Can. J. Math. Vol. **46** (2), 1994 pp. 225–238

DICKSON POLYNOMIALS OF THE SECOND KIND THAT ARE PERMUTATIONS

STEPHEN D. COHEN

ABSTRACT. It is known that the Dickson polynomial of the second kind $\sum_{i=0}^{[n/2]} \binom{n-i}{i}(-1)^i x^{n-2i}$ permutes the elements of the finite prime field $\mathbb{F}_p$ (p odd) when $n+1 \equiv \pm 2$ to each of the moduli p, $\frac{1}{2}(p-1)$ and $\frac{1}{2}(p+1)$. Based on numerical evidence it has been conjectured that these congruences are necessary for the polynomial to permute $\mathbb{F}_p$. The conjecture is established here by a new method.

1. **Introduction.** Let $\mathbb{F}_q$ denote the finite field of order a prime power $q = p^k$. For any positive integer n we shall consider the *Dickson polynomial of the second kind* (DPSK) $f_n(x)$, defined by

$$f_n(x) = \sum_{i=0}^{[n/2]} \binom{n-i}{i}(-1)^i x^{n-2i}, \tag{1.1}$$

as a polynomial in $\mathbb{F}_q[x]$. For properties of DPSK (and a slight generalisation of these) see [2], [3], [4], [6] and [7]. In particular, in his thesis Matthews [6] observed that, if q is odd and n satisfies the system of congruences

$$\begin{cases} n+1 \equiv \pm 2 \pmod{p}, \\ n+1 \equiv \pm 2 \pmod{\frac{1}{2}(q-1)}, \\ n+1 \equiv \pm 2 \pmod{\frac{1}{2}(q+1)}, \end{cases} \tag{1.2}$$

then f_n is a permutation polynomial (PP) of $\mathbb{F}_q$, *i.e.* induces a permutation of $\mathbb{F}_q$. Indeed (1.2) implies that $f_n(-x) = -f_n(x)$ (n is odd) and $f_n(x) = \pm x$ for all x in $\mathbb{F}_q$.

Actually, when $p = 3$ or 5 and q is composite ($k \geq 2$) there are examples of DPSK f_n known which are PP for which (1.2) does not hold; see [3] and [7]. On the other hand, when $q = p$, an odd prime, it has been conjectured in these papers and featured as problem P4 in the list [4] of outstanding unsolved problems that, if f_n is a PP of $\mathbb{F}_q$, then necessarily (1.2) holds. The evidence had been almost entirely numerical because DPSK are awkward to treat. But now we are able to prove the conjecture by a new method.

THEOREM 1. *Suppose that f_n is a* PP *of $\mathbb{F}_p$, where p is an odd prime. Then*

$$\begin{cases} n+1 \equiv \pm 2 \pmod{p}, \\ n+1 \equiv \pm 2 \pmod{\frac{1}{2}(p-1)}, \\ n+1 \equiv \pm 2 \pmod{\frac{1}{2}(p+1)}. \end{cases} \tag{1.3}$$

Received by the editors October 5, 1992.
AMS subject classification: 11T06.

The proof of Theorem 1 is theoretical. Nevertheless, in order to complete the argument, it was necessary to compute the resultants of various pairs of polynomials and pay special attention to those primes p (> 5) for which these were zero, *i.e.*, the polynomials have a common root in $\mathbb{F}_p$. For this purpose, the number-theoretical package PARI (developed by C. Batut, D. Bernardi, H. Cohen and M. Olivier) was most useful and the awkward prime values eliminated without the need to make a direct check that f_n is not a PP of $\mathbb{F}_p$ for any pair (p,n) not satisfying (1.3).

Whilst it is a sensible and unanswered question to ask when f_n can be a PP of $\mathbb{F}_q$ when q is even, we shall assume from now on that q is odd. Further, because a PP f_n of $\mathbb{F}_q$ is also a PP of $\mathbb{F}_p$, our results and methods have preliminary consequences for composite odd q. But, in the main, we shall suppose $q = p$, an odd prime.

2. **Basic results.** As is well-known, in studying DPSK it is illuminating to substitute $x = u + u^{-1}$ in $f_n(x)$. Thus, identically,

$$f_n\left(u+\frac{1}{u}\right) = u^n + u^{n-2} + u^{n-4} + \cdots + u^{-(n-2)} + u^{-n} \tag{2.1}$$

$$= \frac{u^{n+1} - \frac{1}{u^{n+1}}}{u - \frac{1}{u}}, \quad u \neq \pm 1, \tag{2.2}$$

while

$$f_n(2) = n+1, \quad f_n(-2) = (-1)^n(n+1). \tag{2.3}$$

In the above connection we partition $\mathbb{F}_q$ into three sets S_1, S_2, S_0 comprising those $x \in \mathbb{F}_q$ for which the quadratic character of $x^2 - 4$ in $\mathbb{F}_q$ is +1, -1 and 0, respectively. Thus

$$S_1 = \left\{x = u + \frac{1}{u}, \text{ where } u \in \mathbb{F}_q \setminus \{0, \pm 1\}\right\}, \tag{2.4}$$

$$S_2 = \left\{x = u + \frac{1}{u}, \text{ where } u\ (\neq \pm 1) \in \mathbb{F}_{q^2} \text{ and } u^{q+1} = 1\right\}, \tag{2.5}$$

$$S_3 = \{\pm 2\}. \tag{2.6}$$

In the subsequent treatment, for $x \in S_1 \cup S_2$, u will be as described in (2.4) or (2.5) while, if $x \in S_3$, we take $u = \pm 1$, respectively. Note that $0 \in S_1$ or S_2 accordingly as $q \equiv 1$ or $-1 \pmod 4$, respectively, and that $f_n(0) = 0$.

