Canad. Math. Bull. Vol. 33 (2), 1990

PROOF OF A CONJECTURE OF CHOWLA AND ZASSENHAUS ON PERMUTATION POLYNOMIALS

BY
STEPHEN D. COHEN

ABSTRACT. The following conjecture of Chowla and Zassenhaus (1968) is proved. If $f(x)$ is an integral polynomial of degree $\geqq 2$ and p is a sufficiently large prime for which f (considered modulo p) is a permutation polynomial of the finite prime field F_p, then for no integer c with $1 \leqq c < p$ is $f(x)+cx$ a permutation polynomial of F_p.

1. **Introduction.** A *permutation polynomial* (PP) of the finite field F_p of prime order p is one which, regarded as a mapping, permutes the elements of F_p. The conjecture of Chowla and Zassenhaus ennunciated in the abstract featured recently as Problem P8 in a list of open problems on PP by Lidl and Mullen [3]. We prove it here in the following more precise form.

THEOREM 1. *Let $f(x)$ be a polynomial with integral coefficients and degree $n \geqq 2$. Then, for any prime $p > (n^2-3n+4)^2$ for which f (considered modulo p) is a PP of degree n of F_p, there is no integer c with $1 \leqq c < p$ for which $f(x)+cx$ is also a PP of F_p.*

A *complete mapping polynomial* (CMP) $f(x)$ of F_p is one for which both $f(x)$ and $f(x)+x$ are PPs of F_p. In terms of CMPs, Theorem 1 can clearly be expressed in the following equivalent form.

THEOREM 2. *If $n \geqq 2$ and $p > (n^2-3n+4)^2$, then there is no CMP of degree n over F_p.*

Partial results along the lines of Theorems 1 and 2 are known; usually these extend to PPs over general finite fields (not necessarily of prime order). For example, Niederreiter and Robinson [6, Theorem 9] proved that, if $p > (n^2-4n+6)^2$, then ax^n+bx ($n \geqq 2$, $a \neq 0$) cannot be a CMP of F_p. According to Mullen and Niederreiter [5], a similar conclusion applies, provided $p > (9n^2-27n+22)^2$, to any polynomial $bD_n(a,x)+cx$ ($n \geqq 2$, $ab \neq 0$), where $D_n(a,x)$ is the Dickson polynomial defined by

$$D_n(a,x) = \sum_{j=0}^{[n/2]} \frac{n}{(n-j)} \binom{n-j}{j} (-a)^j x^{n-2j}. \tag{1}$$

Received by the editors October 24, 1988 and, in revised form, May 9, 1989.
AMS 1980 Subject Classification: 12C05.
© Canadian Mathematical Society 1988.

https://doi.org/10.4153/CMB-1990-036-3 Published online by Cambridge University Press

These results required the Lang-Weil theorem (equivalent to the Riemann hypothesis for function fields). By contrast, through an elementary discussion strictly applicable to F_p, Wan Daqing [8, Theorem 1.3] proved that $ax^n + bx$ ($n \geqq 2$, $a \neq 0$) is not a CMP of F_p whenever $p > (n-1)^2$.

In our proof, we not only rely on the Lang-Weil theorem, but appeal to a deep theorem of Fried [2, Theorem 1] used in his proof of the "Schur conjecture". Actually, in order to work solely with *monic* polynomials, we prove the following minor variant of Theorem 2.

THEOREM 2$'$. *If $n \geqq 2$ and $p > (n^2 - 3n + 4)^2$, then there is no monic PP of F_p of degree n for which $f(x) + cx$ is also a PP of F_p for some c ($\neq 0$) in F_p.*

We note that, whenever $p > n$, given a PP or CMP of F_p of degree n, by performing a suitable linear translation $x \longmapsto x + c$ ($c \in F_p$), we obtain another whose coefficient of x^{n-1} is zero. A polynomial with this last property is called *normalised*. We assume throughout that f is a monic, normalised polynomial of degree $n \geqq 2$ and, where relevant, $p > n$. As regards references to the literature, instead of offering an extensive list of original sources, where possible we quote the relevant section of [4].

2. **Classification of PPs of** F_p. Given f, define

$$f^*(x,y) = \frac{f(x) - f(y)}{x - y}. \tag{2}$$

f is said to be *exceptional* over F_p if no factor of $f^*(x,y)$ in $F_p[x,y]$ is absolutely irreducible. It is well-known that there is a strong connection between PPs and exceptional polynomials over F_p [4, Section 7.4]. We summarise the relevant facts.

