On constructing permutations of finite fields[☆]

Amir Akbary[a], Dragos Ghioca[b], Qiang Wang[c,*]

[a] *Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada*
[b] *Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada*
[c] *School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada*

Abstract

Motivated by several constructions of permutation polynomials done by several authors (most notably by Zieve), we propose a unified treatment for a large set of classes of permutation polynomials of $\mathbb{F}_q$. Our approach yields a recipe for constructing several new and old classes of permutation polynomials of $\mathbb{F}_q$.

Keywords: permutation polynomials, finite fields
MSC: 11T06

1. Introduction

Let p be a prime number; we are interested in constructing permutation polynomials of a finite field $\mathbb{F}_q$ of $q = p^n$ elements. In this case all the permutations of $\mathbb{F}_q$ can be represented by polynomials in $\mathbb{F}_q[x]$. Note that we may assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q-1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$. The study of permutations of finite fields started in 19th century with the work of Hermite and later Dickson. In recent years, there has been tremendous amount of interest in constructing permutation polynomials of $\mathbb{F}_q$ due to their applications in combinatorics, cryptography, and coding theory. In general finding nontrivial classes of permutation polynomials of finite fields is a difficult problem (for more background material on permutation polynomials we refer to [5, Chapter 7]).

In [11, Lemma 2.1], Zieve gives a very important criterion for constructing permutation polynomials of $\mathbb{F}_q$.

Theorem 1.1 (Zieve). *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 the set μ_d of roots of unity of order dividing d.*

The great importance of the criterion from Theorem 1.1 is that it reduces the problem of determining whether a given polynomial is a permutation polynomial to establishing whether another polynomial permutes a *smaller* set (in this case, the set of roots of unity of order dividing d). The above criterion

[☆] Research of the authors was partially supported by NSERC of Canada
[*] Corresponding author
Email addresses: amir.akbary@uleth.ca (Amir Akbary), dghioca@math.ubc.ca (Dragos Ghioca), wang@math.carleton.ca (Qiang Wang)

was discovered independently by various authors under various forms (see [7, Theorem 2.3], [10, Theorem 1]). In Theorem 1.1, both x^r and $x^{(q-1)/d}$ yield endomorphisms of $(\mathbb{F}_q^\times, \cdot)$. So, it is natural to search for an additive analogue of Theorem 1.1, where x^r and $x^{(q-1)/d}$ are replaced by arbitrary endomorphisms of $(\mathbb{F}_q, +)$. This analogue was found by Zieve in [12, Proposition 3], which allowed him to produce new classes of permutation polynomials.

Inspired by the work of Marcos [6] and Zieve [12], in this paper we prove the following general criterion for permutations of a finite set (which generalizes both [11, Lemma 2.1] and [12, Proposition 3]).

Lemma 1.2. *Let A, S and $\bar{S}$ be finite sets with $\#S = \#\bar{S}$, and let $f : A \to A$, $\bar{f} : S \to \bar{S}$, $\lambda : A \to S$, and $\bar{\lambda} : A \to \bar{S}$ be maps such that $\bar{\lambda} \circ f = \bar{f} \circ \lambda$. If both λ and $\bar{\lambda}$ are surjective, then the following statements are equivalent:*

(i) f is a bijection (a permutation of A); and
(ii) $\bar{f}$ is a bijection from S to $\bar{S}$ and f is injective on $\lambda^{-1}(s)$ for each $s \in S$.

For example, if

1. $A = \mathbb{F}_q$;
2. $f(x) = A(x) + g(B(x))$ (for two additive polynomials $A(x)$ and $B(x)$, while g is any polynomial in $\mathbb{F}_q[x]$);
3. $S = B(\mathbb{F}_q)$ and $\bar{S} = \mathbb{F}_q/A(\ker(B))$ (seen as a quotient of additive groups);
4. $\lambda(x) = B(x)$ and $\bar{\lambda}(x)$ is the canonical projection $\mathbb{F}_q \to \mathbb{F}_q/A(\ker(B))$; and
5. $\bar{f}(x) = A(\hat{B}(x)) + g(x)$ (where $\hat{B}(x)$ is any additive polynomial such that $B(\hat{B}(x))$ is the identity on $B(\mathbb{F}_q)$) seen as an induced map between S and $\bar{S}$,

we obtain [12, Proposition 3] (also note that in [12, Proposition 3] it is immediate first to check that $\ker(A) \cap \ker(B) = \{0\}$ and thus $\#A(\ker(B)) = \#\ker(B)$, which yields that $\#S = \#\bar{S}$). Similarly, if we take

1. $A = \mathbb{F}_q$;
2. $f(x) = g(B(x)) + h(B(x)) \cdot A(x)$, where $B(x)$ is the trace map for the extension $\mathbb{F}_q/\mathbb{F}_p$, while $A(x) \in \mathbb{F}_p[x]$ is an additive polynomial, and $g(x) \in \mathbb{F}_q[x]$ and $h(x) \in \mathbb{F}_p[x]$ are arbitrary polynomials;
3. $S = \bar{S} = \mathbb{F}_p$;
4. $\lambda(x) = \bar{\lambda}(x) = B(x)$; and
5. $\bar{f}(x) = B(g(x)) + h(x) \cdot A(x)$,

we obtain [12, Theorem 6]. Also, if $A = \mathbb{F}_q$, $S = \bar{S} = \mu_d \cup \{0\}$, and $\lambda(x) = \bar{\lambda}(x) = x^{(q-1)/d}$, we obtain Theorem 1.1. Furthermore, if we take

1. $A = \mathbb{F}_{p^n}$;
2. $f(x) = x \cdot h(B(x))$ for any polynomials $h, B \in \mathbb{F}_p[x]$ such that $B(\mathbb{F}_{p^n}) \subseteq \mathbb{F}_p$ and moreover, $B(a\alpha) = a^2 \cdot B(\alpha)$ for each $a \in \mathbb{F}_p$ and each $\alpha \in \mathbb{F}_{p^n}$;
3. $S = \bar{S} = B(\mathbb{F}_p)$;
4. $\lambda(x) = \bar{\lambda}(x) = B(x)$; and
5. $\bar{f}(x) = x \cdot h^2(x)$,

we obtain [6, Proposition 12]. In Section 6 we will give a further generalization of [6, Proposition 12] (see our Theorem 6.3).

Proof of Lemma 1.2. Assume first that f is bijective. Then f is injective on each $\lambda^{-1}(s)$. Furthermore, because $\bar{\lambda}$ and f are surjective and $\bar{\lambda} \circ f = \bar{f} \circ \lambda$, then $\bar{f} : S \to \bar{S}$ is surjective and so is bijective (because S and $\bar{S}$ are finite sets of the same cardinality).

Conversely, assume $f(a_1) = f(a_2)$ for some $a_1, a_2 \in A$. Then $\bar{f}(\lambda(a_1)) = \bar{\lambda}(f(a_1)) = \bar{\lambda}(f(a_2)) = \bar{f}(\lambda(a_2))$. Because $\bar{f}$ is a bijection, we obtain $\lambda(a_1) = \lambda(a_2)$. Hence a_1, a_2 are in $\lambda^{-1}(s)$ for some $s \in S$. Because f is injective on each $\lambda^{-1}(s)$, we conclude that $a_1 = a_2$. So f is injective and in fact, it is bijective (since A is a finite set). □

This simple lemma gives us a recipe in which under suitable conditions one can construct permutations of A out of bijections between two proper subsets of A, for example. In particular, if $\bar{\lambda} = \lambda$, one can construct permutations of A out of the permutations of a subset S of A. Therefore, we are exactly in the same situation as in [11, Lemma 2.1] or [12, Proposition 3 and Theorem 6] where we can reduce the problem of determining whether a given polynomial is a permutation polynomial of $\mathbb{F}_q$ to the simpler question of determining whether another polynomial permutes a smaller set.

So, we will be particularly interested in the case A is a finite field $\mathbb{F}_q$ in Lemma 1.2, and we will prove several new results on permutation polynomials (see Theorems 5.1, 5.5, 5.10, 5.11, 5.12, 6.1, 6.3 and 6.4, Propositions 5.4 and 5.9, and Corollary 6.5). We will also show that some known classes of permutation polynomials can be constructed by a suitable application of Lemma 1.2. These classes include several classes of permutation polynomials found recently by Coulter, Henderson and Matthews [2], Kyureghyan [3], Marcos [6], and Zieve [12] among others. In other words here we give a simple unified treatment of many classes of permutation polynomials and in the process we demonstrate the centrality of Lemma 1.2 in these constructions. We stress out that our work builds on the seminal work of Zieve in the area of permutation polynomials, who envisioned in [12] some important special cases of Lemma 1.2 which led us to formulating and proving the above general criterion.

Several of our constructions can be described in the more general context of permutations of a finite group. To describe our result, first we set up the notation.

Notation 1.3. *Throughout the paper $(G, +)$ denotes a finite group. We denote the operation by "+" although the group may not be abelian. We also denote the additive group of a finite field $\mathbb{F}_q$ by $(\mathbb{F}_q, +)$, moreover the multiplicative group of $\mathbb{F}_q$ is denoted by $(\mathbb{F}_q^\times, \cdot)$.*

We denote by $\mathrm{End}(G)$ the set of all endomorphisms of G.

