ON SOME PERMUTATION POLYNOMIALS OVER $\mathbb{F}_q$ OF THE FORM $x^r h(x^{(q-1)/d})$

MICHAEL E. ZIEVE

Abstract. Several recent papers have given criteria for certain polynomials to permute $\mathbb{F}_q$, in terms of the periods of certain generalized Lucas sequences. We show that these results follow from a more general criterion which does not involve such sequences.

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 [5], Mathieu [25] and Hermite [20] as a way to represent permutations. A general theory was developed by Hermite [20] and Dickson [13], with many subsequent developments by Carlitz and others. The study of permutation polynomials has intensified in the past few decades, due both to various applications (e.g., [8, 11, 14, 30]) and to an increasing appreciation of the depth of the subtleties inherent to permutation polynomials themselves (for instance, work on permutation polynomials led to a bound on the automorphism group of a curve with ordinary Jacobian [19]).

The interesting aspect of permutation polynomials is the interplay between two different ways of representing an object: combinatorially, as a mapping permuting a set, and algebraically, as a polynomial. This is exemplified by one of the first results in the subject, namely that there is no permutation polynomial over $\mathbb{F}_q$ of degree $q-1$ if $q > 2$ [20]. Much recent work has focused on low-degree permutation polynomials, as these have quite remarkable properties: for instance, a polynomial of degree at most $q^{1/4}$ which permutes $\mathbb{F}_q$ will automatically permute $\mathbb{F}_{q^n}$ for infinitely many n. The combined efforts of several mathematicians have led to a handful of families of such polynomials, and to an avenue towards proving that there are no others [13, 12, 9, 15, 26, 10, 23, 16, 17, 18].

2000 *Mathematics Subject Classification.* 11T06.

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

A different line of research focuses not on the degree of a permutation polynomial but instead on the number of terms. The simplest class of nonconstant polynomials are the monomials x^n with $n > 0$, and one easily checks that x^n permutes $\mathbb{F}_q$ if and only if n is coprime to $q-1$. However, for binomials the situation becomes much more mysterious. Despite the attention of numerous authors since the 1850's (cf., e.g., [5, 25, 20, 6, 7, 27, 31, 29, 32, 21, 34, 3, 24]), the known results seem far from telling the full story of permutation binomials. This brings us to the present paper. The recent papers [34, 2, 3, 1] gave criteria for certain binomials to permute $\mathbb{F}_q$, in terms of the period of an associated generalized Lucas sequence. Many of these results involved binomials of the form $x^u + x^r$ where $\gcd(u-r, q-1) \geq (q-1)/7$; in our previous paper [35] we showed that these results can be derived more simply (and more generally) without using such sequences. In this paper we consider the remaining results from [34, 2, 3, 1].

In [3], Akbary and Wang considered binomials of the form $f(x) = x^u + x^r$ with $u > r > 0$. They gave sufficient conditions for f to permute $\mathbb{F}_q$ in terms of the period of the sequence ($a_n \bmod p$), where p is the characteristic of $\mathbb{F}_q$ and, with $d := (q-1)/\gcd(q-1, u-r)$,

$$a_n := \sum_{t=1}^{\frac{d-1}{2}} \left(2\cos\frac{\pi(2t-1)}{d}\right)^n.$$

(One can show that every a_n is an integer.)

As an application, they gave necessary and sufficient conditions for $x^u + x^r$ to permute $\mathbb{F}_q$ in the following two special cases:

(1) $p \equiv 1 \pmod{d}$ and $d \mid \log_p q$.
(2) $p \equiv -1 \pmod{d}$.

The proofs in [3] relied on facts about the coefficients of Chebychev polynomials, Hermite's criterion, properties of recursive sequences, lacunary sums of binomial coefficients, and various unpublished results about factorizations of Chebychev polynomials, among other things. In this paper we give quick proofs which avoid these ingredients and yield more general results. Our treatment does not involve the sequence a_n: instead, we show that when the Akbary–Wang condition on a_n is satisfied, the hypotheses of our more general result are also satisfied.

We will prove the following sufficient condition for permutation binomials, in which (for any $d > 0$) μ_d denotes the set of d^{th} roots of unity in the algebraic closure of $\mathbb{F}_q$:

Theorem 1.1. *Pick $u > r > 0$ and $a \in \mathbb{F}_q^*$. Write $s := \gcd(u-r, q-1)$ and $d := (q-1)/s$. Suppose that $(\eta + a/\eta) \in \mu_s$ for every $\eta \in \mu_{2d}$.*

Then $x^u + ax^r$ *permutes* $\mathbb{F}_q$ *if and only if* $-a \notin \mu_d$, $\gcd(r, s) = 1$ *and* $\gcd(2d, u + r) \leq 2$.

