The Degrees of Permutation Polynomials over Finite Fields*

CHARLES WELLS

Case Western Reserve University, Cleveland, Ohio 44106

Communicated by Alan J. Hoffman

Received January 10, 1968

ABSTRACT

A number of theorems are proved concerning the connection between the cycle structure of a permutation of a finite field GF(q) and the degree of the polynomial representing it. In particular (Section 4) if $K_r$ is the set of permutations of GF(q) moving $\leq r$ elements, then, if $r$ grows slowly enough with respect to $q$ as $q \to \infty$, almost all polynomials of degree $\leq q - 1$ representing permutations in $K_r$ have degree $q - 2$.

1. INTRODUCTION

Let $\phi$ be a permutation of the elements of the finite field GF($q = p^n$). It is well known that there is a unique polynomial of degree $\leq q - 2$ which represents $\phi$ in the sense that for all $a \in$ GF($q$), $f(a) = \phi(a)$. Such a polynomial is called a permutation polynomial. In this paper some results on the degrees of permutation polynomials are presented. Each of the theorems says roughly that, if $K$ is a class of permutations which move a number of elements of GF($q$) which is small compared to $q$, then, as $q \to \infty$, the number of permutations in $K$ represented by polynomials of degree $q - 2$ is asymptotic to the number of permutations in $K$.

2. SOME SPECIAL RESULTS

Let $a, b \in$ GF($q$), $a \neq b$. It may be verified by direct substitution, using the fact that, if $r \neq 0$ in GF($q$), then $r^{q-1} = 1$, that the polynomial

\[ f(a) = x + (a - b)(x - a)^{q-1} + (b - a)(x - b)^{q-1} \]  

(1)

* Supported by NSF Grant GP 6565.
represents the transposition \((a \ b)\). Then, as in the case of any permutation polynomial \([3, \text{p. 59}]\), the coefficient of \(x^{q-1}\) is zero, so \(\deg f \leq q - 2\). But it is not hard to show that the coefficient of \(x^{q-2}\) is \((a - b)^2 \neq 0\), so that every transposition in \(\text{GF}(q)\) is represented by a unique polynomial of degree \(q - 2\).

If \((a \ b \ c)\) is a 3-cycle of elements of \(\text{GF}(q)\), it is represented by

\[
g(x) = x + (a - b)(x - a)^{q-1} + (b - c)(x - b)^{q-1} + (c - a)(x - c)^{q-1}.
\]

(2)

The coefficient of \(x^{q-2}\) here is

\[
\lambda = a(a - b) + b(b - c) + c(c - a),
\]

so that \(\lambda = 0\) if and only if \(a\) is a solution of the quadratic

\[
x^2 - (b + c) x + b^2 + c^2 - bc = 0.
\]

(3)

This has discriminant

\[
D = -3(b - c)^2,
\]

which has a square root in \(\text{GF}(q)\) if and only if \(-3\) is a square in \(\text{GF}(q)\).

We first consider the case in which \(q\) is odd. In this case \(-3\) is a square in \(\text{GF}(p)\) if and only if the Legendre symbol \((-3)/p\) is 1. But by the quadratic reciprocity law, if \(p = 1 \mod 4\), then

\[
\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)
\]

and \((p/3) = 1\) if and only if \(p = 1 \mod 3\). If \(p \equiv 3 \mod 4\), then

\[
\left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right),
\]

yielding the same result. If \(-3\) is a square in \(\text{GF}(p)\), it is a square in \(\text{GF}(p^k)\) for any \(k\). If \(-3\) is not a square in \(\text{GF}(p)\), then it is a square in \(\text{GF}(p^k)\) if and only if \(k\) is even. But \(-3\) is not a square in \(\text{GF}(p)\) if and only if \(p = 2 \mod 3\). Since in this case \(k\) is even if and only if \(p^k = 1 \mod 3\), we have that, when \(p \neq 2, p \neq 3\), then \(-3\) is not a square in \(\text{GF}(q)\) if and only if \(q \equiv 2 \mod 3\).

