ON PERMUTATION POLYNOMIALS WHOSE DIFFERENCE IS LINEAR

by W. W. STOTHERS

(Received 7 November, 1988; revised 15 December, 1988)

1. Introduction. Let q be a power of a prime p, and let S_q be the set of permutations of $\{0, 1, \ldots, q-1\}$. As S_q is isomorphic to the group of permutations of F_q, the field of q elements, each element of S_q can be regarded as a polynomial over F_q. Various authors (e.g. **[1]**, **[2]**, **[3]**) have considered functions $f(x)$ such that

$$f(x) \in S_q, \quad \text{and} \quad (f(x) + \lambda x) \in S_q$$

for some $\lambda \in F_q$. When $\lambda = 1$, $f(x)$ is a *complete mapping polynomial* (**[3]**).

Here, we consider the $f(x)$ for which there are *several* λ. For q prime, such functions arose in (unpublished) work of M. J. Tomkinson on group theory.

DEFINITION. For $f(x) \in F_p[x]$,

$$W_f = \{\lambda \in F_q : (f(x) + \lambda x) \in S_q\},$$

and

$$w_f = |W_f|.$$

Observe that, if $f(x) \in S_q$, then $0 \in W_f$, so that $w_f \geqslant 1$. Also, f is a complete mapping polynomial if and only if $0, 1 \in W_f$. On the other hand, if $(f(x) + \lambda x) \in S_q$, then we must have

$$f(0) + \lambda 0 \neq f(1) + \lambda 1,$$

i.e.

$$\lambda \neq f(0) - f(1).$$

Thus $w_f \leqslant q - 1$.

If we take $f(x) = \alpha x + \beta$, then

$$f(x) + \lambda x = (\alpha + \lambda)x + \beta,$$

so $\lambda \in W_f$ except when $\lambda = -\alpha$. We have proved

PROPOSITION 1. *If f is a linear or constant polynomial over F_q, then $w_f = q - 1$.*

Tomkinson asked how large w_f could be for *non-linear* f. We shall establish an upper bound, and discuss the f which attain the bound.

DEFINITION. A polynomial $f(x)$ over F_q is *reduced* if the degree of f is less than q.

DEFINITION. If $f \in F_q[x]$, then we write $r_q(f)$ for the unique reduced polynomial equal to f (as a function), and $d_q(f)$ for the degree of $r_q(f)$.

PROPOSITION 2. *If $f, g \in F_q[x]$ and $d_q(f) + d_q(g) < p$, then*

$$r_q(fg) = r_q(f)r_q(g),$$

and

$$d_q(fg) = d_q(f) + d_q(g).$$

Glasgow Math. J. **32** (1990) 165–171.

Proof. This follows at once from the uniqueness of the reduced polynomial.

We use (and then generalize) the following result from **[1]**.

LEMMA. *A polynomial $f \in F_q[x]$ belongs to S_q if and only if*

$$\text{(1) } f \text{ has a unique root in } F_q,$$

and

$$\text{(2) for } 1 \leqslant n \leqslant q-2,\ d_q(f^n) \leqslant q-2.$$

2. The case q prime.

THEOREM 1. *If $f \in S_p$ and $1 \leqslant m \leqslant w_f$, then*

$$d_p(f^m) \leqslant p - 2 + m - w_f. \tag{1}$$

Proof. From the Lemma, for $0 < t < p-1$,

$$r_p(f^t(x)) = \sum_{j=0}^{p-2} a_{tj}x^j.$$

Then, for $0 < t < p-1$, the coefficient of x^{p-1} in $r_p((f(x)+\alpha x)^t)$ is

$$\sum_{s=1}^{t-1} \binom{t}{s} \alpha^s a_{(t-s)(p-1-s)}. \tag{2}$$

This is a polynomial in α of degree at most $t-1$, so, if non-zero, has at most $t-1$ roots in F_p. Thus, if $t \leqslant w_f$, it must be the zero polynomial, i.e. for $s \leqslant t \leqslant w_f$,

$$a_{(t-s)(p-1-s)} = 0.$$

Put $m = t - s$. Then, for $m \leqslant t \leqslant w_f$,

$$a_{m(p-1+m-t)} = 0.$$

Since this holds for $t \leqslant w_f$,

$$d_p(f^m(x)) \leqslant p - 2 + m - w_f,$$

as required.

