Permutations in finite fields

By L. CARLITZ in Durham (N. C., U. S. A)

1. 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. That such polynomials exist is evident from the Lagrange interpolation formula for a finite field:

$$f(x) = -\sum_a \frac{x^q - x}{x - a} f(a). \tag{1.1}$$

The formula (1. 1) furnishes a polynomial that is of degree $< q$. We shall say generally that a permutation polynomial is in *reduced* form when its degree $< q$. It is known that for $q > 2$ permutation polynomials of degree $q-1$ cannot occur; more precisely the degree of a non-linear permutation polynomial cannot be a divisor of $q-1$. This follows very easily from

$$\sum_{a \in GF(q)} a^k = \begin{cases} 0 & (0 \leqq k < q-1) \\ -1 & (k = q-1), \end{cases} \tag{1.2}$$

Assume that

$$f(x) = c_0 x^m + \ldots + c_m \quad (c_j \in GF(q),\ c_0 \neq 0)$$

is a permutation polynomial and that $q - 1 = mr$. Then

$$(f(x))^r = c_0^r x^{mr} + \ldots + c_m^r$$

so that

$$0 = \sum_{a \in GF(q)} (f(a))^r = -c_0^r.$$

This contradicts $c_0 \neq 0$.

DICKSON [3] has constructed various classes of permutation polynomials. RÉDEI [5] has considered rational functions over $GF(q)$ that possess an inverse. He has proved in particular that if m is odd, $1 \leqq m < q$, then there exist rational permutation functions of degree m.

The writer [2] has proved that every permutation polynomial is generated by the special polynomials

$$ax + b, \ x^{q-2} \quad (a, b \in GF(q),\ a \neq 0). \tag{1.3}$$

For $q = 5$ this had been proved by BETTI and for $q = 7$ by DICKSON [3, p. 119].

Clearly if $f(x)$ is a permutation polynomial for $GF(q)$, the same is true for $f(x) + (x^q - x)g(x)$, where $g(x)$ is an arbitrary polynomial with coefficients in $GF(q)$. Indeed the theorem quoted above is to be understood in this sense. Thus if $f(x)$

is a permutation polynomial in reduced form then

$$F(x) = f(x) + (x^q - x)g(x), \tag{1.4}$$

where $F(x)$ is the resultant of a finite number of the special permutations (1. 3) and $g(x)$ is some polynomial in $GF[q, x]$. We may call $F(x)$ a *crude* permutation polynomial. Note in particular that in computing the polynomial $F(x)$ reduction (mod $x^q - x$) is not allowed. Also $F(x)$ is not uniquely determined by $f(x)$. For example the polynomials

$$x^{(q-2)2r} \qquad (r = 1, 2, 3, \ldots)$$

are all crude permutation polynomials corresponding to the polynomial x.

2. Now let $f(x)$ be a permutation polynomial for $GF(q)$ in reduced form. It is of interest to ask whether there exist polynomials congruent to $f(x)$ (mod $x^q - x$) that are also permutation polynomials for $GF(q^r)$ where r is assigned. We first prove the following result.

Theorem 1. *Let $f(x)$ be a permutation polynomial for $GF(q)$ in reduced form of degree >1 and let $F(x)$ be a crude permutation polynomial corresponding to $f(x)$. Then $F(x)$ is a permutation polynomial for $GF(q^r)$ if and only if*

$$(2^r - 1, q - 2) = 1. \tag{2.1}$$

Since $\deg f(x) > 1$ we have also $\deg F(x) > 1$. Consequently the permutation x^{q-2} occurs at least once in $F(x)$. Now x^{q-2} effexts a permutation in $GF(q^r)$ if and only if

$$(q^r - 1, q - 2) = 1. \tag{2.2}$$

Since $q^r - 1 \equiv 2^r - 1 \pmod{q-2}$, it follows that the condition (2. 2) is equivalent to (2. 1). This evidently completes the proof of the theorem.

