ON LINEAR COMBINATIONS OF PERMUTATION POLYNOMIALS THAT ARE PERMUTATION POLYNOMIALS

SIMEON BALL, ANDRÁS GÁCS, AND PETER SZIKLAI

ABSTRACT. Let p be a prime and let $f, g \in \mathbb{F}_p[x]$. We prove that if there are more than $(2\lceil\frac{p-1}{6}\rceil+1)(p+2\lceil\frac{p-1}{6}\rceil)/2 \approx 2p^2/9$ pairs $(a,b) \in \mathbb{F}_p^2$ with the property that the mapping $x \mapsto f(x)+ag(x)+bx$ is a permutation of $\mathbb{F}_p$, then there exist elements $c, d, e \in \mathbb{F}_p$ such that $f(x) = cg(x)+dx+e$. We also provide an example, when $p = 1 \bmod 3$, of functions f and g for which there are $2(p-1)^2/9-1$ pairs (a,b) with the property that the mapping $x \mapsto f(x)+ag(x)+bx$ is a permutation of $\mathbb{F}_p$, and there do not exist elements $c, d, e \in \mathbb{F}_p$ with the property that $f(x) = cg(x)+dx+e$.

1. INTRODUCTION

Let p be a prime. We say that $f \in \mathbb{F}_p[x]$ is a *permutation polynomial* if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_p$, and by $M(f)$ we denote the number of elements $a \in \mathbb{F}_p$ for which $f(x)+ax$ is a permutation polynomial.

In [6] Rédei and Megyesi proved that if $M(f) \geq (p-1)/2$, then $f(x) = cx+d$ for some $c, d \in \mathbb{F}_p$; in other words, the graph of f,

$$\{(x, f(x)) \colon \ x \in \mathbb{F}_p\},$$

is a line.

In [6] Megyesi provided an example with $M(f) = d-1$, for each divisor d of $p-1$, which, when $d = (p-1)/2$, shows this bound to be best possible. Namely, let H be a multiplicative subgroup of $\mathbb{F}_p$, let χ_H be the characteristic function of H and let $f(x) = \chi_H(x)x$. If $d \neq 1, p-1$ then $M(f) = d-1$.

In [5] Lovász and Schrijver proved that if $M(f) = (p-1)/2$ then f is affinely equivalent to the example of Megyesi.

In [3] it is proved that if $M(f) \geq 2\lceil\frac{p-1}{6}\rceil+1$, then $(f(x)-(cx+d))(f(x)-(bx+e)) = 0$ for some $b, c, d, e \in \mathbb{F}_p$; in other words, the graph of f is contained in the union of two lines.

In [8] Szőnyi proved that if the graph of f is contained in the union of two lines and $M(f) \geq 2$, then the graph of f is affinely equivalent to a generalised example of Megyesi detailed above. In the generalised Megyesi example H can be replaced by a union of

Date: 14 November 2006.

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 Ministerio de Ciencia y Tecnologia, España. The second and third authors were supported by OTKA grants T 043758, T 049662 and F 043772, TÉT grant E-16/04 and Bolyai scholarship.

cosets of a multiplicative subgroup of $\mathbb{F}_p$. In the generalised example the value of $M(f)$ is again $d-1$ for some divisor d of $p-1$.

Thus, the above results imply that, either $M(f) \leq 2\lceil \frac{p-1}{6} \rceil$, f is affinely equivalent to $x^{\frac{p+1}{2}}$, or f is linear.

In this article we shall prove that if there are more than $(2\lceil \frac{p-1}{6} \rceil + 1)(p + 2\lceil \frac{p-1}{6} \rceil)/2 \approx 2p^2/9$ pairs $(c,d) \in \mathbb{F}_p^2$ with the property that $x \mapsto f(x) + cg(x) + dx$ is a permutation of $\mathbb{F}_p$ then there are elements $a, b, e \in \mathbb{F}_p$ such that $f(x) + ag(x) + bx + e = 0$, for all $x \in \mathbb{F}_p$; in other words the graph of (f,g), $\{(x, f(x), g(x)) \mid x \in \mathbb{F}_p\}$, is contained in a plane.

There is a connection with the directions determined by a function $f(x)$ and the elements c with the property that $f(x)+cx$ is a permutation polynomial. Namely, the set of parallel lines defined by the equation $cX_1 + X_2 = a$, where a runs through the elements of $\mathbb{F}_p$, all contain exactly one point of the graph of f if and only if $f(x) + cx$ is a permutation polynomial. Thus the direction of these lines is not a direction determined by f. The same analogy holds in three dimensions. The set of parallel planes defined by the equation $dX_1 + X_2 + cX_3 = a$, where a runs through the elements of $\mathbb{F}_p$, all contain exactly one point of the graph of (f,g) if and only if $f(x) + cg(x) + dx$ is a permutation polynomial.

