SOME THEOREMS ON PERMUTATION POLYNOMIALS[1]

BY L. CARLITZ

Communicated by G. B. Huff, December 8, 1961

A polynomial $f(x)$ with coefficients in the finite field $GF(q)$ is called a permutation polynomial if the numbers $f(a)$, where $a \in GF(q)$ are a permutation of the a's. An equivalent statement is that the equation

$$f(x) = a \tag{1}$$

is solvable in $GF(q)$ for every a in $GF(q)$. A number of classes of permutation polynomials have been given by Dickson [1]; see also Rédei [3].

In the present note we construct some permutation polynomials that seem to be new. Let $q = 2m+1$ and put

$$f(x) = x^{m+1} + ax. \tag{2}$$

We define

$$\psi(x) = x^m, \tag{3}$$

so that $\psi(x) = -1$, $+1$ or 0 according as x is a nonzero square, a nonsquare or zero in $GF(q)$. Thus (2) may be written as

$$f(x) = x(a + \psi(x)). \tag{4}$$

We shall show that for proper choice of a, the polynomial $f(x)$ is a permutation polynomial. We assume that $a^2 \neq 1$; then $x = 0$ is the only solution in the field of the equation $f(x) = 0$. Now suppose (i) $f(x) = f(y)$, $\psi(x) = \psi(y)$. It follows at once from (4) that $x = y$. Next suppose (ii) $f(x) = f(y)$, $\psi(x) = -\psi(y)$. Then (4) implies

$$\psi\left(\frac{a+1}{a-1}\right) = -1. \tag{5}$$

If we take

$$a = \frac{c^2+1}{c^2-1}, \tag{6}$$

where $c^2 \neq \pm 1$ or 0 but otherwise is an arbitrary square of the field, it is evident that (5) is not satisfied. For $q \geqq 7$ such a choice of c^2 is

[1] Supported in part by National Science Foundation grant G-16485.

possible. Hence $f(x)$ is a permutation polynomial for $q \geqq 7$ and a defined by (6).

We show next that $f(x)$ is not a permutation polynomial for $GF(q^r)$, where $r > 1$. For r even this is evident since

$$q^2 - 1 \equiv 0 \pmod{m + 1}.$$

Replacing r by $2r+1$, put

$$q^{2r+1} = k(m + 1) + m. \tag{7}$$

Then expanding

$$(f(x))^{k+m-1} = (x^{m+1} + ax)^{k+m-1}$$

and reducing the result (mod $x^{q^{2r+1}} - x$), we find that the coefficient of $x^{q^{2r+1}-1}$ is equal to

$$\binom{k + m - 1}{m - 1} a^{m-1}. \tag{8}$$

Since by (7) $k \equiv 1 \pmod{q}$, it follows that the binomial coefficient in (8) is congruent to 1 (mod p). Therefore $f(x)$ is not a permutation polynomial for $GF(q^{2r+1})$.

We may state

THEOREM 1. *The polynomial*

$$f(x) = x^{m+1} + ax \qquad (q = 2m + 1)$$

with a defined by (6) *is a permutation polynomial for $GF(q)$ provided $q \geqq 7$. However it is not a permutation polynomial for any $GF(q^r)$ with $r > 1$.*

We consider next the case $q = 3m+1$ and again put $f(x) = x^{m+1} + ax$. It is now convenient to define

$$\psi_3(x) = x^m. \tag{9}$$

Thus for $x \in GF(q)$, $x \neq 0$, we have $\psi_3(x) = 1$, ω or ω^2, where

$$\omega^2 + \omega + 1 = 0 \qquad (\omega \in GF(q)).$$

We assume first that $a \neq -1, -\omega, -\omega^2$. If we suppose (i) $f(y) = f(x)$, $\psi_3(x) = \psi_3(y)$, it follows that $x = y$. If we suppose (ii) $f(x) = f(y)$, $\psi_3(y) = \omega \cdot \psi_3(x) = \omega\lambda$, it follows that

$$\psi_3\left(\frac{a + \lambda}{a + \omega\lambda}\right) = \omega. \tag{10}$$

If we suppose (iii) $f(x) = f(y)$, $\psi_3(y) = \omega^2$, $\psi_3(x) = \omega^2\lambda$ we get

$$\psi_3\left(\frac{a+\lambda}{a+\omega^2\lambda}\right) = \omega^2. \tag{11}$$

Hence if we can choose a so that

$$\psi_3(a+1) = \psi_3(a+\omega) = \psi_3(a+\omega^2), \tag{12}$$

both (10) and (11) will be contradicted.

Now (12) holds if and only if

$$a+\omega = b^3(a+1), \qquad a+\omega^2 = c^3(a+1), \tag{13}$$

where $b,\ c \in GF(q)$, $b^3 \neq 1$, $c^3 \neq 1$. Eliminating a we get

$$b^3 + \omega c^3 + \omega^2 = 0. \tag{14}$$

Conversely if (14) is satisfied we get (13). By a theorem of Hurwitz which can be extended without difficulty to finite fields the number of solutions of (14) is asymptotic to q. This proves

THEOREM 2. *For $q=3m+1$ sufficiently large it is possible to choose $a \in GF(q)$ so that $f(x)=x^{m+1}+ax$ is a permutation polynomial for $GF(q)$.*

It is not evident whether the second half of Theorem 1 can be carried over to this case.

Finally we state

THEOREM. *Let k be a fixed integer $\geqq 2$ and $q=km+1$. Then there exists a constant N_k and a number $a \in GF(q)$ such that*

$$f(x) = x^{m+1} + ax$$

is a permutation polynomial for $GF(q)$ provided $q > N_k$.

The proof makes use of a theorem of Lang and Weil concerning the number of solutions of system of equations over a finite field [2].

REFERENCES

1. L. E. Dickson, *Linear groups*, New York, Dover, 1958.

2. S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1953), 819–827.

3. L. Rédei, *Über eindeutig umkehrbare Polynome in endlichen Körpern*, Acta Sci. Math. Szeged. **11** (1946–1948), 85–92.

DUKE UNIVERSITY