LEMMA 3. *If f is exceptional over F_p, then n is odd and f is a PP of F_p. Conversely, if $p > (n^2 - 3n + 4)^2$ and f is a PP of F_p, then f is exceptional (and consequently n is odd).*

PROOF. For the first implication see [4, Theorem 7.27 (and note on p. 385), Corollary 7.32]. The converse comes from [4, Theorem 7.29 and the proof of Lemma 7.28 with $c(d) = d^2$ (p. 331)]. This yields the result provided $p > (n-1)(n-2)p^{1/2} + n^2 + n$, i.e.

$$p^{1/2} > \{(n^2 - 3n + 2) + (n^4 - 6n^3 + 17n^2 - 8n + 4)^{1/2}\}/2.$$

However, this is implied by the condition

$$p^{1/2} > (n^2 - 3n + 4) = \{(n^2 - 3n + 2) + (n^4 - 6n^3 + 21n^2 - 36n + 36)^{1/2}\}/2$$

whenever $n > 5$. Special considerations could be applied when $n \leqq 5$ but in any case all PPs of degree $\leqq 5$ are known [4, Table 7.1] and none invalidate the lemma. □

Fried [2, Theorem 1] showed, in essence, that exceptional polynomials which are (functionally) indecomposable over F_p are either cyclic polynomials x^n or Dickson

https://doi.org/10.4153/CMB-1990-036-3 Published online by Cambridge University Press

polynomials having the form (1): by way of explanation here, we recall that f is *decomposable* if there are polynomials f_1 and f_2 of F_p of degree exceeding 1 such that $f = f_2(f_1)$. To assist our statement of this result, we precede it by a simple lemma that applies to decompositions (as above) even when one of f_1 and f_2 is linear.

LEMMA 4. *Suppose that f is a monic, normalised polynomial over F_p of degree n, where $p > n \geqq 2$ and that f decomposes as $f = f_2(f_1)$ over F_p, where, for $i = 1, 2$, $n_i = \deg f_i$ and $n = n_1 n_2$. Then f_1 and f_2 can also be regarded as monic, normalised polynomials over F_p; if so and if $f_1(x) = x^{n_1} + \alpha x^{n_1 - t} + \ldots$, then $f(x) = x^n + n_2 \alpha x^{n-t} + \ldots$.*

PROOF. Suppose, in fact that $\beta\,(\neq 0)$ is the leading coefficient of f_1. Replacing $f_1(x)$ and $f_2(x)$ by $\beta^{-1} f_1(x)$ and $f_2(\beta x)$, respectively, yields f_1 monic and hence f_2 monic (because f is). Denoting the coefficient of $x^{n_2 - 1}$ in f_2 by γ, we substitute $f_1(x)$ for $f_1(x) + n_2^{-1}\gamma$ and $f_2(x)$ for $f_2(x - n_2^{-1}\gamma)$ and find that f_2 is normalised. This being so, the final assertion of the lemma is an elementary calculation; in particular, certainly f_1 must be a normalised polynomial. □

A version of Fried's theorem follows: the reader should consult [7, Section 3] for a discussion which resolves some ambiguities in [2].

LEMMA 5. *Suppose that f is a monic, normalised, indecomposable polynomial of degree n over F_p, where $p > n \geqq 2$. Then, either*

(i) $f(x) = x^n + \alpha$, $\alpha \in F_p$,

(ii) $f(x) = D_n(a, x) + \alpha$, $a\,(\neq 0)$, $\alpha \in F_p$, *or*

(iii) $f^*(x, y)$ (*defined by* (2)) *is absolutely irreducible over* $F_p[x, y]$.

PROOF. This is immediate from [2, Theorem 1] using Lemma 4 to ensure normalisation and to cope with linear composition factors; note that the monic polynomial $b^{-n} D_n(a, bx)$, $ab \neq 0$, is the same as $D_n(ab^{-2}, x)$. □

COROLLARY 6. *Suppose that f is a monic, normalised PP of F_p of (odd) degree $n \geqq 3$ and $p > (n^2 - 3n + 4)^2$. Then $f = f_2(f_1)$ where, for $i = 1, 2$, f_i is a monic normalised polynomial of degree n_i, $n = n_1 n_2$ and, for some integers m_1, m_2 with $m_1 m_2 = n_1 \geqq 3$,*

$$f_1(x) = D_{m_1}(a, x^{m_2}) + \alpha, \quad a\,(\neq 0), \quad \alpha \in F_p. \tag{3}$$

Moreover, in (3), *if $m_1 = 1$ (whence $f_1(x) = x^{n_1} + \alpha$) we can assume $\alpha \neq 0$ unless $f(x) = x^n$.*

PROOF. Decompose f as $f = \hat{f}_r \circ \ldots \circ \hat{f}_1$, where each $\hat{f}_i$ ($i \leqq r$) is a monic normalised indecomposable polynomial of degree > 1. (No question of uniqueness matters here.) Each $\hat{f}_i$ is evidently a PP and consequently is exceptional by Lemma 3. Hence $\hat{f}_i$ has the form governed by Lemma 5. In particular, the result claimed is obtained by setting $f_1 = \hat{f}_s \circ \ldots \circ \hat{f}_1$ for some $s \leqq r$. □

https://doi.org/10.4153/CMB-1990-036-3 Published online by Cambridge University Press

3. **Proof of theorems.** Suppose, contrary to Theorem 2′, f is a monic, normalised PP of F_p of odd degree n ($\geqq 3$), where $p > (n^2 - 3n + 4)^2$ and $g(x) = f(x) + cx$, c ($\neq 0$) $\in F_p$, is also a PP of F_p. By means of Corollary 6, write $f = f_2(f_1)$, $g = g_2(g_1)$, where f_2 and g_2 are normalised and

$$(4)\qquad \left.\begin{array}{lll} f_1(x) = D_{k_1}(a, x^{k_2}) + \alpha, & a(\neq 0), \alpha \in F_p, & k(= k_1 k_2) \geqq 3, \\ g_1(x) = D_{m_1}(b, x^{m_2}) + \beta, & b(\neq 0), \beta \in F_p, & m(= m_1 m_2) \geqq 3. \end{array}\right\}$$

Indeed, in (4) if $k_1 = 1$, then $\alpha \neq 0$ unless $f(x) = x^n$ and there is a similar proviso for g. We consider three cases.

