree of the left-hand side of this equality is at most $p-r-1$, so $k_{r-s}=0$. Each of the r zeros of f is therefore a zero of F_{r-s-1}, which has degree at most $2s-r+1\leq r-5$. Thus $F_{r-s-1}=0$. Similarly $F_{r-s-2}=\ldots=F_s=0$ and so the kernel of ϕ_{r-s-1} is zero. Therefore

$$0\geq s(s+1)/2-(p-3)/2+s+\epsilon-(r-s-2-\epsilon)(r-s-1-\epsilon)/2.$$

If $r\leq 2s+3-t+\epsilon$ then this implies that

$$(p-1-2\epsilon)/t+(t-3)\geq 2s,$$

which it is not. □

The previous two lemmas have the following consequence. Recall that $\epsilon=0$ if $I(f)$ is odd and $\epsilon=1$ if $I(f)$ is even.

THEOREM 2.4. *If $I(f)>(p-1-2\epsilon)/t+t-2+\epsilon$ for some integer t then every line meets the graph of f in at least $I(f)+3-t>(p-1)/t+1$ points or at most $t-1$ points.*

Proof. The line $y=mx+c$ meets the graph of f, $\{(x,f(x))\mid x\in\mathbb{F}_p\}$, in the point (x,y), whenever $mx+c=f(x)$. Define $f_1(x)=f(x)-mx-c$. Since, for all $0<i+j<I(f)$ we have $\sum x^if(x)^j=0$ it follows that $\sum x^if_1(x)^j=0$. Thus $I(f_1)\geq I(f)$. Lemma 2.2 and Lemma 2.3 imply f_1 has at most $t-1$ zeros or at least $I(f)+3-t>(p-1)/t+1$ zeros. □

Note that if $f(x)=x^t$ and t divides $p+1$ then $I(f)=(p+1)/t+t-3$ so the bound is the more or less best possible for the short lines, assuming that for some p and t there will be a and b such that $x^t=ax+b$ has t solutions. And if $f(x)=x^{(p+1)/t}$ then again $I(f)=(p+1)/t+t-3$ and so the bound is also good for the long lines, assuming that for some p and t there will be a and b such that $x^{(p+1)/t}=ax+b$ has $(p+1)/t$ solutions.

The property that the graph of f is incident with at most $t-1$ points or more than $(p-1)/t+1$ points of a line indicates that the following conjecture may hold.

Conjecture 2.5. *If $I(f) > (p-1-2\epsilon)/t + t - 2 + \epsilon$ for some integer t then the graph of f is contained in an algebraic curve of degree $t-1$.*

To prove the conjecture it is sufficient to prove that the $Ker(\psi_{s-t+1})$, where ψ_{s-t+1} is as defined in the proof of Lemma 2.2, is not $\{0\}$. We shall prove the conjecture by other means for $t=2$ and $t=3$ in the following section.

We finish this section by proving Conjecture 2.5 under additional hypothesis.

Theorem 2.6. *If $I(f) > (p-1-2\epsilon)/t + t - 2 + \epsilon$ and there are $t-1$ lines incident with at least t points of the graph of f then the graph of f is contained in the union of these $t-1$ lines.*

Proof. After a suitable affine transformation we can assume that one of the $t-1$ lines, incident with at least t points of the graph of f, is the line $Y=0$ and that the lines $Y = m_i X + c_i$, $i = 1, 2, \ldots, t-2$, are the other $t-2$ lines incident with at least t points of the graph of f.

Recall that $I(f) = 2s + 1 + \epsilon$.

Let $V = \{(F_1, F_2, \ldots, F_{t-1}) \mid F_i^\circ \leq s - i\}$. The dimension of V is $(t-1)s - (t-1)(t-2)/2$ which is greater than $(p-3)/2 - \epsilon - s$, since by assumption $2st > p - 2\epsilon - 1 + t^2 - 3t$.

Define a linear map ψ from V to $\mathbb{F}_p[X]$ by

$$\psi((F_1, F_2, \ldots, F_{t-1})) = F_1 f + F_2 f^2 + \ldots F_{t-1} f^{t-1}.$$

Since $I(f) > 2s$ the product of any two polynomials in the image of ψ cannot have degree $p-1$. The maximum degree of any polynomial in the image of ψ is $p - s - 2 - \epsilon$, so only half of the numbers in the interval $[s+1+\epsilon, \ldots, p-s-2-\epsilon]$ can occur amongst the degrees of polynomials in the image of ψ. Thus at most $(p-3)/2 - s - \epsilon$, which is less than the dimension of V. Hence in the image of ψ there is a polynomial of degree at most $s + \epsilon$ or ψ has a non-trivial kernel.

