PERMUTATION POLYNOMIALS ON $\mathbb{F}_q$ INDUCED FROM RÉDEI FUNCTION BIJECTIONS ON SUBGROUPS OF $\mathbb{F}_q^*$

MICHAEL E. ZIEVE

ABSTRACT. We construct classes of permutation polynomials over $\mathbb{F}_{Q^2}$ by exhibiting classes of low-degree rational functions over $\mathbb{F}_{Q^2}$ which induce bijections on the set of $(Q+1)$-th roots of unity. As a consequence, we prove two conjectures about permutation trinomials from a recent paper by Tu, Zeng, Hu and Li.

1. INTRODUCTION

A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if the function $\alpha \mapsto f(\alpha)$ induces a permutation of $\mathbb{F}_q$. Since they were first studied in the mid-19th century, one of the driving questions about permutation polynomials has been to construct examples having especially simple shapes. This requires polynomials which are nice in two ways: they have a simple algebraic form, and also they induce a function on $\mathbb{F}_q$ which has the nice combinatorial property of being a permutation. The vast majority of known examples of "nice" permutation polynomials have the form $x^r h(x^d)$ where $h \in \mathbb{F}_q[x]$ and $d > 1$ is a divisor of $q-1$. The reason this form is special is that a general result (see Lemma 2.2) asserts that $x^r h(x^d)$ permutes $\mathbb{F}_q$ if and only if $\gcd(r,d) = 1$ and $x^r h(x)^d$ permutes the set of $(q-1)/d$-th roots of unity in $\mathbb{F}_q^*$. This leads to the question of producing collections of polynomials which permute the set μ_k of k-th roots of unity in $\mathbb{F}_q$ for certain values of k. There are two simple types of polynomials which permute μ_k: for arbitrary k one can use polynomials of the form $\beta x^n + (x^k-1)\cdot g(x)$ where $\beta \in \mu_k$ and $\gcd(n,k) = 1$, and if $k = Q-1$ where $q = Q^r$ then one can use $h(x) - h(0)$ where $h(x) \in \mathbb{F}_Q[x]$ permutes $\mathbb{F}_Q$. These two simple types of permutations of μ_k account for essentially all published examples of permutation polynomials over finite fields. Indeed, it is difficult to identify any other polynomials having "nice" form which permute μ_k. In this paper we present classes of permutation polynomials obtained from a new variant of this construction, in which

- μ_k is *not* the multiplicative group of a subfield of $\mathbb{F}_q$

- the induced function on μ_k is most naturally presented as a rational function rather than a polynomial.

It is perhaps surprising that there are permutations of μ_k which can be represented by a rational function having an especially simple form, but which cannot be represented by an especially simple polynomial. We obtain the following classes of permutation polynomials.

Theorem 1.1. *Let Q be a prime power, let $n > 0$ and $k \geq 0$ be integers, and let $\beta, \gamma \in \mathbb{F}_{Q^2}$ satisfy $\beta^{Q+1} = 1$ and $\gamma^{Q+1} \neq 1$. Then*

$$f(x) := x^{n+k(Q+1)} \cdot \big((\gamma x^{Q-1} - \beta)^n - \gamma(x^{Q-1} - \gamma^Q \beta)^n\big)$$

permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(n+2k, Q-1) = 1$ and $\gcd(n, Q+1) = 1$.

Theorem 1.2. *Let Q be a prime power, let n, k be integers with $n > 0$ and $k \geq 0$, and let $\beta, \delta \in \mathbb{F}_{Q^2}$ satisfy $\beta^{Q+1} = 1$ and $\delta \notin \mathbb{F}_Q$. Then*

$$f(x) := x^{n+k(Q+1)} \cdot \big((\delta x^{Q-1} - \beta\delta^Q)^n - \delta(x^{Q-1} - \beta)^n\big)$$

permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(n(n+2k), Q-1) = 1$.

The following corollary illustrates these results in the special case $n = 3$, for certain values of β, γ, δ.

Corollary 1.3. *Let Q be a prime power, and let k be a nonnegative integer. The polynomial $g(x) := x^{k(Q+1)+3} + 3x^{k(Q+1)+Q+2} - x^{k(Q+1)+3Q}$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(2k+3, Q-1) = 1$ and $3 \nmid Q$.*

Specializing even further to the values $k = Q-3$, $k = 1$, and $k = 0$ yields the following consequence.