From now on we *assume that* f_n *is a* PP *of* F_q, where $q = p^k$ is odd. Hence n is odd and $f_n(-2) = -(n+1)$ in (2.3). For any divisor d of $q^2 - 1$ we write ζ_d for a primitive d-th root of unity (in $\mathbb{F}_{q^2}$).

LEMMA 2. *p does does not divide $n+1$.*

PROOF. If $p \mid n+1$, then, by (2.3), $f_n(2) = f_n(-2) = 0$ which means f cannot be a permutation.

LEMMA 3. *Let g be the highest common factor of $n+1$ and q^2-1. Then*

$$g = \begin{cases} 2, & \text{if } q \equiv \pm 1 \pmod 8, \\ 2^s, s \geq 1, & \text{if } q \equiv \pm 3 \pmod 8). \end{cases}$$

PROOF. Suppose that $d\,(>1)$ is an odd divisor either of $(n+1, q-1)$ or of $(n+1, q+1)$. Then $x = \zeta_d + \zeta_d^{-1} \in S_1$ or S_2, respectively, and, in either case, $f(x) = 0$ but $x \neq 0$, by (2.2), a contradiction. Similarly, if $q \equiv \pm 1 \pmod 8$, $x = \zeta_8 + \zeta_8^{-1} (\neq 0) \in S_1 \cup S_2$ and $4 \mid n+1$, then $\zeta_8^{2(n+1)} = 1$ and $f_n(x) = 0$, a contradiction.

LEMMA 4. *Let h be the highest common factor of $n(n+2)$ and q^2-1. Then*

$$h = \begin{cases} 1, & \text{if } p = 3, \\ 3, & \text{otherwise.} \end{cases}$$

PROOF. Suppose $d\,(>3)$ is a divisor either of $(n, q-1)$ or $(n, q+1)$. (In particular, d is odd). Put $x_i = \zeta_d^i + \zeta_d^{-i}$, $i = 1, 2$. Then x_1 and x_2 both belong to S_1 or S_2, respectively, and are unequal since $d > 3$. Moreover, by (2.2), $f_n(x_1) = f_n(x_2) = 1$, a contradiction.

Similarly, if $d\,(>3)$ is a divisor of $(n+2, q-1)$ or $(n+2, q+1)$ then

$$f_n(x_1) = f_n(x_2) = -1, \quad x_1 \neq x_2.$$

We conclude that $h \mid 3$. On the other hand, if $p \neq 3$, then $3 \mid q^2-1$ and hence $3 \nmid n+1$ by Lemma 3; thus $3 \mid n(n+2)$ and $h = 3$. The result follows.

From now on we assume that $q = p$ is an odd prime. In fact, if $p = 3$, then $3 \nmid n+1$ by Lemma 2 and consequently (1.3) holds. We therefore suppose that $p \geq 5$.

3. **Proof of first congruence.**

As noted above, assume that $p\,(\geq 5)$ is prime. Define $\xi = \zeta_{p-1}$, $\eta = \zeta_{p+1}$. Then, by (2.4) and (2.5)

$$S_1 = \left\{\xi^i + \xi^{-i}, 1 \leq i \leq \frac{1}{2}(p-3)\right\}, \tag{3.1}$$

$$S_2 = \left\{\eta^j + \eta^{-j}, 1 \leq j \leq \frac{1}{2}(p-1)\right\}. \tag{3.2}$$

In particular, if $p \equiv 1 \pmod 4$, then 0 is the member of S_1 with $i = (p-1)/4$ in (3.1), while, if $p \equiv 3 \pmod 4$, then 0 is the member of S_2 with $j = (p+1)/4$ in (3.2).

LEMMA 5. $n+1 \equiv \pm 2 \pmod p$.

PROOF. Since f_n is a PP of $\mathbb{F}_p$ with $f_n(0) = 0$,

$$\prod_{x \in \mathbb{F}_p^*} f_n(x) = -1,$$

by Wilson's theorem. Hence, if A is defined to be the product

$$A = \prod_{\substack{x \in S_1 \cup S_2 \\ x \neq 0}} f_n(x)$$

over non-zero members of $S_1 \cup S_2$, then, by (2.3),

$$A = \frac{1}{f_n(2)f_n(-2)} = \frac{1}{(n+1)^2} \tag{3.3}$$

(which, of course, is consistent with Lemma 2). Now, write

$$A_1 = \prod\nolimits_1 \frac{\xi^{i(n+1)} - \xi^{-i(n+1)}}{\xi^i - \xi^{-i}},$$

where $\prod_1$ signifies a product $\prod_{\substack{i=1\\(i\neq(p-1)/4)}}^{(p-3)/2}$ over all i from 1 to $(p-3)/2$ but excluding $i = (p-1)/4$ if $p \equiv 1 \pmod 4$. Similarly, set

$$A_2 = \prod\nolimits_2 \frac{\eta^{j(n+1)} - \eta^{-j(n+1)}}{\eta^j - \eta^{-j}},$$

where $\prod_2$ signifies a product $\prod_{\substack{j=1\\(j\neq(p+1)/4)}}^{(p-1)/2}$ over all j from 1 to $(p-1)/2$ but excluding $j = (p+1)/4$ if $p \equiv 3 \pmod 4$. Then evidently $A = A_1A_2$.