We emphasize that, unlike [3], we allow binomials having non-monic terms. The condition in [3] looks quite different from that in Theorem 1.1, since the former requires a constraint on the period of $(a_n \bmod p)$; however, in Section 3 we will show that the hypotheses of Theorem 1.1 are satisfied whenever the hypotheses of [3, Thm. 1.1] are satisfied.

In [1], the two families of permutation binomials from [3] are generalized to families of permutation polynomials of the form $x^r(1+x^s+x^{2s}+\cdots+x^{ks})$, with similar proofs to those in [3]. We now exhibit two general families of permutation polynomials which include the polynomials from [3] and [1] as special cases.

Theorem 1.2. *Let* $d, r > 0$ *satisfy* $d \mid (q-1)$. *Suppose that* $q = q_0^m$ *where* $q_0 \equiv 1 \pmod{d}$ *and* $d \mid m$, *and pick* $h \in \mathbb{F}_{q_0}[x]$. *Then* $f(x) := x^r h(x^{(q-1)/d})$ *permutes* $\mathbb{F}_q$ *if and only if* $\gcd(r, (q-1)/d) = 1$ *and* h *has no roots in* μ_d.

This is equivalent to a result of Laigle-Chapuy [22], who has a different proof. The first class of permutation binomials from [3] is the special case that $q_0 = p$ and $h = x^e + 1$, where $\gcd(e, d) = 1$.

In our next result we use the notation $h_k(x) := x^{k-1} + x^{k-2} + \cdots + 1$.

Theorem 1.3. *Pick integers* $t \geq 0$ *and* $r, v, k, \ell > 0$, *and put* $s := \gcd(q-1, v)$, $d := (q-1)/s$, *and* $d_0 := d/\gcd(d, \ell-1)$. *Suppose that* $q = q_0^m$, *where* m *is even and* $q_0 \equiv -1 \pmod{d}$. *Pick* $\hat{h} \in \mathbb{F}_{q_0}[x]$ *and let* $h := h_k(x)^t \hat{h}(h_\ell(x)^{d_0})$. *Then* $f := x^r h(x^v)$ *permutes* $\mathbb{F}_q$ *if and only if* $\gcd(r, s) = 1$, $\gcd(2r + (k-1)tv, 2d) = 2$ *and* h *has no roots in* μ_d.

The second class of permutation binomials from [3] is the special case that $q_0 = p$ and $h = h_2$.

Remark. Some of the above results appear in [4]. Specifically, a similar proof of Theorem 1.2 is given as [4, Cor. 2.3], and a special case of Theorem 1.3 is [4, Thm. 4.4]. These results were obtained independently and simultaneously in December 2006. Q. Wang has informed us that he obtained [4, Thm. 4.1] after reading a preliminary version of the present paper. However, [4] does not contain the main result of this paper, namely that recursive sequences are not needed for results on permutation polynomials. The publication of the present paper was delayed due to misunderstandings caused by the overlap with [4].

Notation: Throughout this paper, q is a power of the prime p, and μ_d denotes the set of d^{th} roots of unity in the algebraic closure of $\mathbb{F}_q$. Also, $h_k(x) := x^{k-1} + x^{k-2} + \cdots + 1$.

2. Proofs

We begin with a simple lemma reducing the question of whether a polynomial permutes $\mathbb{F}_q$ to the question of whether a related polynomial permutes a particular subgroup of $\mathbb{F}_q^*$.

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 $(\mathbb{F}_q^*)^s = \mu_d$. $\square$

Remark. A version of this result is in [28, Thm. 2.3]. A different criterion for f to permute $\mathbb{F}_q$ was given by Wan and Lidl [33, Thm. 1.2].

The difficulty in applying Lemma 2.1 is verifying condition (2). Here is one situation where this is easy:

Corollary 2.2. *Pick $d, r, n > 0$ with $d \mid (q-1)$, and let $h \in \mathbb{F}_q[x]$. Suppose $h(\zeta)^{(q-1)/d} = \zeta^n$ for every $\zeta \in \mu_d$. Then $f(x) := x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if* $\gcd(r+n, d) = \gcd(r, (q-1)/d) = 1$.

Our next results give choices for the parameters satisfying the hypotheses of Corollary 2.2.

