PERMUTATION POLYNOMIALS INDUCED FROM PERMUTATIONS OF SUBFIELDS, AND SOME COMPLETE SETS OF MUTUALLY ORTHOGONAL LATIN SQUARES

MICHAEL E. ZIEVE

ABSTRACT. We present a general technique for obtaining permutation polynomials over a finite field from permutations of a subfield. By applying this technique to the simplest classes of permutation polynomials on the subfield, we obtain several new families of permutation polynomials. Some of these have the additional property that both $f(x)$ and $f(x)+x$ induce permutations of the field, which has combinatorial consequences. We use some of our permutation polynomials to exhibit complete sets of mutually orthogonal latin squares. In addition, we solve the open problem from a recent paper by Wu and Lin, and we give simpler proofs of much more general versions of the results in two other recent papers.

1. INTRODUCTION

A *complete mapping* of a group G is a permutation ϕ of G for which the map $\alpha \mapsto \alpha\phi(\alpha)$ is also a permutation of G. Complete mappings were introduced by Mann [8], in the context of constructing orthogonal latin squares. Complete mappings were subsequently shown to have several other combinatorial consequences, including neofields, Bol loops, and partitions of G for which the partial products have certain properties [6, 7, 10, 11]. In the past few decades, several authors have studied complete mappings on the additive group of a finite field $\mathbb{F}_q$. Since every function $\mathbb{F}_q \to \mathbb{F}_q$ can be written as $\alpha \mapsto f(\alpha)$ for some polynomial $f(x) \in \mathbb{F}_q[x]$, complete mappings on $\mathbb{F}_q$ can be studied in terms of polynomials, which facilitates the use of algebraic techniques.

We use the following terminology: a *permutation polynomial* over $\mathbb{F}_q$ is a polynomial $f(x) \in \mathbb{F}_q[x]$ for which the function $\alpha \mapsto f(\alpha)$ defines a permutation of $\mathbb{F}_q$. A *complete permutation polynomial* over $\mathbb{F}_q$ is a polynomial $f(x) \in \mathbb{F}_q[x]$ for which the function $\alpha \mapsto f(\alpha)$ defines a

The author thanks Xiwang Cao, Zhiguo Ding and Baofeng Wu for comments on an earlier version of this paper, and the NSF for support under grant DMS-1162181.

complete mapping on $\mathbb{F}_q$; in other words, both $f(x)$ and $f(x)+x$ are permutation polynomials over $\mathbb{F}_q$. Recently several papers have been written exhibiting families of permutation polynomials, some of which are complete. Many of the results in these papers are easy consequences of a general result (Lemma 2.1) which reduces the question of whether a certain type of polynomial permutes $\mathbb{F}_q$ to the question of whether a different polynomial permutes some subgroup of $\mathbb{F}_q^*$.

In this note we show that this method applies especially well in case the subgroup of $\mathbb{F}_q^*$ is the multiplicative group of a subfield $\mathbb{F}_Q$ of $\mathbb{F}_q$. In this case we can use Lemma 2.1 to produce new permutation polynomials over $\mathbb{F}_q$ from known permutation polynomials over $\mathbb{F}_Q$. Our construction is based on the following result:

Theorem 1.1. *Pick $h \in \mathbb{F}_q[x]$ where $q = Q^m$, and let r be a positive integer. Then $x^r h(x^{(q-1)/(Q-1)})$ permutes $\mathbb{F}_q$ if and only if*

(1) $\gcd(r, (q-1)/(Q-1)) = 1$ *and*
(2) $g(x) := x^r h(x) h^{(Q)}(x) h^{(Q^2)}(x) \dots h^{(Q^{m-1})}(x)$ *permutes* $\mathbb{F}_Q$,

where $h^{(Q^i)}(x)$ denotes the polynomial obtained from $h(x)$ by raising every coefficient to the Q^i-th power.

