CLASSES OF PERMUTATION POLYNOMIALS BASED ON CYCLOTOMY AND AN ADDITIVE ANALOGUE

MICHAEL E. ZIEVE

Abstract. I present a construction of permutation polynomials based on cyclotomy, an additive analogue of this construction, and a generalization of this additive analogue which appears to have no multiplicative analogue. These constructions generalize recent results of José Marcos.

Dedicated to Mel Nathanson on the occasion of his sixtieth birthday

1. Introduction

Writing $\mathbb{F}_q$ for the field with q elements, we consider *permutation polynomials* over $\mathbb{F}_q$, namely polynomials $f \in \mathbb{F}_q[x]$ for which the map $\alpha \mapsto f(\alpha)$ induces a permutation of $\mathbb{F}_q$. These polynomials first arose in work of Betti [6], Mathieu [28], and Hermite [20], as a tool for representing and studying permutations.

Since every mapping $\mathbb{F}_q \to \mathbb{F}_q$ is induced by a polynomial, the study of permutation polynomials focuses on polynomials with unusual properties beyond inducing a permutation. In particular, permutation polynomials of 'nice' shapes have been a topic of interest since the work of Hermite, in which he noted that there are many permutation polynomials of the form

$$f(x) := ax^i(x^{\frac{q-1}{2}} + 1) - bx^j(x^{\frac{q-1}{2}} - 1)$$

with q odd, $i, j > 0$, and $a, b \in \mathbb{F}_q^*$. The reason for this is that $f(\alpha) = 2a\alpha^i$ if $\alpha \in \mathbb{F}_q$ is a square, and $f(\alpha) = 2b\alpha^j$ otherwise; thus, for instance, f is a permutation polynomial if $2a$ and $2b$ are squares and $\gcd(ij, q-1) = 1$.

More generally, any polynomial of the form $f(x) := x^r h(x^{(q-1)/d})$ induces a mapping on $\mathbb{F}_q$ modulo d-th powers, so testing whether f

---

Date: October 15, 2008.

1991 *Mathematics Subject Classification.* 11T06, 11T22.

I thank José Marcos for sending me preliminary versions of his paper [26], and for encouraging me to develop consequences of his ideas while his paper was still under review.

permutes $\mathbb{F}_q$ reduces to testing whether the induced mapping on cosets is bijective (assuming that f is injective on each coset, or equivalently that $\gcd(r,(q-1)/d) = 1$). The vast majority of known examples of 'nice' permutation polynomials have this 'cyclotomic' form for some $d < q-1$; see for instance [1–5, 7, 9–25, 29–34, 36–43]. Moreover, there is a much longer list of papers proving nonexistence of permutation polynomials of certain shapes, and nearly all such papers again address these polynomials $f(x)$ having cyclotomic behavior.

In the recent preprint [26], Marcos gives five constructions of permutation polynomials. His first two constructions are new classes of permutation polynomials having the above cyclotomic form. His third construction is a kind of additive analogue of the first, resulting in polynomials of the form $L(x)+h(T(x))$ where $T(x) := x^{q/p}+x^{q/p^2}+\cdots+x$ is the trace polynomial from $\mathbb{F}_q$ to its prime field $\mathbb{F}_p$, and $L(x) = \sum a_i x^{p^i}$ is any additive polynomial. The idea of the analogy is that $T(x)$ induces a homomorphism $\mathbb{F}_q \to \mathbb{F}_p$, just as $x^{(q-1)/d}$ induces a homomorphism from $\mathbb{F}_q^*$ to its subgroup of d-th roots of unity. The fourth construction in [26] is a variant of the third for polynomials of the form $L(x)+h(T(x))(L(x)+c)$, and the fifth construction replaces $T(x)$ with other symmetric functions in $x^{q/p}$, x^{q/p^2}, ..., x.

In this paper I present rather more general versions of the first four constructions from [26], together with simplified proofs. I can say nothing new about the fifth construction from [26], although that construction is quite interesting and I encourage the interested reader to look into it.

2. Permutation polynomials from cyclotomy

In this section we prove the following result, where for $d \geq 1$ we write $h_d(x) := x^{d-1} + x^{d-2} + \cdots + x + 1$.

Theorem 1. *Fix a divisor $d > 2$ of $q-1$, integers $u \geq 1$ and $k \geq 0$, an element $b \in \mathbb{F}_q$, and a polynomial $g \in \mathbb{F}_q[x]$ divisible by h_d. Then*

$$f(x) := x^u \left(bx^{k(q-1)/d} + g(x^{(q-1)/d})\right)$$

permutes $\mathbb{F}_q$ if and only if the following four conditions hold:

(1) $\gcd(u,(q-1)/d) = 1$,
(2) $\gcd(d, u + k(q-1)/d) = 1$,
(3) $b \neq 0$,
(4) $1 + g(1)/b$ *is a d-th power in* $\mathbb{F}_q^*$.