We have

$$A_1 = \prod\nolimits_1 \frac{\xi^{4i((n+1)/2)} - 1}{\xi^{in}(\xi^{2i} - 1)}. \tag{3.4}$$

Let $I = \{i = 1, \ldots, \frac{1}{2}(p-3), i \neq (p-1)/4\}$. As i ranges through I, ξ^{2i} takes all square values ($\neq 0, \pm 1$) in $\mathbb{F}_p$. Further, by Lemma 3, the odd part of $\frac{1}{2}(n+1)$ is prime to $p-1$ and indeed $\left(\frac{1}{2}(n+1), p-1\right) = 1$ when $p \equiv 1 \pmod 8$. It follows that, when $p \equiv 1 \pmod 4$, as i ranges through I, $\xi^{4i((n+1)/2)}$ takes all 4-th power values ($\neq 0, 1$) in $\mathbb{F}_p$ twice over. On the other hand, when $p \equiv 3 \pmod 4$, for $i \in I$, $\xi^{4i((n+1)/2)}$ takes all 4-th power values ($\neq 0, 1$) in $\mathbb{F}_p$ (which is, incidentally, the same as saying that $\xi^{4i((n+1)/2)}$ takes all square values ($\neq 0, 1$) in $\mathbb{F}_p$). In every case

$$\prod\nolimits_1(\xi^{4i((n+1)/2)} - 1) = \prod\nolimits_1(\xi^{4i} - 1)$$

and, consequently, by (3.4),

$$A_1 = \prod\nolimits_1(\xi^{2i} + 1)/\xi^{in} = \prod\nolimits_1(\xi^i + \xi^{-i})/\xi^{i(n-1)}. \tag{3.5}$$

Similarly,

$$A_2 = \prod\nolimits_2 \frac{\eta^{4j((n+1)/2)} - 1}{\eta^{jn}(\eta^{2j} - 1)}. \tag{3.6}$$

Set $J = \{j = 1, \ldots, \frac{1}{2}(p-1), j \neq (p+1)/4\}$. By comparing the set of squares and 4-th powers ($\neq 0, \pm 1$) of the set of $(p+1)$-st roots of unity (in $\mathbb{F}_{p^2}$) with $\{\eta^{2j}, j \in J\}$ and $\{\eta^{4j((n+1)/2)}, j \in J\}$ and using Lemma 3 as before, we deduce analogously to (3.5) that

$$A_2 = \prod\nolimits_2(\eta^j + \eta^{-j})/\eta^{j(n-1)}. \tag{3.7}$$

Combining (3.5) and (3.7), we obtain

$$A = A_1A_2 = \prod_{\substack{x\in S_1\cup S_2\\ x\neq 0}} x\prod\nolimits_1 \xi^{-i(n-1)}\prod\nolimits_2 \eta^{-j(n-1)}. \tag{3.8}$$

Suppose $p \equiv 1 \pmod 4$. Then

$$\prod\nolimits_2 \eta^{j(n-1)} = \prod_{j=1}^{(p-1)/2} \eta^{j(n-1)} = (\eta^{\frac{p+1}{2}})^{\frac{(n-1)(p-1)}{4}} = 1,$$

since $n-1$ is even and $\eta = \zeta_{p+1}$. Further,

$$\begin{aligned}\prod\nolimits_1 \xi^{i(n-1)} &= \Big\{\prod_{i=1}^{(p-3)/2} \xi^{i(n-1)}\Big\}\xi^{-(n-1)(p-1)/4}\\ &= \xi^{((p-1)(p-3)(n-1)/8)-((n-1)(p-1)/4)} = (\xi^{p-1})^{\frac{(n-1)(p-5)}{8}} = 1\end{aligned}$$

since $\xi = \zeta_{p-1}$ and $8 \mid (n-1)(p-5)$.

A similar calculation is valid when $p \equiv 3 \pmod 4$. For then

$$\prod\nolimits_1 \xi^{i(n-1)} = \prod_{i=1}^{(p-3)/2} \xi^{i(n-1)} = (\xi^{\frac{p-1}{2}})^{\frac{(n-1)(p-3)}{4}} = 1$$

and

$$\prod\nolimits_2 \eta^{j(n-1)} = (\eta^{p+1})^{\frac{(n-1)(p-3)}{8}} = 1.$$

From (3.8) it follows that in every case

$$A = \prod_{\substack{x\in S_1\cup S_2\\ x\neq 0}} x = \frac{1}{4}, \tag{3.9}$$

by Wilson's theorem again. Comparing (3.3) and (3.9) we conclude that, in $\mathbb{F}_p$,

$$(n+1)^2 = 4$$

which is equivalent to $n+1 \equiv \pm 2 \pmod p$, as required. This completes the proof.

Finally in this section we remark that when $p = 5$ or 7, Theorem 1 follows from Lemmas 3 and 5. Hence from now on we assume $p \geq 11$.

4. **Normalisation.** We continue to assume that f_n is a PP of $\mathbb{F}_p$. The motivation for the sequel is the following simple observation (related to the work of Brison [1]).