The line $Y=0$ is incident with at least t points of the graph of f and so by Theorem 2.4 it is incident with at least $I(f) + 3 - t$ points of the graph of f. Therefore f has at least $I(f)+3-t$ distinct zeros and any polynomial in the image of ψ has the zeros of f amongst its zeros and so must have degree at least $I(f) + 3 - t$. Since this number is larger than $s + \epsilon$ we conclude that ψ has a non-trivial kernel.

Let $(F_1, F_2, \ldots, F_{t-1}) \in V$ be such that

$$\sum_{j=1}^{t-1} F_j f^j = 0. \tag{2.1}$$

For all $i = 1, \ldots, t-2$ we have that the line $Y = m_i X + c_i$ is incident with t, and hence by Theorem 2.4, at least $I(f) + 3 - t$ points of the graph of f. Therefore, there are at least $I(f) + 3 - t$ solutions to the equation

$$\sum_{j=1}^{t-1} F_j (m_i X + c_i)^j = 0. \tag{2.2}$$

However, this equation has degree at most s and so is an identity. These $t-2$ equations are linear and homogeneous in the F_j and will have a unique solution up to a scalar factor whenever the determinant

$$\begin{vmatrix} m_1X+c_1 & \cdot\ \cdot\ \cdot & (m_1X+c_1)^{t-2} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ m_{t-2}X+c_{t-2} & \cdot\ \cdot\ \cdot & (m_{t-2}X+c_{t-2})^{t-2} \end{vmatrix}$$

is non-zero. This determinant is the determinant of a Vandermonde matrix, which is non-zero since the lines are distinct.

Now we only have to find a solution of these equations and this is easily done. Define polynomials σ_j in X of degree at most j by

$$\prod_{i=1}^{t-2}(Y-m_iX-c_i)=\sum_{j=0}^{t-2}\sigma_{t-2-j}Y^j.$$

For all $i=1,\ldots,t-2$ we have

$$\sum_{j=0}^{t-2}\sigma_{t-2-j}(m_iX+c_i)^j=0.$$

Putting $F_j=\sigma_{t-1-j}F_{t-1}$ in Equation 2.2 we get

$$F_{t-1}\sum_{j=1}^{t-1}\sigma_{t-1-j}(m_iX+c_i)^j=(m_iX+c_i)F_{t-1}\sum_{j=0}^{t-2}\sigma_{t-2-j}(m_iX+c_i)^j=0.$$

Substituting the solution into Equation 2.1 we have

$$F_{t-1}\sum_{j=1}^{t-1}\sigma_{t-1-j}f^j=0.$$

For every $x\in\mathbb{F}_p$ that is not a zero of F_{t-1}

$$\sum_{j=1}^{t-1}\sigma_{t-1-j}f^j=0.$$

This equation has degree at most $p-2s+t$ and has at least $p-(s-t+1)$ solutions and so is an identity. Thus for all $x\in\mathbb{F}_p$

$$0=f\sum_{j=0}^{t-2}\sigma_{t-2-j}f^j=f\prod_{i=1}^{t-2}(f-m_ix-c_i).$$

$\square$

3. Classification of functions for which $I(f)$ is more than $(p+5)/3$ and consequences for functions determining few directions

Firstly we note that we have proved what Lovász and Schrijver proved in [7], with no restriction on $M(f)$.

Theorem 3.1. *If $I(f) \geq (p+1)/2$ then f is linear.*

Proof. This is an immediate corollary of Theorem 2.4 with $t = 2$. □

Since $I(f) \geq M(f) + 1$ it follows that if $M(f) \geq (p-1)/2$ then f is linear.

The theorem itself holds for all finite fields $\mathbb{F}_q$, that is if $I(f) \geq (q+1)/2$ then f is linear, although there do not seem to be any geometric applications in the case q is not a prime.