Corollary 1.4. *Let Q be a prime power with $3 \nmid Q$. Then*

1. *$x^{2Q-1} + 3x^Q - x^{Q^2-Q+1}$ is a permutation polynomial over $\mathbb{F}_{Q^2}$.*
2. *$x^{Q+4} + 3x^{2Q+3} - x^{4Q+1}$ is a permutation polynomial over $\mathbb{F}_{Q^2}$ if and only if $Q \not\equiv 1 \pmod 5$.*
3. *$x^3 + 3x^{Q+2} - x^{3Q}$ is a permutation polynomial over $\mathbb{F}_{Q^2}$ if and only if $Q \equiv 2 \pmod 3$.*

In case $Q = 2^{2m+1}$, the first two parts of this corollary were conjectured by Tu, Zeng, Hu and Li [11]. Conversely, these conjectures were the impetus which led to the present paper.

The proofs of our results rely on exhibiting certain permutations of the set of $(Q+1)$-th roots of unity in $\mathbb{F}_{Q^2}$. The permutations we exhibit are represented by *Rédei functions*, namely, rational functions over a field K which have the form $\mu \circ x^n \circ \mu^{-1}$ where $\mu(x)$ is a degree-one rational function having coefficients in an extension of K, and μ^{-1} is the rational function such that $\mu^{-1}(\mu(x)) = x$. For further results about

such functions, see for instance [2, 8, 9] and [4, Ch. 5]. Although permutation polynomials on subgroups of $\mathbb{F}_q^*$ have also been studied [1], the present paper is the first to examine Rédei functions as permutations of such subgroups, and especially the first to notice that Rédei functions can permute subgroups of $\mathbb{F}_q^*$ other than the multiplicative groups of subfields of $\mathbb{F}_q$.

We prove Theorems 1.1 and 1.2 in the next two sections, and deduce the corollaries in Section 4. We conclude this paper by using our approach to give a very simple proof of a substantial generalization of the main result of [11].

2. Proof of Theorem 1.1

In this section we prove Theorem 1.1. We begin by describing the permutations of a group of roots of unity which are induced by degree-one rational functions.

Lemma 2.1. *Let K be a field of characteristic $p \geq 0$, let $d > 2$ satisfy $p \nmid d$, and let μ_d be the set of d-th roots of unity in $\overline{K}$. For any degree-one $\ell(x) \in K(x)$, we have $\ell(\mu_d) = \mu_d$ if and only if either*

- *$\ell(x)$ equals either ρx or ρ/x with $\rho \in \mu_d$, or*
- *$p > 0$ and $d = Q + 1$ for some power Q of p, where in addition $\ell(x) = (\epsilon^Q x + \rho)/(\rho^Q x + \epsilon)$ with $\epsilon, \rho \in \mathbb{F}_{Q^2}^*$ and $\epsilon^{Q+1} \neq \rho^{Q+1}$.*

Proof. Write $\ell(x) = (\alpha x + \beta)/(\gamma x + \delta)$ where $\alpha, \beta, \gamma, \delta \in K$ satisfy $\Delta := \alpha\delta - \beta\gamma \neq 0$. We may assume that $\alpha, \beta, \gamma, \delta$ are in the subfield K_0 of K which is generated by μ_d, since if $\ell(\mu_d) = \mu_d$ then $\ell(x)$ is a degree-one rational function which maps at least three elements of K_0 into K_0, whence $\ell(x) \in K_0(x)$. Since $\deg(\ell) = 1$, the condition $\ell(\mu_d) = \mu_d$ is equivalent to $\ell(\mu_d) \subseteq \mu_d$, and hence to the assertion that $(\alpha\rho + \beta)^d = (\gamma\rho + \delta)^d$ for every $\rho \in \mu_d$. Thus $\ell(\mu_d) = \mu_d$ if and only if the polynomial $f(x) := (\alpha x+\beta)^d-(\gamma x+\delta)^d-(\alpha^d-\gamma^d)(x^d-1)$ vanishes on μ_d. Since $\deg(f) < d$, this condition asserts that $f(x)$ is identically zero, or equivalently that $(\alpha x + \beta)^d - (\gamma x + \delta)^d = (\alpha^d - \gamma^d)(x^d - 1)$. Hence $\ell(\mu_d) = \mu_d$ if and only if both of the following conditions hold:

(1) $\beta^d - \delta^d = \gamma^d - \alpha^d$
(2) for each $0 < i < d$ such that $p \nmid \binom{d}{i}$, we have $\alpha^i\beta^{d-i} = \gamma^i\delta^{d-i}$.