Suppose that q is odd and greater than 3. Let 2 belong to the exponent t (mod $q-2$). Then (2. 1) is certainly satisfied when $r \equiv 1 \pmod{t}$ but is not satisfied when $r \equiv 0 \pmod{t}$. When q is even and greater than 4, let 2 belong to the exponent $t \pmod{\frac{1}{2}(q-2)}$. Then again (2. 1) is satisfied when $r \equiv 1 \pmod{t}$ and not satisfied when $r \equiv 0 \pmod{t}$. We have therefore

Theorem 2. *Let $F(x)$ be a crude permutation polynomial for $GF(q)$. Then if $q > 4$ there are infinitely many $GF(q^r)$ for which $F(x)$ is a permutation polynomial and also infinitely many $GF(q^r)$ for which $F(x)$ is not a permutation polynomial.*

When $q = 4$, x^2 is a permutation polynomial for all $GF(2^r)$. When $q = 3$ the special permutations (1. 3) are all of the first degree.

3. Put $q = p^n$, where p is a prime. Then it is easily verified that the polynomial

$$ax^{p^j} + b \qquad (a, b \in GF(q),\ a \neq 0) \tag{3.1}$$

is a permutation polynomial for all $GF(q^r)$ and for all $j = 0, 1, 2, \ldots$.

If $f(x)$ is an arbitrary permutation polynomial for $GF(q)$ then for every $c \in GF(q)$ the equation $f(x) = c$ is solvable in $GF(q)$ and indeed has a unique solution $b \in GF(q)$.

Assume $f(x) \in GF[q, x]$; then

$$f(x) - c = (x-b)^k M(x), \tag{3.2}$$

where $k \geqq 1$, $M(x) \in GF[q, x]$ and either $\deg M(x) = 0$ or $M(x)$ is a product of irreducible polynomials $P_i(x) \in GF[q, x]$, $\deg P_i(x) \geqq 2$. Hence if r is a multiple of any $d_i = \deg P_i(x)$ it follows at once from (3. 2) that $f(x)$ is not a permutation polynomial for $GF(q^r)$. We accordingly suppose that (3. 2) reduces to

$$f(x) - c = a(x-b)^k \qquad (a \neq 0); \tag{3.3}$$

that is for each $c \in GF(q)$ there is $ab = b(c) \in GF(q)$ such that (3. 3) holds. In particular for $c = 1, 0$, (3. 3) implies

$$a(x-b_0)^k - a(x-b_1)^k = 1. \tag{3.4}$$

Replacing x by $x + b_1$, (3. 4) becomes

$$a(x+b)^k - ax^k = 1 \qquad (b = b_1 - b_0).$$

Expanding by the binomial theorem we get

$$\binom{k}{s} \equiv 0 \pmod{p} \qquad (0 < s < k). \tag{3.5}$$

By a known property of binomial coefficients it follows that $k = p^j$ for some j. We have therefore proved the following

Theorem 3. *A polynomial $f(x) \in GF[q, x]$ is a permutation polynomial for all $GF(q^r)$ if and only if it is of the form* (3. 1).

We have incidently proved the following result.

Theorem 4. *If $f(x)$ is a permutation polynomial for $GF(q)$ that is not of the form* (3. 1), *then for infinitely many r, $f(x)$ is not a permutation polynomial for $GF(q^r)$.*

It might seem plausible that if $f(x)$ is a permutation polynomial for $GF(q)$ then it will also be a permutation for infinitely many $GF(q^r)$. We have seen that this is true for crude permutation polynomials (Theorem 2). Two other classes of polynomials with this property are covered by the following two theorems.

Theorem 5. *Let $(k, q-1) = 1$ so that x^k is a permutation polynomial for $GF(q)$. Then there are infinitely many $GF(q^r)$ for which x^k is a permutation polynomial and infinitely many $GF(q^r)$ for which x^k is not a permutation polynomial.*

There is no loss in generality in assuming that $(k, q) = 1$. Let q belong to the exponent $t \pmod{k}$, so that $t > 1$. Then for r divisible by t we have $q^r \equiv 1 \pmod{k}$, so that x^k is certainly not a permutation polynomial for $GF(q^r)$. On the other hand for $r \equiv 1 \pmod{t}$ we have

$$q^r - 1 \equiv q - 1 \pmod{k},$$

so that $(k, q^r - 1) = (k, q-1) = 1$. Hence x^k is a permutation polynomial for all $GF(q^{mt+1})$, $m = 1, 2, 3, \ldots$.

