PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 120, Number 1, January 1994

PERMUTATION PROPERTIES OF THE POLYNOMIALS $1 + x + \cdots + x^k$ OVER A FINITE FIELD

REX MATTHEWS

(Communicated by William Adams)

ABSTRACT. It is shown that a polynomial of the shape $1 + x + \cdots + x^k$ is a permutation polynomial over a finite field $\mathbb{F}_q$ of odd characteristic p if and only if $k \equiv 1 \bmod p(q-1)$.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field of characteristic p, with $q = p^e$, $e \geq 1$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial over $\mathbb{F}_q$ if f induces a bijection of $\mathbb{F}_q$ under substitution. In recent years interest in permutation polynomials has increased because of their use in cryptography [4]. For a comprehensive account of permutation polynomials see Lidl and Niederreiter [6, Chapter 7] and Lidl and Mullen [5] for a recent survey. If $p = 2$, the polynomials which are the subject of this paper arise in the study of ovals in the projective plane $PG(2, q)$. Although a classical result of Hermite provides a necessary and sufficient condition for a polynomial to be a permutation polynomial, it is not usually an easy matter to apply this to a given class of polynomials. Classes of polynomials whose permutation spectra have been determined include the power polynomials, the Chebyshev polynomials of the first kind [6], the cyclotomic polynomials [7], and the linearized polynomials. In the case of polynomials of the shape $1 + x + \cdots + x^k$, several classes of permutation polynomials are known in characteristic 2, and if $k = m - 1$, m prime, such a polynomial is a cyclotomic polynomial. The main result of this paper is to analyse the permutation behaviour of these polynomials in odd characteristic. The final section presents some classes of permutation polynomials that have a similar shape.

The paper is organised as follows. After the introductory definitions and lemmas the main result is established using a result of Segre on ovals in $PG(2, q)$, q odd. Section 4 contains remarks on the characteristic 2 case. The final section contains some results on other classes of permutation polynomials which generalise those considered here.

We now state the main result to be established.

Received by the editors September 22, 1991 and, in revised form, April 24, 1992.
1991 *Mathematics Subject Classification.* Primary 11T06.

Theorem 1.1. *If* q *is odd then* $h_k(x) = 1 + x + \cdots + x^k$ *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if* $k \equiv 1 \bmod p(q-1)$.

2. Notation and preliminary results

Let $k \in \mathbb{Z}$, $k \geq 0$. Let p be a prime, $q = p^e$, $e \geq 1$, and let $\mathbb{F}_q$ be the finite field of order q. By $h_k(x)$ we denote the polynomial $1 + x + \cdots + x^k$.

Lemma 2.1. *If* $k \equiv l \bmod p(q-1)$ *then* $h_k(\alpha) = h_l(\alpha)\ \forall \alpha \in \mathbb{F}_q$.

Proof. If $\alpha = 1$ then $h_k(\alpha) = k + 1 = l + 1 \bmod p$. If $\alpha \neq 1$, let $l = k + \mu p(q-1)$. Then $h_l(\alpha) = (\alpha^{l+1} - 1)/(\alpha - 1) = (\alpha^{k+1+\mu p(q-1)} - 1)/(\alpha - 1)$. Since $\alpha^{q-1} = 1$, $h_l(\alpha) = h_k(\alpha)$.

Lemma 2.2. *If* $k \equiv 1 \bmod p(q-1)$ *then* $h_k(x)$ *is a permutation polynomial over* $\mathbb{F}_q$.

Proof. $h_k(x)$ and $h_1(x)$ induce the same map on $\mathbb{F}_q$ and $h_1(x)$ is a linear permutation polynomial.

We will use the well-known criterion of Hermite [6, p. 349] for a polynomial to induce a permutation.

Lemma 2.3 (Hermite). $f \in \mathbb{F}_q[x]$, $q = p^e$, *is a permutation polynomial over* $\mathbb{F}_q$ *if and only if*:

(i) f *has exactly one root in* $\mathbb{F}_q$, *and*

(ii) *the reduction of* $f^t \bmod (x^q - x)$, $0 < t < q-1$, $t \not\equiv 0 \bmod p$, *has degree less than or equal to* $q-2$.

Lemma 2.4. *If* $h_k(x)$ *is a permutation polynomial over* $\mathbb{F}_q$, q *odd, then* $(k \bmod p(q-1)) < (q-1)$.

Proof. By Lemma 2.1 it suffices to consider $k < p(q-1)$. If $k \geq (q-1)$ then when $h_k(x)$ is reduced $\bmod (x^q - x)$ the coefficient of x^{q-1} is $[k/(q-1)]$, which is not zero $\bmod p$. By Lemma 2.3 with $t = 1$, $h_k(x)$ is not a permutation polynomial.