In particular, condition (2) with $i = 1$ asserts that $\alpha\beta^{d-1} = \gamma\delta^{d-1}$, so since $\alpha\delta \neq \beta\gamma$ we see that $\alpha = 0$ if and only if $\delta = 0$, and likewise $\beta = 0$ if and only if $\gamma = 0$. If either $\alpha = \delta = 0$ or $\beta = \gamma = 0$ then $\ell(x) = \rho x^j$ with $\rho \in K^*$ and $j \in \{1, -1\}$, and plainly such a function $\ell(x)$ permutes μ_d if and only if $\rho \in \mu_d$. Henceforth assume that $\alpha, \beta, \gamma, \delta$ are nonzero. The conclusion of condition (2) can now

be reformulated as $(\alpha\delta/(\beta\gamma))^i = (\delta/\beta)^d$. If this conclusion holds for each of two consecutive integers i, then it follows that $\alpha\delta/(\beta\gamma) = 1$, contrary to our hypothesis that $\Delta \neq 0$. Hence if $\ell(\mu_d) = \mu_d$ then for any $0 < i < d-1$ we have either $p \mid \binom{d}{i}$ or $p \mid \binom{d}{i+1}$, so that $p > 0$ and by Lucas's theorem on binomial coefficients mod p [6, 3] we conclude that $d = Q + 1$ for some power Q of p. Henceforth assume that $p > 0$ and $d = Q + 1$ for some power Q of p, so that $K_0 = \mathbb{F}_{Q^2}$. The hypotheses of condition (2) are only satisfied by $i = 1$ and $i = Q$, so condition (2) asserts that $\alpha\beta^Q = \gamma\delta^Q$ and $\alpha^Q\beta = \gamma^Q\delta$. Upon solving for γ via the first equation and substituting the resulting value into both the second equation and condition (1), we find that $\ell(\mu_d) = \mu_d$ if and only if all of the following hold:

- $\gamma = \alpha(\beta/\delta)^Q$
- $\alpha^Q\beta = \alpha^Q(\beta/\delta)^{Q^2}\delta$
- $\beta^{Q+1} - \delta^{Q+1} = \alpha^{Q+1}(\beta/\delta)^{Q^2+Q} - \alpha^{Q+1}$.

The second condition is automatically true, and the third condition asserts that $(\delta^{Q+1} - \alpha^{Q+1}) \cdot ((\beta/\delta)^{Q+1} - 1) = 0$, or equivalently that at least one of α/δ or β/δ is in μ_{Q+1}. When the above conditions hold, we have $\Delta = \alpha\delta - \beta\alpha(\beta/\delta)^Q = \alpha(\delta - \beta^{Q+1}/\delta^Q)$, so the hypothesis $\Delta \neq 0$ asserts that $\beta/\delta \notin \mu_{Q+1}$. Hence the above conditions hold if and only if $\alpha/\delta \in \mu_{Q+1}$ with $\gamma = \alpha(\beta/\delta)^Q$ and $\beta/\delta \notin \mu_{Q+1}$. Writing $\alpha/\delta = \epsilon^{Q-1}$ with $\epsilon \in \mathbb{F}_{Q^2}^*$, these conditions assert that $\ell(x) = (\delta\epsilon^{Q-1}x + \beta)/(\delta\epsilon^{Q-1}(\beta/\delta)^Q x + \delta) = (\epsilon^Q x + \beta\epsilon/\delta)/((\beta\epsilon/\delta)^Q x + \epsilon)$ where $(\beta\epsilon/\delta)^{Q+1} \neq \epsilon^{Q+1}$, as desired. □

The next lemma was first proved in [12].

