PERMUTATION POLYNOMIALS OF THE FORM $X + \gamma \operatorname{Tr}(X^k)$

GOHAR KYUREGHYAN AND MICHAEL E. ZIEVE

1. Introduction

Let $\mathbb{F}_q$ be the finite field of size q, and let p be the characteristic of $\mathbb{F}_q$. A *permutation polynomial* over $\mathbb{F}_q$ is a polynomial $F(X) \in \mathbb{F}_q[X]$ for which the induced function $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. Permutation polynomials are used in various applications of finite fields, where special importance is attached to permutation polynomials which have few terms. Due in part to this, and also due to the intrinsic interest of the problem, the study of permutation polynomials with few terms has thrived for well over a century. In this paper we make a new contribution to this topic by analyzing permutation polynomials of the form $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ where n and k are positive integers, $\gamma \in \mathbb{F}_{q^n}^*$, and $\operatorname{Tr}_{q^n/q}(X) := X^{q^{n-1}} + X^{q^{n-2}} + \cdots + X^q + X$ (so that $\operatorname{Tr}_{q^n/q}$ induces the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$). We produce the following families of permutation polynomials:

Theorem 1.1. *The polynomial $X+\gamma \operatorname{Tr}_{q^n/q}(X^k)$ is a permutation polynomial over $\mathbb{F}_{q^n}$ in each of the following cases:*

- **(a):** $n = 2$, $q \equiv \pm 1 \pmod 6$, $\gamma = -1/3$, $k = 2q - 1$
- **(b):** $n = 2$, $q \equiv 5 \pmod 6$, $\gamma^3 = -1/27$, $k = 2q - 1$
- **(c):** $n = 2$, $q \equiv 1 \pmod 3$, $\gamma = 1$, $k = (q^2 + q + 1)/3$
- **(d):** $n = 2$, $q \equiv 1 \pmod 4$, $(2\gamma)^{(q+1)/2} = 1$, $k = (q + 1)^2/4$
- **(e):** $n = 2$, $q = Q^2$, $Q > 0$ *odd*, $\gamma = -1$, $k = Q^3 - Q + 1$
- **(f):** $n = 2$, $q = Q^2$, $Q > 0$ *odd*, $\gamma = -1$, $k = Q^3 + Q^2 - Q$
- **(g):** $n = 3$, q *odd*, $\gamma = 1$, $k = (q^2 + 1)/2$
- **(h):** $n = 3$, q *odd*, $\gamma = -1/2$, $k = q^2 - q + 1$
- **(i):** $n = 2\ell r$, $\gamma^{q^{2\ell}-1} = -1$, $k = q^\ell + 1$ *for some positive integers ℓ and r.*

We remark that "at random" one would not expect there to be permutation polynomials of the form $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ over $\mathbb{F}_{q^n}$ when $Q := q^n$ is sufficiently large and $\gamma \in \mathbb{F}_Q^*$, since the polynomials of this

The authors thank the referee for providing several corrections and helpful suggestions. The second author was partially supported by NSF grant DMS-1162181.

form induce fewer than Q^2 distinct functions on $\mathbb{F}_Q$ while the proportion of permutations amongst all functions $\mathbb{F}_Q \to \mathbb{F}_Q$ is $Q!/Q^Q$. Hence it seems that any infinite sequence of examples such as those in Theorem 1.1 should exist for some "good reason", and it is an interesting challenge to understand the different sorts of reasons which can account for such unexpected examples to occur.

An intriguing feature of the present paper is that we need several different methods in order to prove the various cases of Theorem 1.1. In cases (a)–(d) and (g) we use a well-known result (Proposition 2.2) asserting that $Xh(X^{q-1})$ permutes $\mathbb{F}_{q^n}$ if and only if $Xh(X)^{q-1}$ permutes the set $\mu_{(q^n-1)/(q-1)}$ of $(q^n-1)/(q-1)$-th roots of unity. We then reformulate the latter condition in a simpler way (see Proposition 2.4), so that cases (a) and (b) boil down to showing that a certain degree-3 rational function permutes μ_{q+1}, and case (c) boils down to showing that a certain power map X^N permutes μ_{q+1}. Case (d) is more interesting, since we wind up showing that $Xh(X)^{q-1}$ permutes μ_{q+1} by showing that it acts as c_1^2X on the nonsquares in μ_{q+1} and $c_2^2X^N$ on the squares, for certain elements $c_1, c_2 \in \mu_{q+1}$; in this case it seems complicated to analyze $Xh(X)^{q-1}$ at once on all elements of μ_{q+1}, rather than treating the squares and nonsquares separately. In case (g) we use a double application of Proposition 2.2, by first saying that the given polynomial permutes $\mathbb{F}_{q^3}$ if and only if a certain associated polynomial permutes μ_{q^2+q+1}, then composing the associated polynomial with certain power maps X^N which permute μ_{q^2+q+1}, and then reducing the composition mod $X^{q^2+q+1}-1$ to obtain a polynomial which (again by Proposition 2.2) permutes μ_{q^2+q+1} if and only if a certain additive polynomial permutes $\mathbb{F}_{q^3}$; we then finish the proof by directly verifying this last bijectivity. This kind of approach does not seem to work in cases (e) and (f), so for these cases we use a variant of Dobbertin's method [3], which involves computing Gröbner bases of several ideals in a multivariate polynomial ring. This variant involves new features compared to previous applications of Dobbertin's approach, and may be of independent interest. We prove case (h) by composing with certain bijective power maps and additive polynomials to obtain a function which permutes both the squares and the nonsquares in $\mathbb{F}_{q^3}$; this method was inspired by the notion of affine equivalence of planar functions. Finally, in case (i) we use an additive analogue of Proposition 2.2 (see Proposition 2.1) in order to show that the stated polynomial permutes $\mathbb{F}_{q^n}$ if and only if certain associated polynomials permute $\mathbb{F}_q$, and we calculate that each of these associated polynomials induces the same function on $\mathbb{F}_q$ as does $X+c$ for some $c \in \mathbb{F}_q$.