We emphasize that the usefulness of this result is that permutation polynomials over $\mathbb{F}_{Q^m}$ are being constructed from permutation polynomials over $\mathbb{F}_Q$. This enables one to start with well-understood permutation polynomials over $\mathbb{F}_Q$, such as x^n or Dickson polynomials, and use them to construct new permutation polynomials over $\mathbb{F}_{Q^m}$. We also remark that $g(x) = x^r N(h(x))$, where N denotes the norm relative to the field extension $\mathbb{F}_q(x)/\mathbb{F}_Q(x)$; in particular, it follows that $g(x) \in \mathbb{F}_Q[x]$.

Theorem 1.1 becomes especially simple in case $h(x) \in \mathbb{F}_Q[x]$:

Corollary 1.2. *Pick any $h \in \mathbb{F}_Q[x]$, let $q = Q^m$, and let r be a positive integer. Then $x^r h(x^{(q-1)/(Q-1)})$ permutes $\mathbb{F}_q$ if and only if*

(1) $\gcd(r, (q-1)/(Q-1)) = 1$ *and*
(2) $g(x) := x^r h(x)^m$ *permutes* $\mathbb{F}_Q$.

Condition (2) can be simplified when m is coprime to $Q-1$:

Corollary 1.3. *Pick any $h \in \mathbb{F}_Q[x]$, let r, m, n be positive integers such that $mn \equiv 1 \pmod{Q-1}$, and put $q = Q^m$. Then $x^r h(x^{(q-1)/(Q-1)})$ permutes $\mathbb{F}_q$ if and only if*

(1) $\gcd(r, (q-1)/(Q-1)) = 1$ *and*
(2) $g(x) := x^{rn} h(x)$ *permutes* $\mathbb{F}_Q$.

Note that in this corollary we can begin with an arbitrary permutation polynomial $H(x)$ over $\mathbb{F}_Q$; writing $H(x) - H(0) = xh(x)$, it follows that $xh(x^{(q-1)/(Q-1)})$ permutes $\mathbb{F}_q$ whenever $q = Q^m$ with $m \equiv 1 \pmod{Q-1}$. Thus, this special case of our construction enables us to produce permutation polynomials over extensions of $\mathbb{F}_Q$ from an arbitrary permutation polynomial over $\mathbb{F}_Q$. These permutation polynomials have coefficients in $\mathbb{F}_Q$, which is a situation studied by Carlitz and Hayes [3]; however, our approach is different than theirs, and we know no precise connection between our results and theirs.

In the next section we prove Theorem 1.1 and the above corollaries, and also give further applications of Theorem 1.1 in which $h(x) \notin \mathbb{F}_Q[x]$. In these latter applications, we choose h, r and m so that $g(x)$ will have degree at most 5. We restrict to these degrees solely for the purpose of having a short list of applications; our method can be used with higher-degree $g(x)$ to produce arbitrarily many further families of permutation polynomials. In Section 3 we use these new classes of permutation polynomials to construct new families of complete permutation polynomials, and in particular we answer the open problem of Wu and Lin [14] by constructing complete permutation polynomials over $\mathbb{F}_{2^{2^e}}$. In Section 4 we use our new permutation polynomials to construct complete sets of mutually orthogonal latin squares. Quite special cases of some of our applications of Theorem 1.1 were obtained via lengthy computations in two recent papers by Tu, Zeng and Hu [12] and Xu, Cao, Tu, Zeng and Hu [15]. In Section 5 we explain how the results of [12] and [15] follow from our results.

2. Permutation polynomials from permutations of subfields

In this section we exhibit some families of permutation polynomials over $\mathbb{F}_{Q^m}$ which can be obtained from permutation polynomials over $\mathbb{F}_Q$, and in particular we prove Theorem 1.1. Our constructions rely on the following result.

Lemma 2.1. *Pick $h \in \mathbb{F}_q[x]$ and integers $r, s > 0$ such that $s \mid (q-1)$. Then $f(x) := x^r h(x^{(q-1)/s})$ permutes $\mathbb{F}_q$ if and only if*

(1) $\gcd(r, (q-1)/s) = 1$ *and*
(2) $x^r h(x)^{(q-1)/s}$ *permutes the set of s-th roots of unity in $\mathbb{F}_q^*$.*

This lemma has been used in several investigations of permutation polynomials, for instance see [9, 13, 16, 17, 18, 19]. Its short proof is given in [13, 16, 17, 19].

