A NOTE ON PERMUTATION POLYNOMIALS AND FINITE GEOMETRIES

David GLUCK*
Department of Mathematics, Wayne State University, Detroit, Michigan 48202, USA

Received 17 July 1987
Revised 16 December 1987

A polynomial \( f \) over a finite field \( F \) is called a difference permutation polynomial if the mapping \( x \rightarrow f(x + a) - f(x) \) is a permutation of \( F \) for each nonzero element \( a \) of \( F \). Difference permutation polynomials give rise to affine planes. We show that when \( F = GF(p) \), where \( p \) is a prime, the only difference permutation polynomials over \( F \) are quadratic.

1. Introduction

Let \( F \) be a finite field of odd cardinality. A polynomial \( g \) in \( F[x] \) is called a permutation polynomial if \( g \) defines a bijective function on \( F \). We will call a polynomial \( f \) in \( F[x] \) a difference permutation polynomial if \( f(x + a) - f(x) \) is a permutation polynomial for every nonzero \( a \) in \( F \).

Difference permutation polynomials are a special case of planar functions, as defined by Dembowski [2, p. 227], and give rise to affine planes. Quadratic polynomials are clearly difference permutation polynomials, and give rise to desarguesian planes. For \( F \) a prime field, J.F. Dillon (private communication) has asked whether there are any nonquadratic difference permutation polynomials over \( F \). Such polynomials would give rise to nondesarguesian planes. An analogous question for arbitrary fields of odd cardinality is brought up in [3, p. 257].

In this note we show that every difference permutation polynomial over \( GF(p) \) is quadratic. The idea of the proof is roughly as follows. First we show that the graph of a difference permutation polynomial \( f \) is closely related to a \((p + 1)\)-arc \( K \) in the desarguesian projective plane over \( GF(p) \). Then Segre's theorem says that \( K \) is a conic. This implies that \( f \) is a quadratic polynomial.

I have been informed that the result of this paper has been independently obtained by Y. Hiramine. His proof is different from mine and was submitted for publication at about the same time.

* Research partially supported by the National Security Agency and the Deutsche Forschungsgemeinschaft.

2. Preliminaries and notation

Let \( p \) be an odd prime and let \( \zeta \) be a primitive \( p \)th root of 1. If \( f \) is a difference permutation polynomial over \( \text{GF}(p) \), let \( U \) be the circulant matrix with \((i, j)\) entry equal to \( \zeta^{f(i-j)}/\sqrt{p} \) for \( 0 \leq i, j \leq p-1 \). The definition of difference permutation polynomial implies that \( U \) is unitary.

We introduce some notation to handle certain sums of roots of unity. If \((\gamma_0, \ldots, \gamma_{p-1})\) and \((\delta_0, \ldots, \delta_{p-1})\) are \( p \)-tuples of numbers, we write \((\gamma_0, \ldots, \gamma_{p-1}) = (\delta_0, \ldots, \delta_{p-1})\) to mean there is a permutation \( \pi \) of \( \{0, \ldots, p-1\} \) with \( \gamma_i = \delta_{\pi(i)} \) for \( 0 \leq i \leq p-1 \).

A \( k \)-arc in the (desarguesian) projective plane over a field \( F \) is a set of \( k \) points, no three of which are collinear. For \(|F| \) odd, a theorem of Segre ([4], [5, p. 270]) says that every \((|F|+1)\)-arc is an irreducible conic.

3. Main theorem and proof

**Theorem.** Let \( f \) be a difference permutation polynomial over \( \text{GF}(p) \). Suppose the degree of \( f \) is less than \( p \). Then \( f \) is a quadratic polynomial.

**Lemma 1.** Let \( \zeta \) be as above. Let \( \alpha \) be an algebraic integer in \( \mathbb{Q}(\zeta) \). Then \(|\alpha| = \sqrt{p}\) if and only if \( \alpha = \pm \zeta^s (\zeta^{m(0)}, \ldots, \zeta^{m(p-1)}) \) for some integer \( s \).

**Proof.** This is [1, Theorem 1]. \( \square \)

**Lemma 2.** Let \( \delta_0, \ldots, \delta_{p-1} \) be \( p \)th roots of 1 with \( |\delta_0 + \cdots + \delta_{p-1}| = \sqrt{p} \). Then \((\delta_0, \ldots, \delta_{p-1}) = (\zeta^{m(0)}, \ldots, \zeta^{m(p-1)})\) for some quadratic polynomial \( m(x) \) in \( \text{GF}(p)[x] \).

**Proof.** Lemma 1 yields

\[
\delta_0 + \cdots + \delta_{p-1} = \pm \zeta^s (\zeta^{m(0)} + \cdots + \zeta^{m(p-1)}). 
\]

For \( 0 \leq s \leq p-1 \), let \( l_i \) be the number of indices \( j \) such that \( \delta_j = \zeta^i \) and let \( r_i \) be the number of indices \( j \) such that \( \zeta^{i+j} = \zeta^i \).