We computed all permutation polynomials over fields $\mathbb{F}_{q^n}$ of the form $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ with $\gamma \in \mathbb{F}_{q^n}^*$, q odd, $n > 1$, and $q^n < 5000$. Here the hypothesis $n > 1$ is needed to distinguish our study from that of permutation binomials. It is easy to see that, for fixed q, n, γ, we can replace k by qk or by $k + q^n - 1$ without affecting whether $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ permutes $\mathbb{F}_{q^n}$. Modulo this equivalence, the only permutation polynomials arising in our computation which are not listed in Theorem 1.1 are:

- Cases with $k = p^i$, where the polynomial is automatically a member of the much-studied class of *additive* permutation polynomials.
- Cases with $p \mid n$ and $(q^n - 1) \mid k(q^{n/p} - 1)$, where the polynomial induces the identity map on $\mathbb{F}_{q^n}$.
- $q = 7$, $n = 2$, $k = 10$, $\gamma^4 = 1$
- $q = 9$, $n = 2$, $k = 33$, $\gamma^2 - \gamma = 1$
- $q = 27$, $n = 2$, $k = 261$, $(\gamma - 1)^{13} = \gamma^{13}$
- $q = 9$, $n = 3$, $k \in \{11, 19, 33, 57\}$, $\gamma^4 = -1$
- $q = 49$, $n = 2$, $k = 385$, $\gamma^5 = -1$.

Thus, it seems that Theorem 1.1 may explain the bulk of all permutation polynomials of this form, so long as we exclude the simple cases where the polynomial is additive or induces the identity map.

Permutation polynomials of the form $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ were studied in [1, 2]. All examples in those papers had the special feature that γ is a linear translator of $f(X) := \operatorname{Tr}_{q^n/q}(X^k)$, in the sense that there is some $\delta \in \mathbb{F}_q$ for which

$$f(x + u\gamma) - f(x) = u\delta$$

for all $x \in \mathbb{F}_{q^n}$ and $u \in \mathbb{F}_q$. This property is satisfied (with $\delta = 0$) for the polynomials in case (i) of Theorem 1.1, as we show in Remark 10.2. However, the permutation polynomials in cases (a)–(h) of Theorem 1.1 are of a different nature, since for these polynomials γ is *not* a linear translator of $\operatorname{Tr}_{q^n/q}(X^k)$.

This paper is organized as follows. In Section 2 we prove some general properties about maps of the form $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$. Then in Sections 3–10 we prove Theorem 1.1 in each of cases (a)–(i). In addition, we note that Theorems 3.1, 6.1, 7.1 and 9.1 list further families of sparse rational functions which permute either a finite field or a group of roots of unity in a finite field.

2. General remarks and equivalent statements

We begin with two propositions which reformulate the condition that $X + \gamma \operatorname{Tr}_{q^n/q}(X^k)$ should permute $\mathbb{F}_{q^n}$ in terms of properties of some associated functions on $\mathbb{F}_q$. These reformulations play a crucial role in our proof of Theorem 1.1. In fact the reformulations apply to a more general class of functions.

Proposition 2.1. *For any function $f\colon \mathbb{F}_{q^n} \to \mathbb{F}_q$ with $n \geq 2$, and any $\gamma \in \mathbb{F}_{q^n}^*$, the following three statements are equivalent:*

- **(a):** *The map $F\colon x \mapsto x + \gamma \cdot f(x)$ is bijective on $\mathbb{F}_{q^n}$.*
- **(b):** *For each $\alpha \in \mathbb{F}_{q^n}$ the map $x \mapsto x + f(\alpha + \gamma \cdot x)$ is bijective on $\mathbb{F}_q$.*
- **(c):** *For each $\alpha \in \mathbb{F}_{q^n}$ there is a unique $x \in \mathbb{F}_q$ for which $x + f(\alpha + \gamma \cdot x) = 0$.*

Proof. For each $\alpha \in \mathbb{F}_{q^n}$, the function F maps the line $\alpha + \gamma\,\mathbb{F}_q$ into itself, so that F permutes $\mathbb{F}_{q^n}$ if and only if F induces a permutation on each such line. Explicitly, for $u \in \mathbb{F}_q$ we have

$$F(\alpha + \gamma\, u) = \alpha + \gamma(u + f(\alpha + \gamma\, u)),$$

so that F permutes the line $\alpha + \gamma\,\mathbb{F}_q$ if and only if the function $u \mapsto u + f(\alpha + \gamma\, u)$ permutes $\mathbb{F}_q$. Thus (a) and (b) are equivalent. Since (b) immediately implies (c), it remains only to show that (c) implies (b), or equivalently that if (b) did not hold then (c) would not hold. So suppose there is some $\alpha' \in \mathbb{F}_{q^n}$ for which the function $x \mapsto x + f(\alpha' + \gamma \cdot x)$ is not bijective on $\mathbb{F}_q$. Then there are distinct elements $u_1, u_2 \in \mathbb{F}_q$ which have the same image y under this function. Hence for $i = 1, 2$ we have

$$y = u_i + f(\alpha' + \gamma \cdot u_i),$$

or equivalently

$$(u_i - y) + f(\alpha' + \gamma \cdot (u_i - y) + \gamma y) = 0.$$

Thus $x_i := u_i - y$ satisfies $x_i + f(\alpha' + \gamma y + \gamma x_i) = 0$; since x_1 and x_2 are distinct elements of $\mathbb{F}_q$, this contradicts (c) for the value $\alpha := \alpha' + y\gamma$. □

The next result is a special case of [6, Lemma 2.1].

Proposition 2.2. *For any $h(X) \in \mathbb{F}_{q^n}[X]$, the polynomial $Xh(X^{q-1})$ permutes $\mathbb{F}_{q^n}$ if and only if $Xh(X)^{q-1}$ permutes the set of $(q^n-1)/(q-1)$-th roots of unity in $\mathbb{F}_{q^n}^*$.*

We now give further reformulations in case $n = 2$.

Proposition 2.3. *Let $\gamma, \omega \in \mathbb{F}_{q^2}$ be linearly independent over $\mathbb{F}_q$, and let $f\colon \mathbb{F}_{q^2} \to \mathbb{F}_q$ be a function satisfying $f(u \cdot x) = u \cdot f(x)$ for each $u \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^2}$. Then $x \mapsto x + \gamma \cdot f(x)$ permutes $\mathbb{F}_{q^2}$ if and only if $f(\gamma) \neq -1$ and $x \mapsto x + f(\omega + \gamma x)$ permutes $\mathbb{F}_q$.*