We now deduce Theorem 1.1 from Lemma 2.1.

Proof of Theorem 1.1. In light of Lemma 2.1, it suffices to show that $g(x)$ and $\tilde{g}(x) := x^r h(x)^{(q-1)/(Q-1)}$ induce the same mapping on $\mathbb{F}_Q^*$. For $\beta \in \mathbb{F}_Q^*$, the fact that $(q-1)/(Q-1) = 1 + Q + Q^2 + \cdots + Q^{m-1}$ implies that

$$\tilde{g}(\beta) = \beta^r h(\beta)^{(q-1)/(Q-1)} = \beta^r \prod_{j=0}^{m-1} h(\beta)^{Q^j} = \beta^r \prod_{j=0}^{m-1} h^{(Q^j)}(\beta) = g(\beta),$$

which completes the proof. □

Corollary 1.2 follows at once from Theorem 1.1. To deduce Corollary 1.3 from Corollary 1.2, note that x^n permutes $\mathbb{F}_Q$ (since n is coprime to $Q-1$), so $g(x) := x^r h(x)^m$ permutes $\mathbb{F}_Q$ if and only if $g(x)^n = x^{rn} h(x)^{mn}$ permutes $\mathbb{F}_Q$; since $mn \equiv 1 \pmod{Q-1}$, this last condition says that $x^{rn} h(x)$ permutes $\mathbb{F}_Q$.

Corollaries 1.2 and 1.3 apply Theorem 1.1 in the special case that $h(x) \in \mathbb{F}_Q[x]$. In the rest of this section we demonstrate how to apply Theorem 1.1 when $h(x) \notin \mathbb{F}_Q[x]$. For simplicity, we restrict to the case that $g(x)$ is a member of some of the simplest classes of permutation polynomials over $\mathbb{F}_Q$: specifically, we use permutation polynomials over $\mathbb{F}_Q$ of degree at most 5. These low-degree permutation polynomials were classified in Dickson's thesis [5, §87]. We now recall a simplified version of Dickson's result.

Lemma 2.2. *The following polynomials permute $\mathbb{F}_Q$:*

(1) x^3 *if* $Q \not\equiv 1 \pmod 3$

(2) $x^3 - \beta x$ *if* $Q = 3^n$ *and* $\beta \in \mathbb{F}_Q^*$ *is a nonsquare*

(3) $x^4 + \beta x^2 + \gamma x$ *if* $Q = 2^n$ *and* $\beta, \gamma \in \mathbb{F}_Q$ *and* $x^4 + \beta x^2 + \gamma x$ *has no nonzero roots in* $\mathbb{F}_Q$

(4) x^5 *if* $Q \not\equiv 1 \pmod 5$

(5) $x^5 + \beta x^3 + 5^{-1}\beta^2 x$ *if* $Q \equiv \pm 2 \pmod 5$ *and* $\beta \in \mathbb{F}_Q$

(6) $x^5 - \beta x$ *if* $Q = 5^n$ *and* $\beta \in \mathbb{F}_Q$ *is not a fourth power*

(7) $x^5 + 2\beta x^3 + \beta^2 x$ *if* $Q = 5^n$ *and* $\beta \in \mathbb{F}_Q$ *is a nonsquare.*

Conversely, for every degree-3 permutation polynomial $f(x)$ over $\mathbb{F}_Q$, there exist $\theta, \mu, \nu \in \mathbb{F}_Q$ with $\theta \neq 0$ such that $\theta f(x+\mu) + \nu$ is on the above list. The same is true for degree-4 permutation polynomials if

$Q \neq 2, 3, 7$, and for degree-5 permutation polynomials if $Q > 7$ and $Q \neq 13$.

