SOME FAMILIES OF PERMUTATION POLYNOMIALS OVER FINITE FIELDS

MICHAEL E. ZIEVE

Abstract. We give necessary and sufficient conditions for a polynomial of the form $x^r(1 + x^v + x^{2v} + \cdots + x^{kv})^t$ to permute the elements of the finite field $\mathbb{F}_q$. Our results yield especially simple criteria in case $(q-1)/\gcd(q-1,v)$ is a small prime.

1. Introduction

A polynomial over a finite field is called a *permutation polynomial* if it permutes the elements of the field. These polynomials first arose in work of Betti [3], Mathieu [6] and Hermite [5] as a way to represent permutations. A general theory was developed by Hermite [5] and Dickson [4], with many subsequent developments by Carlitz and others.

It is a challenging problem to produce permutation polynomials of 'nice' forms. Recently, Akbary, Wang and Wang [2, 9] studied binomials of the form $x^u + x^r$ over $\mathbb{F}_q$ in the case that $d := \gcd(q-1, u-r)$ satisfies $(q-1)/d \in \{3,5,7\}$. Their results were surprising: they gave necessary and sufficient criteria for such binomials to permute $\mathbb{F}_q$, in terms of the period of a (generalized) Lucas sequence in $\mathbb{F}_q$. Their proofs were quite complicated, using lengthy calculations involving coefficients of Chebychev polynomials, lacunary sums of binomial coefficients, determinants of circulant matrices, and various unpublished results about factorizations of Chebychev polynomials, among other things. Also, their proofs required completely different arguments in each of the cases $(q-1)/d \in \{3,5,7\}$.

One naturally wonders whether there might be a uniform approach which works for arbitrary d, and yields the results of [9, 2] as special cases. We present such an approach in this paper, giving short and simple proofs which do not use any of the above-mentioned ingredients. Our results apply to the more general class of polynomials $f(x) := x^r h_k(x^v)^t$, where $h_k(x) := x^{k-1} + x^{k-2} + \cdots + 1$ and r, v, k, t are positive

Date: March 3, 2008.

2000 *Mathematics Subject Classification.* 11T06.

Key words and phrases. Permutation polynomial, finite field, binomial, Lucas sequence.

integers. The forthcoming paper [1] uses the same methods as [2] to prove some partial results in case $t = 1$ and $v \mid (q-1)$.

The statements of our results use the notation $s := \gcd(v, q-1)$, $d := (q-1)/s$, and $e := v/s$. Note that $\gcd(d, e) = 1$. Also μ_d denotes the set of d^{th} roots of unity in $\mathbb{F}_q$, and p is the characteristic of $\mathbb{F}_q$.

Our first result gives necessary and sufficient conditions for f to be a permutation polynomial:

Proposition 1.1. *f permutes $\mathbb{F}_q$ if and only if all of the following hold:*

(1) $\gcd(r, s) = \gcd(d, k) = 1$
(2) $\gcd(d, 2r + vt(k-1)) \leq 2$
(3) $k^{st} \equiv (-1)^{(d+1)(r+1)} \pmod{p}$
(4) $g(x) := x^r((1 - x^{ke})/(1 - x^e))^{st}$ *is injective on* $\mu_d \setminus \mu_1$
(5) $(-1)^{(d+1)(r+1)} \notin g(\mu_d \setminus \mu_1)$.

In case d is an odd prime, this specializes to the following:

Corollary 1.2. *Suppose the first three conditions of Proposition 1.1 hold, and d is an odd prime. Pick $\omega \in \mathbb{F}_q$ of order d. Then f permutes $\mathbb{F}_q$ if and only if there exists $\theta \in \mathbb{F}_d[x]$ with $\theta(0) = 0$ such that $(2r + (k-1)vt)x + \theta(x^2)$ permutes $\mathbb{F}_d$ and, for every i with $0 < i < d/2$, we have*

$$\omega^{\theta(i^2)} = \left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st}.$$

In the cases $d = 3, 5, 7$ studied in [9] and [2], it remains to consider permutation polynomials of $\mathbb{F}_d$ of certain forms. This is quite simple to analyze directly, and it is also a consequence of the results of Betti (1851) and Hermite (1863). The conclusion is as follows:

Corollary 1.3. *Suppose the first three conditions of Proposition 1.1 hold, and d is an odd prime. Pick $\omega \in \mathbb{F}_q$ of order d.*

(1) *If*

$$(*) \qquad \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \in \mu_{st} \text{ for every } \zeta \in \mu_d \setminus \mu_1$$

then f permutes $\mathbb{F}_q$.