Theorem 6. *Let* $q=p^n$ *and put*

$$f(x) = c_0x + c_1x^p + \ldots + c_{n-1}x^{p^{n-1}} \qquad (c_j \in GF(p)). \tag{3.6}$$

Then $f(x)$ *is a permutation polynomial for* $GF(q)$ *if and only if*

$$(c_0 + c_1x + \ldots + c_{n-1}x^{n-1},\ 1-x^n) = 1. \tag{3.7}$$

Moreover there are infinitely many $GF(q^r)$ *for which* $f(x)$ *is a permutation polynomial and infinitely many* $GF(q^r)$ *for which* $f(x)$ *is not a permutation polynomial.*

The first part of the theorem is a corollary of the existence of a normal basis for $GF(q)$; see for example [4, p. 250].

To prove the second part put

$$C(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}.$$

Then $f(x)$ is a permutation polynomial for $GF(q^r)$ if and only if

$$(C(x), 1-x^{rn}) = 1. \tag{3.8}$$

There is no loss in generality in assuming that $c_0 \neq 0$, so that $(x, C(x)) = 1$. Now let x belong to the exponent $t \pmod{C(x)}$. Then for $r \equiv 1 \pmod{t}$ we have

$$1 - x^{rn} \equiv 1 - x^n \pmod{C(x)},$$

so that $(C(x), 1-x^{rn}) = (C(x), 1-x^n) = 1$; clearly $f(x)$ is a permutation polynomial for $GF(q^r)$. On the other hand if $r \equiv 0 \pmod{t}$, then $1 - x^{rn} \equiv 0 \pmod{C(x)}$ and it follows that $f(x)$ is not a permutation polynomial for such $GF(q^r)$. This completes the proof of the theorem.

4. Dickson [3] showed that the quartic

$$f(x) = x^4 + 3x \tag{4.1}$$

is a permutation polynomial for $GF(7)$ but not for any $GF(7^n)$, $n > 1$. This result can be generalized as follows.

Put $q = 2m+1$. We shall show that for proper choice of $a \in GF(q)$ the polynomial

$$f(x) = x^{m+1} + ax \tag{4.2}$$

is a permutation polynomial for $GF(q)$.

It is convenient to define

$$\psi(x) = x^m. \tag{4.3}$$

Thus $\psi(c) = 1, -1$ or 0 according as c is a non-zero square, a non-square or zero in $GF(q)$. We may rewrite (4.2) as

$$f(x) = x(a + \psi(x)). \tag{4.4}$$

We assume that $a^2 \neq 1$ so that $f(x)$ vanishes only when $x = 0$. Now if $f(x)$ is not a permutation polynomial we must have

$$f(b) = f(c) \qquad (b, c \in GF(q),\ b \neq c,\ bc \neq 0) \tag{4.5}$$

for at least one pair b, c. We consider two cases (i) $\psi(b) = \psi(c)$, (ii) $\psi(b) = -\psi(c)$.

In case (i) it follows from (4. 4) and (4. 5) that

$$b(a+\psi(b)) = c(a+\psi(b));$$

since $a^2 \neq 1$, it follows that $b=c$.

In case (ii) we get similarly

$$b(a+\psi(b)) = c(a-\psi(b)),$$

so that

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

Hence if we choose a so that

$$\psi\left(\frac{a+1}{a-1}\right) = 1 \tag{4. 6}$$

we have a contradiction. Clearly (4. 6) can be satisfied by taking

$$a = (u^2+1)/(u^2-1), \tag{4. 7}$$

where u^2 is an arbitrary square of the field (different from $\pm 1, 0$). For $q \geqq 7$ such u^2 always exist. The value of a furnished by (4. 7) automatically satisfies the condition $a^2 \neq \pm 1$.

This proves the following

Theorem 7. *For $q = 2m+1 \geqq 7$, the polynomial* (4. 2) *is a permutation polynomial for $GF(q)$ provided that a is defined by* (4. 7) *with u^2 an arbitrary square of $GF(q)$ different from* 1, 0.

For $q=7$, $u^2=2$, it is easily verified that (4. 2) reduces to (4. 1).

It can be proved that if k is a fixed integer $\geqq 2$ and $q = mk+1$ then for properly chosen $a \in GF(q)$ the polynomial

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

is a permutation polynomial for $GF(q)$, provided q exceeds a certain bound N_k. The proof is similar to the proof of Theorem 7 but requires an estimate for the number of solutions of certain systems of equations in a finite field.

Theorem 8. *Let $f(x)$ satisfy the hypotheses of the last theorem. Then $f(x)$ is not a permutation polynomial for any $GF(q^r)$ with $r>1$.*

If r is even we have

$$q^r \equiv 1 \pmod{m-1}$$

and the stated result follows immediately. We therefore assume that $r = 2s+1$.