LEMMA 6. *Let F_n be a function from $\mathbb{F}_p$ into itself such that*

$$F_n(x) = \pm f_n(x) \quad \forall x \in \mathbb{F}_p. \tag{4.1}$$

Then, if $p \geq 5$,

$$\sum_{x\in\mathbb{F}_p} \big(F_n(x)\big)^{2r} = 0, \quad r = 1,\ldots,\frac{1}{2}(p-3). \tag{4.2}$$

PROOF. Since f_n is a PP, for any $s = 1, \ldots, p-2$, by Lemma 7.3 of [5],

$$\sum_{x \in \mathbb{F}_p} \big(f_n(x)\big)^s = \sum_{x \in \mathbb{F}_p} x^s = 0. \tag{4.3}$$

In particular, taking $s = 2r$, $r = 1, \ldots, \frac{1}{2}(p-3)$ in (4.3), we see that (4.2) holds with $F_n = f_n$. But for any F_n satisfying the hypothesis, $\big(F_n(x)\big)^{2r} = \big(f_n(x)\big)^{2r}$ and the result follows.

Now set $N = n + 1$. The restriction that $p \geq 11$ comes into play in the next result.

LEMMA 7. *Suppose $p \geq 11$. Then*

$$N \not\equiv 0, \pm 1 \pmod{\frac{1}{2}(p-1)},$$
$$N \not\equiv 0, \pm 1 \pmod{\frac{1}{2}(p+1)}.$$

In fact, if $p \equiv 1 \pmod 4$, then $(p-1)/4$ does not divide N, and, if $p \equiv 3 \pmod 4$, then $(p+1)/4$ does not divide N.

PROOF. If $p \equiv 1 \pmod 4$, then, by Lemma 3, $\big((p-1)/4, N\big)$ divides 2 and $\big(\frac{1}{2}(p+1), N\big) = 1$. Thus, since $p \neq 5$ or 9, $(p-1)/4 \nmid N$ and $\frac{1}{2}(p+1) \nmid N$. Similarly, if $p \equiv 3 \pmod 4$, then $\big(\frac{1}{2}(p-1), N\big) = 1$ and $\big((p+1)/4, N\big)$ divides 2; thus $\frac{1}{2}(p-1) \nmid N$ and $(p+1)/4 \nmid N$ because $p \neq 3, 7$.

Suppose $N \equiv \pm 1 \pmod{\frac{1}{2}(p-1)}$. Then $\frac{1}{2}(p-1) \mid n(n+2)$ and hence, by Lemma 4, $\frac{1}{2}(p-1) \mid 3$. This is impossible because $p \neq 3, 7$. Similarly, $N \equiv \pm 1 \pmod{\frac{1}{2}(p+1)}$ implies $\frac{1}{2}(p+1) \mid 3$ which fails because $p \neq 1, 5$. This completes the proof.

Next, for $p \geq 11$, by Lemma 7, we may define unique integers M, L by

$$N \equiv \pm M \pmod{\frac{1}{2}(p-1)}, \quad 2 \leq M \leq (p-3)/4, \tag{4.4}$$

$$N \equiv \pm L \pmod{\frac{1}{2}(p+1)}, \quad 2 \leq L \leq (p-1)/4, \tag{4.5}$$

Granted Lemma 5, it is evident that Theorem 1 is equivalent to the assertion that

$$M = L = 2. \tag{4.6}$$

We now relate these last definitions to Lemma 6.

Set $m = M - 1$, where $1 \leq m \leq (p-7)/4$, and $\ell = L - 1$, where $1 \leq \ell \leq (p-5)/4$. (Note that m and ℓ may be even or odd). Define a mapping F_n from $\mathbb{F}_p$ into itself by

$$F_n(x) = \begin{cases} f_m(x), & x \in S_1, \\ f_\ell(x), & x \in S_2, \\ x, & x \in S_0. \end{cases} \tag{4.7}$$

LEMMA 8. *For F_n defined by (4.7), (4.1) holds.*

PROOF. By Lemma 5,

$$F_n(x) = \pm f_n(x), \quad x \in S_0.$$

https://doi.org/10.4153/CJM-1994-009-8 Published online by Cambridge University Press

Suppose $x = u + u^{-1} \in S_1$, where $u^{p-1} = 1$. From (4.4)

$$N \equiv \frac{1}{2}\delta(p-1) \pm M \ (\mathrm{mod}(p-1)), \quad \delta = 0 \text{ or } 1.$$

Then

$$f_n^2(x) = \left(\frac{u^N - u^{-N}}{u - u^{-1}}\right)^2 = \left(\frac{u^{\pm M} - u^{\mp M}}{u - u^{-1}}\right)^2 = f_m^2(x),$$

since $u^{\delta(p-1)/2} = u^{-\delta(p-1)/2} = \pm 1$. Thus

$$F_n^2(x) = f_m^2(x), \quad x \in S_1.$$

Similarly, if $x = u + u^{-1} \in S_2$, where $u^{p+1} = 1$, we see from (4.5) that

$$N \equiv \frac{1}{2}\varepsilon(p-1) \pm L \ (\mathrm{mod}(p+1)), \quad \varepsilon = 0 \text{ or } 1,$$

and hence

$$f_n^2(x) = \left(\frac{u^{\pm L} - u^{\mp L}}{u - u^{-1}}\right)^2 = f_\ell^2(x)$$

since $u^{\varepsilon(p+1)/2} = u^{-\varepsilon(p+1)/2} = \pm 1$. Thus

$$F_n^2(x) = f_n^2(x), \quad x \in S_2,$$

and the result follows.