Although in this article we shall only consider fields of prime order, for all prime powers q it has been proved, in [2] and [1] (for small characteristics and a shorter proof), that if $M(f) \geq (q-1)/2$ then f is linear over some subfield $\mathbb{F}_s$ of $\mathbb{F}_q$, and if $s < q$ then $q - (q-1)/(s-1) \leq M(f) \leq q - q/s - 1$.

2. A slight improvement on [3]

Let

$$I(f) = \min\{k + l \mid \sum_{x \in \mathbb{F}_p} x^k f(x)^l \neq 0\}.$$

In [3] it was proved that if $M(f) > (p-1)/4$ and $I(f) \geq 2\lceil \frac{p-1}{6} \rceil + 2$ then the graph of f is contained in the union of two lines.

Let

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

It's a simple matter to check, see [4, Lemma 7.3], that if $x \mapsto f(x) + ax$ is a permutation then $\pi_k(a) = 0$ for all $0 < k < p-1$. Since the polynomial $\pi_k(Y)$ has degree at most $k-1$ (the coefficient of Y^k is $\sum_{x \in \mathbb{F}_p} x^k = 0$) it is identically zero for all $0 \leq k-1 < M(f)$, unless $M(f) = p-1$ in which case f is linear. Hence if f is not linear then $I(f) - 1 \geq M(f)$.

Thus in [3] it was proved that if $M(f) \geq 2\lceil \frac{p-1}{6} \rceil + 1$, then the graph of f is contained in the union of two lines.

To be able to prove the main result of this article we need something a little stronger than [3]. We use the same method and essentially follow the proof there but we have to modify the first part of the proof (Lemma 4.1), we manage to avoid the step involving Lemma 4.2, *Step 1* and *Step 2* are the same, we use a slightly different subspace to be able to reduce *Step 3* and *Step 4* a little and *Step 5* we use in the same way.

In this section we shall prove the following theorem.

THEOREM 2.1. *If $M(f) \geq (p-1)/6$ and $I(f) \geq 2\lceil \frac{p-1}{6} \rceil + 2$ then the graph of f is contained in the union of two lines.*

The values $I(f)$ and $M(f)$ are invariant under affine transformations and inversion. Replacing f by its inverse is the transformation which switches coordinates, in other words if we switch coordinates then the graph of f, $\{(x, f(x)) \mid x \in \mathbb{F}_p\}$, becomes the graph of f^{-1}. Let $E(f)$ denote the set of all polynomials that can be obtained from f by applying affine transformations and inversions.

Let $(f^i)^\circ$ be the degree of the polynomial f^i modulo $x^p - x$. Unless stated otherwise all equations are to be read modulo $x^p - x$.

Note that for any polynomial g of degree less than p the sum

$$-\sum_{x \in \mathbb{F}_p} g(x)$$

is equal to the coefficient of x^{p-1} of g.

LEMMA 2.2. *If $3 \leq f^\circ \leq (p-1)/2$ then $I(f) \leq (p+1)/3$.*

Proof. Write $p - 1 = af^\circ + b$ with $0 \leq b < f^\circ$. The degree of $f(x)^a x^b$ is $p - 1$, so we have $I(f) \leq a + b$.

If $f^\circ = 3$ then $a + b \leq (p-2)/3 + 1 = (p+1)/3$.

If $(p+1)/3 \leq f^\circ \leq (p-1)/2$ then $a + b = 2 + p - 1 - 2f^\circ \leq (p+1)/3$.

If $(p+1)/4 \leq f^\circ \leq (p-1)/3$ then $a + b = 3 + p - 1 - 3f^\circ \leq 3 + p - 1 - 3(p+1)/4 = (p+1)/4 + 1 \leq (p+1)/3$ for $p \geq 11$.

If $4 \leq f^\circ \leq (p+1)/4$ then $a+b \leq (p-b-1)/f^\circ + b \leq p/f^\circ + (bf^\circ - b - 1)/f^\circ \leq p/f^\circ + f^\circ - 2$. This is at most $(p+1)/3$ if and only if the quadratic inequality $3(f^\circ)^2 - (p+7)f^\circ + 3p \leq 0$ is satisfied. For $p \geq 20$, the inequality is satisfied for both $f^\circ = 4$ and $f^\circ = (p+1)/4$, so it holds for all values between 4 and $(p+1)/4$. For $p < 20$ a case by case analysis suffices to show that $a + b \leq (p+1)/3$. □

Note that for $f^\circ = 2$ we have $I(f) = (p-1)/2$ and $M(f) = 0$ and for $f^\circ = 1$ we have $I(f) = p - 1$ and $M(f) = p - 1$.

LEMMA 2.3. *If $f^\circ = (p+1)/2$ then either $I(f) \leq (p+5)/4$ or f is affinely equivalent to $x^{\frac{p+1}{2}}$.*

Proof. After applying a suitable affine transformation we can suppose that $f(x) = x^{\frac{p+1}{2}} + g(x)$ where $g^\circ \leq (p-3)/2$.