REMARKS. (i) Dickson's result (our "Lemma") and Theorem 1 of **[3]** give the result for the cases $m = 1, 2$.

(ii) The proof *fails* for a prime to a power greater than one since some of the binomial coefficients in (2) vanish in F_q; see §3.

In Proposition 1, we saw that if $d_p(f) \leqslant 1$ then $w_f = p-1$. We now show that only linear f have $w_f > (p-3)/2$.

THEOREM 2. *If $f \in S_p$ has $w_f > (p-3)/2$, then $d_p(f) \leqslant 1$.*

Proof. We may as well assume that f is reduced. It is easily checked that all $f \in S_2$ are linear, so we may assume that $p > 2$. Let D be the degree of f. We suppose that $D > 2$. By the Lemma applied to $f^{(p-1)/D}$, we see that $D \nmid (p-1)$, and hence that $p \geqslant 5$.

Let m be the integer such that

$$(p-1)/(m+1) < d < (p-1)/m, \tag{3}$$

https://doi.org/10.1017/S0017089500009186 Published online by Cambridge University Press

so $1 \leqslant m \leqslant (p-3)/2$. Then f^m is reduced and $d_p(f^m) = mD \leqslant (p-3)/2 + m$, by Theorem 1. It now follows from (3) that

$$m(p-1)/(m+1) < (p-3)/2 + m. \tag{4}$$

This implies that $(m-1)(p-3-2m) < 0$, a contradiction.

In particular, this shows that, for $p \leqslant 5$, the only polynomials f with $w_f > 1$ are linear. For $p > 5$, we can have non-linear examples, as we shall see later.

PROPOSITION 3. *Suppose that* $f \in F_p[x]$, *and that* $\alpha, \beta, \gamma \in F_p$, *with* $\alpha \neq 0$. *Let* $g \in F_p[x]$ *be defined by* $g(x) = \alpha f(x+\beta) + \gamma$. *Then*

$$W_g = \{\alpha\lambda : \lambda \in W_f\}$$

and

$$w_g = w_f.$$

Proof. The second part follows at once from the first. To prove the first, we observe that $(g(x) + \mu x) \in S_p$ if and only if it is injective. Now

$$g(x) + \mu x = g(y) + \mu y$$

if and only if

$$\alpha f(x+\beta) + \mu x = \alpha f(y+\beta) + \mu y.$$

We choose λ so that $\mu = \alpha\lambda$. Then the latter becomes (adding $\alpha\lambda\beta$ to each side)

$$\alpha f(x+\beta) + \alpha\lambda(x+\beta) = \alpha f(y+\beta) + \alpha\lambda(y+\beta).$$

Hence $\mu \in W_g \Leftrightarrow \lambda \in W_f$.

DEFINITION. For reduced $f, g \in F_p$ we write $f\rho g$ if there exist $\alpha, \beta, \gamma \in F_p$ with $\alpha \neq 0$ such that

$$g(x) = \alpha f(x+\beta) + \gamma.$$

PROPOSITION 4. *Each* ρ*-class of non-constant reduced polynomials in* $F_p[x]$ *contains a unique member of the form*

$$g(x) = x^d + \alpha_{d-2}x^{d-2} + \ldots + \alpha_1 x. \tag{5}$$

If $d = 1$, *then the class has* $p(p-1)$ *members; otherwise it has* $p^2(p-1)$.

We leave the proof to the reader.

DEFINITION. We say that a polynomial of the form (5) is *normalized.*

THEOREM 3. *For* $p > 5$, $f \in S_p$ *has* $w_f = (p-3)/2$ *if and only if* f *is* ρ*-equivalent to*

$$g(x) = x^{(p+1)/2} + ax$$

for some $a \in F_p$.

Proof. We may as well assume f is reduced. Let D be the degree of f. By Theorem 1,

$$D \leqslant (p-2) - (p-3)/2 + 1 = (p+1)/2.$$

Suppose that $D<(p+1)/2$. Arguing as in Theorem 2 (but with $w_f=(p-3)/2$), we must have $p>7$ and, for some m with $2\leqslant m\leqslant(p-5)/2$,

$$(m-1)(p-3-2m)<m+1.$$

Since $p-3-2m\geqslant 2$, this gives a contradiction unless $m=2$. But then, as $p>7$, $p-3-2m=p-7\geqslant 4$, so we get a contradiction here also. Hence we *must* have $D=(p+1)/2$.

