Internat. J. Math. & Math. Sci.
VOL. 13 NO 2. (1990) 337-342

PERMUTATION BINOMIALS

CHARLES SMALL

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
Canada K7L 3N6

and

Department of Mathematics and Statistics
McMaster University
Hamilton Ontario
Canada L8S 4K1

(Received June 7, 1988 and in revised form December 13, 1988)

ABSTRACT. A polynomial f over a finite field F is a permutation polynomial if the mapping F → F defined by f is one-to-one. We are concerned here with binomials, that is, polynomials of the shape $f=aX^i+bX^j+c$, $i>j>1$. Even in this restricted setting, it is impossible to give general necessary and sufficient conditions on a,b,c for f to be a permutation polynomial. We review, and systematize, what is known.

KEY WORDS AND PHRASES. Permutation polynomials, finite fields, binomials.
1980 AMS SUBJECT CLASSIFICATION CODE. 11T06.

1. INTRODUCTION.

In the introduction to [1] the authors claim "we are able to determine at a glance precisely when $f(X)=aX^i+bX^j+c \in GF(q)$ is a permutation polynomial, in terms of a,b, and c." However, their promise is in fact only partly fulfilled. The purpose of the present paper is to clarify exactly what is known about characterizing permutation polynomials of the given shape.

An additional goal of this paper is to serve as an invitation to a fascinating subject, permutation polynomials over finite fields. This subject is accessible to anyone with some algebraic background, and abounds in unsolved problems and conjectures; it has honourable historical roots (Hermite, Dickson,...) and has attracted renewed interest in recent years because of significant applications in cryptography and combinatorics. For a good discussion of the main conjectures and open problems, and for some references concerning applications, the reader is referred to the recent article [5]. Any reader whose interest is more than superficially aroused (by the present paper and/or [5]) should consult Chapter 7 of [2], where she/he will find an extended discussion together with voluminous historical and bibliographic notes.

The point of focusing on binomials in this paper is twofold. First, they are the simplest non-trivial case (monomials are easily disposed of; see Prop. 1 below) and

they therefore serve as a convenient testing ground for ideas and results which might hold more generally. Second, by restricting attention to polynomials of a special shape, it is often possible to find useful results which may not generalize so readily. Some particularly striking examples of this phenomenon, for binomials, are the theorems of Niederreiter and Robinson referred to as Propositions 9 and 10 below; these say essentially that a binomial, of degree d, say, can permute only those finite fields which are sufficiently small (relative to d).

2. TERMINOLOGY AND MAIN RESULTS.

To begin, let us recall the terminology. Throughout, let F be a finite field, q its cardinality, F(X) the polynomial ring. Let $R = \{f \in F(X) \mid \deg f \leq q-1\}$ and let M be the set of all mappings $F \to F$. These are two vector spaces of the same dimension q over F. Associating to each $f \in F(X)$ the mapping $\hat{f}: F \to F$ it defines gives rise to a commutative diagram

$$\begin{array}{ccccc} & & F(X) & & \\ & \nearrow & & \searrow & \\ R & & \longrightarrow & & M \\ & & \varphi & & \end{array} \qquad \psi$$

(here $R \to F(X)$ is the inclusion). It is immediate that φ is an isomorphism of F-vector spaces: $\ker \varphi$ is trivial because a polynomial h over a field cannot have more than deg h roots. The non-zero elements of F form a multiplicative group F* of order q-1; hence $x^{q-1} = 1$ for all $0 \neq x \in F$ and $x^q = x$ for all x. It follows that the ideal $I = (X^q - X)F[(X)]$ is contained in the kernel of ψ. Since the quotient F[X]/I is clearly isomorphic (as vector space) to R, we have $\ker \psi = I$, so $F[X]/(X^q - X)F[X] \simeq R \simeq M$.

