POLYNOMIALS OVER FINITE FIELDS WHICH COMMUTE WITH LINEAR PERMUTATIONS

GARY L. MULLEN

ABSTRACT. The polynomials over a finite field which commute with an arbitrary linear permutation of the field are characterized. This characterization is obtained through the use of a result from Pólya's theory of enumeration.

Let p be a prime number, $q = p^n$ for some positive integer n , and $\text{GF}(q)$ the finite field with q elements. Let a be a nonzero element of $\text{GF}(q)$. In [3] Wells characterized those polynomials over $\text{GF}(q)$ which commute with a translation by an element of the field, i.e., he characterized those polynomials $f(x)$ with coefficients in $\text{GF}(q)$ for which $f(x + a) = f(x) + a$. In the present paper we characterize those polynomials $f(x)$ for which

$$(1) \quad f(bx + a) = bf(x) + a$$

where $b \in \text{GF}(q)$. Thus if $b = 1$, our characterization reduces to that considered by Wells.

Since, by the Lagrange Interpolation Formula [2, p. 55], every polynomial over $\text{GF}(q)$ is congruent (mod $x^q - x$) to a unique polynomial of degree $< q$, this will characterize all polynomials over $\text{GF}(q)$ satisfying (1). The characterization will be obtained by equating coefficients in (1) and using an elementary result from Pólya's theory of enumeration.

Let $f(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{q-1}x^{q-1}$ where for $r = 0, 1, \dots, q-1$, $b_r \in \text{GF}(q)$. As a simple special case suppose $b = 0$ so that $f(x)$ satisfies (1) if and only if

$$0 = b_0 + (b_1 - 1)a + b_2a^2 + \cdots + b_{q-1}a^{q-1}$$

and thus there are clearly q^{q-1} polynomials with the property that $f(a) = a$. Suppose now that $b \neq 0$.

THEOREM 1. *The polynomial $f(x) = b_0 + b_1x + \cdots + b_{q-1}x^{q-1}$ satisfies (1) if and only if*

$$(2) \quad \begin{aligned} b_0(b-1) &= -a + \sum_{t=1}^{q-1} b_t a^t, \\ b_s(1-b^{s-1}) &= b^{s-1} \sum_{t=s+1}^{q-1} \binom{t}{s} b_t a^{t-s} \quad (1 \leq s \leq q-1). \end{aligned}$$

Received by the editors April 21, 1981 and, in revised form, May 29, 1981.

1980 *Mathematics Subject Classification.* Primary 12C05; Secondary 20B05.

Key words and phrases. Finite field, permutation.

© 1982 American Mathematical Society
0002-9939/81/0000-1012/\$01.75

PROOF. If $b = 1$ the set of conditions (2) are both necessary and sufficient since they reduce to the set of conditions given by Wells in [3]. Hence we assume $b \neq 1$. If c_s denotes the coefficient of x^s in the polynomial $f(bx + a)$ then

$$c_s = b^s \sum_{t=s}^{q-1} \binom{t}{s} b_t a^{t-s}$$

so that if (1) is to hold, $c_0 = bb_0 + a$ and $c_s = bb_s$ for $1 \leq s \leq q-1$. Hence the conditions (2) are necessary if (1) is to hold.

To prove the sufficiency, suppose that the multiplicative order of b is k where $k|q-1$. Hence if $k|s-1$ then b_s can be chosen arbitrarily from $\text{GF}(q)$. If $k \nmid s-1$ then (2) determines b_s uniquely in terms of $b_{s+1}, \dots, b_{q-1}$. If $s=1$ then b_1 can be chosen arbitrarily and thus there are $[(q-2)/k] + 1 = (q-1)/k$ coefficients which can be chosen arbitrarily from $\text{GF}(q)$. The remaining coefficients will be uniquely determined by (2). Hence there are $q^{(q-1)/k}$ polynomials $f(x)$ over $\text{GF}(q)$ of degree $< q$ satisfying (2).