(2) *If $d = 3$ then f always permutes $\mathbb{F}_q$.*
(3) *If $d = 5$ then f permutes $\mathbb{F}_q$ if and only if $(*)$ holds.*
(4) *If $d = 7$ then f permutes $\mathbb{F}_q$ if and only if either $(*)$ holds or there exists $\epsilon \in \{1, -1\}$ such that*

$$\left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st} = \omega^{2\epsilon(2r+(k-1)vt)i}$$

for every $i \in \{1, 2, 4\}$.

It is straightforward to deduce the results of [9, 2, 1] from this result, by writing the generalized Lucas sequences in terms of roots of unity. However, our formulation seems to be more useful for both theoretical and practical purposes.

We can treat larger values of d as well, but at the cost of having a longer list of possibilities. For instance, with the hypotheses and notation of the above result, if $d = 11$ then f permutes $\mathbb{F}_q$ if and only if either $(*)$ holds or there is some $\psi \in \mathcal{C}$ such that

$$\left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st} = \omega^{(2r+(k-1)vt)\psi(i)}$$

for every $i \in (\mathbb{F}_{11}^*)^2$, where $\mathcal{C}$ is the union of the sets $\{mi : m \in \{\pm 3, \pm 5\}\}$, $\{5m^3i^4 + m^7i^3 - 2mi^2 - 4m^5i : m \in \mathbb{F}_{11}^*\}$, and $\{4m^3i^4 + m^7i^3 - 2mi^2 - 5m^5i : m \in \mathbb{F}_{11}^*\}$.

2. Preliminary lemma

We begin with a simple lemma reducing the question whether a polynomial permutes $\mathbb{F}_q$ to the question whether a related polynomial permutes a particular subgroup of $\mathbb{F}_q^*$. Here, for any positive integer d, let μ_d denote the set of d^{th} roots of unity in $\mathbb{F}_q$.

Lemma 2.1. *Pick $d, r > 0$ with $d \mid (q-1)$, and let $h \in \mathbb{F}_q[x]$. Then $f(x) := x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if both*

(1) $\gcd(r, (q-1)/d) = 1$ *and*
(2) $x^r h(x)^{(q-1)/d}$ *permutes* μ_d.

Proof. Write $s := (q-1)/d$. For $\zeta \in \mu_s$, we have $f(\zeta x) = \zeta^r f(x)$. Thus, if f permutes $\mathbb{F}_q$ then $\gcd(r, s) = 1$. Conversely, if $\gcd(r, s) = 1$ then the values of f on $\mathbb{F}_q$ consist of all the s^{th} roots of the values of

$$f(x)^s = x^{rs} h(x^s)^s.$$

But the values of $f(x)^s$ on $\mathbb{F}_q$ consist of $f(0)^s = 0$ and the values of $g(x) := x^r h(x)^s$ on $(\mathbb{F}_q^*)^s$. Thus, f permutes $\mathbb{F}_q$ if and only if g is bijective on $(\mathbb{F}_q^*)^s = \mu_d$. □

Remark. A more complicated criterion for f to permute $\mathbb{F}_q$ was given by Wan and Lidl [8, Thm. 1.2].

3. Proofs

In this section we consider polynomials of the form $f(x) := x^r h_k(x^v)^t$, where $h_k(x) = x^{k-1} + x^{k-2} + \cdots + 1$ and r, v, k, t are positive integers. We maintain this notation throughout this section, and we also define $s := \gcd(v, q-1)$, $d := (q-1)/s$, and $e := v/s$. Note that $\gcd(d, e) = 1$.