Put

$$q^{2s+1} = k(m+1)+n; \tag{4. 8}$$

since

$$q^{2s+1} \equiv -1 \pmod{m+1},$$

it is clear that an integer k can be found for which (4. 8) is satisfied. We shall consider

$$(f(x))^{k+m-1} = (x^{m+1}+ax)^{k+m-1} = \sum_{j=0}^{k+m-1} \binom{k+m-1}{j} a^j x^{(m+1)(k+m-j-1)+j}. \tag{4. 9}$$

Since $s \geqq 1$ it follows easily that

$$q^{2s+1} \leqq (m+1)(k+m-1) < 2(q^{2s+1}-1).$$

Thus reducing (4.9) (mod $x^{q^{2s+1}} - x$) the only term that need be considered is the one corresponding to $j = m-1$, that is

$$\binom{k+m-1}{m-1} a^{m-1} x^{q^{2s+1}} - 1. \tag{4.10}$$

Now it follows form (4.8) that $k(m+1) \equiv m+1 \pmod{q}$. Since $q = 2(m+1)-1$ we have $(m+1, q) = 1$ and therefore $k \equiv 1 \pmod{q}$.

We shall require the following known property of binomial coefficients. Let

$$r = r_0 + r_2 p + r_3 p^2 + \ldots \qquad (0 \leqq r_j < p),$$
$$s = s_0 + s_1 p + s_2 p^2 + \ldots \qquad (0 \leqq s_j < p),$$

where p is a prime. Then

$$\binom{r}{s} \sim \binom{r_0}{s_0}\binom{r_1}{s_1}\binom{r_2}{s_2} \ldots \pmod{p}. \tag{4.11}$$

In particular if $r = ap^n + b$ $(0 \leqq b < p^n)$ $s = cp^n + d$ $(0 \leqq d < p^n)$, then (4.11) implies

$$\binom{r}{s} \equiv \binom{a}{c}\binom{b}{d} \pmod{p}. \tag{4.12}$$

Returning to (4.10) we put $k = tp^n + 1$, where $q = p^n$. Since $m < p^n$ it follows form (4.12) that

$$\binom{k+m-1}{m-1} = \binom{tp^n+m}{m-1} \equiv m \not\equiv 0 \pmod{p}.$$

Thus (4.10) is not zero and therefore $f(x)$ is not a permutation polynomial for $GF(q^{2s+1})$.

5. Let r be a fixed integer $\geqq 1$. We now briefly consider the set of transformations

$$y_i = f_i(x_1, \ldots, x_r) \qquad (i = 1, \ldots, r) \tag{5.1}$$

that possess an inverse of the same general form; the coefficients of the polynomial f_i lie in the fixed field $GF(q)$. The totality of all transformations (5.1) constitute a group $\Gamma_r(q)$ isomorphic with the symmetric group on q^r letters. For some properties of polynomials relative to $\Gamma_r(q)$ see [1].

We can set up a correspondence between $\Gamma_r(q)$ and $\Gamma_1(q^r)$ in the following way. Let $\omega_1, \ldots, \omega_r$ denote a basis of $GF(q^r)$ relative to $GF(q)$ and put

$$u = x_1\omega_1 + \ldots + x_r\omega_r, \quad v = y_1\omega_1 + \ldots + y_r w_r. \tag{5.2}$$

By means of (5.1) every n-tuple $(x_1, \ldots, x_n)$ of the $GF(q)$ is carried into the n-tuple $(y_1, \ldots, y_n)$. By means of (5.2) to the n-tuple $(x_1, \ldots, x_n)$ corresponds the number u of $GF(q^r)$ and to the n-tuple $(y_1, \ldots, y_n)$ corresponds the number v of $GF(q^r)$. Clearly the correspondence between u and v is one to one. We may accord-

ingly write

$$v = f(u), \tag{5.3}$$

where $f(u)$ is a permutation polynomial for $GF(q^r)$. Conversely if (5.3) is given it is evident that (5.1) is uniquely determined. We have therefore established a one to one correspondence between (5.1) and (5.3). This correspondence is evidently an isomorphism.

