PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 46, Number 3, December 1974

POLYNOMIALS OVER FINITE FIELDS WHICH COMMUTE WITH TRANSLATIONS

CHARLES WELLS

ABSTRACT. The polynomials over a finite field which commute with translation by an element of the field are characterized. A generalization of a long-known theorem about centralizers of permutations is used in obtaining the characterization.

Let p be a prime number, $q = p^n$ for some positive integer n, and $GF(q)$ the finite field with q elements. Let a be a nonzero element of $GF(q)$. Theorem 1 below characterizes the polynomials $f(x)$ with coefficients in $GF(q)$ for which $\deg f \leq q - 1$ and

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

This will actually characterize all polynomials over $GF(q)$ satisfying (1), since each such polynomial is congruent $(\mathrm{mod}\, x^q - x)$ to a unique such polynomial of degree $\leq q - 1$.

The characterization will be obtained by equating coefficients in (1), but the computation will be shortened by using a generalization of a long-known theorem about centralizers of permutations (Theorem 2).

Theorem 1. *Let* $f(x) = b_0 + b_1x + b_2x^2 + \cdots + b_ux^u$, *with* $b_r \in GF(q)$ *for* $r = 1, 2, \cdots, u$, *and* $u = q - 1$. *Then* $f(x)$ *satisfies* (1) *if and only if*

$$b_1 = 1 - \sum_{t=2}^{u} b_t a^{t-1},$$

$$sb_s = -\sum_{t=s+1}^{u} \binom{t}{s-1} b_t a^{t-s} \qquad (2 \leq s \leq u - 1,\ s \text{ not divisible by } p), \tag{2}$$

$$b_u = 0.$$

Presented to the Society, October 25, 1973; received by the editors October 18, 1973.

AMS(MOS) subject classifications (1970). Primary 12C05, 20B05; Secondary 20F25, 20M20.

Key words and phrases. Finite field, permutation, wreath product, centralizer.

Proof. Let c_s denote the coefficient of x^s in the polynomial $f(x + a)$. Then

$$c_s = \sum_{t=s}^{u} \binom{t}{s} b_t a^{t-s}, \tag{3}$$

and the requirement (1) implies that $c_0 = b_0 + a$ and $c_s = b_s$ for $1 \leq s \leq u$. It follows easily from this that the conditions in (2) are all necessary if (1) is to hold.

On the other hand, suppose the coefficients $b_0, b_p, b_{2p}, \cdots, b_{q-p}$ are chosen arbitrarily from $GF(q)$. The equations (2) then determine b_u, $b_{u-1}, \cdots, b_0$ uniquely. It follows that there are exactly $q^{p^{n-1}}$ polynomials of degree $\leq q - 1$ satisfying the conditions (2).

The polynomial $x + a$ induces a permutation of $GF(q)$ which is the product of p^{n-1} disjoint p-cycles. Furthermore, each mapping from $GF(q)$ to itself is induced by exactly one polynomial of degree $\leq q - 1$. (See Dickson [2, p. 55].) These two facts, together with Theorem 2 below, imply that there must be *exactly* $q^{p^{n-1}}$ polynomials $f(x)$ of degree $\leq q - 1$ which satisfy (1). This proves that the conditions (2) are sufficient as well as necessary, and also that the conditions on the coefficients obtained when s is divisible by p are redundant. No doubt both the sufficiency of (2) and the redundancy of the remaining conditions could be proved directly, perhaps using induction and the Lucas criterion, but knowledge of Theorem 2 makes those calculations unnecessary.

In the following, Z_d denotes the cyclic group of order d, Trans(e) the semigroup of all functions from a set with e elements to itself, and Sym(e) the group of all permutations of an e-element set. Definitions and basic facts about wreath products may be found in Neumann [3] or Wells [5].

Theorem 2. *Let θ be a permutation of the finite set X, let X have $m = de$ elements, and suppose θ is the product of e disjoint d-cycles. Then the set C_θ of functions $f: X \to X$ such that $\theta f = f\theta$ forms a semigroup on functional composition isomorphic to the wreath product of Z_d by* Trans(e), *and those functions f which are permutations form a subgroup $\overline{C}_\theta$ isomorphic to the wreath product of Z_d by* Sym(e). *Thus C_θ has $d^e e^e = m^e$ elements, and $\overline{C}_\theta$ has $d^e e!$ elements.*

Proof. Elements $x, y \in X$ are in the same cycle of θ if and only if $y = \theta^k(x)$ for some unique integer k, $0 \leq k \leq d - 1$. Let $f \in C_\theta$. Then $y =$

$\theta^k(x)$ if and only if $f(y) = \theta^k(f(x))$. Furthermore, if $x \neq y$, then $k > 0$, so that $f(x) \neq f(y)$. Hence f restricted to an orbit Δ of θ must take Δ bijectively onto another orbit, so that f induces a function $\overline{f}$ from the set Ω of orbits to itself.

Pick elements $\{x_\Delta \mid \Delta \in \Omega, x_\Delta \in \Delta\}$. Let $h_f: \Omega \to Z_d$ be defined by

$$f(x_\Delta) = \theta^{h_f(\Delta)} x_{\overline{f}(\Delta)}. \tag{4}$$

By computing $g(f(x_\Delta))$ one may verify that

$$h_{g \circ f} = h_g \circ \overline{f} + h_f. \tag{5}$$

Set $\lambda(f) = (\overline{f}, h_f)$. Then λ is bijective, and (5) shows that λ is an isomorphism from C_θ to Z_d wr Trans (e). It is easy to show that the permutations in C_θ induce permutations on Ω, and in fact form a subgroup isomorphic to Z_d wr Sym (e). This proves the theorem.

Burnside [1, pp. 224–227], gives the structure of $\overline{C}_\theta$, without, however, using the wreath product terminology. The proof of the more general theorem given above is modeled on Burnside's proof; the proof works in the more general setting essentially because a function $f \in C_\theta$ restricted to an orbit of θ is a bijection onto another orbit of θ; this allows the local coefficients $h_f(\Delta)$ to be well defined by (4). A general exposition of this and related ideas is given in Wells [5], [6].

Note. For $q > 2$, Theorem 1 asserts the existence of a sizeable class of permutation polynomials of degree strictly less that $q - 2$. In particular, it implies that there are many p-cycles represented by polynomials of degree $< q - 2$, for example the p-cycle $(a\ 2a\ 3a \cdots (p-1)a\ 0)$ (which clearly centralizes $x + a$). This may be contrasted with the main theorem in Wells [4] which asserts that almost all polynomials representing permutations which move only a small number of elements must be of degree exactly $q - 2$.

The author is grateful to L. Carlitz for suggesting the problem of characterizing the polynomials satisfying (1).

REFERENCES

1. W. Burnside, *Theory of groups of finite order*, 2nd ed., Dover, New York, 1955. MR 16, 1086.

2. L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover, New York, 1958. MR 21 #3488.

3. B. H. Neumann, *Embedding theorems for semigroups*, J. London Math. Soc. 35 (1960), 184–192. MR 29 #1268.

4. C. Wells, *The degrees of permutation polynomials over finite fields*, J. Combinatorial Theory 7 (1969), 49–55. MR 39 #176.

5. C. Wells, *Some applications of the wreath product* (to appear).

6. ———, *Centralizers of transitive semigroup actions and endomorphisms of trees* (to appear).

DEPARTMENT OF MATHEMATICS AND STATISTICS, CASE WESTERN RESERVE UNIVERSITY, CLEVELAND, OHIO 44118