If $g^\circ \leq 1$ then by applying another linear transformation we can subtract g from f and hence f is affinely equivalent to $x^{\frac{p+1}{2}}$.

Suppose $g^\circ \geq 2$. Write $(p-3)/2 = ag^\circ + b$ with $0 \leq b < g^\circ$ and consider the polynomial

$$f(x)^{a+1} x^b = \sum_{i=0}^{a+1} \binom{a+1}{i} x^{i\frac{p+1}{2}+b} g(x)^{a+1-i}.$$

We claim that the only term in the sum that has a term of degree x^{p-1} (modulo $x^p - x$) is $g(x)^a x^{\frac{p+1}{2}+b}$. Let $r(x) = g(x)^{a+1-i} x^{i\frac{p+1}{2}+b}$ (modulo $x^p - x$), a typical term in the sum (note that all the binomial coefficients are non-zero). If i is even then $r(x) = g(x)^{a+1-i} x^{b+i}$, which has degree $(a+1-i)g^\circ + b + i = (p-3)/2 + g^\circ - (g^\circ - 1)i < p-1$. If $i \neq 1$ is odd then $r(x) = g(x)^{a+1-i} x^{\frac{p-1}{2}+i+b}$, which has degree $(a+1-i)g^\circ + (p-1)/2 + i + b = p - 2 + g^\circ - (g^\circ - 1)i < p-1$.

Hence $f(x)^{a+1}x^b$ has degree $p-1$ which implies $I(f) \leq a+1+b$.

Finally, note that $a + b \leq (p-3)/(2g^\circ) + g^\circ - 1$, which is at most $(p+1)/4$ if $2 \leq g^\circ \leq (p-3)/4$. If $g^\circ > (p-3)/4$ then $a = 1$ and $b = (p-3)/2 - g^\circ < (p-3)/4$ and so $a + b < (p+1)/4$. □

Let $s = \lceil (p-1)/6 \rceil$.

We will assume from now on that $I(f) \geq 2s+2$. By the definition of $I(f)$ the sum

$$\sum_{x \in \mathbb{F}_p} x^k f(x)$$

has no term of degree x^{p-1}, for all $k = 0, 1, \ldots, 2s$, and therefore the degree of f is at most $p - 2s - 2$. By Lemma 2.2 and Lemma 2.3 the degree of f is at least $(p+3)/2$.

LEMMA 2.4. *There is polynomial in $h \in E(f)$ with one of the following properties. Either*

(i) *for all i such that $1 \leq i \leq 2s$, $(h^i)^\circ \leq h^\circ + i - 1$ and $(h^2)^\circ = h^\circ + 1$, or*
(ii) *for all i such that $1 \leq i \leq 2s$, $(h^i)^\circ \leq (h^2)^\circ + i - 2$ and $(h^3)^\circ = (h^2)^\circ + 1$,*

and h has no root in $\mathbb{F}_p$.

Proof. Let

$$d(f) = \max\{(f^i)^\circ - i \mid 1 \leq i \leq 2s\}$$

and let $d = d(f_1)$ be maximal over all polynomials in $E(f)$. The fact that $f^\circ \geq (p+3)/2$ implies that $d \geq (p+1)/2$.

Let $\pi(Y) = \pi_{p-1-d}(Y)$. The coefficient of $Y^{p-1-d-j}$ in $\pi(Y)$ is $\binom{p-1-d}{j} \sum_{x \in \mathbb{F}_p} x^{p-1-d-j} f^j$ which, by the definition of d, is non-zero for at least one j where $1 \leq j \leq 2s$. Hence $\pi(Y) \not\equiv 0$.

If for all a such that $f(x) + ax$ is a permutation polynomial we have $\pi(a) = \pi'(a) = \pi''(a) = 0$ then $(Y-a)^3$ divides $\pi(Y)$ and since $M(f) \geq (p-1)/6$ the degree of π, $\pi^\circ = p - 1 - d \geq 3M(f) \geq (p-1)/2$ which isn't the case.

Since $0 < p - 1 - d < p - 1$ we have already seen that $\pi(a) = 0$, so either $\pi'(a) \neq 0$ or $\pi''(a) \neq 0$ for some a.

Let f_2 be the inverse of the function $f(x) + ax$.