LEMMA 9. *Let $\xi = \zeta_{p-1}$, $\eta = \zeta_{p+1}$. Then, for each $r = 1, \ldots, \frac{1}{2}(p-3)$,*

$$\sum_{i=0}^{p-2} [f_m(\xi^i + \xi^{-i})]^{2r} + \sum_{j=0}^{p} [f_\ell(\eta^j + \eta^{-j})]^{2r} + 2^{2r+2} = 2(M^{2r} + L^{2r}). \tag{4.8}$$

PROOF.

$$\sum_{i=0}^{p-2} [f_m(\xi^i + \xi^{-i})^{2r}] = \sum_{\substack{i=1 \\ i \neq (p-1)/2}}^{p-2} [f_m(\xi^i + \xi^{-i})^{2r}] + [f_m(2)]^{2r} + [f_m(-2)]^{2r}$$
$$= 2 \sum_{x \in S_1} [f_m(x)]^{2r} + 2M^{2r}.$$

Similarly,

$$\sum_{j=0}^{p} [f_\ell(\eta^j + \eta^{-j})]^{2r} = 2 \sum_{x \in S_2} [f_\ell(x)]^{2r} + 2L^{2r}.$$

On the other hand, by Lemmas 6 and 8 and the definition (4.7) we have

$$\sum_{x \in S_1} [f_m(x)]^{2r} + \sum_{x \in S_2} [f_\ell(x)]^{2r} + 2^{2r+1} = 0$$

and the result follows.

The virtue of (4.8) is that we may expand $[f_t(z + z^{-1})]^{2r}$ ($t = m$ or ℓ), by means of (2.1), in powers of z (positive and negative) and use the facts that ξ and η generate cyclic groups in the following form (as in Lemma 7.3 of [5]).

LEMMA 10. *For any integer s*

$$\sum_{i=0}^{p-2} \xi^{is} = \begin{cases} 0, & \text{if } (p-1) \nmid s, \\ -1, & \text{if } (p-1) \mid s; \end{cases}$$

$$\sum_{j=0}^{p} \eta^{js} = \begin{cases} 0, & \text{if } (p+1) \nmid s, \\ +1, & \text{if } (p+1) \mid s. \end{cases}$$

5. **First deductions.** Let D be the difference $D = M - L$ and P the product $P = ML$. To prove (4.6) (and hence Theorem 1) it suffices to show that $D = 0$ and $P = 4$ *as members of* $\mathbb{F}_p$. (Note that $M \neq -2$ in $\mathbb{F}_p$ since otherwise $p - 2 \leq (p-3)/4$, by (4.4)). In this section we shall study the consequences of selecting $r = 1$ or 2 in Lemma 9.

First suppose $r = 1$. Then (4.8) can be written

$$\sum_{i=0}^{p-2} f_m^2(\xi^i + \xi^{-i}) + \sum_{j=0}^{p} f_\ell^2(\eta^j + \eta^{-j}) + 16 = 2(M^2 + L^2). \tag{5.1}$$

Expand $f_t^2(z + z^{-1})$ $(t = m, \ell)$ by (2.1) to obtain

$$f_t^2(z + z^{-1}) = z^{2t} + 2z^{2(t-1)} + \cdots + tz^2 + (t+1) + tz^{-2} + \cdots + z^{-2t}. \tag{5.2}$$

Since $2m \leq (p-7)/2 < p - 1$ and $2\ell \leq (p-5)/2 < p + 1$, it follows from Lemma 10 that when (5.2) is substituted in (5.1) (with $t = m$ and $z = \xi$ and with $t = \ell$ and $z = \eta$) only the constant term yields a non-zero contribution to the sums on the left side of (5.1). Specifically, we obtain, as an equation in $\mathbb{F}_p$,

$$-M + L + 16 = 2(M^2 + L^2)$$

which may be written

$$M^2 + L^2 + \frac{1}{2}(M - L) = 8 \tag{5.3}$$

or

$$(4M + 1)^2 + (4L - 1)^2 = 130,$$

or, as a relation in $\mathbb{F}_p$ between P and D,

$$P = 4 - \frac{D}{4} - \frac{D^2}{2}. \tag{5.4}$$

Now take $r = 2$ in (4.8): this produces

$$\sum_{i=0}^{p-2} f_m^4(\xi^i + \xi^{-i}) + \sum_{j=0}^{p} f_\ell^4(\eta^j + \eta^{-j}) + 64 = 2(M^4 + L^4). \tag{5.5}$$

Square (5.2) to obtain

$$f_t^4(z + z^{-1}) = z^{4t} + 4z^{4t-2} + \cdots + c + \cdots + z^{-4t}, \tag{5.6}$$

https://doi.org/10.4153/CJM-1994-009-8 Published online by Cambridge University Press

where

$$c = 2(1^2 + 2^2 + \cdots + t^2) + (t+1)^2$$
$$= \frac{T(2T^2+1)}{3}, \quad T = t+1.$$

Since $4m \le p-7 < p-1$ and $4\ell \le p-5 < p+1$, we again need only take account of the constant term in (5.6) when substituting in (5.5). Accordingly, by Lemma 10, in $\mathbb{F}_p$ we have

$$M^4 + L^4 + \frac{M^3 - L^3}{3} + \frac{M-L}{6} = 32; \tag{5.7}$$

in terms of D and P this becomes

$$D^4 + 4PD^2 + 2P^2 + \frac{D^3}{3} + PD + \frac{D}{6} = 32. \tag{5.8}$$

Eliminating P from (5.8) by means of (5.4) we deduce that

$$12D^4 + 16D^3 - 189D^2 - 4D = 0.$$

Hence either $D = 0$ (so that, from (5.4), $P = 4$ and we are finished) or, as an equation in $\mathbb{F}_p$,

$$12D^3 + 16D^2 - 189D - 4 = 0. \tag{5.9}$$

If (5.9) is insoluble in $\mathbb{F}_p$ the proof is complete. Obviously, however, for infinitely many primes p, (5.9) has a solution in $\mathbb{F}_p$. Thus we require also to investigate (4.8) when $r = 3$. The details follow in the next section.