Proof of Theorem 1.2. We may assume $\gcd(r, (q-1)/d) = 1$, since otherwise f would not permute $\mathbb{F}_q$ (by Lemma 2.1). Since $q_0 \equiv 1 \pmod{d}$, we have

$$\frac{q_0^d - 1}{q_0 - 1} = \sum_{i=0}^{d-1} q_0^i \equiv 0 \pmod{d}.$$

Hence $q_0 - 1$ divides $(q_0^d - 1)/d$, which divides $(q-1)/d$. Since $d \mid (q_0 - 1)$, it follows that d divides $(q-1)/d$; so since $\gcd(r, (q-1)/d) = 1$ we have $\gcd(r, q-1) = 1$.

For $\zeta \in \mu_d$ we have $\zeta \in \mathbb{F}_{q_0}$, so $h(\zeta) \in \mathbb{F}_{q_0}$. Since $f(0) = 0$, if f permutes $\mathbb{F}_q$ then $h(\zeta) \neq 0$. Conversely, if $h(\zeta) \neq 0$ then (since $q_0 - 1$ divides $(q-1)/d$) we have $h(\zeta)^{(q-1)/d} = 1$. Now the result follows from Corollary 2.2 (with $n = d$). $\square$

Remark. Theorem 1.2 is a reformulation of a result from [22]. Note that [22, Thm. 4.3] is false, a counterexample being $P = x^3 + x$ over $\mathbb{F}_3$; to correct it one should remove the polynomials P.

We now exhibit some polynomials h for which we can determine when h has roots in μ_d.

Corollary 2.3. *Pick positive integers d, e, r, k, t with $d \mid (q-1)$ and $\gcd(d, e) = 1$. Suppose that $q = q_0^m$ where $q_0 \equiv 1 \pmod{d}$ and $d \mid m$. Then $f(x) := x^r h_k(x^{e(q-1)/d})^t$ permutes $\mathbb{F}_q$ if and only if* $\gcd(k, pd) = \gcd(r, (q-1)/d) = 1$.

Remark. The case that $q_0 = p$, $k = 2$, and $t = 1$ was treated in [3]. The case that $q_0 = p$, $t = e = 1$, and both q and d are odd was treated in [1]. The results in both [3] and [1] involved the superfluous condition $\gcd(2r + (k-1)es, d) = 1$.

Proof of Theorem 1.3. Our hypotheses imply the divisibility relations

$$q_0 - 1 = \frac{q_0^2 - 1}{q_0 + 1} \,\Big|\, \frac{q-1}{q_0+1} \,\Big|\, \frac{q-1}{d} = s.$$

We may assume $h(x^e)$ has no roots in μ_d, since otherwise Lemma 2.1 would imply that f does not permute $\mathbb{F}_q$. Since $\gcd(d, e) = 1$, this says that h has no roots in μ_d. Hence $\hat{h}(h_\ell(x)^{d_0})$ has no roots in μ_d. For $\zeta \in \mu_d \setminus \mu_1$, the hypothesis $d \mid (q_0 + 1)$ implies that $\zeta^{q_0} = 1/\zeta$, so

$$h_\ell(\zeta)^{q_0} = \left(\frac{\zeta^\ell - 1}{\zeta - 1}\right)^{q_0} = \frac{\zeta^{-\ell} - 1}{\zeta^{-1} - 1} = \frac{h_\ell(\zeta)}{\zeta^{\ell-1}};$$

hence $h_\ell(\zeta)^{d_0 q_0} = h_\ell(\zeta)^{d_0}$, so $h_\ell(\zeta)^{d_0} \in \mathbb{F}_{q_0}$. Also $h_\ell(1) \in \mathbb{F}_{q_0}$. Thus, for any $\zeta \in \mu_d$ we have $\hat{h}(h_\ell(\zeta^e)^{d_0}) \in \mathbb{F}_{q_0}^*$. Since $(q_0 - 1) \mid s$, we conclude that $h(\zeta^e)^s = h_k(\zeta^e)^{ts}$. As above, $h_k(\zeta)^{t(q_0-1)} = 1/\zeta^{t(k-1)}$, so $h(\zeta^e)^s = 1/\zeta^{e(k-1)ts/(q_0-1)}$; hence the result follows from Corollary 2.2. □

Remark. There would be counterexamples to Theorem 1.3 if we did not require m to be even; such examples would necessarily have $d = 2$. Also, Theorem 1.3 immediately generalizes to the case that h is the product of several polynomials having the same shapes as the two factors of h described in the theorem. Moreover, we may replace h by any polynomial congruent to it modulo $x^d - 1$.