If

$$0 \neq \pi'(a) = -(d+1) \sum_{x \in \mathbb{F}_p} x(f + ax)^{p-2-d}$$

then $\sum_{z\in\mathbb{F}_p} f_2(z)z^{p-2-d} \neq 0$ and so $f_2^\circ \geq d+1$. By the maximality of d, $f_2^\circ = d+1$ and so $(f_2^i)^\circ - i \leq f_2^\circ - 1$. If $(f_2^2)^\circ \leq f_2^\circ$ then let $f_3 = f_2 + cx$ where c is chosen so that $(f_3^2)^\circ \geq f_3^\circ + 1$ and f_3 is not a permutation polynomial. Note that $f_3^2 = f_2^2 + 2cxf_2 + c^2x^2$. If

$$0 \neq \pi''(a) = (d+1)(d+2)\sum_{x\in\mathbb{F}_p} x^2(f+ax)^{p-3-d}$$

then $\sum_{z\in\mathbb{F}_p}(f_2(z))^2 z^{p-3-d} \neq 0$ and so $(f_2^2)^\circ \geq d+2$. By the maximality of d, $(f_2^2)^\circ = d+2$ and so $(f_2^i)^\circ - i \leq (f_2^2)^\circ - 2$. If $(f_2^3)^\circ \leq (f_2^2)^\circ$ then let $f_3 = f_2 + cx$ where c is chosen so that $(f_3^3)^\circ \geq (f_3^2)^\circ + 1$ and f_3 is not a permutation polynomial.

Finally, let e be an element not in the image of f_3 and let $f_4 = f_3 - e$. Then f_4 has no root in $\mathbb{F}_p$. □

The dimension of a subspace of a finite dimensional vector space of polynomials is equal to the number of degrees occurring amongst the elements of a subspace. This is easily seen if we take the canonical basis $\{1, x, x^2, \ldots, x^t\}$. The matrix whose rows form a basis for the subspace can be reduced to a matrix in row echelon form whose rows span the same subspace and correspond to polynomials of different degrees.

LEMMA 2.5. *There is a polynomial in $h \in E(f)$ for which there exist polynomials F, G and H, where $H^\circ - 2 = F^\circ - 1 = G^\circ = r \leq s-2$, $(F,G) = 1$ and*

$$Fh + Gh^2 = H.$$

Note that this implies that h satisfies the conditions of Lemma 2.4 (i).

Proof. Let h be a polynomial satisfying the conditions of Lemma 2.4. Since $I(h) \geq 2s+2$ we have $(h^i)^\circ \leq p - 2s - 3 + i$.

Define subspaces of the vector space of polynomials of maximum degree $p-1$

$$\psi_j = \{Fh + Gh^2 \mid F^\circ \leq j,\ G^\circ \leq j-1\},$$

where $j \leq s-1$. If there are polynomials F and G such that $Fh + Gh^2 = 0$ then since h has no root $F + Gh = 0$ which is impossible since $(hG)^\circ$ is at least $3s$ and at most $5s - 3 < p - 1$. Thus the dimension of ψ_j is $2j+1$.

Since $I(h) \geq 2s+1$ and $2(j+1) \leq 2s$, the sum over $\mathbb{F}_p$ of the evaluation of the product of any two elements of ψ_j is zero, hence the sum of the degrees of any two elements of ψ_{s-1} is not equal to $p-1$. The maximum degree of any element of ψ_{s-1} is $p-s-3$ and so only half of the degrees in the interval $[s+2, \ldots, p-1-(s+2)]$ can occur. But $\dim\psi_{s-1} = 2s-1 > (p-1-(s+2)-(s+1))/2$ and so there is an element H of degree at most $s+1$ in ψ_{s-1}.

Let H be of minimal degree, so $(F,G) = 1$.

If h satisfies case (i) of Lemma 2.4 then $(h^2)^\circ = h^\circ + 1$ and $r = G^\circ = F^\circ - 1$. Moreover $Fh^2 + Gh^3 = Hh$ and $(h^3)^\circ \leq h^\circ + 2$ implies $H^\circ \leq r+2$.

If h satisfies case (ii) of Lemma 2.4 then $(h^3)^\circ = (h^2)^\circ + 1 \geq h^\circ + 2$ and $(h^4)^\circ \leq (h^2)^\circ + 2$. Let $F^\circ = r+1$ and so $G^\circ \leq r$. The equation $Fh^3 + Gh^4 = Hh^2$ implies $H^\circ \leq r+2$. If

$G^\circ \le r-1$ then $Fh^2+Gh^3=Hh$ implies $r+2+h^\circ \ge H^\circ+h^\circ = r+1+(h^2)^\circ$ and so $(h^2)^\circ = h^\circ+1$. But then $Fh+Gh^2=H$ implies $G^\circ = r$.

Either way we have $r = G^\circ = F^\circ - 1 \ge H^\circ - 2$.

Let $h_1 = h+ax$ and $F_1 = F-2axG$, $G_1 = G$ and $H_1 = H - a^2x^2G + axF$. Then $F_1h_1+G_1h_1^2 = H_1$ and we can choose a so that H_1 has degree $r+2$. Now when we look at ψ_{r+1} for h_1 we find F_1, G_1 and H_1 as required. Note that $(F,G)=1$ implies $(F_1,G_1)=1$.