When \(q \equiv 1 \mod 3\), the solutions of (3) are

\[
x = \frac{1}{2}(b + c \pm r(b - c)),
\]

where \(r^2 = -3\). The solutions are easily seen to be distinct from each
other and from $b$ and $c$. So for every one of the $q(q - 1)$ ways of choosing $b$ and $c$ there are exactly two $a$'s for which $(a \ b \ c)$ is a 3-cycle represented by a polynomial of degree $<q - 2$.

Now suppose $q$ is even. We may write (3) here as

$$(x + b)(x + c) = (b + c)^2;$$

setting $s = b + c$ and $y = s^{-1}(x + b)$, this is $y^2 + y + 1 = 0$, which is irreducible over GF($2^n$) if and only if $n$ is odd. Again, the roots of (3'), when they exist, are distinct from each other and from $b$ and $c$, so precisely the same result holds in this case. (The even case is due to D. Hayes.)

Since $(a \ b \ c)$, $(b \ c \ a)$, and $(c \ a \ b)$ are all the same, this proves

**Theorem.** Every transposition over GF($q$) is represented by a unique polynomial of degree $q - 2$. If $q \equiv 2 \pmod{3}$, then every 3-cycle is represented by a polynomial of degree $q - 2$. If $q \equiv 1 \pmod{3}$, then all but $\frac{2}{3}q(q - 1)$ 3-cycles are represented by polynomials of degree $q - 2$.

The connection with the comments at the end of the first section is clear when it is noted that there are $3q(q - 1)$ elements of GF($q$) altogether.

The preceding two theorems have the following corollary:

**Corollary.** The symmetric group of permutations of GF($q$) is generated by the permutations represented by polynomials of degree $q - 2$. If $q \equiv 2 \pmod{3}$, then the alternating group is generated by the even permutations represented by polynomials of degree $q - 2$.

In this connection the results of [6] should be noted.

If $q = 3^n$, one may prove similarly that all but $3^n(3^n - 1)$ 3-cycles are represented by polynomials of degree $q - 2$. Certain other special results may be obtained. For example, an explicit formula may be obtained for products of two disjoint transpositions. But even for 4-cycles an explicit formula seems difficult to get. The procedure used above to obtain the formula for 3-cycles breaks down because, when the polynomial corresponding to (3) has roots, the roots may not be distinct from the other elements already chosen to be in the 4-cycle (this happens already in GF(25)). However, it is true that a polynomial representing a 4-cycle always has degree $q - 2$ if $q \equiv 3 \pmod{4}$.

One may also treat in the same way the question of whether or not other coefficients occurring in the representing polynomial are zero. For example, consider again the transposition $(a \ b)$, $a \neq b$. In general, the
coefficient of \( x^{q-1-r} \) (for \( 0 \leq r \leq q - 1, r \neq q - 2 \)) in the polynomial representing \((a \ b)\) is

\[
(-1)^r \binom{q-1}{q-1-r} (a - b)(a^r - b^r).
\]

However,

\[
\binom{q-1}{q-1-r} \equiv (-1)^r \pmod{p}.
\]

This is clear if \( r = 1 \). It is well known and easy to show that

\[
\binom{q-1}{q-1-r} = \binom{q-1}{q-1-r} - \binom{q-1}{q-1-r+1}.
\]

But the right side is 0 (mod \( p \)) by the Lucas criterion (this may also be shown by induction). Then (4) follows by induction on \( r \).

It follows from (4) that the coefficient of \( x^{q-1-r} \) is simply \((a - b)(a^r - b^r)\) for \( r \neq q - 2 \), and the coefficient of \( x \) is \((a - b)(a^{q-2} - b^{q-2}) + 1\).

Results analogous to the preceding results on degrees can be read off from these formulas. For example, excluding the anomalous case \( r = q - 2 \), there are \( a \) and \( b \) in \( \text{GF}(q) \) for which the coefficient of \( x^{q-1-r} \) in the polynomial representing \((a \ b)\) is zero if and only if \((r, q - 1) \neq 1\).