Corollary 2.4. *Pick positive integers t, d, e, r, k with $d \mid (q-1)$ and $\gcd(d, e) = 1$, and put $s := (q-1)/d$. Suppose that $q = q_0^m$ where m is even and $q_0 \equiv -1 \pmod{d}$. Then $f(x) := x^r h_k(x^{e(q-1)/d})^t$ permutes $\mathbb{F}_q$ if and only if* $\gcd(r, s) = \gcd(k, pd) = 1$ *and* $\gcd(2r + (k-1)tes, 2d) = 2$.

Remark. The hypotheses of Corollary 2.4 are satisfied whenever d is an odd prime divisor of $q-1$ such that p has even order modulo d. The case that $d=7$, $t=1$, and $k=2$ was treated in [2], although the result in [2] includes the superfluous condition $2^s \equiv 1 \pmod{p}$. The case that $q_0 = p$, $t=1$, and $k=2$ was treated in [3]. The case that $q_0 = p$, $t = e = 1$, and both q and d are odd was treated in [1].

Now we prove a general sufficient criterion for permutation binomials:

Theorem 2.5. *Pick $u > r > 0$ and $a \in \mathbb{F}_q^*$. Write $s := \gcd(u-r, q-1)$ and $d := (q-1)/s$. Suppose that $(\eta + a/\eta) \in \mu_s$ for every $\eta \in \mu_{2d}$. Then $x^u + ax^r$ permutes $\mathbb{F}_q$ if and only if $-a \notin \mu_d$, $\gcd(r,s)=1$ and $\gcd(2d, u+r) \le 2$.*

Proof. Write $e := (u-r)/s$, so that $\gcd(e,d)=1$. By Lemma 2.1, $f(x) := x^u + ax^r$ permutes $\mathbb{F}_q$ if and only if $\gcd(r,s)=1$ and $g(x) := x^r(x^e+a)^s$ permutes μ_d. In particular, if $x^u + ax^r$ permutes $\mathbb{F}_q$ then g has no roots in μ_d, or equivalently $-a \notin \mu_d$. Henceforth we assume $\gcd(r,s)=1$ and $-a \notin \mu_d$, so f permutes $\mathbb{F}_q$ if and only if g is injective on μ_d. This condition is equivalent to injectivity of $g(x^2)$ on μ_{2d}/μ_2. But for $\eta \in \mu_{2d}$ we have

$$\begin{aligned} g(\eta^2) &= \eta^{2r}(\eta^{2e}+a)^s \\ &= \eta^{2r+es}\left(\eta^e + \frac{a}{\eta^e}\right)^s \\ &= \eta^{2r+es}. \end{aligned}$$

Finally, x^{2r+es} is injective on μ_{2d}/μ_2 if and only if $\gcd(2r+es, 2d) \le 2$. Since $2r+es = u+r$, this completes the proof. $\square$

Theorem 2.5 can be generalized (with the same proof) to polynomials with more terms:

Theorem 2.6. *Pick $r, e, d, t > 0$ where $d \mid (q-1)$ and $\gcd(e,d)=1$. Put $h = x^t \hat{h}(x^d)$ where $\hat{h} \in \mathbb{F}_q[x]$. Pick $a \in \mathbb{F}_q^*$. Suppose that every $\eta \in \mu_{d\gcd(2,d)}$ satisfies both $\eta + a/\eta \in \mu_{t(q-1)/d}$ and $\hat{h}((\eta^{2e}+a)^d) \in \mu_{(q-1)/d}$. Then $f(x) := x^r h(x^{e(q-1)/d} + a)$ permutes $\mathbb{F}_q$ if and only if $\gcd(2r + et(q-1)/d, d) = 1$ and $\gcd(r, (q-1)/d) = 1$.*

3. Permutation binomials and generalized Lucas sequences

In this section we explain how our sufficient condition for permutation binomials (Theorem 2.5) implies the analogous condition from [3], namely [3, Thm. 1.1]. We begin by stating the latter result.