□

We wish to prove $r=0$. So let us assume $r \ge 1$ and define i to be such that $(i-2)r+1 \le s < (i-1)r+1$ for $r \ge 2$ and $i=s$ for $r=1$. Note that $r \le s-2$ implies $i \ge 3$ and that $s+r-1 \le 2s-i$ if $i=3$ or $i=s$ and also if both $i \ge 4$ and $r \ge 2$, since $r \le (s-1)/2$ and $i \le (s-1)/2$.

LEMMA 2.6. *There is a polynomial $h \in E(f)$ and a polynomial G, where $G^\circ = r \le s-2$, such that for all $j=2,\dots,i$, there is an F_j and an H_j with the property that $(F_j,G)=1$,*

$$F_jh + G^{j-1}h^j = H_j,$$

$F_j^\circ \le (j-1)(r+1)$, $H_j^\circ \le (j-1)r+j$ and $H_i^\circ = (i-1)r+i$.

Proof. Let h_1 satisfy the conditions of Lemma 2.5. We start by proving that there is an $h \in E(f)$ for which $(h^{i-1})^\circ \ge h^\circ + i - 2$.

If $(h_1^{i-1})^\circ \le h_1^\circ + i - 3$ then let $h = h_1 + ax$. Choose a so that $h^{i-1} = \sum_{j=0}^{i-1} \binom{i-1}{j}(ax)^{i-j-1}h_1^j$ has degree at least $h^\circ+i-2$ while at the same time the degree of $F-2axG$ is $r+1$ and the degree of $H - a^2x^2G + axF$ is $r+2$.

We will prove the lemma by induction. Lemma 2.5 implies that for $j=2$ we can take $F_2 = F$ and $H_2 = H$.

Define $F_j = -(F_{j-1}F + H_{j-1}G)$ and $H_j = -HF_{j-1}$. It can be checked by induction, multiplying by Gh and using $Gh^2 = H - Fh$, that

$$F_jh + G^{j-1}h^j = H_j.$$

The degrees satisfy $F_j^\circ \le (j-1)(r+1)$ and $H_j^\circ \le (j-1)r+j$ and $(F_j,G)=1$, since $(F,G)=1$ by Lemma 2.5 and $(F_{j-1},G)=1$ by induction.

Now $(h^{i-1})^\circ \ge h^\circ + i - 2$ and the equation $F_{i-1}h + G^{i-2}h^{i-1} = H_{i-1}$ implies that $F_{i-1}^\circ \ge (i-2)(r+1)$ and so $F_{i-1}^\circ = (i-2)(r+1)$. Finally $H_i = -HF_{i-1}$ implies $H_i^\circ = (i-1)r+i$. □

Let h satisfy the conditions of Lemma 2.6. Note that this implies that h satisfies the conditions of Lemma 2.5 and Lemma 2.4 (i). Define

$$\phi_j = \{Ah + Bh^i \mid A^\circ \le j,\ B^\circ \le j+1-i\}.$$

Note that $H_i \in \phi_{(i-1)r+i-1}$ and that $(i-1)r+i-1 \le s+r+i-2 \le 2s-1$.

LEMMA 2.7. *For $j \le 2s-1$ all polynomials of ϕ_j have degree at least H_i° and those of degree at most $p-2-h^\circ$ are multiples of H_i.*

Proof. If $Ah + Bh^i = 0$ then, since h has no root in $\mathbb{F}_p$, $A + Bh^{i-1} = 0$. The degree of Bh^{i-1} is at most $p-4$ and at least $(p+3)/2$ and so $A = B = 0$. Thus the dimension of ϕ_j is $2j + 3 - i$.

Suppose that ϕ_j contains a polynomial C of degree n but no polynomial of degree $n+1$. Then ϕ_{j+1} contains a polynomial of degree $n+1$, xC for example, and a polynomial of degree one more than the maximum degree of an element of ϕ_j. However $\dim\phi_{j+1} = \dim\phi_j + 2$, so n is unique. Moreover, the polynomials of degree $n+1$ in ϕ_{j+1} are multiples of a polynomial of degree n in ϕ_j.

Since $j \leq 2s-1$, ϕ_j contains no element of degree $p-1-h^\circ$. Now $H_i \in \phi_{(i-1)r+i-1}$ and is a polynomial of degree less than $p-1-h^\circ$. It is not a multiple of any polynomial in ϕ_j for $j < (i-1)r+i-1$, since if it were there would be a non-constant polynomial K and polynomials A and B with the property that $(KA)h + (KB)h^i \in \phi_{(i-1)r+i-1}$, with $(KA)^\circ \leq (i-1)r+i-1$ and $(KB)^\circ \leq (i-1)r$, which would be a constant multiple of H_i. This is not possible since $(F_i, G) = 1$. Thus all polynomials in ϕ_j of degree at most $p-2-h^\circ$ are multiples of H_i and in particular have degree at least H_i°.

□

The following lemma contradicts the previous one which implies that our assumption that $r \geq 1$ was incorrect.