Suppose that the plus sign occurs on the right side of \((*)\). Then \( \sum l_i - \sum r_i = p \), and so \( \sum (l_i - r_i) = 0 \). Since \( \sum (l_i - r_i) \zeta^i = 0 \), and since the \( p \)th roots of 1 satisfy only one rational linear dependence relation, \( l_i - r_i \) is independent of \( i \). Hence \( l_i = r_i \) for all \( i \), and so \((\delta_0, \ldots, \delta_{p-1}) = (\zeta^{m(0)}, \ldots, \zeta^{m(p-1)})\) for \( m(x) = s + x^2 \).

Next suppose that the minus sign occurs on the right side of \((*)\). Then \( \sum l_i = \sum r_i = p \), and so \( \sum (l_i + r_i) = 2p \). Since \( \sum (l_i + r_i) \zeta^i = 0 \), \( l_i + r_i \) is independent of \( i \). Hence \( l_i + r_i = 2 \) for all \( i \). Therefore \( l_i = r_i = 1 \), \( l_i = 0 \) when \( i - s \) is a nonzero square mod \( p \), and \( l_i = 2 \) when \( i \) is not a square mod \( p \). Let \( c \) be a fixed nonsquare mod \( p \), and set \( m(x) = cx^2 + s \). Then \((\delta_0, \ldots, \delta_{p-1}) = (\zeta^{m(0)}, \ldots, \zeta^{m(p-1)}) \). \( \square \)
Lemma 3. Let $f$ be a difference permutation polynomial over $GF(p)$. Then $f$ assumes no value in $GF(p)$ more than twice.

**Proof.** The circulant matrix $U$ defined in the previous section is unitary, and so all its eigenvalues have absolute value 1. Define $M = \sqrt[p]{U}$. The all ones vector is an eigenvector for $M$, with eigenvalue $\xi^{0} + \cdots + \xi^{(p-1)}$. Since all eigenvalues of $M$ have absolute value $\sqrt[p]{p}$, Lemma 2 yields $(\xi^{0}, \ldots, \xi^{(p-1)}) = (\zeta^{m(0)}, \ldots, \zeta^{m(p-1)})$ for some quadratic polynomial $m(x)$. Since $m(x)$ assumes no value in $GF(p)$ more than twice, neither does $f$. □

Lemma 4. Let $f$ be as in Lemma 3. Let $G$ be the graph of $f$ in the (desarguesian) affine plane over $GF(p)$. Then no three points of $G$ are collinear.

**Proof.** Suppose the conclusion of the lemma is false. Then three distinct points $(x_1, f(x_1)), (x_2, f(x_2)),$ and $(x_3, f(x_3))$ lie on the same line $y = ax + b$. Let $h(x) = f(x) - (ax + b)$. Then $h(x_1) = h(x_2) = h(x_3) = 0$. On the other hand, a short computation shows that $h(x)$ is a difference permutation polynomial. By Lemma 3, $h$ assumes no value more than twice, a contradiction. □

**Proof of the theorem.** Let $G$ be as in Lemma 4. Let $x$, $y$ and $z$ be homogeneous coordinates for the (desarguesian) projective plane over $GF(p)$, so that the affine plane is identified with the set of points of the form $(x, y, 1)$. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$, with $a_n \neq 0$ and $2 \leq n \leq p - 1$. Let $g(x, y) = y - f(x)$, and let $g^*(x, y, z) = yzn - (a_0x^n + \cdots + a_{n-1}x^{n-1}z + a_nx^n)$ be the homogeneous polynomial corresponding to $g$. Let $G^*$ be the zero set of $g^*$ in the projective plane.

We have $G^* = G \cup \{(0, 1, 0)\}$. If $x_1 \neq x_2$ in $GF(p)$, then the three row vectors $[0, 1, 0], [x_1, f(x_1), 1],$ and $[x_2, f(x_2), 1]$ are linearly independent. It follows that no three points of $G^*$ are collinear. By the theorem of Segre mentioned in Section 2, $G^*$ is an irreducible conic, say with equation $k^*(x, y, z) = 0$. Let $k(x, y) = k^*(x, y, 1)$. Then the zero set of $k$ is the intersection of $G^*$ with the affine plane, which is $G$.

Thus $G$ is a conic with equation $0 = k(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$. Suppose $c \neq 0$. For a fixed value $x_0$ of $x$, the quadratic equation $k(x_0, y) = 0$ must have a unique solution for $y$, namely $y = -(bx_0 + e)/2c$. But this holds for every $x_0$, and so $G$ is a line, contradicting Lemma 4. Hence $c = 0$. Suppose $b \neq 0$. Then the equation $k(-e/b, y) = 0$ has either 0 or $p$ solutions for $y$, contradicting the fact that $G$ is the graph of a function. Hence $b = 0$. Obviously $e \neq 0$. Hence $f(x)$ is a quadratic polynomial. □
References