It is easy to show that if $f(x) := x^r + x^u$ (with $0 < r < u$) permutes $\mathbb{F}_q$ then $f(x) = x^r(1 + x^{es})$, where

$$(*) \quad sd = q-1,\ \gcd(r,s) = \gcd(e,d) = 1,\ d \text{ is odd, and } r,e,s > 0.$$

Conversely, with p denoting the characteristic of $\mathbb{F}_q$, [3, Thm. 1.1] says:

Theorem 3.1. *For q,s,d,r,e as in $(*)$, the binomial $f(x) = x^r(1+x^{es})$ permutes $\mathbb{F}_q$ if $\gcd(2r+es,d) = 1$, $2^s \equiv 1 \pmod p$, and the sequence*

$$a_n := \sum_{t=1}^{\frac{d-1}{2}} \left(2\cos\frac{\pi(2t-1)}{d}\right)^n$$

consists of integers satisfying $a_n \equiv a_{n+s} \pmod p$ for every $n \geq 0$.

Suppose the hypotheses of Theorem 3.1 are satisfied, and put $\zeta = \exp(\pi i/d)$. Then

$$2a_n = 2\sum_{t=1}^{\frac{d-1}{2}} \left(\zeta^{2t-1} + \frac{1}{\zeta^{2t-1}}\right)^n = \sum_{\substack{\eta\in\mathbb{C}\setminus\{-1\} \\ \eta^d=-1}} \left(\eta + \frac{1}{\eta}\right)^n.$$

Note that the hypotheses of Theorem 3.1 imply that q is odd (since $s > 0$ and $2^s \equiv 1 \pmod p$). Also, we now see that $a_n \in \mathbb{Z}[\zeta]$ and that a_n is fixed by every element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, so $a_n \in \mathbb{Q} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$. Let $\hat{\zeta}$ denote a fixed primitive $(2d)^{\text{th}}$ root of unity in $\mathbb{F}_q$, and let ψ be the homomorphism $\mathbb{Z}[\zeta] \mapsto \mathbb{F}_q$ which maps $\zeta \mapsto \hat{\zeta}$. Then $\psi(a_n) \equiv a_n \pmod p$, so the condition $a_n \equiv a_{n+s} \pmod p$ is equivalent to

$$\sum_{\substack{\eta\in\mathbb{F}_q\setminus\{-1\} \\ \eta^d=-1}} \left(\left(\eta + \frac{1}{\eta}\right)^s - 1\right) \cdot \left(\eta + \frac{1}{\eta}\right)^n = 0.$$

This condition holds for all $n \geq 0$ if and only if

$$\sum_{\substack{\eta\in\mathbb{F}_q\setminus\{-1\} \\ \eta^d=-1}} \left(\left(\eta + \frac{1}{\eta}\right)^s - 1\right) \cdot P\left(\eta + \frac{1}{\eta}\right) = 0$$

for every $P \in \mathbb{F}_q[x]$. Pick representatives $\eta_1, \eta_2, \ldots, \eta_{(d-1)/2}$ for the equivalence classes of $\mu_{2d} \setminus (\mu_d \cup \mu_2)$ under the equivalence relation $\eta \sim 1/\eta$. Then the values $\eta_i + 1/\eta_i$ are distinct elements of $\mathbb{F}_q$, so there are polynomials $P \in \mathbb{F}_q[x]$ taking any prescribed values at all of the $\eta_i + 1/\eta_i$. In particular, choosing P to be zero at all but one of these elements, we find that

$$(1) \qquad \left(\eta + \frac{1}{\eta}\right)^s = 1$$

for every η such that $\eta^d = -1$ but $\eta \neq -1$. The hypotheses of Theorem 3.1 imply that s is even and $2^s \equiv 1 \pmod{p}$, so (1) holds for $\eta = -1$. Moreover, since d is odd and s is even, the fact that (1) holds when $\eta^d = -1$ implies that (1) holds when $\eta^d = 1$ as well.

Thus, whenever the hypotheses of Theorem 3.1 hold, we will have $(\eta + 1/\eta)^s = 1$ for every $\eta \in \mu_{2d}$. Since the latter is precisely the hypothesis of Theorem 2.5 in the case $a = 1$, we see that Theorem 2.5 implies Theorem 3.1.

References

[1] A. Akbary, S. Alaric and Q. Wang, *On some classes of permutation polynomials*, Int. J. Number Theory **4** (2008), 121–133.

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

[3] ———, *A generalized Lucas sequence and permutation binomials*, Proc. Amer. Math. Soc. **134** (2006), 15–22.

[4] ———, *On polynomials of the form $x^r f(x^{(q-1)/l})$*, Int. J. Math. Math. Sci. (2007), Article ID 23408, 7 pages.

[5] E. Betti, *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo*, Annali di Scienze Matematiche e Fisiche **2** (1851), 5–19 (=Opere Matematiche, v. 1, 17–27).