In particular, every mapping $F \to F$ is given by a unique polynomial of degree $\leq q-1$. One says that $f \in F[X]$ is a permutation polynomial if the corresponding mapping $\hat{f}$ is a permutation of F (equivalently, if $\hat{f}$ is onto, or one-to-one). We usually abbreviate "f is a permutation polynomial on F" to "f permutes F" in what follows. The problem of characterizing permutation polynomials (among all polynomials) by necessary and sufficient conditions on the coefficients is (easy in low degree and) intractable in general; see [1] and Chapter 7 of [2]. Even for binomials, by which we mean polynomials of the special form $f(X) = aX^i + bX^j + c$, it is not possible to give a complete answer, although there are important partial results, summarized below.

Now let $f(X) = aX^i + bX^j + c$ with $a,b,c \in F$, card F=q, with $a \neq 0$ and $i > j > 1$. Clearly f permutes F if and only if $X^i - \alpha X^j$ does, where $\alpha = -ba^{-1}$. (More generally, for any polynomial f we are free to alter the constant term, or multiply by a non-zero element, without affecting whether or not f permutes F, since these two operations correspond to composing with mappings which are obviously permutations.)

To determine when $X^i - \alpha X^j$ permutes $F (i > j > 1)$ we may assume $\alpha \neq 0$, for monomials are easily disposed of:

PROPOSITION 1. X^i permutes F if and only if g.c.d.$(i, q-1) = 1$.

PROOF. Put $\ell = $ g.c.d$(i, q-1)$. It is immediate, from the fact that the multiplicative group F* of F is cyclic of order q-1, that $\{x^i \mid x \in F^*\} = \{x^\ell \mid x \in F^*\}$ and that this set has cardinality $(q-1)/\ell$. This proves the claim. (Note, however, that it is not true that $x^i = x^\ell$ for each $x \in F$!)

Similarly, we can reduce to the case where g.c.d.(i,j)=1:

PROPOSITION 2. Let $f(X)=X^i-\alpha X^j$, $i>j\geq 1$, $0\neq\alpha\in F$, $e=$g.c.d.(i,j), $i'=i/e$, $j'=j/e$. Then g.c.d.$(i',j')=1$, and f permutes F if and only if $X^{i'}-\alpha X^{j'}$ permutes F and g.c.d.$(e,q-1)=1$.

PROOF. (see [3], lemma 5) $f(X)=(X^e)^{i'}-\alpha(X^e)^{j'}$ is a permutation polynomial if and only if both X^e and $X^{i'}-\alpha X^{j'}$ are, since the mapping defined by f is the composite of the mappings given by X^e and $X^{i'}-\alpha X^{j'}$; now use Prop. 1.

It is almost trivial to dispose of the case where α is an $(i-j)^{th}$ power:

PROPOSITION 3. Let $f(X)=X^i-\alpha X^j$, $i>j\geq 1$, $0\neq\alpha\in F$, $d=$g.c.d.$(i-j,q-1)$. Suppose $\alpha\in F^{i-j}$ (equivalently, $\alpha\in F^d$). Then f does not permute F. In particular, $f(X)=X^i-\alpha X^j$ is not a permutation polynomial if any of the following applies: $i=j+1$; $\alpha=1$; $\alpha=-1$ and $i-j$ or d is odd; $d=1$; $i-j$ is a power of char. F.

PROOF. $X^i-\alpha X^j=X^j(X^{i-j}-\alpha)$ has more than one root if (and only if) $\alpha\in F^{i-j}$; but permutation polynomials can have only one root. The "in particular" statements are all special cases.

In connection with Proposition 3 we mention the following criterion for α to be an $(i-j)^{th}$ power: in the notation of Proposition 3, $\alpha\in F^{i-j}$ if and only if $\alpha^{(q-1)/d}=1$. This is immediate from the fact that the multiplicative group F^* is cyclic of order $q-1$: in general, in a cyclic group of order $n=kd$ written multiplicatively, the d^{th} powers are exactly the k^{th} roots of unity.

With slightly more effort one can rule out the case $q\equiv 1 \pmod i$:

PROPOSITION 4. Let $f(X)=X^i-\alpha X^j$, $i>j\geq 1$, $0\neq\alpha\in F$, and assume i divides $q-1$. Then f does not permute F.