The proof uses the following simple lemma.

Lemma 2. *Fix a divisor d of $q-1$, an integer $u>0$, and a polynomial $h \in \mathbb{F}_q[x]$. Then $f(x) := x^u h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if the following two conditions hold:*

(1) $\gcd(u,(q-1)/d)=1$,
(2) $\widehat{f}(x) := x^u h(x)^{(q-1)/d}$ *permutes the set μ_d of d-th roots of unity in $\mathbb{F}_q^*$.*

I discovered this lemma in 1997 when writing [35], and used it in seminars and private correspondence, but I did not publish it until recently [42, Lemma 2.1]. For other applications of this lemma, see [27, 42, 43].

Proof of Theorem 1. In light of the lemma, we just need to determine when $\widehat{f}(x)$ permutes μ_d, where

$$\widehat{f}(x) := x^u (bx^k + g(x))^{(q-1)/d}.$$

For $\zeta \in \mu_d \backslash \{1\}$ we have $g(\zeta)=0$, so $\widehat{f}(\zeta) = b^{(q-1)/d}\zeta^{u+k(q-1)/d}$. Thus, $\widehat{f}$ is injective on $\mu_d\backslash\{1\}$ if and only if $b\neq 0$ and $\gcd(d, u+k(q-1)/d)=1$. When these conditions hold, $\widehat{f}(\mu_d\backslash\{1\}) = \mu_d\backslash\{b^{(q-1)/d}\}$, so $\widehat{f}$ permutes μ_d if and only if $\widehat{f}(1)=b^{(q-1)/d}$. Since $\widehat{f}(1) = (b+g(1))^{(q-1)/d}$, the latter condition is equivalent to $(1+g(1)/b)^{(q-1)/d}=1$, as desired. ☐

The case $g=h_d$ of Theorem 1 is [26, Thm. 2], and [26, Prop. 4] is the case that $g = h_5(h_5 - x^3 - x^4)$ and $d=u=k-2=5$.

Remark. The key feature of the polynomials in Theorem 1 as a particular case of Lemma 2 is that the induced mapping $\widehat{f}$ on $\mu_d \setminus \{1\}$ is a monomial, and we know when monomials permute μ_d. For certain values of d, we know other permutations of μ_d: for instance, if $q=q_0^2$ and $d=\sqrt{q_0}-1$ then $\mu_d = \mathbb{F}_{q_0}^*$, so we can obtain permutation polynomials over $\mathbb{F}_q$ by applying Lemma 2 to polynomials $f(x)$ for which the induced map $\widehat{f}$ on $\mathbb{F}_{q_0}^*$ is any prescribed permutation polynomial. This construction already yields interesting permutation polynomials of $\mathbb{F}_q$ coming from degree-3 permutation polynomials of $\mathbb{F}_{q_0}$; see [35] for details and related results.

3. Permutation polynomials from additive cyclotomy

Lemma 2 addresses maps $\mathbb{F}_q \to \mathbb{F}_q$ which respect the partition of $\mathbb{F}_q^*$ into cosets modulo a certain subgroup. In this section we give an analogous result in terms of cosets of the additive group of $\mathbb{F}_q$ modulo a subgroup. Let p be the characteristic of $\mathbb{F}_q$. An *additive* polynomial over $\mathbb{F}_q$ is a polynomial of the form $\sum_{i=0}^k a_i x^{p^i}$ with $a_i \in \mathbb{F}_q$. The key property of additive polynomials $A(x)$ is that they induce homomorphisms on the additive group of $\mathbb{F}_q$, since $A(\alpha+\beta) = A(\alpha)+A(\beta)$

for $\alpha, \beta \in \mathbb{F}_q$. The additive analogue of Lemma 2 is as follows, where we write $\operatorname{im} B$ and $\ker B$ for the image and kernel of the mapping $B\colon \mathbb{F}_q \to \mathbb{F}_q$.