Now we shall prove a generalised version of the main theorem in [5], where the hypothesis on f was $M(f) \geq (p+2)/3$. This was weakened slightly in [2], where the hypothesis on f was $I(f) \geq (p+5)/3$ and $M(f) \geq (p-1)/6$. In both cases the conclusion was that the graph of f is contained in the union of two lines. Here we have no hypothesis on $M(f)$ which allows the possibility that $f(X)$ is of degree 2, so our conclusion is slightly weaker.

Theorem 3.2. *If $I(f) \geq (p+5)/3$ then the graph of f is contained in an algebraic curve of degree 2.*

Proof. Since $(p+5)/3 > (p-1-2\epsilon)/3 + 1 + \epsilon = (p+2+\epsilon)/3$, Theorem 2.4 implies that there is a line incident with at least $(p+5)/3$ points of the graph of f or every line is incident with at most 2 points of the graph of f. In the latter case, Segre's theorem [8] implies that the graph of f is contained in an algebraic curve of degree 2.

Thus we can assume that there is a line meeting the graph of f in at least $(p+5)/3$ points and after making a suitable affine transformation we can assume that this is the line $y = 0$. In other words f has at least $(p+5)/3$ distinct zeros.

Recall that $I(f) = 2s + 1 + \epsilon$, so $2s \geq (p-1)/3 - \epsilon$. By Theorem 3.1 we can assume that $s < p/4$.

Let V be a vector space of pairs of polynomials of dimension $2s-1$ defined by $V = \{(A, B) \mid A^\circ \leq s-1, B^\circ \leq s-2\}$. Define a linear map ϕ from V to $\mathbb{F}_p[X]$ by

$$\phi((A, B)) = Af + Bf^2.$$

The maximum degree of any polynomial in the image of ϕ is $p-s-2$. Arguing as in the previous lemmas, only half of the degrees in the range $[s+1+\epsilon, \ldots, p-s-2-\epsilon]$ can occur amongst the polynomials in the image of ϕ. Since $(p-2s-3)/2 - \epsilon \leq (4s+\epsilon-5)/2 \leq 2s-2 \leq dim(V)$, the image of ϕ contains a polynomial of degree at most s or ϕ has a non-trivial kernel.

Any polynomial g in the image of ϕ has at least $(p+5)/3$ zeros, since any zero of f is a zero of g. However, $(p+5)/3 > s$, so we can conclude that ϕ has a non-trivial kernel.

Let A and B be such that

$$Af + Bf^2 = 0.$$

By removing any common factors, if necessary, we can assume $(A, B) = 1$. This equation has degree at most $p-s-2$ and it holds for all $x \in \mathbb{F}_p$, so it is an identity. Thus A divides

f^2 and B divides f. Moreover A and B have no common factors so f/B has the same zeros as f^2, and since f^2 has the same zeros as f, f/B has the same zeros as f. Since B divides f, the zeros of B are zeros of f and so the zeros of B are zeros of f/B.

Multiplying by Bf and rearranging we see that

$$B^2 f^3 = A^2 f$$

for all $x \in \mathbb{F}_p$, and so

$$Bf^3 = A^2(f/B),$$

for all $x \in \mathbb{F}_p$, such that $B(x) \neq 0$. If x is a zero of B then the left-hand side of this equation is zero and the right hand side is also zero since any zero of B is a zero of f/B. This equation holds for all $x \in \mathbb{F}_p$, it has degree less than p, and so is an identity.

Thus A^2 divides f^3 and B^2 divides f. Again, since A and B have no common factors f/B^2 has the same zeros as f^3, and since f^3 has the same zeros as f, f/B^2 has the same zeros as f. Therefore the zeros of B are zeros of f/B^2.

Repeating the above argument we conclude that

$$Bf^{i+1} = A^i(f/B^{i-1}),$$

for all $i = 1, 2, \ldots$, so long as the degree of this equation is less than p, in other words whenever $B^\circ + (f^{i+1})^\circ \leq p-1$, which is certainly whenever $i \leq s+2$. Thus B^{s+2} divides f, so the degree of B is at most 3. Now we can conclude that $B^\circ + (f^{i+1})^\circ \leq p-1$ whenever $i \leq 2s-3$. Thus B^{2s-3} divides f. The polynomial f/B^{2s-3} has at least $(p+5)/3$ zeros, so $B^\circ \leq 1$ and the equation is an identity for $i = 2s-1$. Now we can conclude that B^{2s-1} divides f and the polynomial f/B^{2s-1} has at least $(p+5)/3$ zeros, which implies $f^\circ - (2s-1)B^\circ \geq (p+5)/3$ which in turn implies $(2s-1)B^\circ \leq 2s-2$ and so B is constant. Now A^{2s-1} divides f^{2s} and the quotient has at least $(p+5)/3$ zeros. Hence $p-2-(2s-1)A^\circ \geq (p+5)/3$, which gives $A^\circ \leq 1$.