PROOF. We show more generally that when $1<i\mid q-1$, no polynomial f of degree i permutes F. This follows from a general criterion of (Hermite and) Dickson (see 7.4 and 7.5 of [2]) but is easy to prove directly from the following well-known fact, which is also the key ingredient of Dickson's criterion:

LEMMA 5. For an integer $s\geq 1$, $\sum_{x\in F} x^s=0$ unless $(q-1)\mid s$, in which case $\sum_{x\in F} x^s=-1$.

PROOF. Put $\sum_s=\sum_{x\in F} x^s$. Since $x^q=x$ for all $x\in F$, $\sum_s$ depends only on the congruence class of s modulo $q-1$. Thus it suffices to show $\sum_s=0$ for $1\leq s<q-1$ (the result for $s=q-1$ being clear). Choose $y\in F^*$ with $y^s\neq 1$ (e.g., let y be a generator for the (cyclic) group F^*). Then $\sum_s=\sum_{x\in F} x^s=\sum_{x\in F}(yx)^s=y^s\sum_s$, so $(1-y^s)\sum_s=0$; done.

Now, we complete the proof of (the indicated generalization of) Proposition 4. Suppose $f(X)=\sum_{j=0}^{i} a_j X^j$ is a polynomial of degree i, where $1<i\mid q-1$, and put $s=(q-1)/i$. Assume f is a permutation polynomial; we derive a contradiction. On the one hand, since f permutes F we have $0=\sum_{x\in F}(f(x))^s$ by Lemma 5. On the other hand, f^s has degree $q-1$, say $f(X)^s=\sum_{j=0}^{q-1} c_j X^j$. Then $0=\sum_{x\in F}(f(x))^s=\sum_{j=0}^{q-1} c_j \sum_{x\in F} x^j$.

Using Lemma 5 again, we get $0 = c_{q-1} \sum_{x \in F} x^{q-1} = -c_{q-1} \neq 0$; done.

A similar argument gives a further useful criterion, in terms of the parameter i-j:

PROPOSITION 6. Let $f(X) = X^i - \alpha X^j$, $i > j \geq 1, 0 \neq \alpha \in F$, and put $k = i-j$. Assume f permutes F, and suppose (without loss of generality) that $i < q-1$ and $k \geq 2$. Then either $i \nmid q-1+k$, or $(q-1+k)/i$ is a multiple of $p = \text{char. } F$. The second case cannot arise unless $p \mid k-1$.

PROPOSITION 6 generalizes [1], Theorem 2.8, which is the special case k=2. The proof of Proposition 6 is a natural generalization of the proof of Proposition 4; that is, Lemma 5 is the primary ingredient.

PROOF OF PROPOSITION 6. The last statement is clear since q is a multiple (actually, a power) of p. Now suppose $i \mid q-1+k$, say $is = q-1+k$, so $1 < s < q-1$, and assume f permutes F; we show $p \mid s$. Since $f(X) = X^i - \alpha X^j$ permutes F we have

$0 = \sum_{x \in F} (x^i - \alpha x^j)^s = \sum_{t=0}^{s} \binom{s}{t} (-\alpha)^t \sum_{x \in F} x^{i(s-t)+jt}$. But $i(s-t)+jt = is-kt = q-1+(1-t)k$, so the exponents in the sum, for $t = 0, 1, \ldots$, are $q-1+k$, $q-1$, $q-1-k, \ldots$ As before, it is only from t=1 that we get a non-zero contribution. But then the equation collapses to $0 = s\alpha$, a contradiction unless s=0 in F, that is, $p \mid s$. Done.

The problem of determining when $f(X) = aX^i + bX^j + c$ is a permutation polynomial is reduced, by the foregoing elementary observations, to the following: first, f permutes F if and only $X^i - \alpha X^j$ does, where $\alpha = -ba^{-1}$. For $X^i - \alpha X^j$, $i > j \geq 1$, we may assume $i < q-1$ and α is not an $(i-j)^{th}$ power (in particular $\alpha \neq 0$, and $i \neq j+1$, so $1 \leq j < i-1 < q-2$). We may assume further that g.c.d.$(i,j) = 1$ and $i \nmid q-1$. Finally, put $k = i-j$, then we may assume $d = $ g.c.d.$(k, q-1) > 1$ and $\alpha^{(q-1)/d} \neq 1$, and either $i \nmid q-1+k$ or $p \mid$ g.c.d.$(k-1, (q-1+k)/i)$.