The coefficient of \( x \) is more complicated, but it may be proved using the same kind of arguments as for the case of the 3-cycle that there are \( a, b \in \text{GF}(q) \) for which the coefficient of \( x \) is zero if and only if one of these two possibilities occurs: (1) \( p = 2 \) (here setting \( a = 0 \) or \( b = 0 \) is sufficient, but there are pairs \((a, b)\) neither of which is zero which yields a zero coefficient of \( x \) as well); (2) \( p \neq 2 \) and \( q \equiv 1 \) or 4 (mod 5).

3. An Asymptotic Result

Let \( r \) and \( s \) be fixed positive integers, and \( k_2, \ldots, k_s \) non-negative integers for which

\[
\sum_{i=2}^{s} ik_i = r. \tag{5}
\]

Let \( P(k_2, \ldots, k_s) \) be the set of permutations of \( \text{GF}(q) \) which are the disjoint products of \( k_2 \) transpositions, \( k_3 \) 3-cycles, etc. Such permutations move exactly \( r \) elements.

**Theorem.** There is a constant \( C = C(k_2, \ldots, k_s) \) for which \( P(k_2, \ldots, k_s) \)
contains $Cq!/(q - r)!$ permutations, of which not more than $2q!/(q - r + 1)!$ are represented by polynomials of degree less than $q - 2$.

**Corollary.** The number of permutations in $P(k_2, \ldots, k_s)$ represented by polynomials of degree $q - 2$ is asymptotic to the number of all permutations in $P(k_2, \ldots, k_s)$ as $q \to \infty$.

**Proof of Theorem:** Let $(a_1, \ldots, a_r)$ be an arbitrary $r$-tuple of distinct elements of $GF(q)$. There are clearly $q!/(q - r)!$ such $r$-tuples. The map $\beta$ which takes each $r$-tuple $(a_1, \ldots, a_r)$ into the (unique) permutation in $P = P(k_2, \ldots, k_s)$ which contains $a_1, \ldots, a_r$ in that order is not injective. For example, $(a, b, c)$ and $(b, c, a)$ both go into $(a b c)$. But there is a number $B = B(k_2, \ldots, k_s)$ not dependent on $(a_1, \ldots, a_r)$ with the property that each permutation in $P$ comes under $\beta$ from exactly $B$ such $r$-tuples. In fact [5, p. 67]:

$$B = \prod_{i=2}^{s} i^{k_i} (k_i!)$$

(6)

If we now let $C = 1/B$, we have the first part of the theorem.

Now a permutation of $P(k_2, \ldots, k_s)$ is represented by a polynomial

$$f(x) = x + \sum_{i=2}^{s} \sum_{j=1}^{k_i} \sum_{n=1}^{i} (a_{i,j,n} - a_{i,j,n+1})(x - a_{i,j,n})^{n-1}$$

(7)

(cf. (1) and (2)), where the given permutation takes $a_{i,j,n}$ into $a_{i,j,n+1}$ ($i = 2, \ldots, s; j = 1, \ldots, k_i; n = 1, \ldots, i$) and where one sets $a_{i,j,i+1} = a_{i,j,1}$.

It follows that the coefficient of $x^{q-2}$ is given by a quadratic in $a_{2,1,1}$ with coefficients which are polynomials in the other $a_{i,j,n}$. This quadratic is

$$Q(a_{2,1,1}) = \sum_{i=2}^{s} \sum_{j=1}^{k_i} \sum_{n=1}^{i} a_{i,j,n}(a_{i,j,n} - a_{i,j,n+1})$$

(8)

Thus an $r$-tuple $(a_1, \ldots, a_r)$ determines a permutation in $P(k_2, \ldots, k_s)$ of degree less than $q - 2$ if and only if $a_{2,1,1}$ (which is $a_1$) satisfies

$$Q(a_{2,1,1}) = 0.$$

There are $q!/(q - r + 1)!$ possible choices for $a_2, \ldots, a_r$; once these are chosen there are at most 2 possibilities for $a_1$. Thus there are at most $2q!/(q - r + 1)!$ permutations in $P(k_2, \ldots, k_s)$ represented by polynomials of degree less than $q - 2$.