We denote by $\mathrm{im}(\varphi) = \varphi(G)$ the image of an endomorphism $\varphi : G \longrightarrow G$, and we denote by $\ker(\varphi)$ its kernel.

We say that $\varphi, \psi \in \mathrm{End}(G)$ commute if $\varphi \circ \psi = \psi \circ \varphi$.

Our first theorem provides necessary and sufficient conditions under which one can construct a permutation of a finite group G from two given endomorphisms of $(G, +)$. More precisely in part (a) of Theorem 1.4, we use Lemma 1.2 to give necessary and sufficient conditions for permutations of the form

$$f(x) := \varphi(x) + g(\psi(x))$$

where φ and ψ are two endomorphisms of G satisfying $\varphi \circ \psi = \bar{\psi} \circ \varphi$ for some endomorphism $\bar{\psi}$, and $g : G \to G$ is any mapping. More precisely, we prove the following.

Theorem 1.4. *Let $(G, +)$ be a finite group, and let $\varphi, \psi, \bar{\psi} \in \mathrm{End}(G)$ be group endomorphisms such that $\bar{\psi} \circ \varphi = \varphi \circ \psi$ and $\#\mathrm{im}(\psi) = \#\mathrm{im}(\bar{\psi})$. Let $g : G \longrightarrow G$ be any mapping, and let $f : G \longrightarrow G$ be defined by*

$$f(x) = \varphi(x) + g(\psi(x)).$$

Then,

(a) f permutes G if and only if the following two conditions hold:

(i) $\ker(\varphi) \cap \ker(\psi) = \{0\}$ *(or equivalently, φ induces a bijection between* $\ker(\psi)$ *and* $\ker(\bar{\psi})$*); and*
(ii) the function $\bar{f}(x) := \varphi(x) + \bar{\psi}(g(x))$ restricts to a bijection from $\mathrm{im}(\psi)$ *to* $\mathrm{im}(\bar{\psi})$*.*

(b) For any fixed endomorphisms φ, ψ and $\bar{\psi}$ satisfying (i)*, there are*

$$(\#\mathrm{im}(\psi))! \cdot \left(\#\ker(\bar{\psi})\right)^{\#\mathrm{im}(\psi)}$$

such permutation functions f (when g varies).

(c) Let $g : G \longrightarrow G$ be such that $\left(\bar{\psi} \circ g\right)|_{\mathrm{im}(\psi)} = 0$. Then $f = \varphi + g \circ \psi$ permutes G if and only if φ is a permutation of G.

(d) Assume $\varphi \circ \psi = 0$ and $g : G \longrightarrow G$ be a mapping such that $g(x)$ restricted to $\mathrm{im}(\psi)$ *is a permutation of* $\mathrm{im}(\psi)$*. Then*

$$f(x) = \varphi(x) + g(\psi(x))$$

permutes G if and only if φ and ψ satisfy (i)*, and $\bar{\psi}$ restricted to* $\mathrm{im}(\psi)$ *is a bijection from* $\mathrm{im}(\psi)$ *to* $\mathrm{im}(\bar{\psi})$*.*

We prove the above theorem in Section 2.

In Section 3 we apply the above theorem in the case $(G, +) = (\mathbb{F}_q^\times, \cdot)$, the multiplicative group, which immediately gives us the known results due to Wan-Lidl [9], Park-Lee [7], Akbary-Wang [1], Wang [10], and Zieve [11]. The main observation here is that the group endomorphisms of $\mathbb{F}_q^\times$ are maps of the form x^s for $s \in \mathbb{Z}$.

In Section 4 we describe the natural analogue of parts (a) and (c) of Theorem 1.4 for an elliptic curve E defined over a finite field, and under multiplication-by-m-maps (for various integers m), or the Frobenius map for the endomorphisms φ and ψ.

Next we consider the additive group of $\mathbb{F}_q$. The situation in this case is far more interesting than $\mathbb{F}_q^\times$ and E, and it was also studied by Zieve [12]. We point out that most of our results from Section 5 were motivated by [12, Proposition 3 and Theorem 6]. Proposition 3 of [12] deals with permutation polynomials of the form $A(x) + g(B(x))$ where both A and B are additive polynomials, while Theorem 6 of [12] deals with permutation polynomials of the form $h(B(x))A(x) + g(B(x))$ where A is an additive polynomial and $B(x) = x^q + x^{q/p} + \cdots + x^p$. Most of our results from Section 5 are written for polynomials of the form $h(B(x))A(x) + g(B(x))$ for *any* additive polynomials A and B, thus extending both [12, Proposition 3 and Theorem 6].

One can show that the group endomorphisms of $(\mathbb{F}_q, +)$ are *additive* polynomials over $\mathbb{F}_q$ (or p-polynomials over $\mathbb{F}_q$). These endomorphisms of $(\mathbb{F}_q, +)$ are given by polynomials

$$\varphi(x) = \sum_{j=0}^{s} a_j x^{p^j}, \quad \text{where } a_j \in \mathbb{F}_q.$$

If $\varphi(x) = \sum_{j=0}^{s} a_j x^{q^j}$ with $a_j \in \overline{\mathbb{F}_q}$, the closure of $\mathbb{F}_q$, then we call $\varphi(x)$ an $\mathbb{F}_q$-*linear polynomial*; obviously, each additive polynomial is actually an $\mathbb{F}_p$-linear polynomial. If in addition, each $a_j \in \mathbb{F}_q$, then we call φ an $\mathbb{F}_q$-*linear polynomial over* $\mathbb{F}_q$ (or q-polynomial over $\mathbb{F}_q$). It is clear that any two $\mathbb{F}_q$-linear polynomials φ and ψ over $\mathbb{F}_q$ commute, i.e. $\varphi(\psi(x)) = \psi(\varphi(x))$ for all $x \in \overline{\mathbb{F}_q}$.

The following result is essentially part (a) of our Theorem 5.1.

Theorem 1.5. *Let q be a power of the prime number p. Consider any polynomial $g \in \mathbb{F}_q[x]$, any additive polynomials $\varphi, \psi, \bar{\psi} \in \mathbb{F}_q[x]$ satisfying $\varphi \circ \psi = \bar{\psi} \circ \varphi$ and $\#\psi(\mathbb{F}_q) = \#\bar{\psi}(\mathbb{F}_q)$, and any polynomial $h \in \mathbb{F}_q[x]$ such that $h(\psi(\mathbb{F}_q)) \subseteq \mathbb{F}_p \setminus \{0\}$.*

Then, $f(x) := h(\psi(x))\varphi(x) + g(\psi(x))$ permutes $\mathbb{F}_q$ if and only if

(i) $\ker(\varphi) \cap \ker(\psi) = \{0\}$*; and*

(ii) $\bar{f}(x) := h(x)\varphi(x) + \bar{\psi}(g(x))$ *is a bijection between $\psi(\mathbb{F}_q)$ and $\bar{\psi}(\mathbb{F}_q)$.*

The above theorem is a generalization of [12, Theorem 6], which treated the case

$$\psi(x) = \bar{\psi}(x) = x^q + x^{q/p} + \cdots + x^p.$$

Also, in Theorem 1.5 when $h(x) = 1$ and $\psi = \bar{\psi}$, we obtain [12, Corollary 5]. We also point out that in [12, Proposition 3], Zieve gives a necessary and sufficient criterion for a polynomial of the form $A(x)+g(B(x))$ to be a permutation polynomial (where $A(x)$ and $B(x)$ are arbitrary additive polynomials). Finally, note that in the additive setting (unlike the multiplicative case) there are additive polynomials φ, ψ, $\bar{\psi}$ such that $\varphi \circ \psi = \bar{\psi} \circ \varphi$ and $\psi \neq \bar{\psi}$. See Example 5.2 for polynomials with this property.

We can use Theorem 5.1 to construct many classes of permutation polynomials. To illustrate the power of our method, in Section 5, we give a sample of such results for two different choices of the endomorphism ψ in Theorem 5.1. Firstly we consider $\psi(x) = \bar{\psi}(x) = x^{q^{n-1}} + \cdots + x^q + x$; this polynomial is the trace function for the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and is denoted by $\mathrm{Tr}_n(x)$. Secondly by considering $\psi(x) = \bar{\psi}(x) = x^q - x$, and suitable choices for the additive polynomial $\varphi(x)$ in Theorem 5.1 we are able to generate several other classes of permutation polynomials; for example we have the following (see part (b) of Theorem 5.10).

Theorem 1.6. *Let p be a prime number, let q be a power of p, let $h(x) \in \mathbb{F}_{q^n}[x]$ be any polynomial such that $h(x^q - x) \in \mathbb{F}_q \setminus \{0\}$ for all $x \in \mathbb{F}_{q^n}$, and let $g(x) \in \mathbb{F}_{q^n}[x]$ be a polynomial that induces a permutation of $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^n}\}$. Then the polynomial $f(x) := h(x^q - x)\mathrm{Tr}_n(x) + g(x^q - x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $p \nmid n$.*

In Theorem 5.11 we prove that in the case $q = p = 2$ and $h(x) = 1$, in the above theorem, one can relax the condition on g by assuming only that $g \mid_S$ is a one-to-one mapping onto $S' := \{\delta + y : y \in S\}$, where δ is any given element of $\mathbb{F}_{2^n}$. We note that neither Theorem 1.6 nor Theorem 5.11 are consequences of the results from [12].

In Section 5 we also construct the following classes of permutations of $\mathbb{F}_{q^2}$.