[6] F. Brioschi, *Des substitutions de la forme $\Theta(r) \equiv \varepsilon(r^{n-2} + ar^{(n-3)/2})$ pour un nombre n premier de lettres*, Math. Ann. **2** (1870), 467–470 (=Opere Matematiche, v. 5, 193–197).

[7] L. Carlitz, *Some theorems on permutation polynomials*, Bull. Amer. Math. Soc. **68** (1962), 120–122.

[8] W. Chu and S. W. Golomb, *Circular Tuscan-k arrays from permutation binomials*, J. Comb. Theory A **97** (2002), 195–202.

[9] S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **17** (1970), 255–271.

[10] S. D. Cohen and R. W. Matthews, *A class of exceptional polynomials*, Trans. Amer. Math. Soc. **345** (1994), 897–909.

[11] C. J. Colbourn, T. Klove and A. C. H. Ling, *Permutation arrays for powerline communication and mutually orthogonal Latin squares*, IEEE Trans. Inf. Theory **50** (2004), 1289–1291.

[12] H. Davenport and D. J. Lewis, *Notes on congruences. I*, Quart. J. Math. Oxford Ser. (2) **14** (1963), 51–60.

[13] 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 Math. **11** (1896-7), 65–120 and 161–183.

[14] J. F. Dillon and H. Dobbertin, *New cyclic difference sets with Singer parameters*, Finite Fields Appl. **10** (2004), 342–389.

[15] M. D. Fried, R. M. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), 157–225.

[16] R. M. Guralnick and P. Müller, *Exceptional polynomials of affine type*, J. Algebra **194** (1997), 429–454.

[17] R. M. Guralnick, P. Müller and M. E. Zieve, *Exceptional polynomials of affine type, revisited*, preprint.
[18] R. M. Guralnick, J. Rosenberg and M. E. Zieve, *A new family of exceptional polynomials in characteristic two*, Ann. of Math. (2), to appear, arXiv:0707.1837 [math.NT].
[19] R. M. Guralnick and M. E. Zieve, *Automorphism groups of curves with ordinary Jacobians*, in preparation.
[20] Ch. Hermite, *Sur les fonctions de sept lettres*, C. R. Acad. Sci. Paris **57** (1863), 750–757.
[21] S. Y. Kim and J. B. Lee, *Permutation polynomials of the type* $x^{1+((q-1)/m)}+ax$, Commun. Korean Math. Soc. **10** (1995), 823–829.
[22] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. **13** (2007), 58–70.
[23] H. W. Lenstra, Jr., and M. E. Zieve, *A family of exceptional polynomials in characteristic three*, in: Finite Fields and Applications (Glasgow, 1995), 209–218.
[24] A. M. Masuda and M. E. Zieve, *Permutation binomials over finite fields*, Trans. Amer. Math. Soc., to appear, arXiv:0707.1108.
[25] É. Mathieu, *Mémoire sur l'etud des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, Jour. de Math. Pure Appl. **6** (1861), 241–323.
[26] P. Müller, *New examples of exceptional polynomials*, in: Finite Fields: Theory, Applications, and Algorithms (Las Vegas, NV, 1993), 245–249.
[27] H. Niederreiter and K. H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. (Series A) **33** (1982), 197–212.
[28] Y. H. Park and J. B. Lee, *Permutation polynomials and group permutation polynomials*, Bull. Austral. Math. Soc. **63** (2001), 67–74.
[29] C. Small, *Permutation binomials*, Internat. J. Math. Math. Sci. **13** (1990), 337–342.
[30] J. Sun, O. Y. Takeshita and M. P. Fitz, *Permutation polynomial based deterministic interleavers for turbo codes*, in: Proceedings 2003 IEEE International Symposium on Information Theory (Yokohama, Japan, 2003), 319.
[31] G. Turnwald, *Permutation polynomials of binomial type*, in: Contributions to General Algebra 6, (1988), 281–286.
[32] D. Wan, *Permutation binomials over finite fields*, Acta Math. Sinica (New Series) **10** (1994), 30–35.
[33] 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.
[34] L. Wang, *On permutation polynomials*, Finite Fields Appl. **8** (2002), 311–322.
[35] M. E. Zieve, *Some families of permutation polynomials over finite fields*, Int. J. Number Theory **4** (2008), 851–857, arXiv:0707.1111 [math.NT].

Hill Center, Department of Mathematics, Rutgers University, 110 Frelinghuysen Road, Piscataway NJ 08854
E-mail address: `zieve@math.rutgers.edu`
URL: `http://www.math.rutgers.edu/∼zieve`