Proposition 3. *Pick additive $A, B \in \mathbb{F}_q[x]$ and an arbitrary $g \in \mathbb{F}_q[x]$. Then $f(x) := A(x) + g(B(x))$ permutes $\mathbb{F}_q$ if and only if $A(\ker B) + \widehat{f}(\operatorname{im} B) = \mathbb{F}_q$, where $\widehat{f}(x) := g(x) + A(\widehat{B}(x))$ and $\widehat{B} \in \mathbb{F}_q[x]$ is any polynomial for which $B(\widehat{B}(x))$ is the identity on $\operatorname{im} B$. In other words, f permutes $\mathbb{F}_q$ if and only if $\widehat{f}$ induces a bijection $\operatorname{im} B \to \mathbb{F}_q/A(\ker B)$, where $\mathbb{F}_q/A(\ker B)$ is the quotient of the additive group of $\mathbb{F}_q$ by the subgroup $A(\ker B)$.*

Proof. For $\beta \in \ker B$ we have $f(x+\beta) = A(x) + A(\beta) + g(B(x)) = f(x) + A(\beta)$. Thus, for $\alpha \in \mathbb{F}_q$ we have $f(\alpha + \ker B) = f(\alpha) + A(\ker B)$. Since $\mathbb{F}_q = \ker B + \widehat{B}(\operatorname{im} B)$, it follows that $f(\mathbb{F}_q) = f(\widehat{B}(\operatorname{im} B)) + A(\ker B)$. Since $f(\widehat{B}(\gamma)) = A(\widehat{B}(\gamma)) + g(B(\widehat{B}(\gamma))) = A(\widehat{B}(\gamma)) + g(\gamma)$ for $\gamma \in \operatorname{im} B$, the result follows. $\square$

Corollary 4. *If f permutes $\mathbb{F}_q$ then A is injective on $\ker B$ and $\widehat{f}$ is injective on $\operatorname{im} B$.*

Proof. If $A(\ker B) + \widehat{f}(\operatorname{im} B) = \mathbb{F}_q$ then

$$q \le \#A(\ker B) \cdot \#\widehat{f}(\operatorname{im} B) \le \#(\ker B) \cdot \#(\operatorname{im} B) = q,$$

where the last equality holds because B defines a homomorphism on the additive group of $\mathbb{F}_q$. The result follows. $\square$

Corollary 5. *Suppose $A(B(\alpha)) = B(A(\alpha))$ for all $\alpha \in \mathbb{F}_q$. Then f permutes $\mathbb{F}_q$ if and only if A permutes $\ker B$ and $A(x) + B(g(x))$ permutes $\operatorname{im} B$.*

Proof. Since A and B commute, and $A(0) = 0$, it follows that $A(\ker B) \subseteq \ker B$. Thus, by the previous corollary, if f permutes $\mathbb{F}_q$ then A permutes $\ker B$. Henceforth assume that A permutes $\ker B$. By the proposition, f permutes $\mathbb{F}_q$ if and only if $\ker B + \widehat{f}(\operatorname{im} B) = \mathbb{F}_q$; since the left side is the preimage under B of $B(\widehat{f}(\operatorname{im} B))$, this condition may be restated as $B(\widehat{f}(\operatorname{im} B)) = \operatorname{im} B$. For $\gamma \in \operatorname{im} B$ we have $B(\widehat{f}(\gamma)) = B(g(\gamma)) + B(A(\widehat{B}(\gamma))) = B(g(\gamma)) + A(B(\widehat{B}(\gamma))) = B(g(\gamma)) + A(\gamma)$, so $B(\widehat{f}(x))$ permutes $\operatorname{im} B$ if and only if $B(g(x)) + A(x)$ permutes $\operatorname{im} B$. $\square$

One way to get explicit examples satisfying the conditions of this result is as follows: if $B = x^{q/p} + x^{q/p^2} + \cdots + x^p + x$ and $A \in \mathbb{F}_p[x]$, then $A(B(x)) = B(A(x))$, so f permutes $\mathbb{F}_q$ if and only if A permutes

$\ker B$ and $A(x)+B(g(x))$ permutes $\operatorname{im} B = \mathbb{F}_p$. In case g is a constant (in $\mathbb{F}_q$) times a polynomial over $\mathbb{F}_p$, this becomes (a slight generalization of) [26, Thm. 6]. The following case of [26, Cor. 8] exhibits this.

Example. In case $q = p^2$ and $B = x^p + x$ and $A = x$, the previous corollary says $f(x) := x+g(x^p+x)$ permutes $\mathbb{F}_{p^2}$ if and only if $x+g(x)^p+g(x)$ permutes $\mathbb{F}_p$, which trivially holds when $g = \gamma h(x)$ with $h \in \mathbb{F}_p[x]$ and $\gamma^{p-1} = -1$. For instance, taking $h(x) = x^2$, it follows that $x + \gamma(x^p+x)^2$ permutes $\mathbb{F}_{p^2}$. By using other choices of h, we can make many permutation polynomials over $\mathbb{F}_{p^2}$ whose degree is a small multiple of p. This is of interest because heuristics suggest that 'at random' there would be no permutation polynomials over $\mathbb{F}_q$ of degree less than $q/(2\log q)$. The bulk of the known low-degree permutation polynomials are *exceptional*, in the sense that they permute $\mathbb{F}_{q^k}$ for infinitely many k; a great deal is known about these exceptional polynomials, for instance see [19]. It is known that any permutation polynomial of degree at most $q^{1/4}$ is exceptional. However, the examples described above have degree on the order of $q^{1/2}$ and are generally not exceptional.