Proof. By Proposition 2.1, $x \mapsto x + \gamma \cdot f(x)$ permutes $\mathbb{F}_{q^2}$ if and only if $F_\alpha\colon x \mapsto x + f(\alpha + \gamma \cdot x)$ permutes $\mathbb{F}_q$ for each $\alpha \in \mathbb{F}_{q^2}$. The elements $\alpha \in \mathbb{F}_{q^2}$ are precisely the elements $\alpha := u \cdot \gamma + v \cdot \omega$ with $u, v \in \mathbb{F}_q$, so we treat each choice of u, v in turn. If $v = 0$ then for $x \in \mathbb{F}_q$ we have

$$F_\alpha(x) = x + f((u + x)\gamma) = x + (u + x)f(\gamma) = (1 + f(\gamma))\, x + uf(\gamma),$$

so that F_α permutes $\mathbb{F}_q$ if and only if $f(\gamma) \neq -1$. If $v \neq 0$ then for $x \in \mathbb{F}_q$ we have

$$F_\alpha(x) = x + f(v\omega + (u + x)\gamma) = v\left(\frac{x}{v} + f\left(\omega + \frac{u + x}{v}\gamma\right)\right),$$

so that F_α permutes $\mathbb{F}_q$ if and only if $x \mapsto x + f(\omega + (x + \frac{u}{v})\gamma)$ permutes $\mathbb{F}_q$, or equivalently $x \mapsto x + f(\omega + x\gamma)$ permutes $\mathbb{F}_q$. □

Proposition 2.4. *Let $k := (q - 1)N + 1$ for some integer $N \geq 0$, and pick any $\gamma \in \mathbb{F}_{q^2}^*$. Then the polynomial $F(X) := X + \gamma \operatorname{Tr}_{q^2/q}(X^k)$ permutes $\mathbb{F}_{q^2}$ if and only if*

$$H(X) := \frac{X^N + \gamma^q(1 + X^{2N-1})}{X^{N-1} + \gamma(X^{2N-1} + 1)}$$

permutes the set μ_{q+1} of $(q+1)$-th roots of unity in $\mathbb{F}_{q^2}^*$, or equivalently this rational function is injective on μ_{q+1} and its denominator has no roots in μ_{q+1}.

Proof. By Proposition 2.2, $F(X)$ permutes $\mathbb{F}_{q^2}$ if and only if

$$G(X) := X\big(1 + \gamma(X^N + X^{qN+1})\big)^{q-1}$$

permutes μ_{q+1}. For any $x \in \mu_{q+1}$ such that $G(x) \neq 0$, we have

$$\begin{aligned}
\frac{G(x)}{x} &= \big(1 + \gamma(x^N + x^{qN+1})\big)^{q-1} \\
&= \frac{1 + \gamma^q(x^{Nq} + x^{q^2N+q})}{1 + \gamma(x^N + x^{qN+1})} \\
&= \frac{1 + \gamma^q(x^{-N} + x^{N-1})}{1 + \gamma(x^N + x^{-N+1})} \\
&= \frac{H(x)}{x}.
\end{aligned}$$

Therefore $G(X)$ permutes μ_{q+1} if and only if $H(X)$ permutes μ_{q+1}. Finally, if the denominator of $H(X)$ has no roots in μ_{q+1} then the above computation shows that G and H agree on μ_{q+1}, and thus $H(\mu_{q+1}) = G(\mu_{q+1}) \subseteq \mu_{q+1}$, so that bijectivity of H on μ_{q+1} follows from injectivity. □

3. The case that $n = 2$ and $k = 2q - 1$

In this section we prove cases (a) and (b) of Theorem 1.1. We begin with a proof of (a), which also produces some degree-3 rational functions which permute $\mathbb{F}_q$, as well as some degree-3 rational functions which permute the set μ_{q+1} of $(q+1)$-th roots of unity in $\mathbb{F}_{q^2}^*$.

Theorem 3.1. *If* $\gcd(q, 6) = 1$ *then the following are true:*

(a): $F_1(X) := X - \dfrac{1}{3}\operatorname{Tr}_{q^2/q}(X^{2q-1})$ *permutes* $\mathbb{F}_{q^2}$.

(b): *For any nonsquare* $\nu \in \mathbb{F}_q$, *the function* $\dfrac{X(X^2 - 9\nu)}{X^2 - \nu}$ *permutes* $\mathbb{F}_q$.

(c): $g(X) := \dfrac{X^3 - 3X^2 + 1}{X^3 - 3X + 1}$ *permutes* μ_{q+1}.

Proof. First we show that (a) and (b) are equivalent. Pick $\omega \in \mathbb{F}_{q^2}$ with $\omega^q = -\omega \neq 0$. Then ω and $-1/3$ are linearly independent over $\mathbb{F}_q$. We apply Proposition 2.3 with $\gamma = -\frac{1}{3}$ and $f(X) := \operatorname{Tr}_{q^2/q}(X^{2q-1})$, noting that $f(a \cdot x) = a \cdot f(x)$ for $a \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^2}$ since $2q - 1 \equiv 1 \pmod{q-1}$. Since $f(-\frac{1}{3}) = -\frac{2}{3} \neq -1$, it follows that (a) holds if and only if

$$h(X) := X + \operatorname{Tr}_{q^2/q}\big((\omega - \frac{1}{3}X)^{2q-1}\big)$$

permutes $\mathbb{F}_q$. For $x \in \mathbb{F}_q$ we have

$$\begin{aligned} h(3x) &= 3x + \frac{(\omega - x)^{2q}}{\omega - x} + \frac{(\omega - x)^{2q^2}}{(\omega - x)^q} \\ &= 3x + \frac{(-\omega - x)^2}{\omega - x} + \frac{(\omega - x)^2}{(-\omega - x)} \\ &= \frac{x^3 - 9\omega^2 x}{x^2 - \omega^2}. \end{aligned}$$

Since the above equivalence holds for each ω with $\omega^q = -\omega \neq 0$, and the set of all corresponding values ω^2 coincides with the set of nonsquares in $\mathbb{F}_q$, this shows that (a) and (b) are equivalent. The equivalence of (a) and (c) follows from Proposition 2.4 with $N = 2$ and $\gamma = -\frac{1}{3}$. So it is enough to verify (c). By Proposition 2.4, it suffices to show that

g is both well-defined and injective on μ_{q+1}. If some $\alpha \in \mu_{q+1}$ is a root of $r(X) := X^3 - 3X + 1$, then also α^q is a root of $r(X)$; since neither 1 nor -1 is a root of $r(X)$, it follows that $\alpha \neq \alpha^q$. Since the product of the roots of $r(X)$ is -1, the third root of $r(X)$ must be $-1/\alpha^{q+1} = -1$, which is not the case since $r(-1) \neq 0$. Thus g is well-defined on μ_{q+1}. The numerator of $g(X) - g(Y)$ is

$$\begin{aligned}(X^3 - 3X^2 + 1)(Y^3 - 3Y + 1) - (Y^3 - 3Y^2 + 1)(X^3 - 3X + 1)\\ = 3(X - Y)(XY - X + 1)(XY - Y + 1).\end{aligned}$$