LEMMA 2.8. *There is a non-zero polynomial of degree less than H_i° in ϕ_j for some $j \leq 2s-2$.*

Proof. Suppose $r \geq 2$ and so $i \leq s$. Let

$$\Delta = \{Ah + B_2h^2 + \ldots + B_{i-1}h^{i-1} + Ch^i \mid A^\circ \leq s-1,\ B_j^\circ \leq r-1,\ C^\circ \leq s-i\}.$$

Since $I(h) \geq 2s+1$ the sum of the degrees of any two elements of Δ is not equal to $p-1$. The maximum degree of any element of Δ is $p-s-3$ and so only half of the degrees in the interval $[s+2, \ldots, p-1-(s+2)]$ can occur, in other words at most $\lfloor (p-4-2s)/2 \rfloor \leq 2s-2$ of the degrees in this interval occur. If $\dim\Delta = (i-2)r+2s-i+1$ then there is a polynomial

$$E = Ah + B_2h^2 + \ldots + B_{i-1}h^{i-1} + Ch^i$$

in Δ of degree at most $s+2-((i-2)r+2s-i+1-(2s-2)) = s-(i-2)r+i-1$. If $\dim\Delta < (i-2)r+2s-i+1$ then $E = 0 \in \Delta$ non-trivially. Either way there is a polynomial $E \in \Delta$ with not all A, B_j, C zero where $E^\circ \leq s-(i-2)r+i-1$.

Substituting $G^{j-1}h^j = H_j - hF_j$ we have

$$G^{i-2}E = G^{i-2}Ah + CG^{i-2}h^i + \sum_{j=2}^{i-1} B_jG^{i-1-j}(H_j - hF_j)$$

and rearranging

$$G^{i-2}E - \sum_{j=2}^{i-1} B_jG^{i-1-j}H_j = (G^{i-2}A - \sum_{j=2}^{i-1} B_jF_jG^{i-1-j})h + CG^{i-2}h^i.$$

Checking the degrees on the right-hand side we see that the left-hand side is a polynomial in ϕ_j for some $j \leq 2s-2$.

The degree of the left-hand side is at most $\max\{s+i-1, ir-r+i-2\}$ which is less than $H_i^\circ = (i-1)r+i$.

If $r=1$ then take $i=s$ and define Δ as above. There is a polynomial E in Δ of degree at most $s+1$ and the degree of $G^{i-2}E$ is at most $2s-1$ which is the degree of H_s. If we have equality then by Lemma 2.7 the polynomial

$$(G^{s-2}A - \sum_{j=2}^{s-1} B_j F_j G^{s-1-j})h + CG^{s-2}h^s$$

is a constant multiple of $F_s h + G^{s-1}h^s$ which implies CG^{s-2} is a constant multiple of G^{s-1} which it is not since one has degree $s-2$ and the other $s-1$.

□

We can now prove Theorem 2.1.

Proof. By the previous lemmas there exists polynomials $h \in E(f)$ and F of degree 1 and H of degree 2 such that $h^2+Fh = H$. Thus $(h+F/2)^2 = H+F^2/4$. All values of $H+F^2/4$ are squares and so $H+F^2/4 = (ax+b)^2$. Hence $(h+F/2-ax-b)(h+F/2+ax+b) = 0$ and the graph of h (and so the graph of f too) is contained in the union of two lines. □

3. Linear combinations of three permutation polynomials

In this section we will need the following theorem which can de deduced from [7, Theorem 0.1].

Theorem 3.1. *Let $\pi(Y,Z)$ be an absolutely irreducible polynomial of degree d with coefficients in $\mathbb{F}_p$ such that $1 < d < p$. The number of solutions N to the equation $\pi(y,z) = 0$ in $\mathbb{F}_p^2$ satisfies*

$$N \leq d(d+p-1)/2.$$

Let $M(f,g)$ be the number of pairs $(a,b) \in \mathbb{F}_p^2$ for which $f(x)+ag(x)+bx$ is a permutation polynomial. Let

$$I(f,g) = \min\{k+l+m \mid \sum_{x\in\mathbb{F}_p} x^k f(x)^l g(x)^m \neq 0\}.$$

Recall $s = \lceil \frac{p-1}{6} \rceil$. Before we prove the main result of this section we need the following lemma

Lemma 3.2. *If $M(f,g) > (2s+1)(p+2s)/2$ then $I(f,g) \geq 2s+2$ or there are elements $c,d,e \in \mathbb{F}_p$ such that $f(x)+cg(x)+dx+e = 0$ for all $x \in \mathbb{F}_p$.*

Proof. Let $\pi_k(Y,Z) = \sum_{x\in\mathbb{F}_p}(f(x)+g(x)Y+xZ)^k$.

By [4, Lemma 7.3], if $f(x)+ag(x)+bx$ is a permutation polynomial then $\pi_k(a,b) = 0$ for all $0 < k < p-1$. Write

$$\pi_k = \prod \sigma_j(Y,Z),$$

where each σ_j is absolutely irreducible. Then $\sum \sigma_j^\circ = \pi_k^\circ \leq k$.