Our final result generalizes the above example in a different direction than Proposition 3.

Theorem 6. *Pick any $g \in \mathbb{F}_q[x]$, any additive $A \in \mathbb{F}_p[x]$, and any $h \in \mathbb{F}_p[x]$. For $B := x^{q/p} + x^{q/p^2} + \cdots + x^p + x$, the polynomial $f(x) := g(B(x)) + h(B(x))A(x)$ permutes $\mathbb{F}_q$ if and only if A permutes $\ker B$ and $B(g(x)) + h(x)A(x)$ permutes $\mathbb{F}_p$ and h has no roots in $\mathbb{F}_p$.*

Proof. For $\beta \in \ker B$ we have $f(x+\beta) = f(x) + h(B(x))A(\beta)$. Thus, if f permutes $\mathbb{F}_q$ then A is injective on $\ker B$ and h has no roots in $\mathbb{F}_p$. Since $A(B(x)) = B(A(x))$ and $A(0) = 0$, also $A(\ker B) \subseteq \ker B$, so if f permutes $\mathbb{F}_q$ then A permutes $\ker B$. Henceforth assume A permutes $\ker B$ and h has no roots in $\mathbb{F}_p$. Since $\operatorname{im} B = \mathbb{F}_p$ and $h(\mathbb{F}_p) \subseteq \mathbb{F}_p \setminus \{0\}$, we have $h(B(\alpha)) \in \mathbb{F}_p \setminus \{0\}$ for $\alpha \in \mathbb{F}_q$. Thus, for $\alpha \in \mathbb{F}_q$ we have $f(\alpha + \ker B) = f(\alpha) + \ker B$, so f permutes $\mathbb{F}_q$ if and only if $B(f(\mathbb{F}_q)) = \operatorname{im} B$. Now for $\alpha \in \mathbb{F}_q$ we have $B(f(\alpha)) = B(g(B(\alpha))) + B(h(B(\alpha))A(\alpha))$, and since $h(B(\alpha)) \in \mathbb{F}_p$ this becomes $B(f(\alpha)) = B(g(B(\alpha))) + h(B(\alpha))B(A(\alpha)) = B(g(B(\alpha)) + h(B(\alpha))A(B(\alpha))$, so $B(f(\mathbb{F}_q))$ is the image of $\operatorname{im} B$ under $B(g(x)) + h(x)A(x)$. The result follows. $\square$

In case $g = \gamma h + \delta$ with $\gamma, \delta \in \mathbb{F}_q$, the above result becomes a generalization of [26, Thm. 10]. In view of the analogy between Lemma 2 and Proposition 3, it is natural to seek a 'multiplicative' analogue of Theorem 6. However, I have been unable to find such a result: the obstacle is that the polynomial f in Theorem 6 is the sum of products of polynomials, which apparently should correspond to a product of powers of polynomials, but the latter is already included in Lemma 2.

References

[1] S. Ahmad: Split dilations of finite cyclic groups with applications to finite fields. Duke Math. J. **37**, 547–554 (1970)

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

[3] A. Akbary and Q. Wang: On some permutation polynomials over finite fields. Int. J. Math. Math. Sci. **16**, 2631–2640 (2005)

[4] A. Akbary and Q. Wang: A generalized Lucas sequence and permutation binomials. Proc. Amer. Math. Soc. **134**, 15–22 (2006)

[5] A. Akbary and Q. Wang: On polynomials of the form $x^r f(x^{(q-1)/l})$. Int. J. Math. Math. Sci. (2007) art. ID 23408.