Now let g be the normalised polynomial ρ-equivalent to f. Then g has degree $(p+1)/2$ and

$$g(x)=x^{(p+1)/2}+\alpha x^k+\text{terms of lower degree},$$

where $k\leqslant(p-3)/2$. We note that $(x^{(p+1)/2})^2$ reduces to x^2. Thus

$$r_p(g^2(x))=(2\alpha x^{k+(p+1)/2}+\dots)+x^2.$$

From Theorem 1, we have

$$\begin{aligned} d_p(g^2(x)) &\leqslant (p-2)-(p-3)/2+2 \\ &=(p+3)/2. \end{aligned}$$

If $\alpha\neq 0$, then we must have $k+(p+1)/2\leqslant(p+3)/2$, so that $k\leqslant 1$. As g is normalised (so has no constant term),

$$g(x)=x^{(p+1)/2}+ax. \tag{5}$$

To complete the proof, we must show that each g of the form (5) has $w_g=(p-3)/2$. We recall that $x^{(p-1)/2}\equiv(x/p)$ (the Legendre symbol) (modulo p) so that

$$g(x)+\lambda x=\begin{cases} 0 & \text{if } x=0,\\ (a+\lambda+1)x & \text{if } x \text{ is a quadratic residue modulo } p,\\ (a+\lambda-1)x & \text{otherwise.}\end{cases}$$

Since for all residues (resp. non-residues) x, $(a+\lambda+1)x$ (resp. $(a+\lambda-1)x$) will have the same quadratic character, $(g(x)+\lambda x)\in S_p$ if and only if $(a+\lambda+1)$ and $(a+\lambda-1)$ have same quadratic character, i.e. for some $\alpha\neq 0$,

$$(a+\lambda+1)=\alpha^2(a+\lambda-1)$$

i.e.

$$\lambda=\frac{\alpha^2+1}{\alpha^2-1}-a.$$

Since there are $(p-3)/2$ distinct squares modulo p, other than 0 and 1, there are $(p-3)/2$ valid λ, as required.

COROLLARY 1. *For* $p>5$, *there are* $p^3(p-1)$ *non-linear functions* f *with* $w_f=(p-3)/2$.

Proof. From the proof above, there are p *normalised* functions g, and (by Proposition 4), each corresponds to $p^2(p-1)$ functions f.

REMARK. It is probably neater to re-cast the description of "g" in Theorem 3 as

$$g(x)=\begin{cases}0 & \text{if } x=0,\\ Ax & \text{if } x \text{ is a quadratic residue modulo } p,\\ Bx & \text{otherwise,}\end{cases} \tag{6}$$

where A and B are distinct modulo p, but of the same quadratic character. This form would have helped to simplify the discussion of [**2**].

COROLLARY 2 (c.f. Theorem 8 of [**3**]). *For $p>5$ there exist non-linear complete polynomial mappings of F_p.*

Proof. Since $p>3$, we can choose A and B distinct quadratic residues, and define g by (6). As $(A/p)=(B/p)=1$, $0\in W_g$. Now $w_g=(p-3)/2\geqslant 2$ (as $p>5$), so we have $\lambda\in W_g$, $\lambda\neq 0$. Now apply Proposition 3 to μg (with $\mu\lambda\equiv 1$ (modulo p) to see that $0,1\in W_{\lambda g}$, i.e. that λg is of the required type.

The ideas above can be used to construct other non-linear f with $1<w_f<(p-3)/2$ as follows.

CONSTRUCTION. If $p>5$, choose h such that $h\mid(p-1)$ and $2<h<(p-1)/2$. Let χ_h denote the hth power residue symbol. Choose A, B distinct members of F_p and define $g(x)$ on F_p by

$$g(x)=\begin{cases}0 & \text{if } x=0,\\ Ax & \text{if } \chi_h(x)=1,\\ Bx & \text{otherwise.}\end{cases}$$

Much as before, $\lambda\in W_g$ if and only if

$$(A+\lambda)=\alpha^h(B+\lambda)$$

for some non-zero $\alpha\in F_p$. Rearranging:

$$\lambda=(A-B\alpha^h)/(\alpha^h-1).$$

Since α^h takes $((p-1)/h)-1$ distinct values other than 1, we have

$$w_g=((p-1)/h)-1.$$

We observe that, as a polynomial,

$$g(x)=x(A(x^{p-1}-1)/(x^{(p-1)/h}-1)+B(x^h-1)$$

so that

$$d_p(g)=1+(p-1)-(p-1)/h=p-2-((p-1)/h)-1)+1,$$

giving *equality* in Theorem 1.