For a concrete example which is not ruled out by any of the foregoing criteria, consider $f(X) = X^{45} - \alpha X^{17}$ where α is a non-square in the field F with 3^5 elements. Here f falls in the second case discussed in Proposition 6, and nothing we have done so far suffices to answer the question whether f permutes F. Of course that question can be answered by a finite computation, but what we are after is general criteria, similar to the above but more far-reaching, which settle the question not for a single f, but for all f satisfying some hypothesis.

For f of small degree a complete answer can be given from Dickson's criterion (cf. [2], page 352):

PROPOSITION 7. With $f(X) = X^i - \alpha X^j$ as above and $i \leq 5$, the only permutation polynomials over F (the field with cardinality q and characteristic p) are as follows:

(i) $f(X) = X^3 - \alpha X$, $p = 3$, $\alpha \notin F^2$

(ii) $f(X) = X^4 \pm 3X$, $q = 7$

(iii) $f(X) = X^4 - \alpha X$, $p = 2$, $\alpha \notin F^3$

(iv) $f(X) = X^5 - \alpha X$, $p = 5$, $\alpha \notin F^4$,

(v) $f(X) = X^5 \pm iX$, $q = 9$, $i^2 = -1$

(vi) $f(X) = X^5 \pm 2X^2$, $q = 7$.

The examples in (i), (iii) and (iv) generalize:

PROPOSITION 8. Let $f(X) = X^{p^s} - \alpha X^{p^r}$ where $s>r\geq 0, 0\neq\alpha\in F$, and F has cardinality q and characteristic p. Then

(a) f permutes F if and only if α is not a $(p^s - p^r)^{th}$ power in F;

(b) If α is a primitive root in F (i.e., a generator for the multiplicative group) then f permutes F, unless p=2 and g.c.d.$(s-r,n)=1$ where $q=p^n$.

PROOF. We have the "only if" part of (a) already, from Proposition 3. Conversely, suppose f fails to permute F; we show α is a $(p^s-p^r)^{th}$ power. Since f does not permute F we have $c_1 \neq c_2$ with $f(c_1)=f(c_2)$, i.e. $c_1^{p^s} - \alpha c_1^{p^r} = c_2^{p^s} - \alpha c_2^{p^r}$. But then $(c_1-c_2)^{p^s} = c_1^{p^s} - c_2^{p^s} = \alpha(c_1^{p^r} - c_2^{p^r})\ \alpha = (c_1 - c_2)^{p^r}$, so $\alpha = (c_1-c_2)^{p^s-p^r}$. This proves (a). For (b) it suffices to note that a primitive root is never a k^{th} power unless g.c.d.$(k,q-1)=1$, whereas for $k=p^s-p^r$ we have g.c.d.$(k,q-1)>1$, with the one exception indicated in the statement.

REMARK 1. Proposition 8 generalizes Proposition 2.10 of [1], where the case r=0 is dealt with. (Of course, this case together with Proposition 2 gives the full story: everything is a p^rth power, so α is a (p^s-p^r)th power if and only if α is a $(p^{s-r}-1)$th power.)

REMARK 2. The content of Proposition 8 is the observation that in characteristic p, $f(X)=X^{p^s} - \alpha X^{p^r}$ is nearly linear: $f(X \pm Y)=f(X) \pm f(Y)$. Hence f permutes F if and only if f has trivial kernel, that is, a unique root. (Since $f(X) = X^{p^s} - \alpha X^{p^r} = X^{p^r}(X^{p^s-p^r} - \alpha)$, f has a unique root if and only if α is not a $(p^s-p^r)^{th}$ power.) This observation proves more generally that when char. F=p, a polynomial of the shape $f(X) = \sum_{i\geq 0} a_i X^{p^i}$ (with all exponents powers of p) is a permutation polynomial on F if and only if f has no non-zero root in F, for any such f gives a map on F with the same nearly-linear property as above: $f(X \pm Y)=f(X) \pm f(Y)$. Compare [2], Theorem 7.9.