6. **Further working.** Since $p \ge 11$ we may take $r = 3$ in Lemma 9. The algebraic manipulation, however, becomes considerably greater. Moreover, the normalisation of Section 4 no longer guarantees that we need only have regard for the constant term in the expansion of f_t^6; the coefficient of $z^{\pm(p\pm 1)}$ may also be significant. Nevertheless, with some effort, we are able to show that no further values of r are required to ensure that $D = 0$. We proceed with the details.

When $r = 3$, (4.8) becomes

$$\sum_{i=0}^{p-2} f_m^6(\xi^i + \xi^{-i}) + \sum_{j=0}^{p} f_\ell^6(\eta^j + \eta^{-j}) + 256 = 2(M^6 + L^6). \tag{6.1}$$

We require some facts on the expansion of $f_t^6(z + z^{-1})$.

LEMMA 11. *For any non-negative even integer $j \le 6t$ let c_j denote the coefficient of z^j (or of z^{-j}) in the expansion of $f_t^6(z + z^{-1})$. Then*

$$c_0 = \frac{T(11T^4 + 5T^2 + 4)}{20}, \quad T = t+1. \tag{6.2}$$

https://doi.org/10.4153/CJM-1994-009-8 Published online by Cambridge University Press

Further, if $j \geq 4t$ and $J = \frac{1}{2}(6t-j)$, then

$$c_j = \frac{(J+1)(J+2)(J+3)(J+4)(J+5)}{120} = \binom{J+5}{5}. \tag{6.3}$$

PROOF. Cube (5.2). The constant term arises from products

$$(a+1)(b+1)z^{4t-2(a+b)}.(c+1)z^{-(2t-2c)}, \quad 0 \leq a,\, b, c \leq t,$$

where $4t-2(a+b)-2t+2c = 0$ (*i.e.* $c = a+b-t$) together with those obtained by substituting z^{-1} for z. This yields

$$c_0 = 6 \sum_{\substack{0 \leq a,b \leq t \\ a+b \geq t}} (a+1)(b+1)(a+b-t+1) - 6\sum_{a=0}^{t}(a+1)^2(t+1) + (t+1)^3$$

and leads to (6.2) with some calculation. (The reader might care to verify a few cases by means of computer algebra, for example).

For (6.3) the restriction that $j \geq 4t$ means that all relevant terms are products

$$(a+1)(b+1)(c+1)a^{6t-2(a+b+c)}, \quad 0 \leq a,\, b, c \leq t,$$

where $j = 6t-2(a+b+c)$. Thus

$$c_j = \sum_{\substack{0 \leq a,b,c \leq t \\ a+b+c = J}} (a+1)(b+1)(c+1)$$

which leads to (6.3) after further calculation.

In a discussion of (6.1), if $m < (p-1)/6$ and $\ell < (p+1)/6$ (*i.e.* $M < (p+5)/6$ and $L < (p+7)/6$), only the constant terms in $f_t^6(z+z^{-1})$, $t = m, \ell$, matter. We deal with this situation in case (i) below. When other values of M ($\leq (p-3)/4$) or L ($\leq (p-1)/4$) are involved (as permitted by (4.4) and (4.5)) we also need to take into account the coefficients of $z^{\pm(p-1)}$ and/or of $z^{\pm(p+1)}$, respectively. This occurs in cases (ii) and (iii).

CASE (i). $m < (p-1)/6$, $\ell < (p+1)/6$.

In this case, by Lemma 10 and (6.2), (6.1) yields

$$M^6 + L^6 + \frac{1}{2}\left\{\frac{M(11M^4+5M^2+4)}{20} - \frac{L(11L^4+5L^2+4)}{20}\right\} = 128. \tag{6.4}$$

Plainly (6.4) can be written as a polynomial relation (of degree 6 in D). Eliminating P by means of (5.4) we derive a polynomial in D of degree 6 and zero constant term. Specifically, this shows that either $D = 0$ or

$$960D^5 + 1564D^4 - 18560D^3 - 10435D^2 + 60220D + 2816 = 0 \tag{6.5}$$

(after multiplication by -640 to make the coefficients integral). (Again this could be checked by computer algebra).

The proof is therefore complete in this case unless p is a prime for which the polynomials in (5.9) and (6.5) have a common root D. In fact, by means of the package PARI, we calculated this resultant to be

$$17,921,557,947,801,600 = 2^{13}.\,3^2.\,5^2.\,5569.\,1,745,927$$

(its prime decomposition). Thus there is a common root when $p\ (\geq 11) = p_1 = 5569$ or $p_2 = 1,745,927$.