Theorem 5.12 *Let $q = p^m$. Then the following are permutation polynomials of $\mathbb{F}_{q^2}$:*

(a) $f_{a,b,k}(x) := ax^q + bx + (x^q - x)^k$, for $a, b \in \mathbb{F}_q$ such that $a \neq \pm b$, and for all even positive integers k.

(b) $f_{a,k}(x) := ax^q + ax + (x^q - x)^k$, if $a \in \mathbb{F}_q^\times$, and p and k are odd, and in addition k is relatively prime with $q - 1$.

A *complete mapping* f over $\mathbb{F}_q$ is a permutation polynomial of $\mathbb{F}_q$ such that $f(x) + x$ is again a permutation polynomial of $\mathbb{F}_q$. We note that the above class of polynomials $f_{a,b,k}(x) := ax^q + bx + (x^q - x)^k$ over $\mathbb{F}_{q^2}$ contains complete mappings. More precisely we have the following.

Corollary 1.7. *The polynomial $f_{a,b,k}(x) := ax^q + bx + (x^q - x)^k$ is a complete mapping over $\mathbb{F}_{q^2}$ for any $a, b \in \mathbb{F}_q$ such that $b \neq \pm a$ and $b + 1 \neq \pm a$, and for all even positive integers k.*

In Section 6 we construct new classes of permutation polynomials by direct applications of Lemma 1.2. These results are not consequences of Theorem 1.4 and well illustrate the power of Lemma 1.2 in generating permutations of $\mathbb{F}_q$. Our theorems from Section 6 generalize several known constructions of permutation polynomials such as the ones from [2] and [3]. In Section 6 we prove the following result (which generalizes [2, Theorem 3]).

Theorem 6.1 *Let q be a prime power, let n be a positive integer, and let L_1, L_2, L_3 be $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$ seen as endomorphisms of $(\mathbb{F}_{q^n}, +)$. Let $g(x) \in \mathbb{F}_{q^n}[x]$ be such that $g(L_3(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$. Then*

$$f(x) = L_1(x) + L_2(x)g(L_3(x))$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the following two conditions hold

(i) $\ker(F_y) \cap \ker(L_3) = \{0\}$*, for any $y \in \mathrm{im}(L_3)$, where $F_y : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ is defined by*

$$F_y(x) := L_1(x) + L_2(x)g(y).$$

(ii) $\bar{f}(x) := L_1(x) + L_2(x)g(x)$ *permutes* $\mathrm{im}(L_3)$.

We also point out that in the above result, $f(x)$ cannot be written as $h(B(X))A(X)+g(B(x))$ for some additive polynomials A and B; therefore, Theorem 6.1 is neither covered by our results from Section 5 nor is covered by the results from [12].

We conclude our paper by considering mappings that are not necessarily additive even though they satisfy a certain translation property. More precisely we define the following class of mappings of $\mathbb{F}_q$.

Definition 1.8. *Let $S \subseteq \mathbb{F}_q$ and let $\gamma, b \in \mathbb{F}_q$. We say that γ is a b-linear translator with respect to S for the mapping $F : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, if*

$$F(x + u\gamma) = F(x) + ub$$

for all $x \in \mathbb{F}_{q^n}$ and for all $u \in S$.

The above definition is a generalization of the concept of b-linear translator given in [3] which deals with the case $q = p^{mn}$ (for a prime number p), and $S = \mathbb{F}_{p^m}$. In our definition S can be any subset of $\mathbb{F}_q$. The relaxation on the condition for S provides a much richer class of functions (see Examples 6.6).

Our final result (see Section 6) is a generalization of [3, Theorem 11].

Theorem 6.4 *Let $S \subseteq \mathbb{F}_q$ and $F : \mathbb{F}_q \longrightarrow S$ be a surjective map. Let $\gamma \in \mathbb{F}_q$ be a b-linear translator with respect to S for the map F. Then for any $G \in \mathbb{F}_q[x]$ which maps S into S, we have that $x + \gamma G(F(x))$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $x + bG(x)$ permutes S.*

In conclusion, Lemma 1.2 provides a criterion which can be used for finding numerous classes of permutation polynomials. Important special cases of Lemma 1.2 were previously discovered by Michael Zieve (whom we thank both for his comments on our paper, and also for inspiring our results through his work from [12]). We believe the merits of this paper lie not only in connecting various results in the literature (see Sections 3 and 5) and introducing some genuinely new classes of permutation polynomials (see Sections 5 and 6), but they also lie in proving Theorem 1.4 which we believe many authors will be able to use it in the future to generate permutations of various finite groups (not necessarily of $\mathbb{F}_q$). For example, in Theorem 1.4 one may take G to be the group of $\mathbb{F}_q$-rational points for any algebraic group (not necessarily an elliptic curve as we do in Section 4) and then one may generate permutations of G.

2. Proof of Theorem 1.4

Proof. (a) We apply Lemma 1.2 with $A = G$, $S = \mathrm{im}(\psi)$, $\bar{S} = \mathrm{im}(\bar{\psi})$, $\lambda = \psi$, $\bar{\lambda} = \bar{\psi}$, because $\bar{f} \circ \psi = \bar{\psi} \circ f$ (here we use that $\varphi \circ \psi = \bar{\psi} \circ \varphi$). We conclude that f is a permutation of G if and only if $\bar{f}$ induces a bijection from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$ (this is exactly condition (ii) from our conclusion), and if f is injective on each $\psi^{-1}(i) := \{\alpha \in G : \psi(\alpha) = i\}$ (for each $i \in \mathrm{im}(\psi)$). Now, for each $i \in \mathrm{im}(\psi)$, and for any distinct $\alpha, \beta \in \psi^{-1}(i)$, we have

$$0 \neq f(\alpha) - f(\beta) = \varphi(\alpha) + g(\psi(\alpha)) - g(\psi(\beta)) - \varphi(\beta) = \varphi(\alpha - \beta)$$

if and only if $\ker(\varphi) \cap \ker(\psi) = \{0\}$, because $\alpha - \beta \in \ker(\psi)$. Finally, note that because $\varphi \circ \psi = \bar{\psi} \circ \varphi$, we deduce that $\varphi(\ker(\psi)) \subseteq \ker(\bar{\psi})$. Because $\ker(\varphi) \cap \ker(\psi) = \{0\}$, we obtain that the induced map by φ on $\ker(\psi)$ is injective. Because $\#\mathrm{im}(\psi) = \#\mathrm{im}(\bar{\psi})$, we conclude that $\#\ker(\psi) = \#\ker(\bar{\psi})$, and thus φ induces a bijection between $\ker(\psi)$ and $\ker(\bar{\psi})$, as desired.

(b) Now, for a finite group G we fix φ and ψ satisfying (i), and we count the number of distinct permutations f of G of the form $\varphi + g \circ \psi$ (when g varies). Indeed, we first note that f is determined uniquely by the values of g on $\mathrm{im}(\psi)$. On the other hand, for each bijection σ from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$, according to (ii) we solve for g such that

$$\varphi(x) + \bar{\psi}(g(x)) = \sigma(x) \text{ for each } x \in \mathrm{im}(\psi). \tag{2.1}$$

As φ, $\bar{\psi}$ and σ are fixed, then for each $x \in \mathrm{im}(\psi)$, there are $\#\ker(\bar{\psi})$ possibilities for $g(x)$. Because there are $(\#\mathrm{im}(\psi))!$ bijections σ from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$, our conclusion follows.

(c) The result follows from part (a) since the associated function $\bar{f}(x)$ corresponding to $f(x)$ (restricted to $\mathrm{im}(\psi)$) is

$$\varphi(x) + \bar{\psi}(g(x)) = \varphi(x),$$

and so, $f(x)$ permutes G if and only if $\varphi(x)$ induces a bijection from $\ker(\psi)$ to $\ker(\bar{\psi})$ (which is condition (i)) and induces a bijection from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$ (which is condition (ii)). However these two conditions are equivalent to φ being a permutation of G.

To see the equivalence of conditions (i) and (ii) with the fact that φ is a permutation of G, in Lemma 1.2, we let $A = G$, $f = \varphi$, $\lambda = \psi$, $\bar{\lambda} = \bar{\psi}$, $S = \mathrm{im}(\psi)$, $\bar{S} = \mathrm{im}(\bar{\psi})$, and $\bar{f} = \varphi \mid_S$. Since $\bar{\psi} \circ \varphi = \varphi \circ \psi$, by Lemma 1.2 we know that φ is a permutation of G if and only if φ is a bijection from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$ and φ is injective on $\psi^{-1}(s)$ for any $s \in \mathrm{im}(\psi)$. Since φ, and ψ are group endomorphisms, the latter condition is equivalent to injectivity of φ on $\psi^{-1}(0) = \ker(\psi)$.