Let N_j be the number of solutions of $\sigma_j(a,b)=0$ in $\mathbb{F}_p$ for which $f(x)+ag(x)+bx$ is a permutation polynomial.

If $\lambda\sigma_j \in \mathbb{F}_p[Y,Z]$, for some λ in an extension of $\mathbb{F}_p$, and $\sigma_j^\circ \geq 2$ then by Theorem 3.1 $N_j \leq \sigma_j^\circ(p+\sigma_j^\circ-1)/2$.

Suppose $\sigma_j^\circ = 1$ and there are at least $(p+1)/2$ pairs (a,b) for which $\sigma_j(a,b)=0$ and $f(x)+ag(x)+bx$ is a permutation polynomial. Let $\sigma_j = \alpha Y+\beta Z+\gamma$. If $\alpha \neq 0$ then there are $(p+1)/2$ elements $b\in\mathbb{F}_p$ with the property that $\alpha f(x)-(\beta b+\gamma)g(x)+b\alpha x = \alpha f(x)-\gamma g(x)+b(\alpha x-\beta)$ is a permutation polynomial. By Rédei and Megyesi's theorem mentioned in the introduction, this implies that $\alpha f(x)-\gamma g(x)$ is linear and hence there are elements $c,d,e\in\mathbb{F}_p$ such that $f(x)+cg(x)+dx+e=0$ for all $x\in\mathbb{F}_p$. If $\alpha=0$ then there are $(p+1)/2$ elements $a\in\mathbb{F}_p$ with the property that $\beta f(x)-\gamma x+a\beta g(x)$ is a permutation polynomial. The set of p points $\{(\beta f(x)-\gamma x, \beta g(x)) \mid x\in\mathbb{F}_p\}$ may not be the graph of a function but it is a set of p points that does not determine at least $(p+1)/2$ directions. Thus it is affinely equivalent to a graph of a function that does not determine at least $(p-1)/2$ directions and so by Rédei and Megyesi's theorem, it is a line. Hence, there are elements c, d and e with the property that $c(\beta f(x)-\gamma x)+d\beta g(x)+e=0$ for all $x\in\mathbb{F}_p$. Thus, either there are elements $c,d,e\in\mathbb{F}_p$ such that $f(x)+cg(x)+dx+e=0$ for all $x\in\mathbb{F}_p$ or $N_j\leq(p-1)/2$.

Suppose $\lambda\sigma_j \notin \mathbb{F}_p[Y,Z]$ for any λ in any extension of $\mathbb{F}_p$. The polynomials $\sigma_j = \sum \alpha_{nm}Y^nZ^m$ and $\hat{\sigma}_j = \sum \alpha_{nm}^p Y^nZ^m$ have at most $(\sigma_j^\circ)^2$ zeros in common by Bezout's theorem. However if $(y,z)\in\mathbb{F}_p^2$ and $\sigma_j(y,z)=0$ then $\hat{\sigma}_j(y,z)=0$. Hence

$$N_j \leq (\sigma_j^\circ)^2 \leq \sigma_j^\circ(p+\sigma_j^\circ-1)/2,$$

whenever $\sigma_j^\circ \leq (p-1)/2$.

Thus if $\pi_k \not\equiv 0$ and $k\leq(p-1)/2$ then $N(\pi_k)$, the number of solutions of $\pi_k(y,z)=0$ in $\mathbb{F}_p$ for which $f(x)+ag(x)+bx$ is a permutation polynomial, satisfies

$$N(\pi_k) \leq \sum N_j \leq \sum \sigma_j^\circ(p+\sigma_j^\circ-1)/2 \leq k(p-1)/2 + \frac{1}{2}\sum(\sigma_j^\circ)^2$$

$$\leq k(p-1)/2 + \frac{1}{2}(\sum \sigma_j^\circ)^2 = (k(p-1)+k^2)/2.$$

By hypothesis $\pi_k \equiv 0$ or

$$(2s+1)(p+2s)/2 < N_k \leq (k(p-1)+k^2)/2,$$

which gives $k\geq 2s+2$. Now

$$\pi_k(Y,Z) = \sum_{l=0}^{k}\sum_{m=0}^{k-l}\binom{k}{l}\binom{k-l}{m}\left(\sum_{x\in\mathbb{F}_p} x^{k-l-m}f(x)^l g(x)^m\right)Y^mZ^{k-l-m},$$

and so $I(f,g)\geq 2s+2$.

□

THEOREM 3.3. *If $M(f,g) > (2s+1)(p+2s)/2$ then there are elements $c,d,e\in\mathbb{F}_p$ such that $f(x)+cg(x)+dx+e=0$.*

Proof. If $p = 3$ and $M(f,g) > (2s+1)(p+2s)/2 = 15/2$ then there is a c such that $f(x)+cg(x)+bx$ is a permutation polynomial for all $b \in \mathbb{F}_p$, which can only occur if there is a constant e such that $f(x) + cg(x) + e = 0$.