In [1] it is shown that if g and h are permutations of finite sets D and R where the types of g and h are $(d_1, d_2, \dots)$ and $(e_1, e_2, \dots)$, respectively, then the number of functions $f: D \rightarrow R$ for which $fg = hf$ is

$$(3) \quad \prod_i \left(\sum_{j|i} j e_j \right)^{d_i}.$$

We consider the case where $D = R = \text{GF}(q)$ and $g = h = bx + a$ with $b \neq 0$. Since $b \neq 1$, it is not difficult to show that the polynomial $bx + a$ induces a permutation of $\text{GF}(q)$ which is the product of $(q-1)/k$ disjoint k -cycles and one cycle of length one, the fixed point being $a/(1-b)$. Thus $d_1 = 1$, $d_k = (q-1)/k$ and $d_i = 0$ if $i \neq 1$ or k so that (3) reduces to $q^{(q-1)/k}$. By the Lagrange Interpolation Formula each function from $\text{GF}(q)$ to itself is induced by exactly one polynomial of degree $< q$. Hence there are exactly $q^{(q-1)/k}$ polynomials $f(x)$ of degree $< q$ which satisfy (1) so that the conditions (2) are also sufficient. In addition we have proved

COROLLARY 2. *If $b \in \text{GF}(q)$ has multiplicative order k then the number of polynomials $f(x)$ of degree $< q$ with the property that $f(bx + a) = bf(x) + a$ is $q^{(q-1)/k}$.*

Of course not all of the $q^{(q-1)/k}$ polynomials are permutations. By using another result from [1], it is easily seen that the number of f which are 1-1 is given by

$$(4) \quad \prod_j j^d e_j (e_j - 1) \cdots (e_j - d_j + 1)$$

so that we can state

COROLLARY 3. *If $b \in \text{GF}(q)$ has multiplicative order k then the number of permutation polynomials $f(x)$ of degree $< q$ with the property that $f(bx + a) = bf(x) + a$ is $k^{(q-1)/k}((q-1)/k)!$.*

One can also easily obtain Wells' results by using (3) and (4). In particular, since $x + a$ induces a permutation which is the product of p^{n-1} disjoint p -cycles, the number of polynomials $f(x)$ with the property that $f(x + a) = f(x) + a$ is $q^{p^{n-1}}$ while the number of such permutation polynomials is $p^{p^{n-1}}(p^{n-1})!$.

Let $F_{m \times m}$ denote the algebra of $m \times m$ matrices over $F = \text{GF}(q)$. If $b \neq 0$, $a \in \text{GF}(q)$, then $\theta(x) = bx + a$ induces a permutation of $F_{m \times m}$ via substitution where if $D \in F_{m \times m}$ then $\theta(D) = bD + aI_m$ where I_m is the $m \times m$ identity matrix. If $D = (d_{ij})$, $i = 1, \dots, m$; $j = 1, \dots, m$, then the matrix $\theta(D)$ is determined by $\theta(D) = (bd_{ij} + a\delta_{ij})$ where δ_{ij} is the Kronecker delta symbol. Hence if $b \neq 1$ has multiplicative order k then $\theta(x)$ induces a permutation on $F_{m \times m}$ which is the product of $(q^{m^2} - 1)/k$ disjoint k -cycles and one cycle of length one, the fixed matrix being $D = (d_{ij}) = (a\delta_{ij}/(1 - b))$. Proceeding as before we can prove

THEOREM 4. *If $b \in \text{GF}(q)$ has multiplicative order k then the number of functions $f: F_{m \times m} \rightarrow F_{m \times m}$ with the property that*

$$f(bx + a) = bf(x) + aI_m$$

is $(q^{m^2})^{(q^{m^2}-1)/k}$ of which $k^{(q^{m^2}-1)/k}((q^{m^2} - 1)/k)!$ are permutations of $F_{m \times m}$.

If $b = 1$ then $\theta(x)$ induces a permutation on $F_{m \times m}$ which is the product of q^{m^2}/p disjoint p -cycles so we can state

THEOREM 5. *The number of functions $f: F_{m \times m} \rightarrow F_{m \times m}$ with the property that $f(x + a) = f(x) + aI_m$ is $(q^{m^2})^{q^{m^2}/k}$ of which $p^{p^{m^2}-1}(p^{m^2}-1)!$ are permutations of $F_{m \times m}$.*

We note that if $m = 1$ the results of Theorems 4 and 5 reduce to those of Corollaries 2 and 3 along with the results of Wells.

REFERENCES

1. N. G. deBruijn, *Pólya's theory of counting*, Applied Combinatorial Mathematics, (Ed., E. F. Beckenbach), Wiley, New York, 1964.
2. L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover, New York, 1958.
3. C. Wells, *Polynomials over finite fields which commute with translation*, Proc. Amer. Math. Soc. **46** (1974), 347-350.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, SHENANGO VALLEY CAMPUS, SHARON, PENNSYLVANIA 16146