Hence if $g(\alpha) = g(\beta)$ for some distinct $\alpha, \beta \in \mu_{q+1}$ then $\alpha\beta \in \{\alpha - 1, \beta - 1\}$. Assume without loss that $\alpha\beta = \alpha - 1$, so that $(\alpha - 1)^{q+1} = 1$. But

$$(\alpha - 1)^{q+1} = \alpha^{q+1} - \alpha^q - \alpha + 1 = 2 - \frac{1}{\alpha} - \alpha,$$

so that $\alpha + \frac{1}{\alpha} = 1$ and thus $\beta = 1 - \frac{1}{\alpha} = \alpha$, a contradiction. □

We now show that the permutation property of the polynomials in case (b) of Theorem 1.1 follows at once from the analogous property in case (a).

Theorem 3.2. *If $q \equiv 5 \pmod 6$ and $\gamma \in \mathbb{F}_{q^2}$ satisfies $\gamma^3 = -\frac{1}{27}$, then*

$$F_2(X) := X + \gamma \operatorname{Tr}_{q^2/q}(X^{2q-1})$$

permutes $\mathbb{F}_{q^2}$.

Proof. Since $\omega := -3\gamma$ satisfies $\omega^3 = 1$, we have $\omega^{2q-1} = 1$ and thus

$$\begin{aligned}F_2(\omega X) &= \omega X - \frac{1}{3}\omega \operatorname{Tr}_{q^2/q}(\omega^{2q-1} X^{2q-1})\\ &= \omega\big(X - \frac{1}{3} \operatorname{Tr}_{q^2/q}(X^{2q-1})\big),\end{aligned}$$

so the result follows from Theorem 3.1. □

Remark 3.3. A different proof of bijectivity of F_1 was given in the recent paper [4].

4. The case that $n = 2$ and $k = (q^2 + q + 1)/3$

We now prove case (c) of Theorem 1.1.

Theorem 4.1. *If $q \equiv 1 \pmod 3$, then*

$$F_3(X) := X + \operatorname{Tr}_{q^2/q}(X^{(q^2+q+1)/3})$$

permutes $\mathbb{F}_{q^2}$.

Proof. By Proposition 2.4 with $N = \frac{q+2}{3}$, it suffices to show that

$$g(X) := \frac{X^N + 1 + X^{2N-1}}{X^{N-1} + X^{2N-1} + 1}$$

permutes μ_{q+1}. Here $3N \equiv 1 \pmod{q+1}$, so by putting $Y = X^N$ our condition becomes that

$$\frac{Y + 1 + \frac{1}{Y}}{\frac{1}{Y^2} + \frac{1}{Y} + 1}$$

should permute μ_{q+1}. This function is the identity function $y \mapsto y$ so long as μ_{q+1} contains no roots of $Y^2 + Y + 1$, which is the case since those roots have order 3. Hence $g(X)$ induces the same function on μ_{q+1} as does X^N, so that g permutes μ_{q+1}. □

5. The case that $n = 2$ and $k = (q+1)^2/4$

We now prove case (d) of Theorem 1.1.

Theorem 5.1. *Let $q \equiv 1 \pmod 4$, and let $\gamma \in \mathbb{F}_{q^2}$ satisfy $(2\gamma)^{(q+1)/2} = 1$. Then*

$$F_4(X) := X + \gamma \operatorname{Tr}_{q^2/q}(X^{(q+1)^2/4})$$

permutes $\mathbb{F}_{q^2}$.

Proof. By Proposition 2.2, it suffices to show that

$$g(X) := X(\gamma^{-1} + X^N + X^{qN+1})^{q-1}$$

induces a bijection on μ_{q+1} in case $N = \frac{q+3}{4}$. Note that every element of μ_{q+1} can be written in exactly one way as $\pm y^2$ with $y \in \mu_{(q+1)/2}$. By hypothesis 2γ is a square in μ_{q+1}, so that -2γ is a nonsquare in μ_{q+1}, and thus $\gamma^{-1} + 2y$ is nonzero for each $y \in \mu_{(q+1)/2}$. For $y \in \mu_{(q+1)/2}$ we compute

$$(y^2)^N = y^{(q+3)/2} = y \text{ and } (y^2)^{qN+1} = y^{q+2} = y$$

so that

$$\begin{aligned} g(-y^2) &= -y^2(\gamma^{-1} + y(-1)^N + y(-1)^{qN+1})^{q-1} \\ &= -y^2\gamma^{1-q} = -(2y\gamma)^2, \end{aligned}$$

and

$$\begin{aligned} g(y^2) &= y^2(\gamma^{-1} + y + y)^{q-1} = y^2\,\frac{(\gamma^{-1} + 2y)^q}{\gamma^{-1} + 2y} \\ &= y^2\,\frac{4\gamma + 2y^{-1}}{\gamma^{-1} + 2y} = 2\gamma y. \end{aligned}$$

Since 2γ is in $\mu_{(q+1)/2}$, and squaring is a bijective map on $\mu_{(q+1)/2}$, it follows that g induces a bijection on $\mu_{(q+1)/2}$ and also a bijection on $-\mu_{(q+1)/2}$, so that g induces a bijection on μ_{q+1} as desired. $\square$

Remark 5.2. In fact, the polynomial F_4 fixes each nonsquare in $\mathbb{F}_{q^2}$. Moreover, we have

$$F_4(x) = \begin{cases} x + 2\gamma \cdot x^{\frac{(q+1)^2}{4}} & \text{if } x \text{ is a square in } \mathbb{F}_{q^2} \\ x & \text{if } x \text{ is a nonsquare in } \mathbb{F}_{q^2}. \end{cases}$$

To see this, note that for any $x \in \mathbb{F}_{q^2}$ the element $x^{(q^2-1)/4}$ is either zero or a fourth root of unity, and since $q \equiv 1 \pmod 4$ it follows that $x^{(q^2-1)/4}$ lies in the subfield $\mathbb{F}_q$. Thus for $x \in \mathbb{F}_{q^2}$ we have

$$F_4(x) = x + \gamma \operatorname{Tr}_{q^2/q}(x^{\frac{q^2-1}{4}} x^{\frac{q+1}{2}}) = x + \gamma\, x^{\frac{q^2-1}{4}} \operatorname{Tr}_{q^2/q}(x^{\frac{q+1}{2}}).$$