We can, of course, modify the construction above to introduce A's for each residue class. This gives greater flexibility, and allows us to prove that we need not have equality in Theorem 1.

EXAMPLE. For $p=13$, let $f(x)=6x(x^4+6x^2+4)$. It is a simple matter to check that $w_f=\{0,1\}$, but $d_p(f)$ is only 5.

This example arises from 6th power residues (hence the appearance of even powers inside the brackets). There are, however, many f with $1 < w_f < (p-3)/2$ which do *not* arise from our construction (these of necessity have $w_f = ((p-1)/h) - 1$ for some h; for example, there are 110 *classes* in $F_{11}[x]$ with $w_f = 3$).

3. The general case. As noted earlier, the proof of Theorem 1 fails for $q = p^r$ with $r > 1$. We can prove a weaker version which shows that, except in special cases, a reduced $f \in F_q[x]$ with $w_f > 1$ begins with powers x^d, where $p \mid d$. The result is incomplete, so we omit it. Based on our experimental evidence (see section 4) we are, however, prepared to make the following conjecture.

CONJECTURE. *If* $f \in F_q[x]$ *with* $w_f > (p-3)/2$, *then* $f(x) = g^p(x) + ax$, *where* $d_p(g) \leq q/p$.

We give an example to show that the situation is more complicated than that in §2.

EXAMPLE. Let $f(x) = x^q - ax$. Then, calculating in F_{q^2}, $f(x) = f(y)$ if and only if

$$a = (x^q - y^q)/(x-y) = (x-y)^q/(x-y).$$

Thus, $f(x)$ fails to permute F_{q^2} if and only if a is a $(q-1)$th power, i.e. $a^{q+1} = 1$. Since there are $q+1$ elements with this property,

$$w_f = (q^2 - 1) - (q+1) + 1 = q^2 - q - 1.$$

REMARK. The construction introduced in §2 works for prime powers, provided that the value of h is prime to p. These seem to account for "large" values of w_f. We have *proved* this for $q = 4, 8, 9, 16$ and 25, verifying the experimental results in the first four cases.

4. Experimental results. We have written a program which checks each permutation $f(x)$ to see whether $f(x) + x$ is also a permutation, and, if so, finds the λ for which $f(x) + \lambda x$ belongs to S_q. For each such f, it checks the degree of the reduced version of f.

These computations take a considerable time (hours of mainframe time), so it is unlikely to be sensible to carry them much further.

We show below the total number, C_q, of complete mapping polynomials for small values of q. Of course, the actual output was much more detailed. The results of the calculations suggest that the permutations are *not* randomly spread amongst the polynomials. Since there are $q!$ permutations and q^{q-1} polynomials of degree at most $q-2$, a random distribution would predict about $(q!)^2/q^{q-1}$ polynomials $f(x)$ with $f(x) + x$ also in S_q.

q	C_q	$(q!)^2/q^{q-1}$
5	20	25
7	133	216
8	384	775
9	2241	3059
11	37851	61431
13	1030367	1664334
16	244744192	379698995
17	1606008513	2599885897

The figures in the last column are rounded to the nearest integer. We observe that, for prime q, the ratio $C_q/(q!)^2q^{q-1}$ is remarkably close to the golden section!

Acknowledgement. I should like to thank the referee for suggesting a better way of presenting the argument in Theorems 2 and 3.

REFERENCES

1. L. E. Dickson, *Linear Groups* (Dover, 1958).

2. G. Mullen and H. Niederreiter, The structure of a group of permutation polynomials, *J. Austral. Math. Soc. Ser. A* **38** (1985), 164–170.

3. H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33** (1982), 197–212.

DEPARTMENT OF MATHEMATICS,
UNIVERSITY GARDENS,
GLASGOW G12 8QW