Examples (ii), (v) and (vi) in Proposition 7 point to a difficulty in the general problem: the "true" story is obscured by irritating anomalies in small fields. Indeed, at least in the case j=1, we have:

PROPOSITION 9. Let $f(X)=X^i - \alpha X$ with i not a power of char. F. Assume $q > (i^2-4i+6)^2$. Then f permutes F if and only if $\alpha=0$ and g.c.d.$(i,q-1)=1$.

For the proof see [1], Corollary 3.3., and [3], Lemma 3, page 208. Of course the "if" part is trivial. The point is that the "only if" part, which we have seen violated in small examples, becomes true as soon as the field is large enough (relative to the degree of f).

In fact the same phenomenon (good behavior as soon as the field is sufficiently large) holds for j>1 too, although it is harder to be explicit about the bound:

PROPOSITION 10. Let $f(X) = X^i - \alpha X^j$, $0\neq\alpha\in F$, $1<j<i$, g.c.d.$(i,j)=1$. There is a constant $C = C(i)$ such that if $q>C$ then f does not permute F.

This is essentially Lemma 7 of [3], to which we refer for the proof.

An interesting complement to Propositions 9 and 10 is the following result, proved as Theorem 2 in [4]. Suppose $d|q-1$ and $d<q-1$. Then, provided q is sufficiently large, $X^{d+1}-\alpha X$ is a permutation polynomial for at least one choice of α.

3. CONCLUSION.

In a sense, the results summarized above provide a complete answer to our question of when $f(X) = X^i - \alpha X^j$ permutes F: Use Proposition 2 to reduce to the case where g.c.d.(i,j) = 1, and then refer to Propositions 8 or 9 (if j = 1) or Proposition 10 (if j > 1). In either case we find essentially that f can permute F only if F is one of a finite family of finite fields.

Thus for fixed $f(X) = X^i - \alpha X^j$ our question loses interest as soon as q is sufficiently large relative to i. Nonetheless, it would be of interest to have criteria, in addition to the elementary ones discussed here, to better handle the question in those small fields not ruled out by Proposition 9 and (an explicit version of) Proposition 10. One reason for the desirability of such criteria is that permutation polynomials do arise in applications of finite fields. Of special significance in this regard are the complete mapping polynomials over F (see [3]). These are permutation polynomials f such that f(X) + X is also a permutation polynomial. For our binomials $f(X) = X^i-\alpha X^j$, f(X) + X is not a binomial unless j=1. Thus, criteria for $X^i-\alpha X$ to permute F, for those small fields not ruled out by Proposition 9, would enable us to discuss complete mapping binomials of the same shape. For further results in this direction, especially in the case i=(q+1)/2, q odd, see [3], 3 as well as [2], 7.11 and 7.13.

ACKNOWLEDGEMENTS. Research supported in part by a grant from Advisory Research Committee, Queen's University, Kingston, Ontario. This research was completed during a sabbatical leave spent at McMaster University, Hamilton, Ontario, whose hospitality the author is happy to acknowledge.

REFERENCES.

1. MOLLIN, R.A. and SMALL, C., On Permutation Polynomials over Finite Fields, Int. Jour. Maths. and Math. Sci. 10(1987), 535-544.
2. LIDL, R. and NIEDERREITER, H., Finite Fields, Addison-Wesley, 1983.
3. NIEDERREITER, H. and ROBINSON, K.H., Complete Mappings of Finite Fields, J. Austral. Math. Soc. (Series A) 33(1982), 197-212.
4. CARLITZ, L. and WELLS, C., The number of solutions of a special system of equations in a finite field, Acta. Arith. 12 (1966), 77-84.
5. LIDL, R. and MULLEN, G.L., When Does a Polynomial Over a Finite Field Permute the Elements of the Field? Amer. Math. Monthly 95 (1988), 243-246.