[6] E. Betti: Sopra la risolubilitá per radicali delle equazioni algebriche irriduttibili di grado primo. Annali Sci. Mat. Fis. **2**, 5–19 (1851) [= Op. Mat. **1**, 17–27 (1903)]

[7] F. Brioschi: Des substitutions de la forme $\theta(r) \equiv \epsilon(r^{n-2} + ar^{(n-3)/2})$ pour un nombre n premier de lettres. Math. Ann. **2**, 467–470 (1870) [= Op. Mat. **5**, 193–197 (1909)]

[8] L. Carlitz: Permutations in a finite field. Proc. Amer. Math. Soc. **4**, 538 (1953)

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

[10] L. Carlitz: Permutations in finite fields. Acta Sci. Math. (Szeged) **24**, 196–203 (1963)

[11] L. Carlitz and C. Wells: The number of solutions of a special system of equations in a finite field. Acta Arith. **12**, 77–84 (1966)

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

[13] S. D. Cohen and R. W. Matthews: Exceptional polynomials over finite fields. Finite Fields Appl. **1**, 261–277 (1995)

[14] 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**, 65–120 (1896)

[15] L. E. Dickson: Linear Groups with an Exposition of the Galois Field Theory, Teubner, Leipzig (1901) [Reprinted by Dover, New York (1958)]

[16] A. B. Evans: Orthomorphism Graphs of Groups, Springer-Verlag, Heidelberg (1992)

[17] A. B. Evans: Cyclotomy and orthomorphisms: a survey. Congr. Numer. **101**, 97–107 (1994)

[18] J. P. Fillmore: A note on split dilations defined by higher residues. Proc. Amer. Math. Soc. **18**, 171–174 (1967)

[19] R. M. Guralnick and M. E. Zieve: Polynomials with PSL(2) monodromy. Annals of Math., to appear, arXiv:0707.1835

[20] Ch. Hermite: Sur les fonctions de sept lettres. C. R. Acad. Sci. Paris. **57**, 750–757 (1863) [= Ouvres **2**, 280–288 (1908)]

[21] N. S. James and R. Lidl: Permutation polynomials on matrices. Linear Algebra Appl. **96**, 181–190 (1987)

[22] S. Y. Kim and J. B. Lee: Permutation polynomials of the type $x^{1+(q-1)/m}+ax$. Comm. Korean Math. Soc. **10**, 823–829 (1995)

[23] Y. Laigle-Chapuy: Permutation polynomials and applications to coding theory. Finite Fields Appl. **13**, 58–70 (2007)

[24] J. B. Lee and Y. H. Park: Some permuting trinomials over finite fields. Acta Math. Sci. **17**, 250–254 (1997)

[25] H. W. Lenstra, Jr. and M. Zieve: A family of exceptional polynomials in characteristic three. In: Finite Fields and Applications, Cambridge Univ. Press, Cambridge 209–218 (1996)

[26] J. E. Marcos: Specific permutation polynomials over finite fields. submitted for publication, arXiv:0810.2738v1

[27] A. M. Masuda and M. E. Zieve: Permutation binomials over finite fields. Trans. Amer. Math. Soc., to appear, arXiv:0707.1108

[28] E. 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**, 241–323 (1861)

[29] G. Mullen and H. Niederreiter: The structure of a group of permutation polynomials. J. Austral. Math. Soc. (Ser. A) **38**, 164–170 (1985)

[30] H. Niederreiter and K. H. Robinson: Complete mappings of finite fields. J. Austral. Math. Soc. (Ser. A) **33**, 197–212 (1982)

[31] H. Niederreiter and A. Winterhof: Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields. Discrete Math. **295**, 161–171 (2005)

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

[33] Y. H. Park and J. B. Lee: Permutation polynomials and group permutation polynomials. Bull. Austral. Math. Soc. **63**, 67–74 (2001)

[34] L. J. Rogers: On the analytical representation of heptagrams. Proc. London Math. Soc. **22**, 37–52 (1890)

[35] T. J. Tucker and M. E. Zieve: Permutation polynomials, curves without points, and Latin squares. preprint (2000)

[36] D. Wan: Permutation polynomials over finite fields. Acta Math. Sinica **3**, 1–5 (1987)

[37] D. Wan: Permutation binomials over finite fields. Acta Math. Sinica **10**, 30–35 (1994)

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

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

[40] C. Wells: Groups of permutation polynomials. Monatsh. Math. **71**, 248–262 (1967)

[41] C. Wells: A generalization of the regular representation of finite abelian groups. Monatsh. Math. **72**, 152–156 (1968)

[42] M. E. Zieve: Some families of permutation polynomials over finite fields. Internat. J. Number Theory **4**, (2008), to appear, arXiv:0707.1111

[43] M. E. Zieve: On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. Proc. Amer. Math. Soc., to appear, arXiv:0707.1110

Michael E. Zieve, Rutgers University, Department of Mathematics, 110 Frelinghuysen Road, Piscataway, NJ 08854–8019, USA
E-mail address: zieve@math.rutgers.edu
URL: www.math.rutgers.edu/∼zieve