Our claimed expression for $F_4(x)$ now follows from the fact that

$$\begin{aligned} \operatorname{Tr}_{q^2/q}(x^{\frac{q+1}{2}}) &= x^{\frac{q+1}{2}} + x^{\frac{q^2+q}{2}} \\ &= x^{\frac{q+1}{2}}(1 + x^{\frac{q^2-1}{2}}) \\ &= \begin{cases} 2x^{\frac{q+1}{2}} & \text{if } x \text{ is a square in } \mathbb{F}_{q^2} \\ 0 & \text{if } x \text{ is a nonsquare in } \mathbb{F}_{q^2}. \end{cases} \end{aligned}$$

6. The case that $n = 2$ and $q = Q^2$ where Q is an odd prime power and $k = Q^3 - Q + 1$

In this section we prove case (e) of Theorem 1.1, by showing that

$$F_5(X) := X - \operatorname{Tr}_{Q^4/Q^2}(X^{Q^3-Q+1})$$

is a permutation on $\mathbb{F}_{Q^4}$, when Q is an odd prime power. Our proof relies on a variant of Dobbertin's method [3]. We also exhibit certain sparse rational functions which permute either $\mathbb{F}_{Q^2}$ or the set of (Q^2+1)-th roots of unity in $\mathbb{F}_{Q^4}^*$.

Theorem 6.1. *For any odd prime power Q, we have:*

(a): $F_5(X) = X - \operatorname{Tr}_{Q^4/Q^2}(X^{Q^3-Q+1})$ *permutes* $\mathbb{F}_{Q^4}$.

(b): $\dfrac{X^{Q+2} + 3\nu X^Q + 4\nu^{(Q+1)/2} X}{X^2 - \nu}$ *permutes* $\mathbb{F}_{Q^2}$, *where* ν *is any nonsquare in* $\mathbb{F}_{Q^2}^*$.

(c): $\dfrac{X^{2Q-1} - X^Q + 1}{X^{2Q-1} - X^{Q-1} + 1}$ *permutes the set of* (Q^2+1)*-th roots of unity in* $\mathbb{F}_{Q^4}^*$.

We begin with some simple lemmas about the preimages under F_5 of some special values.

Lemma 6.2. *The only root of $F_5(X)$ in $\mathbb{F}_{Q^4}$ is 0.*

Proof. Suppose to the contrary that $x \in \mathbb{F}_{Q^4}^*$ is a root of F_5. Then

$$x^{Q^3-Q} + x^{-Q^3+Q^2+Q-1} = 1,$$

and $y := x^{Q^2-1}$ is an element of μ_{Q^2+1} satisfying

$$y^Q + y^{1-Q} = 1. \tag{6.3}$$

In particular, y cannot be ± 1. Since $y^{Q^2} = 1/y$, we obtain

$$y^{-1} + y^{Q+1} = (y^Q + y^{1-Q})^Q = 1^Q = 1^{Q^3} = (y^Q + y^{1-Q})^{Q^3} = y + y^{-Q-1},$$

or equivalently

$$(y^{Q+2} + 1) \cdot (y^Q - 1) = 0.$$

Since $y \neq 1$, we obtain $y^{Q+2} = -1$, so that $y^{2Q+4} = 1$. Hence the order of y divides

$$\gcd(2Q+4, Q^2+1) = 2\gcd(Q+2, Q^2+1) = 2\gcd(Q+2, 5),$$

so that $y^{10} = 1$. Since $y^{Q+2} = -1$, it follows that $y^5 = -1$. Now (6.3) simplifies to

$$-y^{-2} - y^3 = 1,$$

and since $y^5 = -1$ this yields the contradiction $0 = 1$. □

Lemma 6.4. *The set S of elements $x \in \mathbb{F}_{Q^4}^*$ for which $x^{2Q^2} - x^{Q^2+1} + x^2 = 0$ is nonempty only when $3 \mid Q$, in which case S consists of the (Q^2-1)-th roots of -1 and F_5 fixes each element of S.*

Proof. Write $u := x^{Q^2-1}$ with $x \in S$, so that $u^{Q^2+1} = 1$ (since plainly $x \neq 0$). If $3 \nmid Q$ then the equation $u^2 - u + 1 = 0$ implies that u is a primitive sixth root of unity, which is impossible since $6 \nmid (Q^2+1)$. Hence $3 \mid Q$, so that $X^{2Q^2} - X^{Q^2+1} + X^2 = (X^{Q^2} + X)^2$ and thus S consists of the (Q^2-1)-th roots of -1. Therefore for $x \in S$ and $k := Q^3 - Q + 1$ we have $F_5(x) = x - x^k - x^{Q^2 k} = x - x^k - (-x)^k = x$. □

Proof of Theorem 6.1. Write $q := Q^2$. The equivalence of (a), (b) and (c) follows from Propositions 2.3 and 2.4 in the same manner as in our previous results. In the remainder of the proof we show that F_5 is bijective on $\mathbb{F}_{Q^4}$. In light of Lemma 6.2, it suffices to show that each $d \in \mathbb{F}_{Q^4}^*$ has at most one preimage x in $\mathbb{F}_{Q^4}^*$.

Pick any d in $\mathbb{F}_{Q^4}^*$, and write

$$e := d^Q,\ f := d^{Q^2},\ g := d^{Q^3}.$$

Let x be an element of $\mathbb{F}_{Q^4}^*$ for which $F_5(x) = d$, and write

$$y := x^Q,\ z := x^{Q^2},\ w := x^{Q^3}.$$

The equations $F_5(x^{Q^i}) = d^{Q^i}$ for $i = 0, 1, 2, 3$ may be written as

$$x - \frac{xw}{y} - \frac{yz}{w} = d \tag{6.5}$$

$$y - \frac{yx}{z} - \frac{zw}{x} = e \tag{6.6}$$

$$z - \frac{zy}{w} - \frac{wx}{y} = f \tag{6.7}$$

$$w - \frac{wz}{x} - \frac{xy}{z} = g. \tag{6.8}$$

By Lemma 6.4, if the set $S := \{u \in \mathbb{F}_{Q^4} \colon u^{2Q^2} - u^{Q^2+1} + u^2 = 0\}$ is nonempty then $3 \mid Q$ and S consists of the (Q^2-1)-th roots of -1, each of which is fixed by F_5. We claim that if $d \in S$ then $x \in S$. For, if $d \in S$ then $3 \mid Q$ and $f = -d$, so that the sum of the left sides of (6.5) and (6.7) is zero. The numerator of this sum factors as $(w + y)(wx + zy)$, so we must have either $w = -y$ or $wx = -zy$. If $w = -y$ then $y^{Q^2-1} = -1$, so that $y \in S$ and hence $x = y^{Q^3} \in S$. If $wx = -zy$ then $(yz)^{Q^2-1} = -1$, so that $y^{(Q+1)(Q^2-1)} = -1$; but since $y \in \mathbb{F}_{Q^4}^*$ it follows that the order of y divides $\gcd(2(Q + 1)(Q^2 - 1), Q^4 - 1) = 2(Q^2 - 1)$, so that $y^{(Q+1)(Q^2-1)} = 1 \neq -1$, a contradiction. Thus if $d \in S$ then $x \in S$.