Suppose $p = p_1$. Again using PARI we found the common root to be $D = 14$ (or -5555 if, as positive integers, $M < L$) so that (as a member of $\mathbb{F}_p$), $P = 2687$. Hence $D^2 + 4P = (M+L)^2 = 5375$ in $\mathbb{F}_p$. But 5375 is a non-square in F_{p_1}. Hence *integers* M, L do not exist with $(M+L)^2 = 5375$ (in $\mathbb{F}_p$). Thus no exceptional PPf_n arises in this way.

The possibility that $p = p_2$ can be discarded in similar fashion. In this case the common root is $D = 94,134$ which means that, in $\mathbb{F}_p$, $P = 1,407,182$ and $D^2 + 4P = (M+L)^2 = 1,021,378$, a *non-square* in $\mathbb{F}_{p_2}$. This completes case (i).

CASE (ii). $(p-1)/6 \leq m \leq (p-7)/4, (p+1)/6 \leq \ell \leq (p-5)/4$. (Hence $p \geq 17$).
By Lemma 10, (4.8) with $r = 3$ now yields

$$M^6 + L^6 + \frac{1}{2}\big(c_0(m) - c_0(\ell)\big) + c_{p-1}(m) - c_{p+1}(\ell) = 128, \tag{6.6}$$

where $c_j(t)$ is the coefficient of z^j (and of z^{-j}) in $f_t^6(z + z^{-1})$. In deriving (6.4) in case (i) the term $c_{p-1}(m) - c_{p+1}(\ell)$ was zero, but in this case, by (6.3) we have

$$120c_{p-1}(m) = \Big(3M - \frac{3}{2}\Big)\Big(3M - \frac{1}{2}\Big)\Big(3M + \frac{1}{2}\Big)\Big(3M + \frac{3}{2}\Big)\Big(3M + \frac{5}{2}\Big) \tag{6.7}$$

and

$$120c_{p+1}(\ell) = \Big(3L - \frac{5}{2}\Big)\Big(3L - \frac{3}{2}\Big)\Big(3L - \frac{1}{2}\Big)\Big(3L + \frac{1}{2}\Big)\Big(3L + \frac{3}{2}\Big). \tag{6.8}$$

It follows that there is a polynomial $G(x)$ (where $1920G$ has integral coefficients) such that the difference $c_{p-1}(m) - c_{p+1}(\ell)$ has the form

$$3\big(MG(M^2) - LG(L^2)\big) + \frac{5}{2}\big(G(M^2) + G(L^2)\big)$$

and so can be expressed as a polynomial in D and P. When this is calculated explicitly, multiplied by -640 and added to D times the left hand side of (6.5), we deduce from (6.6) that D satisfies (over $\mathbb{F}_p$) the sextic

$$960D^6 + 1888D^5 - 18560D^4 - 11200D^3 + 72640D^2 + 92203D - 32175 = 0. \tag{6.9}$$

Note that, this time, since $p \geq 17$, (6.9) does not allow the conclusion $D = 0$. Indeed, the proof is complete in this case unless p is a prime for which the polynomials in (5.9) and (6.9) have a common root D. Their resultant is

$$40,096,467,800,319,150,683,136 \quad (= 4.0\cdots \times 10^{22})$$

which has prime decomposition

$$2^{10}.\,3^2.\,29.\,4217.\,6709.\,5,302,787,933 = 2^{10}.\,3^2 p_1 p_2 p_3 p_4,$$

say, where p_1 $(= 29), \ldots, p_4$ are the remaining primes (in increasing order). By further use of PARI we calculate that the common root D in the four cases is

$$\begin{cases} D = 6 \text{ in } \mathbb{F}_{p_1}, \\ D = 2333 \text{ in } \mathbb{F}_{p_2}, \\ D = 1592 \text{ in } \mathbb{F}_{p_3}, \\ D = 4,295,621,420 \text{ in } \mathbb{F}_{p_4}. \end{cases} \tag{6.10}$$

When, for example, $p = p_1$, this means that $D = 6$ if the integer M exceeds L and $D = -23$ if M is less than L and similarly in the other cases. On the other hand, the range of values assumed by m and ℓ in this case implies that $|m - \ell| = |M - L| = |D| < p/12$. Yet, in each case in (6.10), the positive integers D and $p_j - D$ both exceed $p_j/12, j = 1, \ldots, 4$. We conclude that for no prime p does (5.9) and (6.9) have a common root with the corresponding m, ℓ in the indicated ranges. Hence the proof in this case is complete.

CASE (iii). (a) $(p-1)/6 \leq m \leq (p-7)/4$, $\ell < (p+1)/6$ $(p \geq 19)$, or
(b) $m < (p-1)/6$, $(p+1)/6 \leq \ell \leq (p-5)/4$ $(p \geq 17)$.
This time, in addition to the cubic equation (5.9) satisfied by D over $\mathbb{F}_p$, the condition derived from (4.8) with $r = 3$ analogous to (6.5) or (6.9) naturally involves M or L as well as D; it is not easy to eliminate explicitly M or L. Accordingly we define the non-zero integer Q by

$$Q = \begin{cases} M, & \text{if (a) holds,} \\ -L, & \text{if (b) holds.} \end{cases}$$

Then certainly (since we can assume $D \neq 0$)

$$\begin{cases} 0 < D < Q < p/4, & \text{if (a) holds,} \\ -p/4 < Q < D < 0, & \text{if (b) holds.} \end{cases}$$