CASE (i). $k_1 = m_1 = 1$. Then, identically,

$$(5)\qquad cx = g_2(x^m + \beta) - f_2(x^k + \alpha).$$

We derive from the fact that the coefficient of x on the right side of (5) is non-zero the conclusion that either $m = 1$ or $k = 1$, contrary to (4).

CASE (ii). $m_1 > 1$, $k_1 = 1$. Lemma 4 yields

$$(6)\qquad \begin{aligned} cx &= g_2(x^m - m_1 bx^{m-2m_2} + \ldots + \beta) - f_2(x^k + \alpha) \\ &= -nm_2^{-1} bx^{n-2m_2} + \ldots - nk^{-1}\alpha x^{n-k} - \ldots. \end{aligned}$$

Because $n - 2m_2$ is odd and $n - k$ is even, when $\alpha \neq 0$, (6) implies that $n - 2m_2 = 1$ and $n - k = 0$. Further, by assumption, when $\alpha = 0$, $k = n$ and again it must be that $n - 2m_2 = 1$. Thus m_2 (a divisor of n) equals 1 and hence $n = 3 = m_1$. This contradicts the truth that $D_3(b, x)$, $b \neq 0$, cannot be a PP [4, Theorem 7.16].

CASE (iii). $m_1 > 1$, $k_1 > 1$. Now we derive from Lemma 4,

$$(7)\qquad \begin{aligned} cx &= g_2(x^m - m_1 bx^{m-2m_2} + \ldots) - f_2(x^k - k_1 ax^{k-2k_2} + \ldots) \\ &= G(x^{m_2}) - F(x^{k_2}), \quad \text{say,} \end{aligned}$$

$$(8)\qquad = (-nm_2^{-1} bx^{n-2m_2} + \ldots) + (nk_2^{-1} ax^{n-2k_2} - \ldots).$$

Let d be the highest common factor of k_2 and m_2. By (7), x is a polynomial function of x^d; hence $d = 1$. On the other hand, since as in case (ii), neither $n - 2m_2 = 1$ nor $n - 2k_2 = 1$, (8) implies that $n - 2m_2 = n - 2k_2 > 1$. Thus $k_2 = m_2$ and so $k_2 = m_2 = 1$. Hence $k = k_1$, $m = m_1$ and, crucially, by (8), $a = b$. Applying the identity

$$D_k\left(a, x + \frac{a}{x}\right) = x^k + \frac{a^k}{x^k}$$

[4, formula (7.8)] we deduce that

$$(9)\qquad \begin{aligned} cx^{n-1}(x^2 + a) &= x^n g\left(x + \frac{a}{x}\right) - x^n f\left(x + \frac{a}{x}\right) \\ &= x^n g_2\left(x^m + \frac{a^m}{x^m} + \beta\right) - x^n f_2\left(x^k + \frac{a^k}{x^k} + \alpha\right) \\ &= G(x^m) - F(x^k) \end{aligned}$$

https://doi.org/10.4153/CMB-1990-036-3 Published online by Cambridge University Press

for some polynomials F, G. Because the right side of (9) must contain the non-zero term cx^{n+1}, either k or m must divide $n+1$. Yet each of these is also a divisor of n. Thus either k or $m = 1$, contradicting (4). This proves Theorem 2′ and Theorems 1 and 2 follow. □

Finally we remark that it would be possible to extend our theorems to include "tame" PPs over general finite fields.

References

1. S. Chowla and H. Zassenhaus, *Some conjectures concerning finite fields*, Norske Vid. Selsk. Forh. (Trondheim), **41** (1968), 34–35.

2. M. Fried, *On a conjecture of Schur*, Michigan Math. J., **17** (1970), 41–55.

3. 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.

4. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopaedia of Math. and its Appl., vol. 20, Addison-Wesley, Reading, Mass., 1983.

5. G. L. Mullen and H. Niederreiter, *Dickson polynomials over finite fields and complete mappings*, Canad. Math. Bull., **30** (1987), 19–27.

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

7. G. Turnwald, *On a problem concerning permutation polynomials*, Trans. Amer. Math. Soc., **302** (1987), 251–267.

8. Wan Daqing, *Permutation polynomials over finite fields*, Acta. Math. Sinica, New Series, **3** (1987), 1–5.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW
Scotland

https://doi.org/10.4153/CMB-1990-036-3 Published online by Cambridge University Press