Since F_5 fixes every element of S, and maps $T := \mathbb{F}_{Q^4}^* \setminus S$ into itself, it remains to show that each $d \in T$ has at most one preimage in T under F_5. Thus we assume henceforth that $d, x \in T$, so that $f^2 - df - d^2 \neq 0$ and $z^2 - xz + x^2 \neq 0$, and raising to the Q-th power yields $g^2 - eg - e^2 \neq 0$ and $w^2 - yw + y^2 \neq 0$. Since $z \neq 0$ we can use (6.6) to solve for w, obtaining

$$w = (y - \frac{yx}{z} - e)\frac{x}{z}. \tag{6.9}$$

Substituting (6.9) into (6.8) and simplifying yields

$$y = -z\frac{e(x - z) + gz}{x^2 + z^2 - xz}. \tag{6.10}$$

Substituting (6.9) and (6.10) into (6.5) and (6.7) yields $A, B \in \mathbb{F}_{Q^4}(X, Z)$ such that $A(x, z) = B(x, z) = 0$. Now compute a Gröbner basis for the ideal of $\mathbb{F}_{Q^4}[Z', X', V', Z, X]$ generated by the numerators of $A(X, Z)$ and $B(X, Z)$ as well as the elements $ZZ' - 1$, $XX' - 1$ and $(X^2 - XZ + Z^2)V' - 1$. Since each element of this ideal vanishes when

we substitute $\frac{1}{z}, \frac{1}{x}, \frac{1}{x^2-xz+z^2}, z, x$ for Z', X', V', Z, X, we may make this substitution into each element of the Gröbner basis to conclude that

$$z = x - d + f \tag{6.11}$$

and $C(x) = 0$ for a certain degree-5 polynomial $C(X) \in \mathbb{F}_{Q^4}[X]$.

Suppose that $x' \in T \setminus \{x\}$ satisfies $F_5(x') = F_5(x)$; then we must have $C(x') = 0$. The coefficients of $C(X)$ are rational functions in d, e, f, g; by using (6.5)–(6.8) we may replace these by rational functions in x, y, z, w, and after multiplying by a suitable polynomial in x, y, z, w we can rewrite the resulting polynomial as $(X - x)D(X)E(X)$ where

$$\begin{aligned} D(X) &:= yw(x^2 - xz + z^2)X^2 + xyz(y - w)(x - z)^2 \\ &\qquad + (z - x)(x^2yw + xy^2z - xyzw - xzw^2 + yz^2w)X \\ E(X) &:= (x^2y^2 - xyzw + z^2w^2)X^2 + wz(y - w)(x - z)^3 \\ &\qquad + (z - x)(x^2yw + xy^2z - xyzw - xzw^2 - yz^2w + 2z^2w^2)X. \end{aligned}$$

Hence x' is a root of at least one of $D(X)$ and $E(X)$. We must have $z \neq x$ (and equivalently $w \neq y$), since otherwise $D(X) = x^2y^2X^2 = E(X)$, which is impossible since x' is a nonzero root of one of these polynomials. Also $x^2y^2 - xyzw + z^2w^2 \neq 0$, since otherwise $(xy)^2 - (xy)^{Q^2+1} + (xy)^{2Q^2} = 0$ so that $(xy)^{Q^2-1} = -1$, but then the order of x divides both $2(Q+1)(Q^2-1)$ and Q^4-1 and hence divides $2(Q^2-1)$, which yields the contradiction $(xy)^{Q^2-1} = 1 \neq -1$. Thus both D and E have degree 2.

If $D(x') = 0$ then $D(x')^Q = 0$, so that $(x')^Q$ is a root of the polynomial $D_2(X)$ obtained from $D(X)$ by replacing each coefficient by its Q-th power. Equations (6.10) and (6.11) imply that $y = G(x)$ where

$$G(X) := -(X - d + f)\frac{e(d - f) + g(X - d + f)}{X^2 + (X - d + f)^2 - X(X - d + f)}.$$

Since these equations were deduced from the identity $F_5(x) = d$, it follows that $(x')^Q = G(x')$, so that x' is a root of the numerator of $D_2(G(X))$. This numerator factors as $E(X)H(X)$ where

$$\begin{aligned} H(X) &:= (x^2y^2 - xy^2z + xyzw - xzw^2 + z^2w^2)X^2 + x^2y(x - z)^2(y - w) \\ &\qquad + (z - x)(2x^2y^2 - x^2yw - xy^2z + xyzw - xzw^2 + yz^2w)X. \end{aligned}$$

Thus x' is a root of at least one of $E(X)$ and $H(X)$. If $E(x') = 0$ then x' is a common root of $D(X)$ and $E(X)$, so the resultant of $D(X)$ and $E(X)$ must vanish. This resultant equals $-xz(x - z)^4(y - w)^2(x^2y^2 - xyzw + z^2w^2)u^{Q+1}$ where

$$u := x^2y^2 - x^2yw + xyzw - yz^2w + z^2w^2,$$

so we must have $u = 0$. But then a routine computation shows that $D(X) = yw(x^2 - xz + z^2)(X - x)^2$, which yields the contradiction $x' = x$. Thus if $D(x') = 0$ then we must have $H(x') = 0$. If H has degree 2 then as above the resultant of $D(X)$ and $H(X)$ must vanish, so that

$$0 = xyzw(x - z)^6(y - w)^2(x^2y^2 - xyzw + z^2w^2)^{Q+1},$$

which we know is false. Thus $\deg H < 2$. Since the constant term of $H(X)$ is nonzero, the condition $H(x') = 0$ forces $\deg H = 1$, so the resultant of $D(X)$ and $H(X)$ is $xy(x - z)^4(w - y)v$ where

$$\begin{aligned} v := {} & x^5y^3w - 2x^4y^4z + x^4y^3zw - 2x^4y^2zw^2 + 3x^3y^4z^2 - 3x^3y^3z^2w \\ & + 6x^3y^2z^2w^2 - 2x^3yz^2w^3 + x^3z^2w^4 - x^2y^4z^3 - 2x^2y^3z^3w - x^2y^2z^3w^2 \\ & - x^2z^3w^4 + 2xy^3z^4w - xy^2z^4w^2 + 2xyz^4w^3 - y^2z^5w^2. \end{aligned}$$