Lemma 2.5. *Suppose* $h_k(x)$ *is a permutation polynomial over* $\mathbb{F}_q$. *Then* $(k, q-1) = 1$. *If* q *is even then* $(k+1, q-1) = 1$ *else* $(k+1, q-1) = 2$. *If* q *is even then* $k + 1 \equiv 0 \bmod p$ *else* $k + 1 \not\equiv 0 \bmod p$.

Proof. We note that $h_k(0) = 1$ and so $h_k(1) \neq 1$, $h_k(1) = (k+1) \bmod p$, and $k \not\equiv 0 \bmod p$. Assume q odd. If $x \neq 1$, then $h_k(x) = (x^{k+1} - 1)/(x - 1)$. The solutions of $h_k(x) = 1$ are the solutions of $x^{k+1} = x$ less the solution $x = 1$, so there are $(k, q-1)$ solutions to $h_k(x) = 1$. As $h_k(x)$ is a permutation polynomial $(k, q-1) = 1$. Now consider the solutions to $h_k(x) = 0$. If $(k+1) \equiv 0 \bmod p$ then $h_k(1) = 0$, and this must be the only solution to $x^{k+1} = 1$. Thus $(k+1, q-1) = 1$. These two conditions are incompatible since q is odd, so $(k+1) \not\equiv 0 \bmod p$. Thus $h_k(1) \neq 0$; hence, the equation $x^{k+1} = 1$ must have two solutions (one being 1), so $(k+1, q-1) = 2$.

If q is even then $k \not\equiv 0 \bmod p$ implies $k + 1 \equiv 0 \bmod p$, so $h_k(1) = 0$. Hence $x^{k+1} = 1$ must have 1 as its only solution and so $(k+1, q-1) = 1$. Now consider $h_k(x) = 1$. The solutions of $x^{k+1} = x$ are 0 and $(k, q-1)$ other solutions, one of which is 1. Since no other solutions to $h_k(x) = 1$ are allowed, we have $(k, q-1) = 1$.

Lemma 2.6. *If $h_k(x)$ is a permutation polynomial over $\mathbb{F}_q$, q odd, then $k < (q-1)/2$.*

Proof. Consider $(h_k(x))^2$. If $t \leq k$ then the coefficient of x^t in this expansion is $(t+1)$. Suppose $k \geq (q-1)/2$. Since $k < (q-1)$, the coefficient of x^{q-1} in the expansion of $(h_k(x))^2$ equals the coefficient of $x^{(2k-q+1)}$ in this expansion. Since $(2k-q+1) < k$, this coefficient is $(2k-q+2)$. As the highest degree term in the expansion is x^{2k}, no other terms reduce to x^{q-1}. Thus the coefficient of the term in x^{q-1} is $(2k+2) \bmod p$. By Lemma 2.5 this is not zero as q is odd. Thus $h_k(x)$ fails the Hermite criterion for $t = 2$.

In $PG(2, q)$, the projective plane of order q with q odd, an oval is defined as a set of $(q+1)$ points, no three of which are collinear. A famous theorem of Segre [8] connects this combinatorial definition with an algebraic one.

Lemma 2.7 (Segre). *An oval in $PG(2, q)$, q odd, is an irreducible conic.*

3. Proof of Theorem 1.1

Assume q odd. The method of this proof is to construct an oval in $PG(2, q)$ under the assumption that $h_k(x)$ is a permutation polynomial. By Segre's theorem this oval is an irreducible conic. We then deduce that $k = 1$.

Suppose that $PG(2, q)$ is coordinatised as triples (x, y, z); see [3].

Let $O_k = \{(c^{k+1}, c, 1) : c \in \mathbb{F}_q\} \cup \{(1, 0, 0)\}$ and assume that $h_k(x)$ is a permutation polynomial over $\mathbb{F}_q$. O_k contains $q+1$ points. We show that O_k is an oval by showing that no three points of O_k are collinear. Consider first a line passing through $(1, 0, 0)$. Such a line L has a projective equation $ay + cz = 0$. There is a unique point on L with $z = 1$, so L can meet O_k at only one point other than $(1, 0, 0)$. Now consider a line L passing through three points on O_k obtained by letting c take the distinct values α, β, γ. Then the determinant

$$\Delta = \begin{vmatrix} \alpha^{k+1} & \alpha & 1 \\ \beta^{k+1} & \beta & 1 \\ \gamma^{k+1} & \gamma & 1 \end{vmatrix}$$

is zero.