Lemma 2.2. *Pick $h \in \mathbb{F}_q[x]$ and integers $d, r > 0$ such that $d \mid (q-1)$. 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 the set of d-th roots of unity in $\mathbb{F}_q^*$.*

This lemma has been used in several investigations of permutation polynomials, for instance see [7, 12, 13, 14, 15]. Since the proof of Lemma 2.2 is short, we include it here for the reader's convenience.

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 permutes $(\mathbb{F}_q^*)^s$, which equals the set of d-th roots of unity in $\mathbb{F}_q^*$. □

We now prove Theorem 1.1.

Proof of Theorem 1.1. Write $h(x) := (\gamma x - \beta)^n - \gamma(x - \gamma^Q\beta)^n$ and $r := n + k(Q+1)$. By Lemma 2.2, $f(x) = x^r h(x^{Q-1})$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(n+k(Q+1), Q-1) = 1$ and $g(x) := x^r h(x)^{Q-1}$ permutes the set μ_{Q+1} of $(Q+1)$-th roots of unity in $\mathbb{F}_{Q^2}$. Henceforth we assume that $\gcd(n+k(Q+1), Q-1) = 1$, or equivalently $\gcd(n+2k, Q-1) = 1$; note that this implies n is odd if Q is odd, so that $(-1)^n = -1$ in $\mathbb{F}_Q$.

We begin by showing that $h(x)$ has no roots in μ_{Q+1}. For $\alpha \in \mu_{Q+1}$, if $h(\alpha) = 0$ then one easily verifies that $\alpha \neq \gamma^Q\beta$ so that $\delta := (\gamma\alpha - \beta)/(\alpha - \gamma^Q\beta)$ satisfies $\delta^n = \gamma$, and thus in particular $\delta \notin \mu_{Q+1}$. But we compute

$$\delta^Q = \frac{\gamma^Q\alpha^{-1} - \beta^{-1}}{\alpha^{-1} - \gamma\beta^{-1}} = \frac{\gamma^Q\beta - \alpha}{\beta - \gamma\alpha} = \delta^{-1},$$

which is impossible since $\delta \notin \mu_{Q+1}$. Hence $h(x)$ has no roots in μ_{Q+1}, so $h(\mu_{Q+1}) \subseteq \mathbb{F}_{Q^2}^*$, whence $g(\mu_{Q+1}) \subseteq \mu_{Q+1}$. Thus, g permutes μ_{Q+1} if and only if g is injective on μ_{Q+1}.

Next, for $\alpha \in \mu_{Q+1}$ we compute

$$h(\alpha)^Q = (\gamma^Q\alpha^{-1} - \beta^{-1})^n - \gamma^Q(\alpha^{-1} - \gamma\beta^{-1})^n = \frac{(\gamma^Q\beta - \alpha)^n - \gamma^Q(\beta - \gamma\alpha)^n}{(\beta\alpha)^n},$$

so that

$$g(\alpha) = \alpha^{r-n}\beta^{-n}\frac{(\gamma^Q\beta - \alpha)^n - \gamma^Q(\beta - \gamma\alpha)^n}{(\gamma\alpha - \beta)^n - \gamma(\alpha - \gamma^Q\beta)^n}.$$

Thus g is injective on μ_{Q+1} if and only if

$$G(x) := \beta\frac{(\gamma^Q\beta - x)^n - \gamma^Q(\beta - \gamma x)^n}{(\gamma x - \beta)^n - \gamma(x - \gamma^Q\beta)^n}$$

is injective on μ_{Q+1}. For $\ell(x) := (x - \gamma^Q\beta)/(\gamma x - \beta)$, we have

$$G = \ell^{-1} \circ x^n \circ \ell,$$

so G is injective on μ_{Q+1} if and only if x^n is injective on $\ell(\mu_{Q+1})$. Since $\beta \in \mu_{Q+1}$ we have $\beta = -1/\epsilon^{Q-1}$ for some $\epsilon \in \mathbb{F}_{Q^2}^*$, so that $\ell(x) = (x + \gamma^Q/\epsilon^{Q-1})/(\gamma x + 1/\epsilon^{Q-1}) = (\epsilon^Q x + \gamma^Q\epsilon)/(\gamma\epsilon^Q x + \epsilon)$. By Lemma 2.1 we have $\ell(\mu_{Q+1}) = \mu_{Q+1}$, so x^n is injective on $\ell(\mu_{Q+1})$ if and only if $\gcd(n, Q+1) = 1$. This concludes the proof. □