Thus we must have $v = 0$, and also the coefficient of X^2 in $H(X)$ must vanish. But we can express $yz^6w^2(y - w)^3(y^2 + w^2)$ as a sum of the products of these two quantities with certain polynomials in x, y, z, w, so that this expression vanishes and thus $y^2 = -w^2$, whence $y^{2Q^2-2} = -1$. However, there are no $(2Q^2 - 2)$-th roots of -1 in $\mathbb{F}_{Q^4}^*$, since $2Q^2-2$ is divisible by the largest power of 2 which divides Q^4-1.

This completes the proof when $D(x') = 0$, and the proof when $E(x') = 0$ is similar. □

7. The case that $n = 2$ and $q = Q^2$ where Q is an odd prime power and $k = Q^3 + Q^2 - Q$

Case (f) of Theorem 1.1 is contained in the following result.

Theorem 7.1. *For any odd prime power Q, we have:*

(a): $F_6(X) := X - \mathrm{Tr}_{Q^4/Q^2}(X^{Q^3+Q^2-Q})$ *permutes* $\mathbb{F}_{Q^4}$.

(b): $\dfrac{X^{Q+2} + 3\nu X^Q - 4\nu^{(Q+1)/2}X}{X^2 - \nu}$ *permutes* $\mathbb{F}_{Q^2}$, *where* ν *is any nonsquare in* $\mathbb{F}_{Q^2}$.

(c): $\dfrac{X^{2Q+1} - X^{Q+1} + 1}{X^{2Q+1} - X^Q + 1}$ *permutes the set of* $(Q^2 + 1)$*-th roots of unity in* $\mathbb{F}_{Q^4}^*$.

We note that assertions (b) and (c) of this result are extremely similar to the corresponding assertions in Theorem 6.1. However, we have not been able to find a direct proof that these similar assertions are logically equivalent to one another. If we could find such a proof, then Theorem 7.1 would follow from Theorem 6.1. At present, the best we

can do is to prove Theorem 7.1 via a similar argument to our proof of Theorem 6.1.

Proof. The equivalence of (a), (b) and (c) follows from Propositions 2.3 and 2.4 in the same manner as in our previous results. The proof of assertion (a) is nearly identical to the proof of assertion (a) in Theorem 6.1, so the details can safely be left to the reader. □

8. The case that $n = 3$ and $k = (q^2 + 1)/2$

We now prove case (g) of Theorem 1.1.

Theorem 8.1. *If q is odd, then*

$$F_7(X) := X + \mathrm{Tr}_{q^3/q}\left(X^{\frac{q^2+1}{2}}\right)$$

permutes $\mathbb{F}_{q^3}$.

Proof. By Proposition 2.2, it suffices to show that

$$g(X) := X(1 + X^{(q+1)/2} + X^{(q^2+q+2)/2} + X^{(q^2+2)(q+1)/2})^{q-1}$$

permutes the set μ_{q^2+q+1} of $(q^2 + q + 1)$-th roots of unity in $\mathbb{F}_{q^3}^*$. For $x \in \mu_{q^2+q+1}$ we compute

$$\begin{aligned} g(x^{2q}) &= x^{2q}\,(1 + x^{-1} + x^q + x^{q-1})^{q-1} \\ &= x^{2q} \cdot (1 + x^{-1})^{q-1} \cdot (1 + x^q)^{q-1} \\ &= x^{q^2+q} \cdot (1 + x^{-1})^{q^2-1} = x^{-1}(1 + x^{-1})^{q^2-1}, \end{aligned}$$

so that (since $1 + x^{-1} \neq 0$)

$$g(x^{2q})^{-q} = x^q(1 + x^{-1})^{-1+q} = x(x + 1)^{q-1}.$$

Again by Proposition 2.2, $X(X + 1)^{q-1}$ permutes μ_{q^2+q+1} if and only if $X^q + X$ permutes $\mathbb{F}_{q^3}$, which is indeed the case since $X^q + X$ is an additive polynomial having no nonzero roots in $\mathbb{F}_{q^3}$. Therefore $g(X^{2q})^{-q}$ permutes μ_{q^2+q+1}, so that also $g(X)$ permutes μ_{q^2+q+1}, whence F_7 permutes $\mathbb{F}_{q^3}$. □

9. The case that $n = 3$ and $k = q^2 - q + 1$

In this section we prove case (h) of Theorem 1.1.

Theorem 9.1. *If q is odd then*

$$F_8(X) := X - \frac{1}{2}\,\mathrm{Tr}_{q^3/q}\left(X^{q^2-q+1}\right)$$

permutes $\mathbb{F}_{q^3}$.

Proof. Define

$$\begin{aligned} H(X) &:= 2X^{(q^4+q^2)/2} - \mathrm{Tr}_{q^3/q}(X) \\ L(X) &:= 2X^q - \mathrm{Tr}_{q^3/q}(X) \\ G(X) &:= L(H(X)). \end{aligned}$$