Then $\Delta = (\beta^{k+1} - \alpha^{k+1})(\gamma - \alpha) - (\gamma^{k+1} - \alpha^{k+1})(\beta - \alpha)$.

Since not all of α, β, γ are 0, we may assume wlog that $\alpha \neq 0$. Then

$$\Delta = \alpha^{k+2}\left\{\left[\left(\frac{\beta}{\alpha}\right)^{k+1} - 1\right]\left[\frac{\gamma}{\alpha} - 1\right] - \left[\left(\frac{\gamma}{\alpha}\right)^{k+1} - 1\right]\left[\frac{\beta}{\alpha} - 1\right]\right\}.$$

If $\Delta = 0$ then substituting $\beta' = \beta/\alpha$, $\gamma' = \gamma/\alpha$, we have $\beta' \neq 1$, $\gamma' \neq 1$, $\beta' \neq \gamma'$, and $(\beta'^{(k+1)} - 1)/(\beta' - 1) = (\gamma'^{(k+1)} - 1)/(\gamma' - 1)$, so $h_k(\beta') = h_k(\gamma')$, in contradiction to the assumption that $h_k(x)$ is a permutation polynomial. O_k has now been shown to be an oval, so by Segre's theorem all the points of O_k lie on an irreducible conic. The points with $z = 1$ lie on an affine conic of the form

$$\varphi(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

with coefficients in $\mathbb{F}_q$.

Since (α^{k+1}, α) lies on this curve $\forall \alpha \in \mathbb{F}_q$,

$$(*) \qquad a\alpha^{2(k+1)} + b\alpha^{k+2} + c\alpha^2 + d\alpha^{k+1} + e\alpha + f = 0 \quad \forall \alpha \in \mathbb{F}_q.$$

By Lemma 2.6 $k \leq (q-3)/2$, so $2(k+1) \leq (q-1)$, and all terms in $(*)$ have exponents less than q. Cancellation can only occur if $k = 1$ or $k = 0$. Thus if $k > 1$, all the coefficients a, b, c, d, e, f are zero, contradicting Segre's theorem. If $k = 1$, the term in α^2 is $(c + d)$, and in this case we conclude that $a = b = e = f = 0$ and $(c + d) = 0$, so $\varphi(x, y) = y^2 - x$.

In this case where $q = p$ or $q = p^2$ the author has obtained another proof of Theorem 1.1 which uses Hermite's criterion alone.

4. The case of characteristic 2

In characteristic 2 an oval is defined as a set of $(q+2)$ points, no three being collinear. For any polynomial f define $O(f)$ to be

$$\{(f(c), c, 1) : c \in \mathbb{F}_q\} \cup \{(1, 0, 0), (0, 1, 0)\};$$

see [6, §9.3]. In this case we have the following result.

Proposition 4.1. *$h_k(x)$ is a permutation polynomial over $\mathbb{F}_q$, q even, if and only if $O(x^{k+1})$ is an oval.*

To show this we quote the following result [3, 6]: $O(x^k)$ is an oval if and only if

(i) $(k, q-1) = 1$,
(ii) $(k-1, q-1) = 1$,
(iii) $[(x+1)^k + 1]/x$ is a permutation polynomial over $\mathbb{F}_q$.

To prove Proposition 4.1 we observe that Lemma 2.5 implies that conditions (i) and (ii) above are implied by (iii).

In the case of characteristic 2 there are relationships amongst the polynomials which generate ovals. If $O(x^k)$ is an oval then so is $O(x^t)$ with t equal to $1/k$, $1-k$, $1/(1-k)$, $k/(k-1)$, and $(k-1)/k$, all taken $\bmod(q-1)$. Consider such sets of ovals to be equivalent. The following classes of ovals in $\mathbb{F}_q$, $q = 2^e$, have been described [1].

(i) $O(x^2)$, which corresponds to $h_1(x)$.
(ii) $O(x^a)$, $a = 2^n$, $(n, e) = 1$. $h_{a-1}(x+1) = x^{a-1}$, which is a permutation polynomial over $\mathbb{F}_{2^e} \Leftrightarrow (2^n - 1, 2^e - 1) = 1 \Leftrightarrow (n, e) = 1$.
(iii) $O(x^6)$, e odd (Segre [9]). $h_5(x+1) = g_5(x)$, a Dickson polynomial of the first kind, which is a permutation polynomial over $\mathbb{F}_{2^e} \Leftrightarrow (5, 2^{2e} - 1) = 1 \Leftrightarrow e$ is odd. (See [6, p. 356].)
(iv) The two classes of ovals described by Glynn [1].

Ovals $O(x^k)$ inequivalent to one in (i)–(iv) do not occur when $e \leq 28$ [2], but a complete description has not yet appeared.