(d) The result follows from part (a) since the associated function $\bar{f}(x)$ corresponding to $f(x)$ (restricted to $\mathrm{im}(\psi)$) is

$$\varphi(x) + \bar{\psi}(g(x)) = (\bar{\psi} \circ g)(x),$$

and so, $f(x)$ permutes G if and only if $\varphi(x)$ induces a bijection from $\ker(\psi)$ to $\ker(\bar{\psi})$ (which is condition (i)) and $\bar{\psi} \circ g$ induces a bijection from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$ (which is condition (ii)). Since g permutes $\mathrm{im}(\psi)$, the latter condition is the same with asking that $\bar{\psi}$ induces a bijection from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$. □

3. Multiplicative Group Case

In this section we deal with the case $(G, +) = (\mathbb{F}_q^\times, \cdot)$. Since $\mathbb{F}_q^\times$ is a finite cyclic group, the endomorphisms of $\mathbb{F}_q^\times$ are maps of the form x^s for $s \in \mathbb{Z}$. So, part (a) of Theorem 1.4 in the case $\mathbb{F}_q^\times$ yields the following result for permutation polynomials of $\mathbb{F}_q$ (note that any $\varphi \in \mathrm{End}(\mathbb{F}_q^\times)$ extends naturally to $\mathbb{F}_q$ by letting $\varphi(0) = 0$).

Proposition 3.1. *Let r and s be positive integers. Then $x^r g(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(r, s, q-1) = 1$ and $x^r g(x)^s$ permutes $(\mathbb{F}_q^\times)^s$.*

Proposition 3.1 is essentially [11, Lemma 2.1]. In the above Proposition the case that $s \mid (q-1)$ is of special interest, since one can show that any polynomial $f(x)$ satisfying $f(0) = 0$ can be written in the form $x^r g(x^s)$ for a suitable polynomial g and with the condition $s \mid (q-1)$.

The following is a direct corollary of Theorem 1.4 for $(\mathbb{F}_q^\times, \cdot)$.

Proposition 3.2. *Let r, ℓ be positive integers such that $\ell \mid q-1$ and let $s = \frac{q-1}{\ell}$. Then*

(a) $x^r g(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(r, s) = 1$, and $x^r g(x)^s$ permutes μ_ℓ where μ_ℓ is the subset of $\mathbb{F}_q$ containing all the ℓ-th roots of unity.

(b) For each relatively prime r and s as above, there are $\ell! \cdot s^\ell$ distinct permutation polynomials of $\mathbb{F}_q$ of the form $x^r g(x^s)$.

(c) Assume that $g(x)^s = 1$ for any $x \in \mu_\ell$. Then $x^r g(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(r, q-1) = 1$.

(d) Assume that $g \in \mathbb{F}_q[x]$ restricted to μ_ℓ induces a permutation of μ_ℓ. Then $x^\ell g(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(\ell, s) = 1$.

Part (a) is the well-known criterion from Theorem 1.1, part (b) is a result of Wan and Lidl [9, Corollary 3.5], and part (c) is a result of Akbary and Wang [1, Theorem 3.1] (see also [5, Theorem 7.10], and [4, Theorem 3.1] for examples of g satisfying the condition $g(x)^s = 1$ for all $x \in \mu_\ell$).

The following result is a special case of part (d) of Proposition 3.2.

Corollary 3.3. *Let q be a prime power, and let $n \in \mathbb{N}$. Then for any polynomial $g \in \mathbb{F}_{q^n}[x]$ which permutes $\mu_{q-1} = \mathbb{F}_q^\times$ the polynomial $x^{q-1} g\left(x^{(q^n-1)/(q-1)}\right)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $\gcd(n, q-1) = 1$.*

Proof. In this case, let $\ell = q-1$ and $s = \frac{q^n-1}{q-1} = q^{n-1} + \cdots + q + 1 = (q-1)a + n$ for some integer a. So $\gcd(\ell, s) = 1$ if and only if $\gcd(n, q-1) = 1$. Hence the result follows from part (d) of Proposition 3.2. □

4. Elliptic Curve Case

In the case G is the group of rational points of an elliptic curve E defined over $\mathbb{F}_q$, we can also construct permutations of $E(\mathbb{F}_q)$ as in Theorem 1.4. Note that each elliptic curve E defined over $\mathbb{F}_q$ has roughly q points, or more precisely it has $q + 1 + t$ points, where $|t| \leq 2\sqrt{q}$ according to the Hasse's bound (see [8, Chapter V]). The following result is an immediate consequence of parts (a) and (c) of Theorem 1.4 in the case that G is an elliptic curve defined over $\mathbb{F}_q$.

Proposition 4.1. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let m and n be positive integers. Then for any map $g : E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_q)$, we have that $mx + g(nx)$ is a permutation of $E(\mathbb{F}_q)$ if and only if $\gcd(m, n, \#E(\mathbb{F}_q)) = 1$ and $mx + ng(x)$ is a permutation of $nE(\mathbb{F}_q)$. Moreover, if $\#E(\mathbb{F}_q) = n_1 n_2$ then $mx + n_2 g(n_1 x)$ is a permutation of $E(\mathbb{F}_q)$ if and only if $\gcd(m, n_1 n_2) = 1$.*

Since the Frobenius endomorphism for an elliptic curve E defined over $\mathbb{F}_q$ induces a permutation on each finite group $E(\mathbb{F}_{q^n})$, our next result is an easy application of Theorem 1.4 (c).

Proposition 4.2. *Let E be an elliptic curve defined over $\mathbb{F}_q$, and let m and n be any positive integers. We denote by $E[m](\mathbb{F}_{q^n})$ the set of points of $E(\mathbb{F}_{q^n})$ which are killed by the multiplication-by-m-map on E. Let $g : E(\mathbb{F}_{q^n}) \longrightarrow E[m](\mathbb{F}_{q^n})$ be any function, and let* Frob *be the Frobenius corresponding to $\mathbb{F}_q$ seen as an endomorphism of $E(\mathbb{F}_{q^n})$. Then* $\mathrm{Frob}(x) + g(mx)$ *is a permutation of $E(\mathbb{F}_{q^n})$.*

5. Additive Group Case

Since $(\mathbb{F}_q, +, \cdot)$ is a field, we can extend Theorem 1.4 in this case by inserting a suitable polynomial $h(x)$ (our result is a generalization of [12, Theorem 6], which also motivated our extension).

Theorem 5.1. *Consider any polynomial $g \in \mathbb{F}_{q^n}[x]$, any additive polynomials $\varphi, \psi \in \mathbb{F}_{q^n}[x]$, any $\mathbb{F}_q$-linear polynomial $\bar{\psi} \in \mathbb{F}_{q^n}[x]$ satisfying $\varphi \circ \psi = \bar{\psi} \circ \varphi$ and $\#\psi(\mathbb{F}_{q^n}) = \#\bar{\psi}(\mathbb{F}_{q^n})$, and any polynomial $h \in \mathbb{F}_{q^n}[x]$ such that $h(\psi(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q \setminus \{0\}$.*

Then,

(a) $f(x) := h(\psi(x))\varphi(x) + g(\psi(x))$ permutes $\mathbb{F}_{q^n}$ if and only if

(i) $\ker(\varphi) \cap \ker(\psi) = \{0\}$; and

(ii) $\bar{f}(x) := h(x)\varphi(x) + \bar{\psi}(g(x))$ is a bijection between $\psi(\mathbb{F}_{q^n})$ and $\bar{\psi}(\mathbb{F}_{q^n})$.

(b) For any fixed h, φ, ψ and $\bar{\psi}$ satisfying the above hypothesis plus condition (i) from part (a), there are $(\#\mathrm{im}(\psi))! \cdot \left(\#\ker(\bar{\psi})\right)^{\#\mathrm{im}(\psi)}$ such permutation functions f (when g varies) (where ψ and $\bar{\psi}$ are viewed as endomorphisms of $(\mathbb{F}_{q^n}, +)$).

(c) Assume in addition that $\left(\bar{\psi} \circ g\right)|_{\mathrm{im}(\psi)} = 0$. Then $f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$ permutes $\mathbb{F}_{q^n}$ if and only if $\ker(\varphi) \cap \ker(\psi) = \{0\}$ and $h(x)\varphi(x)$ induces a bijection from $\psi(\mathbb{F}_{q^n})$ to $\bar{\psi}(\mathbb{F}_{q^n})$.

(d) Assume in addition that $\varphi \circ \psi = 0$, and that $g(x)$ restricted to $\mathrm{im}(\psi)$ is a permutation of $\mathrm{im}(\psi)$. Then $f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$ permutes $\mathbb{F}_{q^n}$ if and only if $\ker(\varphi) \cap \ker(\psi) = \{0\}$ and $\bar{\psi}$ restricted to $\mathrm{im}(\psi)$ is a bijection between $\mathrm{im}(\psi)$ and $\mathrm{im}(\bar{\psi})$.

Proof. (a) We apply Lemma 1.2 with $A = \mathbb{F}_{q^n}$, $S = \psi(\mathbb{F}_{q^n})$, $\bar{S} = \bar{\psi}(\mathbb{F}_{q^n})$, $\lambda = \psi$, and $\bar{\lambda} = \bar{\psi}$. It is obvious that $\bar{\psi}(f(x)) = \bar{\psi}(g(\psi(x)) + h(\bar{\psi}(x))\varphi(x)) = \bar{\psi}(g(\psi(x))) + \bar{\psi}(h(\psi(x))\varphi(x)) = \bar{\psi}(g(\psi(x))) + h(\psi(x))\bar{\psi}(\varphi(x)) = \bar{\psi}(g(\psi(x))) + h(\psi(x))\varphi(\psi(x)) = \bar{f}(\psi(x))$. In the last computation we used the fact that $\bar{\psi}$ is an $\mathbb{F}_q$-linear polynomial, and that $h(\psi(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$.