The graph of f is contained in the algebraic curve

$$A(X)Y + B(X)Y^2 = 0,$$

which is of degree two. $\square$

Corollary 3.3. *If $M(f) \geq (p+2)/3$ then the graph of f is contained in the union of two lines.*

Proof. Since $I(f) \geq M(f)+1$, by Theorem 3.2 the graph of f is contained in an algebraic curve of degree two. If this curve is irreducible then f determines every direction, since

$$((y^2 + ay + b) - (x^2 + ax + b))/(y - x) = x + y + a.$$

If not then after a suitable affine transformation there exsits a linear polynomial $A(X) = aX + b$ and a constant polynomial $B(X) = c$ such that

$$f(x)(ax + b + cf(x)) = 0,$$

for all $x \in \mathbb{F}_p$. $\square$

We can also prove Corollary 3.3 as a corollary to Theorem 2.4.

Proof. Since $I(f) \geq M(f)+1$ Theorem 2.4 implies that every line meets the graph of f in at least $(p+5)/3$ points or at most 2 points. If a point of the graph of f is incident only with lines incident with at most 2 points of the graph of f, then $M(f) \leq 1$. Therefore, every point of the graph of f is incident with a line which is incident with at least $(p+5)/3$ points of the graph of f. The graph of f is a set of p points and so is contained in the union of two such lines. □

In the article [9] T. Szőnyi proves that if $M(f) \geq 2$ and the graph of f is contained in the union of two lines then f is affinely equivalent to a generalized example of Megyesi, which is constructed using cosets of the multiplicative group. For more details of this construction see [9] or [5].

In the article [3] A. Biró proves that if the graph of f is contained in the union of two lines then $I(f) = p-1$ or $I(f) = (p-1)/3$ or $I(f) \leq (p-1)/4$ and classifies all examples when $I(f) = p-1$, $I(f) = (p-1)/3$ or $I(f) = (p-1)/4$.

If the graph of f is contained in an irreducible curve of degree 2 then f is of degree two and $I(f) = (p-1)/2$.

We are unaware of any results concerning $I(f)$ (or $M(f)$) obtained under the assumption that the graph of f is contained in an algebraic curve of degree three.

4. Acknowledgement

The authors wish to thank Péter Sziklai for his astute observations that led to many improvements on earlier versions of this article.

References

[1] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory Ser. A*, **104** (2003) 341–350.

[2] S. Ball, A. Gács and P. Sziklai, On linear combinations of permutation polynomials that are permutation polynomials, *J. Combin. Theory Ser. A.*, to appear.

[3] A. Biró, On polynomials over prime fields taking only two values on the multiplicative group, *Finite Fields Appl.*, **6** (2000) 302–308.

[4] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes of the graph of a function defined over a finite field, *J. Combin. Theory Ser. A*, **86** (1999) 187–196.

[5] A. Gács, On a generalization of Rédei's theorem, *Combinatorica*, **23** (2003) 585–598.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, Second Edition, Cambridge University Press, 1997.

[7] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981) 449–454.

[8] B. Segre, Ovals in a finite projective plane, *Canad. J. Math.*, **7** (1955) 414–416.

[9] T. Szőnyi, Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica*, **19** (1991) 197–212.

[10] D. Wan, G. L. Mullen and P. J.-S. Shiue, The number of permutation polynomials of the form $f(x) + c(x)$ over a finite field, *Proc. Edinburgh Math. Soc*, **38** (1995) 133–149.

Simeon Ball
Departament de Matemàtica Aplicada IV,
Universitat Politècnica de Catalunya, Jordi Girona 1-3, Mòdul C3, Campus Nord,
08034 Barcelona, Spain
simeon@mat.upc.es

András Gács
Eötvös University Budapest,
Pázmány P. sétány 1/c,
Budapest, Hungary H-1117
gacs@cs.elte.hu