First note that $L(X)$ has no nonzero roots in $\mathbb{F}_{q^3}$, since any such root x would satisfy $2x^q = \mathrm{Tr}_{q^3/q}(x) \in \mathbb{F}_q$ so that $x \in \mathbb{F}_q$, whence $L(x) = -x$. Since $L(X)$ is an additive polynomial in $\mathbb{F}_{q^3}[X]$, it follows that $L(X)$ permutes $\mathbb{F}_{q^3}$. Next, for every $x \in \mathbb{F}_{q^3}$ we have

$$G(x^2) = L(x)^2.$$

Writing S for the set of squares in $\mathbb{F}_{q^3}$, it follows that

$$G(S) = \big(L(\mathbb{F}_{q^3})\big)^2 = S,$$

since L permutes $\mathbb{F}_{q^3}$. Let w be any nonsquare in $\mathbb{F}_q^*$, so that also w is a nonsquare in $\mathbb{F}_{q^3}^*$ and thus $\mathbb{F}_{q^3} = S \cup wS$. Since all terms of both L and H have degree congruent to 1 (mod $q-1$), the same is true of G, so the hypothesis $w^{q-1} = 1$ implies that

$$G(wS) = wG(S) = wS.$$

Therefore G permutes both S and wS, so G permutes $S \cup wS = \mathbb{F}_{q^3}$. Hence also H permutes $\mathbb{F}_{q^3}$, and since $\gcd(q^2-q+1, q^3-1) = 1$ it follows that $H(X^{q^2-q+1})$ permutes $\mathbb{F}_{q^3}$. It follows that $F_8(X^q)$ (and hence $F_8(X)$) permutes $\mathbb{F}_{q^3}$ since $H(0) = 0 = F_8(0)$ and for $x \in \mathbb{F}_{q^3}^*$ we have

$$H(x^{q^2-q+1}) = 2x^q - \mathrm{Tr}_{q^3/q}(x^{q^2-q+1}) = 2F_8(x^q). \qquad \square$$

Our proof of bijectivity of H is inspired by the proof of [5, Thm. 3.7], which also distinguished the behavior of a function on squares and nonsquares. The key identity $L(H(x^2)) = L(x)^2$ in our proof says that $x \mapsto H(x^2)$ is a planar function which is affine equivalent to $x \mapsto x^2$. Since the nucleus of any semifield induced by $x \mapsto H(x^2)$ is $\mathbb{F}_{q^3}$, the hypotheses of [5, Thm. 3.7] do not apply in our situation; however, it appears that those hypotheses can be relaxed to cover both our situation and several others. Our proof of Theorem 9.1 uses our key identity to avoid the bulk of the work involved in the proof of [5, Thm. 3.7].

10. The case that $k = q^\ell + 1$ with $\ell \mid n$

We now prove case (i) of Theorem 1.1.

Theorem 10.1. *For any prime power q and any positive integers ℓ, n with $2\ell \mid n$, if $\gamma \in \mathbb{F}_{q^n}$ satisfies $\gamma^{q^{2\ell}-1} = -1$ then the polynomial $F_9(x) := X + \gamma \operatorname{Tr}_{q^n/q}(X^{q^\ell+1})$ permutes $\mathbb{F}_{q^n}$.*

Note that if q is odd then $\mathbb{F}_{q^n}$ contains elements γ as in Theorem 10.1 if and only if n is divisible by 4ℓ.

Proof. By Proposition 2.1, F_9 permutes $\mathbb{F}_{q^n}$ if and only if for each $\alpha \in \mathbb{F}_{q^n}$ the polynomial $h_\alpha(X) := X + \operatorname{Tr}_{q^n/q}\Big((\alpha+\gamma X)^{q^\ell+1}\Big)$ permutes $\mathbb{F}_q$. For $x \in \mathbb{F}_q$ and $Q := q^\ell$ we have

$$\begin{aligned}(\alpha+\gamma x)^{Q+1} &= \gamma^{Q+1}x^{Q+1} + \alpha\gamma^Q x^Q + \alpha^Q\gamma x + \alpha^{Q+1}\\ &= \gamma^{Q+1}x^2 + \alpha\gamma^Q x + \alpha^Q\gamma x + \alpha^{Q+1},\end{aligned}$$

so that

$$\operatorname{Tr}_{q^n/q}((\alpha+\gamma x)^{Q+1}) = \operatorname{Tr}_{q^n/q}(\gamma^{Q+1})x^2 + \operatorname{Tr}_{q^n/q}(\alpha\gamma^Q+\alpha^Q\gamma)x + \operatorname{Tr}_{q^n/q}(\alpha^{Q+1}).$$

Since $\gamma^{Q^2-1} = -1$, we have $\gamma^{Q+Q^2} = -\gamma^{Q+1}$ and thus

$$\operatorname{Tr}_{q^n/q}(\gamma^{Q+1}) = \operatorname{Tr}_{q^n/Q^2}(\operatorname{Tr}_{Q/q}(\operatorname{Tr}_{Q^2/Q}(\gamma^{Q+1}))) = 0.$$

Likewise,

$$\operatorname{Tr}_{q^n/q}(\alpha\gamma^Q + \alpha^Q\gamma) = \operatorname{Tr}_{q^n/q}(\alpha^Q\gamma^{Q^2} + \alpha^Q\gamma) = \operatorname{Tr}_{q^n/q}(0) = 0.$$

Thus h_α induces the same function on $\mathbb{F}_q$ as does the polynomial $X + \operatorname{Tr}_{q^n/q}(\alpha^{Q+1})$, so that indeed h_α permutes $\mathbb{F}_q$ as required. □

Remark 10.2. The proof of Theorem 10.1 shows that every $\alpha \in \mathbb{F}_{q^n}$ satisfies

$$\operatorname{Tr}_{q^n/q}((\alpha+\gamma x)^{Q+1}) - \operatorname{Tr}_{q^n/q}(\alpha^{Q+1}) = 0,$$

so that γ is a linear translator of $\operatorname{Tr}_{q^n/q}(x^{Q+1})$ (as was claimed on page 3). Theorem 10.1 is a generalization of [2, Thm. 6], which addressed the case of prime q.

References

[1] P. Charpin and G. Kyureghyan, On a class of permutation polynomials over $\mathbb{F}_{2^n}$, pp. 368–376 in: *Sequences and their Applications—SETA 2008*, Lecture Notes in Comput. Sci. 5203, Springer, 2008. 3

[2] P. Charpin and G. Kyureghyan, Monomial functions with linear structure and permutation polynomials, pp. 99–111 in: *Finite Fields: Theory and Applications*, Contemp. Math. 518, Amer. Math. Soc., 2010. 3, 16

[3] H. Dobbertin, Uniformly representable permutation polynomials, pp. 1–22 in: *Sequences and their Applications (Bergen, 2001)*, Springer, 2002. 2, 9

[4] X.-D. Hou, Determination of a type of permutation trinomials over finite fields, *Acta Arith.* **166** (2014), 253–278. 7

[5] G. Weng and X. Zeng, Further results on planar DO functions and commutative semifields, *Des. Codes Cryptogr.* **63** (2012), 413–423. 15

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

Otto-von-Guericke University, Magdeburg, Germany
E-mail address: gohar.kyureghyan@ovgu.de

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, USA
E-mail address: zieve@umich.edu