We begin with some easy cases with d small:

Proposition 3.1. *If $d = 1$ then $f(x)$ permutes $\mathbb{F}_q$ if and only if $\gcd(k,p) = \gcd(r,s) = 1$. If $d = 2$ then $f(x)$ permutes $\mathbb{F}_q$ if and only if $\gcd(k,2) = \gcd(r,s) = 1$ and $k^{st} \equiv (-1)^{r+1} \pmod{p}$.*

Proof. By Lemma 2.1, f permutes $\mathbb{F}_q$ if and only if $\gcd(r,s) = 1$ and $g(x) := x^r h_k(x^e)^{st}$ permutes μ_d. If $d = 1$, the latter condition just says $\gcd(k,p) = 1$, since $g(1) = k^{(q-1)t}$. If $d = 2$ then we must have $h_k(-1) \neq 0$, so k is odd, whence $g(-1) = (-1)^r$; since $g(1) = k^{st}$, the result follows. $\square$

We could treat a few more values of d by the same method as above, but this requires handling several cases already for $d = 3$. We will return to this question later, after proving some results which simplify the analysis.

Our next result gives necessary and sufficient conditions for f to permute $\mathbb{F}_q$; these conditions refine the ones we get directly from Lemma 2.1.

Proposition 3.2. *f permutes $\mathbb{F}_q$ if and only if all of the following hold:*

1. $\gcd(r,s) = \gcd(d,k) = 1$
2. $\gcd(d, 2r + vt(k-1)) \leq 2$
3. $k^{st} \equiv (-1)^{(d+1)(r+1)} \pmod{p}$
4. $g(x) := x^r((1-x^{ke})/(1-x^e))^{st}$ *is injective on* $\mu_d \setminus \mu_1$
5. $(-1)^{(d+1)(r+1)} \notin g(\mu_d \setminus \mu_1)$.

Proof. By Lemma 2.1, f permutes $\mathbb{F}_q$ if and only if $\gcd(r,s) = 1$ and $\hat{g}(x) := x^r h_k(x^e)^{st}$ permutes μ_d. So assume $\gcd(r,s) = 1$. For $\zeta \in \mu_d \setminus \mu_1$, we have

$$\hat{g}(\zeta) = \zeta^r \left(\frac{1-\zeta^{ke}}{1-\zeta^e}\right)^{st},$$

so $\hat{g}(\zeta) = 0$ if and only if $\zeta \in \mu_{ke}$. Thus, if $\hat{g}$ permutes μ_d then $\gcd(d,k) = 1$ and $\gcd(p,k) = 1$ (since $\hat{g}(1) = k^{st}$). Henceforth we assume $\gcd(pd,k) = 1$, so $\hat{g}$ maps μ_d into μ_d, and thus bijectivity of $\hat{g}$ is equivalent to injectivity.

If $\hat{g}$ permutes μ_d then

$$\prod_{\zeta \in \mu_d} \hat{g}(\zeta) = \prod_{\zeta \in \mu_d} \zeta = (-1)^{d+1};$$

but we compute

$$\prod_{\zeta\in\mu_d} \hat{g}(\zeta) = k^{st} \prod_{\zeta\in\mu_d\setminus\mu_1} \zeta^r \left(\frac{1-\zeta^{ke}}{1-\zeta^e}\right)^{st}$$
$$= (-1)^{(d+1)r} k^{st} \quad \text{(since } \gcd(d,k)=1).$$

Thus, if $\hat{g}$ permutes μ_d then $k^{st} = (-1)^{(d+1)(r+1)}$ in $\mathbb{F}_q$.