So suppose $p \geq 5$ and that there are no elements $c, d, e \in \mathbb{F}_p$ with the property that $f(x) + cg(x) + dx + e = 0$.

Clearly $I(f + ag) \geq I(f,g)$ for all $a \in \mathbb{F}_p$ and $I(f,g) \geq 2s + 2$ by Lemma 3.2.

There is an $a_1 \in \mathbb{F}_p$ with the property that

$$M(f + a_1 g) \geq M(f,g)/p \geq (p-1)/6.$$

By Theorem 2.1 there are constants $c, d, c', d' \in \mathbb{F}_p$ with the property that

$$(f + a_1 g + cx + d)(f + a_1 g + c'x + d') = 0$$

so the graph of (f,g), the set of points $\{(x, f(x), g(x)) \mid x \in \mathbb{F}_p\}$, is contained in the union of two planes.

By Rédei and Megyesi's theorem, since we have assumed that the graph of $f + a_1 g$ is not a line, $M(f + a_1 g) \leq (p-1)/2$ and so there is an $a_2 \neq a_1$ with the property that

$$M(f + a_2 g) \geq (M(f,g) - (p-1)/2)/(p-1) \geq (p-1)/6.$$

Thus the graph of (f,g) is contained in the union of two other planes, different from the ones before. The intersection of the two planes with the two planes is four lines and so the graph of (f,g) is contained in the union of four lines.

Similarly, since $(M(f,g)-(p-1))/(p-2) \geq (p-1)/6$ and $(M(f,g)-3(p-1)/2)/(p-3) \geq (p-1)/6$, there is an a_3 and an a_4 with that property that $M(f + a_3 g) \geq (p-1)/6$ and $M(f + a_4 g) \geq (p-1)/6$ and so the graph of (f,g) is contained in two other distinct pairs of planes. The four lines span three different pairs of planes and so the graph of (f,g) is contained in the union of two lines and hence a plane, which is a contradiction. □

There is an example when q is an odd prime (power) congruent to 1 modulo 3 with $M(f,g) = 2(q-1)^2/9 - 1$ where the graph of (f,g) is not contained in a plane, which shows that the bound is the right order of magnitude.

Let $E = \{e \in \mathbb{F}_q \mid e^{(q-1)/3} = 1\} \cup \{0\}$. Then the set $S = \{(e,0,0),\ (0,e,0),\ (0,0,e) \mid e \in E\}$ is a set of q points. If π, the plane defined by

$$X_1 + aX_2 + bX_3 = c,$$

is incident with $(e,0,0)$ for some $e \in E$ then $c \in E$. Likewise if it is incident with $(0,e,0)$ for some $e \in E$ then $a/c \in E$ and if it is incident with $(0,0,e)$ for some $e \in E$ then $b/c \in E$.

If π is incident with two points of S then either $a \in E$, $b \in E$ or $a/b \in E$. Thus if a, b and a/b are not elements of E then π and all the planes parallel to π are incident with exactly one point of S. There are $2(q-1)^2/9$ such sets of parallel lines.

If we make a change of coordinates so that $\{X_1 = x \mid x \in \mathbb{F}_q\}$ is one such set of parallel planes then there are functions f and g for which $S = \{(x, f(x), g(x)) \mid x \in \mathbb{F}_q\}$. Each other set of parallel lines with the above property corresponds to a pair (a,b) such that $f(x)+ag(x)+bx$ is a permutation polynomial. Thus $M(f,g) = 2(q-1)^2/9-1$. Explicitly

the functions f and g can be defined by $f(x) = \chi_H(x)x$ and $g(x) = \chi_{\epsilon H}(x)x$, where χ_H is the characteristic function of $H = \{t^3 \mid t \in \mathbb{F}_p\}$ and ϵ is a primitive third root of unity.

4. Acknowledgements

We are grateful to Tamas Szőnyi for some valuable discussions and to Vsevolod Lev for his help in making the article accessible to a wider audience.

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] 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.
[3] A. Gács, On a generalization of Rédei's theorem, *Combinatorica*, **23** (2003) 585–598.
[4] R. Lidl and H. Niederreiter, *Finite Fields*, Second Edition, Cambridge University Press, 1997.
[5] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981) 449–454.
[6] L. Rédei, *Lückenhafte Polynome über endlichen Körpen*, Birkhäuser-Verlag, Basel, 1970. (English translation: *Lacunary Polynomials over finite fields*, North-Holland, Amsterdam, 1973.)
[7] K-O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.*, **52** (1986) 1–19.
[8] T. Szőnyi, Combinatorial problems for Abelian groups arising from geometry, *Periodica Polytechnica*, **19** (1991) 197–212.

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 and Peter Sziklai

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