In this case (4.8) with $r = 3$ implies that an equation like (6.6) is valid except that the term $-c_{p+1}(\ell)$ is omitted when (a) holds and the term $c_{p-1}(m)$ is omitted when (b) holds. Further we see from (6.7) and (6.8) that the term $c_{p-1}(m)$ or $-c_{p+1}(\ell)$ (respectively) which remains takes the form

$$\left\{\left(3Q - \frac{3}{2}\right)\left(3Q - \frac{1}{2}\right)\left(3Q + \frac{1}{2}\right)\left(3Q + \frac{3}{2}\right)\left(3Q + \frac{5}{2}\right)\right\}\Big/120$$

in either case. Multiplying through by 1280, we derive (in analogy to (6.9)) the equation

$$f(Q, D) = 0, \tag{6.12}$$

over $\mathbb{F}_p$, where

$$f(Q,D) = 2592Q^5 + 2160Q^4 - 720Q^3 - 600Q^2 + 18Q + 15 \\ - (1920D^6 + 3128D^5 - 37120D^4 - 20870D^3 + 120440D^2 + 5632D).$$

Moreover,

$$4Q^2 - 4QD = 4P = 16 - D - 2D^2$$

by (5.4). Hence in $\mathbb{F}_p$,

$$g(Q, D) = 0, \tag{6.13}$$

where

$$g(Q, D) = 4Q^2 - 4QD + 2D^2 + D - 16.$$

For reference we also write the trinomial equation (5.9) as

$$h(D) = 0.$$

Suppose there are integers $D = D_0$, $Q = Q_0$ (subject to (6.11)) satisfying (5.9), (6.12) and (6.13). Then $f(Q, D_0)$ and $g(Q, D_0)$ have a common root in $\mathbb{F}_p$, namely $Q = Q_0$. Thus the resultant of f and g as polynomials in Q with coefficients in $\mathbb{F}_p[D]$ (which resultant is a polynomial in D), itself has a root $D = D_0$. Now, very conveniently, PARI could calculate the resultant of f and g as $R(D)$, where

$$\begin{aligned} R(D) = {} & 3774873600D^{12} + 13573816320D^{11} - 131528622080D^{10} \\ & - 340313128960D^9 + 1704016117760D^8 + 2064134430720D^7 \\ & - 9471958415360D^6 + 1591540812800D^5 + 21370601518080D^4 \\ & - 22233526876160D^3 - 6079909376000D^2 + 2590552673280D \\ & - 5045962521600. \end{aligned}$$

Next, since the polynomials h and R have a common root $D = D_0$ in $\mathbb{F}_p$, their resultant must be zero in the field. Again PARI was sufficient to calculate this resultant (ignoring its sign) as

$$13,117,496,913,601,213,844,923,052,653,971,935,231,744,566,886,400,000,$$

a number with 53 digits and prime decomposition

$$2^{49}3^6 5^5 11 p_1 p_2 p_3,$$

where

$$p_1 = 31,\ p_2 = 424,928,167,\ p_3 = 70,588,464,402,288,705,233.$$

From the above, the proof is complete unless $p = p_1$, p_2 or p_3. We treat each of these in turn beginning with a calculation of D_0. First, when $p = p_1 = 31$ then $D_0 = 9$ and neither possibility indicated in (6.11) can hold. Next, when $p = p_2$

$$D_0 = 380,858,452 = -44,069,715,$$

which (by (6.11)) means that $D < 0$, *i.e.* (b) holds and $Q = -L$. Further, the roots L of $f(-L, D_0)$ in $\mathbb{F}_p$ are $124, 277, 976$ and $424, 928, 167$ neither of which yields a value of L compatible with (b). Finally, when $p = p_3$,

$$D_0 = 55, 163, 881, 953, 837, 280, 929$$

which again is consistent with (6.11) only if (b) holds and $Q = -L$. In fact, the common root of $f(Q, D_0)$ and $g(Q, D_0)$ was calculated to be

$$Q = -L = 1, 763, 423, 151, 823, 514, 026,$$

which, of course, can only lead to a value of L outside the permitted range.

In summary, we see from the above that there are no "freak" values of p and n for which (4.2) holds for $r \leq 3$. Had there been, while, in principle, it would have been possible to use (4.8) with $r = 4$, in practice it would have been a daunting task to accomplish this even for a particular n and prime p (of the order of p_3 above, say). Thus, with some relief, we can say that the proof of the conjecture is complete.

REFERENCES

1. O. J. Brison, *On group permutation polynomials*, Portugal. Math. **50**(1993), 365–383.

2. M. Fried and R. Lidl, *On Dickson polynomials and Rédei functions*, Proc. Salzburg Conf., Contributions to General Algebra **5**, Springer-Verlag Hölder-Pichler-Tempsky, Wien, 1987, 139–149.

3. N. S. James and R. Lidl, *Permutation polynomials on matrices*, Linear Algebra Appl. **96**(1987), 181–190.

4. R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly **95**(1988), 243–246.

5. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclo. Math. Appls. **20**, Addison-Wesley, Reading, Massachusetts, 1983.

6. R. W. Matthews, *Permutation polynomials in one and several variables*, Ph.D. Dissertation, University of Tasmania, 1982.

7. G. L. Mullen, *Dickson polynomials over finite fields*, Adv. in Math. (Beijing) **20**(1991), 24–32.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW
Scotland