So all we need to check now is that f is injective on each $\psi^{-1}(s)$ for $s \in \psi(\mathbb{F}_{q^n})$ if and only if $\ker(\varphi) \cap \ker(\psi) = \{0\}$. Indeed, for each $a \neq b \in \psi^{-1}(s)$ we must have $f(a) \neq f(b)$ which is equivalent with $h(s)\varphi(a) \neq h(s)\varphi(b)$. The last inequality is equivalent with $h(s) \neq 0$ (which is known due to our hypothesis) and $a - b \notin \ker(\varphi)$. Since $a - b \in \ker(\psi)$, this concludes the proof of part (a) of Theorem 5.1.

(b) Indeed, we first note that f is determined uniquely by the values of g on $\mathrm{im}(\psi)$. On the other hand, for each bijection σ from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$, according to (ii) we solve for g such that

$$h(x)\varphi(x) + \bar{\psi}(g(x)) = \sigma(x) \text{ for each } x \in \mathrm{im}(\psi). \tag{5.1}$$

As h, φ, $\bar{\psi}$ and σ are fixed, then for each $x \in \mathrm{im}(\psi)$, there are $\#\ker(\bar{\psi})$ possibilities for $g(x)$. Because there are $(\#\mathrm{im}(\psi))!$ bijections σ from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$, our conclusion follows.

(c) The result follows from part (a) since the associated function $\bar{f}(x)$ corresponding to $f(x)$ (restricted to $\mathrm{im}(\psi)$) is $h(x)\varphi(x) + \bar{\psi}(g(x)) = h(x)\varphi(x)$.

(d) The result follows from part (a) since the associated function $\bar{f}(x)$ corresponding to $f(x)$ (restricted to $\mathrm{im}(\psi)$) is $h(x)\varphi(x) + \bar{\psi}(g(x)) = (\bar{\psi} \circ g)(x)$; using that g permutes $\mathrm{im}(\psi)$, we conclude that $\bar{f}(x)$ induces a bijection between $\mathrm{im}(\psi)$ and $\mathrm{im}(\bar{\psi})$ if and only if $\ker(\varphi) \cap \ker(\psi) = \{0\}$ and $\bar{\psi}$ induces a bijection between $\mathrm{im}(\psi)$ and $\mathrm{im}(\bar{\psi})$. □

Next we show an example of three additive polynomials φ, ψ, and $\bar{\psi}$ defined over a finite field $\mathbb{F}_q$ satisfying $\varphi \circ \psi = \bar{\psi} \circ \varphi$ and $\psi \neq \bar{\psi}$.

Example 5.2. Let $q = p^n$, where p is any odd prime number, and n is any even positive integer not divisible by p. Denote by $\mathrm{Tr}_n(x) := x + x^p + \cdots + x^{p^{n-1}}$. Because n is even, we can find some $\epsilon \in \mathbb{F}_q$ such that $\epsilon^{p-1} = -1$. Let $\varphi(x) = \epsilon \cdot \mathrm{Tr}_n(x)$, $\psi(x) = x - x^p$, and $\bar{\psi}(x) = x + x^p$. Then it is immediate to check that $\varphi \circ \psi = \bar{\psi} \circ \varphi$. Furthermore, we claim that $\ker(\varphi) \cap \ker(\psi) = \{0\}$ seen as endomorphisms of $\mathbb{F}_q$. Indeed, if $c \in \ker(\psi)$, then $c \in \mathbb{F}_p$, and so, $c \in \ker(\varphi)$ would imply that $nc = 0$, which yields that $c = 0$ since $p \nmid n$.

Using the above observation, the following result is a direct consequence of Theorem 5.1 (a).

Proposition 5.3. *Let $q = p^n$, where p is any odd prime number, and n is any even positive integer not divisible by p. Denote by $\mathrm{Tr}_n(x) := x + x^p + \cdots + x^{p^{n-1}}$. Let $\epsilon \in \mathbb{F}_q$ such that $\epsilon^{p-1} = -1$. Let $\varphi(x) = \epsilon \cdot \mathrm{Tr}_n(x)$, $\psi(x) = x - x^p$, and $\bar{\psi}(x) = x + x^p$. For any polynomial $h(x) \in \mathbb{F}_q[x]$ such that $h(\psi(\mathbb{F}_q)) \subseteq \mathbb{F}_p \setminus \{0\}$, and for any $g(x) \in \mathbb{F}_q[x]$, the map $f(x) := h(\psi(x))\varphi(x) + g(\psi(x))$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\bar{f}(x) := h(x)\varphi(x) + \bar{\psi}(g(x))$ induces a bijection between $\mathrm{im}(\psi)$ and $\mathrm{im}(\bar{\psi})$.*

Proof. It is immediate to check that $\#\psi(\mathbb{F}_q) = \#\bar{\psi}(\mathbb{F}_q)$ since both ψ and $\bar{\psi}$ have precisely p elements in their kernel as endomorphisms of $\mathbb{F}_q$. Then the result follows immediately from Theorem 5.1 (a) and the discussions from Example 5.2. □

Next note that Theorem 5.1 also holds under the stronger assumption that $\varphi, \psi \in \mathrm{End}(G)$ are commuting endomorphisms; in this case, $\bar{\psi} = \psi$.

From Section 1 recall that a class of commuting additive polynomials over $\mathbb{F}_q$ are the $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$, which are of the form

$$\sum_{j=0}^{s} a_j x^{q^j} \text{ with } a_j \in \mathbb{F}_q.$$

We note that any $\mathbb{F}_q$-linear polynomial φ over $\mathbb{F}_q$ acts as a linear polynomial on $\mathbb{F}_q$, i.e.

$$\varphi(x) = \left(\sum_{j=0}^{s} a_j \right) x, \quad \text{for } x \in \mathbb{F}_q.$$

Moreover, if φ is an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$, then φ induces a permutation of $\mathbb{F}_q$ if and only if its restriction on $\mathbb{F}_q$ is not the trivial function.

Since $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$ are commuting endomorphisms of $(\mathbb{F}_{q^n}, +)$, one can generate permutations of $(\mathbb{F}_{q^n}, +)$ by applying Theorem 5.1 for different choices of $\mathbb{F}_q$-linear polynomials. More precisely, we have the following.

Proposition 5.4. *Let $\varphi(x)$ and $\psi(x)$ be two $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$ seen as endomorphisms of $\mathbb{F}_{q^n}$, and let $g \in \mathbb{F}_{q^n}[x]$ and $h \in \mathbb{F}_{q^n}[x]$ such that $h(\psi(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q \setminus \{0\}$. Then*

$$f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the following two conditions hold

(i) $\ker(\varphi) \cap \ker(\psi) = \{0\}$*; and*
(ii) $h(x)\varphi(x) + \psi(g(x))$ *permutes* $\psi(\mathbb{F}_{q^n})$.

Our next result is an easy consequence of our Proposition 5.4.

Theorem 5.5. *Let q be a prime power, $a \in \mathbb{F}_q$, and let $b \in \mathbb{F}_{q^n}$. Let $P(x)$ and $L(x)$ be $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$. Let $H(x) \in \mathbb{F}_{q^n}[x]$ be such that $H(L(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q \setminus \{-a\}$. Then*

$$f(x) = aP(x) + (P(x) + b)H(L(x))$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the following two conditions hold

(i) $\ker(P) \cap \ker(L) = \{0\}$.
(ii) $\bar{f}(x) := aP(x) + (P(x) + L(b))H(x)$ *permutes* $L(\mathbb{F}_{q^n})$.

Proof. We apply Proposition 5.4 with $h(x) = a + H(x)$, $\varphi(x) = P(x)$, $\psi(x) = L(x)$ and $g(x) = b \cdot H(x)$. We also note that for $x \in L(\mathbb{F}_{q^n})$, since $H(x) \in \mathbb{F}_q$ we obtain

$$L(b) \cdot H(x) = L(b \cdot H(x)) = \psi(g(x)),$$

and thus $\bar{f}(x) = (a + H(x))P(x) + L(b)H(x) = h(x)\varphi(x) + \psi(g(x))$, as in Theorem 5.1. □

The above theorem for $H(x) \in \mathbb{F}_q[x]$ and $L(x) = \mathrm{Tr}_n(x)$ will give us [6, Theorem 10] (which is written for prime q in [6]). We also note that Zieve generalized [6, Theorem 10] in his [12, Theorem 6], but in a different direction since in [12, Theorem 6], the result there is written only for $L(x) = \mathrm{Tr}_n(x)$.

Next we study in detail some of the consequences of Proposition 5.4 (or alternatively of Theorem 5.1 when $\psi = \bar{\psi}$) for two specific choices of $\mathbb{F}_q$-linear polynomials. First we consider the case $\psi(x) = \mathrm{Tr}_n(x)$ and next we study the case $\psi(x) = x^q - x$.

Case 1: $\psi(x) = \bar{\psi}(x) = \mathrm{Tr}_n(x) = x^{q^{n-1}} + \cdots + x^q + x$

The following result is an immediate consequence of parts (a) and (b) of Theorem 5.1. We only need to observe that $\mathrm{Tr}_n : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ is surjective, and moreover that for each $\beta \in \mathbb{F}_q$, the set

$$\mathrm{Tr}_n^{-1}(\beta) := \{\alpha \in \mathbb{F}_{q^n} : \mathrm{Tr}_n(\alpha) = \beta\},$$

has q^{n-1} elements; hence also $\ker(\mathrm{Tr}_n)$ has q^{n-1} elements. We also note that part (a) of our result is essentially [12, Theorem 6].