5. Related polynomials

In [7] Mollin and Small analysed the permutation properties of the cyclotomic polynomials. Their result is as follows.

Proposition 5.1. *The cyclotomic polynomial $\varphi_m(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $m = 2$ or both m and q are powers of 2.*

When m is prime, $\varphi_m(x) = h_{m-1}(x)$. If q is odd then Theorem 1.1 yields $m \equiv 2 \bmod p(q-1)$. If $m = \alpha p(q-1) + 2$, $\alpha \neq 0$, then $2|m$, so $m = 2$ is the only permutation polynomial, which is consistent with Proposition 5.1.

A further class of polynomials can be defined which generalise those of the title.

Define $P(l, j, k)(x) = x^l(1 + x^j + \cdots + (x^j)^k)$, $l, j, k \in \mathbb{Z}$. Then $h_k(x) = 1 + P(1, 1, k-1) = P(0, 1, k)$. If $(l, j) = d$ and $(d, q-1) > 1$ then $P(l, j, k)(x)$ is not a permutation polynomial over $\mathbb{F}_q$. If $(d, q-1) = 1$, then $P(l, j, k)(x)$ is a permutation polynomial if and only if $P(l/d, j/d, k)$ is a permutation polynomial. Thus we may suppose $d = 1$. Define $J = \{x \in \mathbb{F}_q : x^j = 1\}$.

Theorem 5.1. *The polynomial* $P(l, j, k)$, $l > 0$, $j > 0$, $(l, j) = 1$, *is a permutation polynomial over* $\mathbb{F}_q$ *if*

$$k + 1 \equiv 1 \bmod (q-1)/(j, q-1) \quad \textit{and} \quad (l, q-1) = 1 \textit{ and } (k+1) \in J$$

or

$$k + 1 \equiv -1 \bmod (q-1)/(j, q-1) \quad \textit{and} \quad (l-j, q-1) = 1 \textit{ and } (k+1) \in -J.$$

Proof. In the first case, if $x^j \neq 1$, then

$$P(l, j, k)(x) = x^l[(x^{j(k+1)} - 1)/(x^j - 1)] = x^l.$$

If $x^j = 1$, then $P(l, j, k)(x) = (k+1)x^l$. Since $(l, q-1) = 1$, the polynomial x^l permutes $\mathbb{F}_q$. Since $(l, j) = 1$, x^l maps $\mathbb{F}_q \backslash J$ to itself, as x^l permutes J. The polynomial $(k+1)x^l$ permutes J, since $(k+1) \in J$, so $P(l, j, k)(x)$ permutes $\mathbb{F}_q$. In the second case, if $x^j \neq 1$, then

$$P(l, j, k)(x) = x^l[(x^{-j} - 1)/(x^j - 1)] = -x^{l-j}.$$

If $x \in J$, then $P(l, j, k)(x) = (k+1)x^l$. The image of J under $-x^{l-j}$ is $-J$. Thus $P(l, j, k)(x)$ maps $\mathbb{F}_q \backslash J$ to $\mathbb{F}_q \backslash (-J)$, x^l permutes J, and $(k+1)x^l$ maps J to $-J$, since $(k+1) \in -J$.

References

1. D. G. Glynn, *Two new sequences of ovals in finite Desarguesian planes of even order*, Combinatorial Mathematics X (Adelaide 1982), Lecture Notes in Math., vol. 1036, Springer, New York, 1983, pp. 217–229.
2. ———, *A condition for the existence of ovals in* $PG(2, q)$, q *even*, Geometriae Dedicata **32** (1989), 247–252.
3. J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford, 1979.
4. R. Lidl and W. B. Müller, *Permutation polynomials in RSA-cryptosystems*, Adv. in Cryptology, Plenum, New York, 1984, pp. 293–301.
5. 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.
6. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, MA, 1983. (Now distributed by Cambridge Univ. Press.)
7. R. A. Mollin and C. Small, *On permutation polynomials over finite fields*, Internat. J. Math. Math. Sci. **10** (1987), 535–544.
8. B. Segre, *Ovals in a finite projective plane*, Canad. J. Math. **7** (1955), 414–416.
9. ———, *Ovali e curve* σ *nei piani di Galois di caratteristica due*, Atti. Accad. Naz. Lincei Rend. (8) **32** (1962), 785–790.

School of Information Science and Technology, The Flinders University of South Australia, GPO Box 2100, Adelaide, South Australia 5001

Current address: Department of Computer Science, The University of Queensland, Brisbane 4042, Australia

E-mail address: rex@cs.uq.oz.au