3. Proof of Theorem 1.2

In this section we prove Theorem 1.2. Throughout this section, Q is a prime power,and μ_d denotes the set of d-th roots of unity in $\overline{\mathbb{F}}_Q$. We begin by determining the bijections $\mu_{Q+1} \to \mathbb{F}_Q \cup \{\infty\}$ which are induced by degree-one rational functions.

Lemma 3.1. *Let Q be a prime power, and let $\ell \in \overline{\mathbb{F}}_Q(x)$ be a degree-one rational function. Then $\ell(x)$ induces a bijection from μ_{Q+1} to $\mathbb{F}_Q \cup \{\infty\}$ if and only if $\ell(x) = (\rho x + \rho^Q)/(\epsilon x + \epsilon^Q)$ for some $\rho, \epsilon \in \mathbb{F}_{Q^2}^*$ such that $\rho^{Q-1} \neq \epsilon^{Q-1}$.*

Proof. If ℓ maps μ_{Q+1} into $\mathbb{F}_Q \cup \{\infty\}$ then ℓ maps at least $Q+1 \geq 3$ elements of $\mathbb{F}_{Q^2}$ into $\mathbb{F}_{Q^2} \cup \{\infty\}$, so $\ell \in \mathbb{F}_{Q^2}(x)$. Thus we may write $\ell = (\alpha x+\beta)/(\gamma x+\delta)$ where $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{Q^2}$ satisfy $\alpha\delta \neq \beta\gamma$. Moreover, we may assume that $\ell^{-1}(\infty)$ is in μ_{Q+1}, so that $\gamma \neq 0$ and $\delta/\gamma \in \mu_{Q+1}$. Then ℓ induces a bijection from μ_{Q+1} to $\mathbb{F}_Q \cup \{\infty\}$ if and only if the numerator of $\ell(x)^Q - \ell(x)$ is divisible by $h(x) := (x^{Q+1}-1)/(x+\delta/\gamma)$. The product of this numerator with $(\gamma x + \delta)$ is

$$\begin{aligned}&(\alpha^Q x^Q + \beta^Q)(\gamma x + \delta) - (\gamma^Q x^Q + \delta^Q)(\alpha x + \beta)\\ &\quad = (\alpha^Q\gamma - \gamma^Q\alpha)x^{Q+1} + (\alpha^Q\delta - \gamma^Q\beta)x^Q + (\beta^Q\gamma - \delta^Q\alpha)x + (\beta^Q\delta - \delta^Q\beta),\end{aligned}$$

which is congruent mod $x^{Q+1}-1$ to

$$g(x) := (\alpha^Q\delta - \gamma^Q\beta)x^Q + (\beta^Q\gamma - \delta^Q\alpha)x + (\alpha^Q\gamma - \gamma^Q\alpha + \beta^Q\delta - \delta^Q\beta).$$

Thus $g(x)$ is divisible by $h(x)$ if and only if $g(x)$ is a constant multiple of $h(x)$. Since

$$h(x) = \frac{x^{Q+1} - (-\delta/\gamma)^{Q+1}}{x + \delta/\gamma} = \sum_{i=0}^{Q} x^i(-\delta/\gamma)^{Q-i},$$

we see that $h(x)$ has a term of degree $Q-1$, but if $Q > 2$ then $g(x)$ has no such term. Thus if $Q > 2$ then $g(x)$ is divisible by $h(x)$ if and only if $g(x)$ is the zero polynomial, or equivalently

$$\alpha^Q\delta = \gamma^Q\beta \quad \text{and} \quad \alpha^Q\gamma + \beta^Q\delta \in \mathbb{F}_Q.$$