Proposition 5.6. *Let $\varphi(x)$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$ and $\mathrm{Tr}_n(x)$ be the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Let $g(x)$ be any polynomial in $\mathbb{F}_{q^n}[x]$ and $h(x) \in \mathbb{F}_{q^n}[x]$ be any polynomial such that $h(\mathbb{F}_q) \subseteq \mathbb{F}_q \setminus \{0\}$. Then*

(a) $f(x) := h(\mathrm{Tr}_n(x))\varphi(x) + g(\mathrm{Tr}_n(x))$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if

(i) $\ker(\varphi) \cap \ker(\mathrm{Tr}_n) = \{0\}$*; and*
(ii) $\bar{f}(x) := h(x)\varphi(x) + \mathrm{Tr}_n(g(x))$ *is a permutation polynomial when restricted to $\mathbb{F}_q$.*

(b) For each fixed h and $\varphi(x)$ satisfying the above hypothesis plus condition (i), there are $q! \cdot q^{(n-1)q}$ distinct permutation polynomials f of $\mathbb{F}_{q^n}$ of the form $h(\mathrm{Tr}_n(x))\varphi(x) + g(\mathrm{Tr}_n(x))$.

In particular, we obtain the following corollary which is essentially [6, Theorem 1].

Corollary 5.7 (Marcos, 2009). *Let q be a prime power and $\varphi(x) = a_0x + a_1x^q + \cdots + a_{n-1}x^{q^{n-1}} \in \mathbb{F}_q[x]$ be a permutation polynomial of $\mathbb{F}_{q^n}$. Let $g(x) \in \mathbb{F}_q[x]$, let $\gamma \in \mathbb{F}_{q^n}$, and let $a = \mathrm{Tr}_n(\gamma)$. Then $f(x) = \varphi(x) + \gamma g(\mathrm{Tr}_n(x))$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $(a_0 + a_1 + \cdots + a_{n-1})x + ag(x)$ is a permutation polynomial of $\mathbb{F}_q$.*

The above corollary is a straightforward application of part (a) of Proposition 5.6 (and it also follows from [12]). Note that if $\varphi(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$, then it is always true that $\ker(\varphi) \cap \ker(\mathrm{Tr}_n) = \{0\}$. The following result is another consequence of our Theorem 5.1 (c)-(d).

Theorem 5.8. *Let φ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$, let $g(x) \in \mathbb{F}_{q^n}[x]$, and let $h(x) \in \mathbb{F}_{q^n}[x]$ such that $h(\mathbb{F}_q) \subseteq \mathbb{F}_q \setminus \{0\}$.*

(a) Then $f(x) := h(\mathrm{Tr}_n(x))\varphi(x) + g(\mathrm{Tr}_n(x))^q - g(\mathrm{Tr}_n(x))$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $h(x)\varphi(x)$ restricts to a permutation of $\mathbb{F}_q$, and $\ker(\varphi) \cap \ker(\mathrm{Tr}_n) = \{0\}$.

(b) Assume $g(x)$ restricted to $\mathbb{F}_q$ induces a permutation of $\mathbb{F}_q$. Then $f(x) := h(\mathrm{Tr}_n(x))(x^q - x) + g(\mathrm{Tr}_n(x))$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $p \nmid n$.

Proof. (a) We apply part (c) of Theorem 5.1 and note that $\mathrm{Tr}_n(x) \circ (x^q - x) = 0$.

(b) In part (d) of Theorem 5.1, we let $\varphi(x) = x^q - x$, and $\psi = \bar{\psi} = \mathrm{Tr}_n$. Since $\varphi \circ \psi = 0$, we conclude that $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if

(i) $\ker(x^q - x) \cap \ker(\mathrm{Tr}_n(x)) = \{0\}$, and

(ii) $\mathrm{Tr}_n(x)$ is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$.

Since $\ker(x^q - x) = \mathbb{F}_q$ and for $x \in \mathbb{F}_q$, $\mathrm{Tr}_n(x) = nx$, both (i) and (ii) hold if and only if $p \nmid n$. □

Case 2: $\psi(x) = \bar{\psi}(x) = x^q - x$

The following result is an immediate consequence of parts (a) and (b) of our Theorem 5.1. Observe that $\psi(\mathbb{F}_{q^n}) = \ker(\mathrm{Tr}_n) = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^n}\}$, $\ker(\psi) = \mathbb{F}_q$, and so, $\ker(\varphi) \cap \ker(\psi) = \{0\}$ if and only if $\varphi(x)$ induces a permutation polynomial of $\mathbb{F}_q$.

Proposition 5.9. *Let $\varphi(x)$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$, $h(x) \in \mathbb{F}_{q^n}[x]$ be any polynomial such that $h(x^q - x) \in \mathbb{F}_q \setminus \{0\}$ for all $x \in \mathbb{F}_{q^n}$, and let $g(x) \in \mathbb{F}_{q^n}[x]$ be any polynomial. Then*

(a) $h(x^q - x)\varphi(x) + g(x^q - x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if

(i) $\varphi(x)$ induces a permutation polynomial of $\mathbb{F}_q$.

(ii) $h(x)\varphi(x) + g(x)^q - g(x)$ permutes $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^n}\}$.

(b) For each $\varphi(x)$ satisfying (i), we have $(q^{n-1})! \cdot q^{q^{n-1}}$ permutation polynomials of $\mathbb{F}_{q^n}$ of the form $\varphi(x) + g(x^q - x)$.

We also obtain the following result.

Theorem 5.10. *Let φ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$, let $h \in \mathbb{F}_{q^n}[x]$ such that $h(x^q - x) \in \mathbb{F}_q \setminus \{0\}$ for all $x \in \mathbb{F}_{q^n}$, and $g \in \mathbb{F}_{q^n}[x]$ be any polynomial. Let $S = \{x^q - x : x \in \mathbb{F}_{q^n}\}$.*

(a) Then $f_1(x) := h(x^q - x)\varphi(x) + \mathrm{Tr}_n(g(x^q - x))$ and $f_2(x) := h(x^q - x)\varphi(x) + g(x^q - x)^{(q^n-1)/(q-1)}$ are permutation polynomials of $\mathbb{F}_{q^n}$ if and only if $\ker(\varphi) \cap \mathbb{F}_q = \{0\}$ and $h(x)\varphi(x)$ induces a permutation of S.

(b) Assume in addition that g restricted to S induces a permutation of S. Then the polynomial $f(x) := h(x^q - x)\mathrm{Tr}_n(x) + g(x^q - x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $p \nmid n$.

Proof. (a) We apply part (c) of Theorem 5.1, while noting that both $\mathrm{Tr}_n(g(x))$ and $g(x)^{(q^n-1)/(q-1)}$ are in $\mathbb{F}_q$ for all $x \in \mathbb{F}_{q^n}$, and thus are killed by $\psi(x) = x^q - x$.

(b) In part (d) of Theorem 5.1, we let $\varphi(x) = \mathrm{Tr}_n(x)$, and $\psi(x) = \bar{\psi}(x) = x^q - x$. Since $\varphi \circ \psi = 0$, we conclude that $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if

(i) $\ker(\mathrm{Tr}_n(x)) \cap \ker(x^q - x) = \{0\}$, and

(ii) $x^q - x$ induces a bijection from S to S.

Since $\ker(x^q - x) = \mathbb{F}_q$ and for $x \in \mathbb{F}_q$, $\mathrm{Tr}_n(x) = nx$, if (i) holds then $p \nmid n$. Conversely if $p \nmid n$ then (i) holds. Moreover if $\alpha^q - \alpha \in \ker(x^q - x)$ then $\alpha^q - \alpha \in \mathbb{F}_q$, and so $0 = \mathrm{Tr}_n(\alpha^q - \alpha) = n(\alpha^q - \alpha)$. Since $p \nmid n$ this implies that $\alpha^q - \alpha = 0$, so (ii) holds. In other words (i) and (ii) hold if and only if $p \nmid n$. □

Next we show that in the case $q = p = 2$ and $h(x) = 1$, we can relax the condition on g in part (b) of Proposition 5.10. Note that in this case $\mathrm{Tr}_n(x) = x^{2^{n-1}} + \cdots + x^2 + x$.

Theorem 5.11. *Let $S = \{\alpha^2 - \alpha \mid \alpha \in \mathbb{F}_{2^n}\}$. For a fixed $\delta \in \mathbb{F}_{2^n}$, let $g(x)$ be a polynomial in $\mathbb{F}_{2^n}[x]$ such that $g\,|_S$ is a one-to-one mapping onto $S' := \{\delta + y : y \in S\}$. Then $f(x) = \mathrm{Tr}_n(x) + g(x^2 - x)$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if n is odd.*

Proof. If f is a permutation polynomial, then $f(1) \neq f(0)$, which means that $\mathrm{Tr}_n(1) = n \neq 0 = \mathrm{Tr}_n(0)$, i.e. n is odd.

Now suppose that n is odd. In particular, this means that $\mathrm{Tr}_n(x)$ is a permutation polynomial of $\mathbb{F}_2$.