We may state

Theorem 9. *To every invertible transformation* (5.1) *there corresponds the permutation* (5.3) *and conversely. This correspondence induces an isomorphism between* $\Gamma_r(q)$ *and* $\Gamma_1(q^r)$.

If ξ denotes the column vector $(x_1, \ldots, x_r)$ and η the column vector $(y_1, \ldots, y_r)$, (5.1) can be written compactly in the form

$$\eta = \varphi(\xi), \tag{5.4}$$

where φ is a vector function of the vector ξ; $\varphi = (f_1, \ldots, f_r)$.

We shall now define two special transformations (5.4), first the linear transformation

$$\eta = A\xi + \beta, \tag{5.5}$$

where A is a non-singular matrix of order r and β is a column vector; the elements of both A and β are in $GF(q)$. In the second place corresponding to the transformation

$$u \to u^{q^r - 2}$$

we define an involution

$$\eta = \xi^\sigma = (x_1^\sigma, \ldots, x_r^\sigma) \tag{5.6}$$

by means of

$$(x_1\omega_1 + \ldots + x_r\omega_r)^{q^r - 2} = x_1^\sigma\omega_1 + \ldots + x_r^\sigma\omega_r. \tag{5.7}$$

Then we have the following

Theorem 10. *Every transformation of the group* $\Gamma_r(q)$ *can be generated by the special transformation* (5.5) *and* (5.6).

It is evidently not necessary to use all the transformations (5.5). It would suffice to restrict A to a certain cyclic subgroup of nonsingular matrices of order $q^r - 1$. We shall however not take the space to state a stronger version of Theorem 10.

We remark that the involution (5.6) is not uniquely determined but is dependent upon the choice of basis $\omega_1, \ldots, \omega_r$. If we make a change of basis:

$$\omega' = Cu, \tag{5.8}$$

where w is the column vector $(\omega_1, \ldots, \omega_r)$ and C is a non-singular matrix with elements in $GF(q)$, then (5.7) becomes

$$(x_1'\omega_1' + \ldots + x_r'\omega_r')^{q^r - 2} = x_1'^\tau\omega_1' + \ldots + x_r'^\tau\omega_r', \tag{5.9}$$

where τ is the involution corresponding to the ω_i' and

$$\xi = C^t\xi', \quad \xi' = (x_1', \ldots, x_r');$$

C^t is the transpose of C. Comparing (5. 9) with (5. 8) it is evident that

$$\xi'^{\tau} = (C^t)^{-1}(C^t\xi')^{\sigma}. \tag{5. 10}$$

This proves

Theorem 11. *Under the change of basis* (5. 8) *the involutions* σ, τ *corresponding to* ω_i, ω_i', *respectively, are related by means of* (5. 10).

The special transformation ($q > 2$)

$$y_1 = x_i^{q-2} \qquad (i = 1, \ldots, r) \tag{5. 11}$$

is an involution. However for $r > 1$ it cannot be identified with any of the involutions (5. 7). If we assume that (5. 11) can be defined by means of (5. 7) then it follows that

$$(x_1\omega_1 + \ldots + x_r\omega_r)(x_1^{q-2}\omega_1 + \ldots + x_r^{q-2}\omega_r) = 1 \tag{5. 12}$$

for all $x_1, \ldots, x_r \in GF(q)$ except $(0, \ldots, 0)$. We may assume that $\omega^2 \neq 1$. Then if we take $x_1 = \ldots = x_{r-1} = 0$, $x_r = 1$, (5. 12) leads to a contradiction.

When $q = 3$ the transformation (5. 11) reduces to the identity; for $r > 1$ the transformations (5. 5) generate a proper subgroup of $\Gamma_r(q)$. It would be of interest to identify the group generated by (5. 5) and (5. 11) when $q > 3$ and $r > 1$.

References

[1] L. Carlitz, Invariant theory of equations in a finite field, *Transactions Amer. Math. Soc.*, **75** (1953), 405–427.

[2] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.*, **4** (1953), 538.

[3] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Annals of Math.*, **11** (1896–7), 65–120.

[4] O. Ore, Contributions to the theory of finite fields, *Transactions Amer. Math. Soc.*, **36** (1934), 243–274.

[5] L. Rédei, Über eindeutig umkehrbare Polynome in endlichen Körpern, *Acta Sci. Math.*, **11** (1946–48), 85–92.

DUKE UNIVERSITY
DURHAM, NORTH CAROLINA, U. S. A

(Received December 5, 1961)