Since $\delta/\gamma \in \mu_{Q+1}$, the second condition follows from the first, as $\alpha^Q\gamma + \beta^Q\delta = \gamma^{Q+1}\beta/\delta + \beta^Q\delta = \delta^Q\beta + \beta^Q\delta$ is in $\mathbb{F}_Q$. If these conditions hold then $\alpha\delta - \beta\gamma = \alpha\delta - \alpha^Q\delta/\gamma^{Q-1}$ is nonzero precisely when $\alpha/\gamma \notin \mathbb{F}_Q$. Writing $\delta/\gamma = \epsilon^{Q-1}$ with $\epsilon \in \mathbb{F}_{Q^2}^*$, the condition $\ell(\mu_{Q+1}) = \mathbb{F}_Q \cup \{\infty\}$ therefore asserts (if $Q > 2$) that $\ell(x) = (\alpha x + (\alpha/\gamma)^Q\delta)/(\gamma x+\delta) = (\alpha x + \epsilon^{Q-1}\alpha^Q/\gamma^{Q-1})/(\gamma x + \gamma\epsilon^{Q-1})$ or equivalently $\ell(x) = (\rho x + \rho^Q)/(\epsilon x + \epsilon^Q)$ where $\rho = \alpha\epsilon/\gamma$, in which case $\alpha/\gamma \notin \mathbb{F}_Q$ asserts that $\rho/\epsilon \notin \mathbb{F}_Q$. This

yields the desired conclusion when $Q > 2$, and it is easy to check that the same conclusion holds when $Q = 2$. □

Remark 3.2. A geometric explanation for the "if" implication of Lemma 3.1 is given in [5], based on analyzing singular cubic curves via [10, Prop. III.2.5].

We now prove Theorem 1.2.

Proof of Theorem 1.2. Write $h(x) := (\delta x - \beta\delta^Q)^n - \delta(x-\beta)^n$ and $r := n + k(Q+1)$. By Lemma 2.2, $f(x) = x^r h(x^{Q-1})$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(n + k(Q+1), Q-1) = 1$ and $g(x) := x^r h(x)^{Q-1}$ permutes μ_{Q+1}. Henceforth we assume that $\gcd(n + k(Q+1), Q-1) = 1$, or equivalently $\gcd(n + 2k, Q-1) = 1$; note that this implies n is odd if Q is odd, so that $(-1)^n = -1$ in $\mathbb{F}_Q$.

We begin by showing that $h(x)$ has no roots in μ_{Q+1}. Our hypothesis $\delta \notin \mathbb{F}_Q$ implies that $h(\beta) = (\delta\beta - \beta\delta^Q)^n = \beta^n(\delta - \delta^Q)^n \neq 0$. For $\alpha \in \mu_{Q+1} \setminus \{\beta\}$, if $h(\alpha) = 0$ then $\theta := (\delta\alpha - \beta\delta^Q)/(\alpha - \beta)$ satisfies $\theta^n = \delta$, so in particular $\theta \notin \mathbb{F}_Q$. But we compute

$$\theta^Q = \frac{\delta^Q\alpha^{-1} - \beta^{-1}\delta}{\alpha^{-1} - \beta^{-1}} = \frac{\delta^Q\beta - \alpha\delta}{\beta - \alpha} = \theta,$$

which is a contradiction. Hence $h(x)$ has no roots in μ_{Q+1}, so $h(\mu_{Q+1}) \subseteq \mathbb{F}_{Q^2}^*$, whence $g(\mu_{Q+1}) \subseteq \mu_{Q+1}$. Thus, g permutes μ_{Q+1} if and only if g is injective on μ_{Q+1}.

Next, for $\alpha \in \mu_{Q+1}$ we compute

$$h(\alpha)^Q = (\delta^Q\alpha^{-1} - \beta^{-1}\delta)^n - \delta^Q(\alpha^{-1} - \beta^{-1})^n = \frac{(\delta^Q\beta - \alpha\delta)^n - \delta^Q(\beta - \alpha)^n}{(\alpha\beta)^n},$$

so that

$$g(\alpha) = \alpha^{r-n}\beta^{-n}\frac{(\delta^Q\beta - \alpha\delta)^n - \delta^Q(\beta - \alpha)^n}{(\delta\alpha - \beta\delta^Q)^n - \delta(\alpha - \beta)^n}.$$