Now, $g(x)^2 - g(x) + \mathrm{Tr}_n(x)$ maps S to S since $\mathrm{Tr}_n(x) = 0$ for each $x \in S$. We will prove that $g(x)^2 - g(x) + \mathrm{Tr}_n(x)$ is one-to-one on S, which will yield that f is a permutation polynomial (by Proposition 5.9 (a)). Let $\beta, \gamma \in \mathbb{F}_{2^n}$ such that

$$g(\beta^2 - \beta)^2 - g(\beta^2 - \beta) = g(\gamma^2 - \gamma)^2 - g(\gamma^2 - \gamma).$$

If $g(\beta^2 - \beta) \neq g(\gamma^2 - \gamma)$, then $g(\beta^2 - \beta) + g(\gamma^2 - \gamma) - 1 = 0$ and so,

$$\mathrm{Tr}_n(g(\beta^2 - \beta)) + \mathrm{Tr}_n(g(\gamma^2 - \gamma)) - 1 = 0$$

because $\mathrm{Tr}_n(1) = 1$ (since n is odd). However, $\mathrm{Tr}_n(g(\beta^2 - \beta)) = \mathrm{Tr}_n(g(\gamma^2 - \gamma)) = \mathrm{Tr}_n(\delta)$ because g maps S onto $S' = \delta + S$. This yields a contradiction. Hence $g(\beta^2 - \beta) = g(\gamma^2 - \gamma)$. Because g is a one-to-one mapping when restricted to S, we must have $\beta^2 - \beta = \gamma^2 - \gamma$, and so we are done. □

We observe that in the above proposition there are many polynomials $g(x) \in \mathbb{F}_{2^n}[x]$ which map S injectively to S'. Indeed, for each fixed δ, we have $(2^{n-1})! \cdot 2^{n2^{n-1}}$ possibilities for the choices of $g(x)$, which yield $(2^{n-1})!$ distinct permutation polynomials $f(x)$ of $\mathbb{F}_{2^n}$.

Finally, we have the following result which follows from Proposition 5.9 (a) by letting $h(x) = 1$.

Theorem 5.12. *Let $q = p^m$. Then the following are permutation polynomials of $\mathbb{F}_{q^2}$:*

(a) $f_{a,b,k}(x) := ax^q + bx + (x^q - x)^k$, for $a, b \in \mathbb{F}_q$ such that $a \neq \pm b$, and for all even positive integers k.

(b) $f_{a,k}(x) := ax^q + ax + (x^q - x)^k$, if $a \in \mathbb{F}_q^\times$, and p and k are odd, and in addition k is relatively prime with $q - 1$.

Proof. (a) Let $L(x) := ax^q + bx$. Since a, b ($a \neq \pm b$) are both in $\mathbb{F}_q$, we conclude that $L(x)$ is an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$ which is also a permutation polynomial of $\mathbb{F}_{q^2}$ (note that the only elements $c \in \mathbb{F}_q^\times \cap (\mathbb{F}_{q^2}^\times)^{q-1}$ are ± 1). According to Proposition 5.9 (a) all we need to show is that $\bar{f}(x) := L(x) + x^{qk} - x^k$ induces a permutation of $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^2}\}$. This is clear because

$$\bar{f}(\alpha^q - \alpha) = L(\alpha^q - \alpha) + (\alpha^{q^2} - \alpha^q)^k - (\alpha^q - \alpha)^k = L(\alpha^q - \alpha) = L(\alpha)^q - L(\alpha) \in S, \tag{5.2}$$

and because $L(x)$ induces a permutation of $\mathbb{F}_{q^2}$. In deriving Equation (5.2) we also used that $\alpha^{q^2} = \alpha$ (since $\alpha \in \mathbb{F}_{q^2}$) and that k is even.

(b) It is clear that $x^q + x$ is a permutation polynomial of $\mathbb{F}_q$ (here we use that $2 \neq 0$ in $\mathbb{F}_q$). So, using Proposition 5.9 (a), it suffices to show that

$$\bar{f}(x) := ax^q + ax + x^{kq} - x^k$$

induces a permutation of $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^2}\}$. It is immediate to check that for any $\alpha \in \mathbb{F}_{q^2}$, we have

$$\bar{f}(\alpha^q - \alpha) = (\alpha^q - \alpha)^{kq} - (\alpha^q - \alpha)^k.$$

Let $\epsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\epsilon^{q-1} = -1$ (we use that q is odd). Then each $\alpha \in \mathbb{F}_{q^2}$ is uniquely written as $a + b\epsilon$ for some $a, b \in \mathbb{F}_q$. We compute then easily that $\alpha^q - \alpha = -2b\epsilon$. Hence

$$\begin{aligned} \bar{f}(\alpha^q - \alpha) &= (\alpha^q - \alpha)^{kq} - (\alpha^q - \alpha)^k \\ &= (-2b\epsilon)^{kq} - (-2b\epsilon)^k \\ &= (-2b)^k(-\epsilon)^k - (-2b)^k\epsilon^k \\ &= -2(-2b)^k\epsilon^k, \end{aligned}$$

since k is odd. Now, if $\bar{f}(\alpha^q - \alpha) = h(\beta^q - \beta)$ for some $\alpha, \beta \in \mathbb{F}_{q^2}$, where $\alpha = a + b\epsilon$ and $\beta = c + d\epsilon$ (with $a, b, c, d \in \mathbb{F}_q$), then we obtain that $(-2b)^k = (-2d)^k$. However, because $\gcd(k, q-1) = 1$, we conclude that $b = d$; this yields that $\alpha - \beta \in \mathbb{F}_q$, and so, $\alpha^q - \alpha = \beta^q - \beta$. Therefore $\bar{f}(x)$ induces a permutation of S, as desired. □

6. Other Applications of Lemma 1.2

Using Lemma 1.2, we can also obtain the following results.

Theorem 6.1. *Let q be a prime power, let n be a positive integer, and let L_1, L_2, L_3 be $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$ seen as endomorphisms of $(\mathbb{F}_{q^n}, +)$. Let $g(x) \in \mathbb{F}_{q^n}[x]$ be such that $g(L_3(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$. Then*

$$f(x) = L_1(x) + L_2(x)g(L_3(x))$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the following two conditions hold

(i) $\ker(F_y) \cap \ker(L_3) = \{0\}$, *for any* $y \in \mathrm{im}(L_3)$, *where*

$$F_y(x) := L_1(x) + L_2(x)g(y).$$

(ii) $\bar{f}(x) := L_1(x) + L_2(x)g(x)$ *permutes* $L_3(\mathbb{F}_{q^n})$.

Proof. We apply Lemma 1.2 with $A = \mathbb{F}_{q^n}$, $f = L_1 + L_2 \cdot (g \circ L_3)$, $S = \bar{S} = L_3(\mathbb{F}_{q^n})$, $\lambda = \bar{\lambda} = L_3$ and $\bar{f} = L_1 + L_2 \cdot g$ (note that because L_1, L_2 and L_3 are $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$, and because $g(L_3(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$ we obtain that $\bar{f}$ induces a well-defined self-map on S). Also, because $g(L_3(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$, and L_1, L_2, and L_3 are $\mathbb{F}_q$-linear over $\mathbb{F}_q$ we have $\lambda \circ f = \bar{f} \circ \lambda$. So by Lemma 1.2, $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $\bar{f}(x)$ is a permutation polynomial of $L_3(\mathbb{F}_{q^n})$ and $f(x)$ is injective on each $L_3^{-1}(y) \subseteq \mathbb{F}_{q^n}$ for all $y \in L_3(\mathbb{F}_{q^n})$. Since $f(\alpha) = L_1(\alpha) + L_2(\alpha)g(y) = F_y(\alpha)$ for each $\alpha \in L_3^{-1}(y)$, then $F_y(\alpha) \neq F_y(\beta)$ for any $\alpha \neq \beta$ in $L_3^{-1}(y)$ is equivalent to $\ker(F_y) \cap \ker(L_3) = \{0\}$. □

In particular, if $L_2(x) = x$ and $L_3(x) = \mathrm{Tr}_n(x)$, we obtain the following result from [2, Theorem 3] as a corollary.

Corollary 6.2 (Coulter-Henderson-Matthews, 2009). *Let q be a prime power, let $g(x) \in \mathbb{F}_q[x]$, let $L(x)$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$, and let $f(x) = L(x) + xg(\mathrm{Tr}_n(x))$. Then $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the following two conditions hold*

(i) For any $y \in \mathbb{F}_q$ and any $x \in \mathbb{F}_{q^n}$ we have $L(x) + xg(y) = 0$ and $\mathrm{Tr}_n(x) = 0$ if and only if $x = 0$.
(ii) $\bar{f}(x) = L(x) + xg(x)$ is a permutation polynomial of $\mathbb{F}_q$.

We point out that in Theorem 6.1 it is crucial that L_1 and L_2 are $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$, since otherwise they may not commute with L_3, and so we may not be able to employ Lemma 1.2.

Using directly Lemma 1.2 we can prove the following generalization of [6, Proposition 12] (simply take $S = \mathbb{F}_q$ and $k(x) = x^2$ in our Theorem 6.3). We note that in [12], Zieve mentioned that his method does not yield any generalization of [6, Proposition 12], even though it would be desirable to find such a generalization.