Next, if $\hat{g}$ permutes μ_d then for $\zeta \in \mu_d \setminus \mu_2$ we have $\hat{g}(\zeta) \neq \hat{g}(1/\zeta)$; but $\hat{g}(1/\zeta) = \hat{g}(\zeta)/\zeta^{2r+est(k-1)}$, so we conclude that $\gcd(d, 2r+est(k-1)) \leq 2$. The proof is complete. □

Remark. The fact that $k^{st} \equiv (-1)^{(d+1)(r+1)} \pmod p$ was proved by Park and Lee [7] (in case $t = 1$) by means of a lengthy computation of the determinants of some circulant matrices. The case $t = 1$ of Proposition 3.2 improves the main result of [1]; those authors gave some necessary conditions for f to permute $\mathbb{F}_q$, and some sufficient conditions, and gave necessary and sufficient conditions in the special case that d is an odd prime less than $2p + 1$.

When d is an odd prime, the criteria of Proposition 3.2 can be stated in terms of permutations of $\mathbb{F}_d$:

Corollary 3.3. *Suppose the first three conditions of Proposition 3.2 hold, and d is an odd prime. Pick $\omega \in \mathbb{F}_q$ of order d. Then f permutes $\mathbb{F}_q$ if and only if there exists $\theta \in \mathbb{F}_d[x]$ with $\theta(0) = 0$ and $\deg(\theta) < (d-1)/2$ such that $(2r+(k-1)vt)x+\theta(x^2)$ permutes $\mathbb{F}_d$ and, for every i with $0 < i < d/2$, we have*

$$\omega^{\theta(i^2)} = \left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st}.$$

Proof. Since d is odd, squaring permutes μ_d, so condition (4) of Proposition 3.2 is equivalent to injectivity of $g(x^2)$ on $\mu_d \setminus \mu_1$. For $\zeta \in \mu_d \setminus \mu_1$, we have

$$g(\zeta^2) = \zeta^{2r} \left(\frac{1-\zeta^{2ke}}{1-\zeta^{2e}}\right)^{st} = \zeta^{2r+(k-1)est} \left(\frac{\zeta^{ke} - \zeta^{-ke}}{\zeta^e - \zeta^{-e}}\right)^{st}.$$

For $i \in \mathbb{Z} \setminus d\mathbb{Z}$, let $\psi(i)$ be the unique element of $\mathbb{Z}/d\mathbb{Z}$ such that

$$\omega^{\psi(i)} = \left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st}.$$

Defining $\psi(i) = 0$ if $i \in d\mathbb{Z}$, it follows that ψ induces a map from $\mathbb{Z}/d\mathbb{Z}$ to itself, with the properties $\psi(-i) = \psi(i)$ and $g(\omega^{2i}) = \omega^{i(2r+(k-1)vt)+\psi(i)}$. Conditions (4) and (5) are equivalent to bijectivity of the map $\chi : i \mapsto in + \psi(i)$ on $\mathbb{Z}/d\mathbb{Z}$, where $n := 2r + (k-1)vt$. Since $\psi(-i) = \psi(i)$, we can write $\psi(i) = \theta(i^2)$ where $\theta \in \mathbb{F}_d[x]$ has degree less than $(d-1)/2$ and has no constant term. $\square$

For small d, there are only a few maps $\hat{\theta} : \mathbb{F}_d \to \mathbb{F}_d$ for which $x+\hat{\theta}(x^2)$ permutes $\mathbb{F}_d$; this in turn yields manageable descriptions of the possible permutation polynomials in these cases. Assuming $\hat{\theta}(0) = 0$ and $\deg(\hat{\theta}) < (d-1)/2$, the only such map for $d = 3$ and $d = 5$ is $\hat{\theta} = 0$. For $d = 7$ there are three possibilities for $\hat{\theta}$, namely $\hat{\theta} = \mu x^2$ with $\mu \in \{0, 2, -2\}$. For $d = 11$ there are 25 possibilities for $\hat{\theta}$, but these comprise just five classes modulo the equivalence $\hat{\theta}(x) \sim \hat{\theta}(\alpha^2 x)/\alpha$ with $\alpha \in \mathbb{F}_d^*$. For $d = 13$ there are 133 possibilities for $\hat{\theta}$, including 14 classes under the above equivalence. We checked via computer that, for these values of d, every such map $\hat{\theta}$ occurs as $\theta/(2r + (k-1)vt)$ for some permutation polynomial f as in Corollary 3.3, even if we restrict to $k = 2$ and $t = e = 1$.