Since the ratio of this number to the order of $P(k_2, \ldots, k_s)$ is $2/[C(q - r + 1)]$, the corollary follows.
4. Further Results

The theorem of Section 3 requires \( r \) to be fixed. It is possible to allow \( r \) to grow slowly with respect to \( q \) and obtain the same result, as the following theorem asserts.

Let \( \Gamma \) denote the usual \( \Gamma \) function restricted to the real numbers \( \geq 1 \). Then, for any integer \( n > 0 \), \( \Gamma(n) = (n - 1)! \), and \( \Gamma \) is injective. We define the factorial root \( \Gamma^{-1}(x) \) of an arbitrary real number \( x \geq 1 \) by

\[
\Gamma^{-1}(x) = 1 - \frac{1}{x}.
\]

Let \( N(q, r) \) be the number of permutations of \( GF(q) \) which move at most \( r \) elements, and let \( M(q, r) \) be the number of such permutations represented by polynomials of degree \( < q - 2 \). Then we have

**Theorem.** For any \( \epsilon > 0 \), as \( q \to \infty \),

\[
\frac{M(q, \Gamma^{-1}(q^{1-\epsilon}))}{N(q, \Gamma^{-1}(q^{1-\epsilon}))} \to 0.
\]

**Corollary.** For fixed \( r \), as \( q \to \infty \),

\[
\frac{M(q, r)}{N(q, r)} \to 0.
\]

**Proof of Theorem:** By the theorem of Section 3,

\[
N(q, u) = 1 + \sum_{r=2}^{u} \frac{q!}{(q - r)!} \sum_{P_r} C_{P_r},
\]

where \( P_r \) ranges over the set of all \( P(k_2, \ldots, k_s) \) such that \( k_2, \ldots, k_s \) satisfy (5) and where \( C_{P_r} \) is the constant \( C \) of the theorem of Section 3 for that \( P(k_2, \ldots, k_s) \). If \( A_u \) is the number of cycle classes of permutations which move not more than \( u \) elements and if \( C_0 = \min_{r, P_r} C_{P_r} \), then

\[
N(q, u) > A_u C_0 q! / (q - u)!.
\]

We now estimate \( C_0 \). Let \( B_{P_r} = B \) defined by (6). We recall that \( B_{P_r} \) is the number of \( r \)-tuples yielding the same permutation of \( P_r \) and that \( B_{P_r} \) depends only on \( P_r \), not on the particular permutation of \( P_r \). Moreover, \( C_{P_r} = 1 / B_{P_r} \). Now if two \( r \)-tuples give the same permutation of \( P_r \), then one must be a rearrangement of the other, so that \( \max_{r, P_r} B_{P_r} \leq u! \). Hence \( C_0 \geq 1 / u! \). Therefore

\[
N(q, u) > A_u q! / u! (q - u)!.
\]
Now

\[ M(q, u) \leq 2A_u q!/(q - u + 1)! \]

so that

\[ \frac{M(q, u)}{N(q, u)} \leq \frac{2u!}{q - u + 1}. \]

If \( u \leq R_t(q^{1-e}) \), then

\[
\frac{M(q, u)}{N(q, u)} \leq \frac{2q^{1-e}}{q - u} < \frac{2q^{1-e}}{q - q^{1-e}} = \frac{2q^{1-e}}{q^{1-e}(q^e - 1)} \to 0
\]

as \( q \to \infty \). This proves the theorem.

The corollary follows by an easy adjustment of the proof of the theorem.

**Acknowledgment**

The author wishes to acknowledge the helpful suggestions of L. Carlitz and D. Hayes.

**References**

The author will be happy to supply on request an extensive bibliography of works concerned with permutations of algebraic structures.