Theorem 6.3. *Let q be any power of the prime number p, let n be any positive integer, and let S be any subset of $\mathbb{F}_{q^n}$ containing 0. Let $h, k \in \mathbb{F}_{q^n}[x]$ be any polynomials such that $h(0) \neq 0$ and $k(0) = 0$, and let $B \in \mathbb{F}_{q^n}[x]$ be any polynomial satisfying*

(a) $h(B(\mathbb{F}_{q^n})) \subseteq S$; and
(b) $B(a\alpha) = k(a) \cdot B(\alpha)$ for all $a \in S$ and all $\alpha \in \mathbb{F}_{q^n}$.

Then the polynomial $f(x) := xh(B(x))$ is a permutation polynomial for $\mathbb{F}_{q^n}$ if and only if $\bar{f}(x) := xk(h(x))$ induces a permutation of $B(\mathbb{F}_{q^n})$.

Proof. We apply our Lemma 1.2 for $f, \bar{f}$ above, and for $\lambda = \bar{\lambda} = B$. Hypothesis (a) and (b) yield

$$B(f(x)) = B(xh(B(x))) = k(h(B(x))) \cdot B(x) = \bar{f}(B(x)).$$

We also note that for each $s \in B(\mathbb{F}_{q^n})$, we have that $f(x)$ is injective on $B^{-1}(s)$ as long as $h(s) \neq 0$. On the other hand, if $h(s) = 0$, then $s \neq 0$ (since we assumed that $h(0) \neq 0$). But then $\bar{f}(s) = 0 = \bar{f}(0)$ contradicting our assumption that $\bar{f}$ induces a permutation of $B(\mathbb{F}_q)$ (we remark that $0 \in B(\mathbb{F}_{q^n})$ by hypothesis (b) and the fact that $k(0) = 0$). Therefore the hypotheses of our Lemma 1.2 are verified and thus the conclusion of Theorem 6.3 follows. □

There are several examples of functions $B(x)$ satisfying hypothesis (b) as in Theorem 6.3 when $S = \mathbb{F}_q$ and $k(x) = x^\ell$ for any positive integer ℓ. For example, we may take

$$B(x) = \sum_{1 \leq i_1 < i_2 < \cdots i_\ell \leq n} x^{q^{i_1} + q^{i_2} + \cdots q^{i_\ell}},$$

or we may take $B(x) = \sum_{i=1}^{n} x^{\ell q^i} = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x^\ell)$, or we may take $B(x) = \sum_{1 \leq i \neq j \leq n} x^{(\ell-1)q^i + q^j}$ (this time the sum is not ordered since i and j are not interchangeable).

There are also many examples of functions $B(x) \in \mathbb{F}_{q^n}[x]$ satisfying hypothesis (b) from Theorem 6.3 when S is *not* $\mathbb{F}_q$. Let d be any divisor of $(q^n - 1)$, and let $S = \mathbb{F}_{q^n}$. Then $B(x) := x^d$ satisfies hypothesis (b) above together with the function $k(x) := x^d$. Therefore Theorem 6.3 yields that for any polynomial $h \in \mathbb{F}_{q^n}[x]$, we have that

$$xh(x^d) \text{ is a permutation polynomial for } \mathbb{F}_{q^n} \text{ if and only}$$

$$xh(x)^d \text{ induces a permutation on } \mu_{(q^n-1)/d},$$

where $\mu_{(q^n-1)/d}$ is the set of roots of unity of order dividing $(q^n-1)/d$. The above statement is essentially Theorem 1.1.

We also remark that Theorem 6.3 can be generalized for $f(x) := A(x)h(B(x))$ and $\bar{f}(x) := C(x)k(h(x))$ where $A(x), C(x) \in \mathbb{F}_{q^n}[x]$ are any polynomials such that $B(A(x)) = C(B(x))$ with $C(0) = 0$ and $A(x)$ is injective on $B^{-1}(s)$ for each $s \in B(\mathbb{F}_{q^n})$, under the similar assumptions $h(B(\mathbb{F}_{q^n})) \subseteq S \setminus \{0\}$ and $B(a\alpha) = k(a) \cdot B(\alpha)$ for all $a \in S$ and all $\alpha \in \mathbb{F}_{q^n}$.

The following result is for the class of functions which admit a linear translator, as defined in Section 1 (see Definition 1.8).

Theorem 6.4. *Let $S \subseteq \mathbb{F}_q$ and $F : \mathbb{F}_q \longrightarrow S$ be a surjective map. Let $\gamma \in \mathbb{F}_q$ be a b-linear translator with respect to S for the map F. Then for any $G \in \mathbb{F}_q[x]$ which maps S into S, we have that $x + \gamma G(F(x))$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $x + bG(x)$ permutes S.*

Proof. In Lemma 1.2 set $A = \mathbb{F}_q$, $f(x) = x+\gamma G(F(x))$, $S = \bar{S} = F(\mathbb{F}_q)$, $\lambda = \bar{\lambda} = F$, and $\bar{f}(x) = x+bG(x)$. Since γ is a b-linear translator of $F : \mathbb{F}_q \longrightarrow S$ with respect to S, and since $G(S) \subseteq S$, we have $F(x + \gamma G(F(x))) = F(x) + bG(F(x))$. So by Lemma 1.2, $x + \gamma G(F(x))$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $x + bG(x)$ is a permutation of S and $x + \gamma G(F(x))$ is injective on $F^{-1}(s)$ for any $s \in S$. Since $x + \gamma G(F(x))$ is injective on $F^{-1}(s)$ for any $s \in S$ the result follows. □

Corollary 6.5. *Under the conditions of the above theorem we have the following:*

(a) If $G(x) = x$ we have that $x + \gamma F(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $b \neq -1$.

(b) If q is odd and $2S = S$, then $x + \gamma F(x)$ is a complete mapping of $\mathbb{F}_q$ if and only if $b \notin \{-1, -2\}$.

Proof. (a) This is true since $x + bx$ permutes S if and only if $b \neq -1$ (also note that $S + b \cdot S \subseteq S$ since $F : \mathbb{F}_q \longrightarrow S$ admits a b-linear translator).

(b) Because q is odd and $2S = S$, we have that $\frac{\gamma}{2}$ is a $\frac{b}{2}$-linear translator of F with respect to S. Then the result follows since both $x + \gamma F(x)$ and $2x + \gamma F(x) = 2 \cdot \left(x + \frac{\gamma}{2} F(x)\right)$ are permutation polynomials using part (a). □

Theorem 6.4 and Corollary 6.5 are generalizations of results given in [3] in which b-linear translators with respect to $\mathbb{F}_{p^m}$ (p prime) for maps $F : \mathbb{F}_{p^{mn}} \longrightarrow \mathbb{F}_{p^m}$ are being considered (see Theorem 2(a), Corollary 1 and Theorem 11 of [3]). To see that our results in fact produce new classes of permutation polynomials (different from the ones given by our Section 5, and the ones constructed in [3]), we need to construct non-additive maps $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ and $\gamma, b \in \mathbb{F}_q$ for which γ is a b-linear translator with respect to $\mathrm{im}(f)$ for f. The following are examples of such maps.

Examples 6.6. Let p be an odd prime and $q = p^{2m}$. Let $\epsilon \in \mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ such that $\epsilon^{p^m-1} = -1$. Then any element of $\mathbb{F}_{p^{2m}}$ can be written uniquely as $\alpha + \beta\epsilon$ with $\alpha, \beta \in \mathbb{F}_{p^m}$.

(a) Define $f : \mathbb{F}_{p^{2m}} \longrightarrow \mathbb{F}_{p^{2m}}$ by

$$f(\alpha + \beta\epsilon) = \alpha^2\epsilon.$$

It is clear that f is not additive. Moreover 1 is a 0-translator with respect to $S = \mathrm{im}(f) = \epsilon(\mathbb{F}_{p^m})^2 \neq \mathbb{F}_{p^m}$ for f. So, by part (a) of Corollary 6.5, $x + f(x)$ is a permutation polynomial of $\mathbb{F}_{p^{2m}}$.

(b) Define $f : \mathbb{F}_{p^{2m}} \longrightarrow \mathbb{F}_{p^{2m}}$ by

$$f(\alpha + \beta\epsilon) = (\alpha^2 + \beta)\epsilon.$$

Then 1 is a 1-translator with respect to $\mathrm{im}(f) = \epsilon \cdot \mathbb{F}_{p^m} \neq \mathbb{F}_{p^m}$ for the non-additive mapping f. Again, $x + f(x)$ is a permutation polynomial of $\mathbb{F}_{p^{2m}}$. Moreover, using part (b) of Corollary 6.5, $x + f(x)$ is a complete mapping of $\mathbb{F}_{p^{2m}}$ for any $p > 3$.

References

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

[2] R. Coulter, M. Henderson, R. Matthews, *A note on constructing permutation polynomials*, Finite Fields Appl. **15** (2009), 553–557.

[3] G. M. Kyureghyan, *Constructing permutations of finite fields via linear translators*, preprint, available online at `http://arxiv.org/abs/0903.0743v2`.

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

[5] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[6] J. E. Marcos, *Specific permutation polynomials over finite fields*, Finite Fields Appl. (2009), doi:10.1016/j.ffa.2009.02.004.

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

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[9] 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.

[10] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, Sequences, subsequences, and Consequences (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007), Lecture Notes in Comput. Sci. 4893, 119–128.

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

[12] M. Zieve, *Classes of permutation polynomials based on cyclotomy and an additive analogue*, to appear in Additive Number Theory, Springer, 2010, available online at `http://arxiv.org/abs/0810.2830`.