Corollary 3.4. *Suppose the first three conditions of Proposition 3.2 hold, and d is an odd prime. Pick $\omega \in \mathbb{F}_q$ of order d.*

(a) *If*

$$(*) \qquad \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \in \mu_{st} \text{ for every } \zeta \in \mu_d \setminus \mu_1$$

then f permutes $\mathbb{F}_q$.

(b) *If $d = 3$ then f always permutes $\mathbb{F}_q$.*

(c) *If $d = 5$ then f permutes $\mathbb{F}_q$ if and only if $(*)$ holds.*

(d) *If $d = 7$ then f permutes $\mathbb{F}_q$ if and only if either $(*)$ holds or there exists $\epsilon \in \{1, -1\}$ such that*

$$\left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st} = \omega^{2\epsilon(2r+(k-1)vt)i}$$

for every $i \in \{1, 2, 4\}$.

(e) *If $d = 11$ then f permutes $\mathbb{F}_q$ if and only if either $(*)$ holds or there is some $\psi \in \mathcal{C}$ such that*

$$\left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st} = \omega^{(2r+(k-1)vt)\psi(i)}$$

for every $i \in (\mathbb{F}_{11}^*)^2$, where $\mathcal{C}$ is the union of the sets $\{mi : m \in \{\pm 3, \pm 5\}\}$, $\{5m^3i^4 + m^7i^3 - 2mi^2 - 4m^5i : m \in \mathbb{F}_{11}^*\}$, and $\{4m^3i^4 + m^7i^3 - 2mi^2 - 5m^5i : m \in \mathbb{F}_{11}^*\}$.

Proof. We maintain the notation of Corollary 3.3. Condition $(*)$ is the trivial case $\theta = 0$. If $d = 3$ or $d = 5$, we plainly must have $\theta = 0$ (as was first proved by Betti in 1851 [3]). This proves the result for $d = 5$.

For $d = 3$, condition (3) implies $k \equiv \pm 1 \pmod 3$, so for $\zeta \in \mu_d \setminus \mu_1$ we have $\zeta^k - \zeta^{-k} = \pm(\zeta - \zeta^{-1})$; since either q or s is even, this implies $(\zeta^k - \zeta^{-k})^s = (\zeta - \zeta^{-1})^s$, so $(*)$ holds.

Suppose $d = 7$, and write $n := 2r + (k-1)vt$; then $\gcd(7, n) = 1$ by condition (2). It is easy to determine the possibilities for θ, as was first done by Hermite in 1863 [5]: $\theta = \mu x^2$ where $\mu \in \{0, 2n, -2n\}$. The result follows.

The case $d = 11$ is treated similarly. □

References

[1] A. Akbary, S. Alaric and Q. Wang, *On some classes of permutation polynomials*, Int. J. Number Theory, to appear.

[2] A. Akbary and Q. Wang, *On some permutation polynomials over finite fields*, Int. J. Math. Math. Sci. (2005) 2631–2640.

[3] E. Betti, *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo*, Ann. Sci. Mat. Fis. **2** (1851) 5–19; (=Opere Matematiche, v.1, 17–27).

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

[5] Ch. Hermite, *Sur les fonctions de sept lettres*, C. R. Acad. Sci. Paris **57** (1863) 750–757.

[6] É. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, J. Math. Pures Appl. **6** (1861) 241–323.

[7] Y. H. Park and J. B. Lee, *Permutation polynomials with exponents in an arithmetic progression*, Bull. Austral. Math. Soc. **57** (1998) 243–252.

[8] D. Wan and R. Lidl, *Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure*, Monatsh. Math. **112** (1991) 149–163.

[9] L. Wang, *On permutation polynomials*, Finite Fields Appl. **8** (2002) 311–322.

Center for Communications Research, 805 Bunn Drive, Princeton NJ 08540-1966, USA.

E-mail address: zieve@math.rutgers.edu

URL: http://www.math.rutgers.edu/~zieve/