Since $r - n = k(Q+1)$ and $\alpha^{Q+1} = 1$, it follows that g is injective on μ_{Q+1} if and only if

$$G(x) := -\beta\frac{(\delta^Q\beta - x\delta)^n - \delta^Q(\beta - x)^n}{(\delta x - \beta\delta^Q)^n - \delta(x - \beta)^n}$$

is injective on μ_{Q+1}. For $\ell(x) := (\delta x - \beta\delta^Q)/(x - \beta)$, we have

$$G = \ell^{-1} \circ x^n \circ \ell.$$

so G is injective on μ_{Q+1} if and only if x^n is injective on $\ell(\mu_{Q+1})$. Writing $-\beta = \epsilon^{Q-1}$ with $\epsilon \in \mathbb{F}_{Q^2}^*$, we see that $\ell(x) = (\delta\epsilon x + (\delta\epsilon)^Q)/(\epsilon x + \epsilon^Q)$, so by Lemma 3.1 we have $\ell(\mu_{Q+1}) = \mathbb{F}_Q \cup \{\infty\}$. Thus x^n is

injective on $\ell(\mu_{Q+1})$ if and only if $\gcd(n, Q-1) = 1$, which concludes the proof. □

4. Proofs of Corollaries 1.3 and 1.4

In this section we prove Corollaries 1.3 and 1.4.

Proof of Corollary 1.3. If $Q \equiv 0 \pmod 3$ then $g(1) = 0 = g(0)$ so $g(x)$ does not permute $\mathbb{F}_{Q^2}$. If $Q \equiv 1 \pmod 3$ then put $n = 3$ and $\beta = 1$, and let γ be a primitive cube root of unity in $\mathbb{F}_Q$. In this case, Theorem 1.1 says that $(\gamma - 1)g(x)$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(3 + 2k, Q - 1) = 1$. Finally, if $Q \equiv 2 \pmod 3$ then put $n = 3$ and $\beta = \delta$, where δ is a primitive cube root of unity in $\mathbb{F}_{Q^2}$. In this case, Theorem 1.2 says that $(\delta - 1)g(x)$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(3 + 2k, Q - 1) = 1$. □

Proof of Corollary 1.4. Items (2) and (3) follow at once from the cases $k = 1$ and $k = 0$ of Corollary 1.3. The case $k = Q - 3$ of Corollary 1.3 asserts that $g(x) := x^{Q^2-2Q} + 3x^{Q^2-Q-1} - x^{Q^2+Q-3}$ is a permutation polynomial over $\mathbb{F}_{Q^2}$ if and only if $\gcd(2Q - 3, Q - 1) = 1$, which always holds. Thus $g(x^{Q^2-2})$ is a permutation polynomial over $\mathbb{F}_{Q^2}$, as is the reduction of $g(x^{Q^2-2})$ mod $x^{Q^2} - x$. Since this reduction equals $x^{2Q-1} + 3x^Q - x^{Q^2-Q+1}$, item (1) of Corollary 1.4 follows. □

5. The main result of [11]

In this section we give a simple proof of a generalization of [11, Thm. 1]. Our proof is completely different from the one in [11]. Once again, μ_{Q+1} denotes the set of $(Q+1)$-th roots of unity in $\overline{\mathbb{F}}_Q$.

Theorem 5.1. *Let Q be a prime power, let r be a positive integer, and let β be a $(Q+1)$-th root of unity in $\mathbb{F}_{Q^2}$. Let $h(x) \in \mathbb{F}_{Q^2}[x]$ be a polynomial of degree d such that $h(0) \neq 0$ and*

$$\big(x^d \cdot h(1/x)\big)^Q = \beta \cdot h(x^Q).$$

Then $f(x) := x^r h(x^{Q-1})$ permutes $\mathbb{F}_{Q^2}$ if and only if all of the following hold:

(1) $\gcd(r, Q-1) = 1$
(2) $\gcd(r - d, Q+1) = 1$
(3) *$h(x)$ has no roots in μ_{Q+1}.*

Remark 5.2. The polynomials $h(x)$ satisfying the hypotheses of Theorem 5.1 can be described explicitly in terms of their coefficients. They are $h(x) = \sum_{i=0}^d a_i x^i$ where $a_0 \neq 0$ and, for $0 \leq i \leq d/2$, we have $a_i \in \mathbb{F}_{Q^2}$ and $a_{d-i} = (\beta a_i)^Q$.

Proof of Theorem 5.1. By Lemma 2.2, we see that $f(x)$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(r, Q-1) = 1$ and $g(x) := x^r h(x)^{Q-1}$ permutes μ_{Q+1}. We may assume that $h(x)$ has no roots in μ_{Q+1}, since otherwise g cannot permute μ_{Q+1}. Then any $\alpha \in \mu_{Q+1}$ satisfies

$$g(\alpha) = \alpha^r \frac{h(\alpha)^Q}{h(\alpha)} = \alpha^r \frac{h(\alpha^{-Q})^Q}{h(\alpha)} = \alpha^{r-d}\beta,$$

so g permutes μ_{Q+1} if and only if $\gcd(r-d, Q+1) = 1$. □

We now illustrate Theorem 5.1 in the special case $h(x) = x^d + \beta^{-1}$.

Corollary 5.3. *Let Q be a prime power, let r and d be positive integers, and let β be a $(Q+1)$-th root of unity in $\mathbb{F}_{Q^2}$. Then $x^{r+d(Q-1)} + \beta^{-1}x^r$ permutes $\mathbb{F}_{Q^2}$ if and only if all of the following hold:*

(1) $\gcd(r, Q-1) = 1$
(2) $\gcd(r-d, Q+1) = 1$
(3) $(-\beta)^{(Q+1)/\gcd(Q+1,d)} \neq 1$.

Proof. Since $h(x) := x^d + \beta^{-1}$ satisfies the hypotheses of Theorem 5.1, the Corollary will follow from Theorem 5.1 once we show that the final conclusion in the Corollary is equivalent to the final conclusion in the Theorem. For this, note that $h(x)$ has roots in μ_{Q+1} if and only if $-\beta^{-1}$ is in $(\mu_{Q+1})^d$, which equals $\mu_{(Q+1)/\gcd(Q+1,d)}$. □

In case Q is even, Corollary 5.3 is a refinement of [11, Thm. 1].

References

[1] O. J. Brison, On group-permutation polynomials, *Portugal. Math.* **50** (1993), 363–383. 3

[2] L. Carlitz, A note on permutation functions over a finite field, *Duke Math. J.* **29** (1962), 325–332. 3

[3] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic Mathematics*, CMS Conf. Proc. 20, Amer. Math. Soc. (1997), 253–276. 4

[4] R. M. Guralnick, P. Müller and J. Saxl, The rational function analogue of a question of Schur and exceptionality of permutation representations, *Mem. Amer. Math. Soc.* **162** (2003), no. 773. 3

[5] T. G. Hyde, Seeking conceptual explanations of these nice bijections on roots of unity (answer). MathOverflow. `http://mathoverflow.net/a/191488`. 7

[6] É. Lucas, Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier, *Bull. Soc. Math. France* **6** (1877–1878), 49–54. 4

[7] A. M. Masuda and M. E. Zieve, Permutation binomials over finite fields, *Trans. Amer. Math. Soc.* **361** (2009), 4169–4180. 4

[8] W. Nöbauer, Rédei-Funktionen für Zweierpotenzen, *Period. Math. Hungar.* **17** (1986), 37–44. 3

[9] L. Rédei, Über eindeutig umkehrbare Polynome in endlichen Körpern, *Acta Sci. Math.* (Szeged) **11** (1946), 85–92. 3

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, Dordrecht, 2009. 7

[11] Z. Tu, X. Zeng, L. Hu and C. Li, A class of binomial permutation polynomials, arXiv:1310.0337v1, 28 Sep 2013. 2, 3, 8, 9

[12] T. J. Tucker and M. E. Zieve, Permutation polynomials, curves without points, and Latin squares, preprint, 2000. 4

[13] M. E. Zieve, Some families of permutation polynomials over finite fields, *Internat. J. Number Theory* **4** (2008), 851–857. 4

[14] 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.* **137** (2009), 2209–2216. 4

[15] M. E. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, in *Additive Number Theory*, Springer (2010), 355–359. 4

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA

E-mail address: zieve@umich.edu

URL: www.math.lsa.umich.edu/∼zieve/