We now use degree-3 permutation polynomials over $\mathbb{F}_Q$ to construct degree-$(Q+2)$ permutation polynomials over $\mathbb{F}_{Q^2}$:

Corollary 2.3. *Pick $\alpha \in \mathbb{F}_{Q^2}^*$, and write $f_\alpha(x) := x^{Q+2} + \alpha x$. Then f_α permutes $\mathbb{F}_{Q^2}$ if and only if one of the following occurs:*

1. *$Q \equiv 5 \pmod 6$ and α^{Q-1} has order 6;*
2. *$Q \equiv 2 \pmod 6$ and α^{Q-1} has order 3; or*
3. *$Q \equiv 0 \pmod 3$ and $\alpha^{Q-1} = -1$.*

In particular, the number of elements $\alpha \in \mathbb{F}_{Q^2}^*$ for which f_α permutes $\mathbb{F}_{Q^2}$ is either $2(Q-1)$ or $Q-1$ or 0, depending on whether Q is congruent to 2, 0 or 1 modulo 3.

This result is from [13]. Since that paper is unpublished, we include the proof.

Proof. By Theorem 1.1, f_α permutes $\mathbb{F}_{Q^2}$ if and only if the polynomial $g_\alpha(x) := x(x+\alpha)(x+\alpha^Q)$ permutes $\mathbb{F}_Q$. By Lemma 2.2, the latter condition never occurs if $Q \equiv 1 \pmod 3$.

Now suppose that $Q \equiv 2 \pmod 3$, so that g_α permutes $\mathbb{F}_Q$ if and only if $g_\alpha(x) = (x+\mu)^3 - \mu^3$ for some $\mu \in \mathbb{F}_Q$. Note that $\mu \neq 0$ (since $\alpha \neq 0$). We have $(x+\mu)^3 - \mu^3 = x(x+\mu-\omega\mu)(x+\mu-\omega^2\mu)$ where ω is a primitive cube root of unity. By unique factorization in $\mathbb{F}_{Q^2}[x]$, and the fact that $\omega \notin \mathbb{F}_Q$, it follows that f_α permutes $\mathbb{F}_{Q^2}$ if and only if $\alpha = \mu(1-\omega)$ for some primitive cube root of unity ω and some $\mu \in \mathbb{F}_Q^*$. Equivalently, $\alpha^{Q-1} = (1-\omega)^{Q-1}$, which we compute to be

$$(1-\omega)^{Q-1} = \frac{(1-\omega)^Q}{1-\omega} = \frac{1-\omega^Q}{1-\omega} = \frac{1-\omega^2}{1-\omega} = 1+\omega = -\omega^2.$$

It follows that $(1-\omega)^{Q-1}$ has order six if Q odd, and order three if Q even, and conversely each element of these orders occurs as $(1-\omega)^{Q-1}$ for some choice of ω. This concludes the proof when $Q \equiv 2 \pmod 3$.

Now suppose that $Q \equiv 0 \pmod 3$. By Lemma 2.2, the only cubic permutation polynomials over $\mathbb{F}_Q$ which are monic and divisible by x are the polynomials $x^3 - \beta x$ where $\beta \in \mathbb{F}_Q$ is either 0 or a nonsquare. For $\beta \neq 0$, any such polynomial is the product of x and an irreducible quadratic in $\mathbb{F}_Q[x]$, so it equals $x(x+\alpha)(x+\alpha^Q)$ if and only if $\alpha^2 = \beta$. It follows that, for $\alpha \in \mathbb{F}_{Q^2}^*$, the polynomial g_α permutes $\mathbb{F}_Q$ if and only if α^2 is a nonsquare in $\mathbb{F}_Q$, or equivalently $\alpha^{Q-1} = -1$. □

Likewise, using degree-4 permutation polynomials over $\mathbb{F}_r$ yields the following result from [13].

Corollary 2.4. *Let Q be a prime power. For $\alpha \in \mathbb{F}_{Q^3}^*$, the polynomial $x^{Q^2+Q+2} + \alpha x$ permutes $\mathbb{F}_{Q^3}$ if and only if one of the following occurs:*

(1) *Q is even and $\alpha^{Q^2} + \alpha^Q + \alpha = 0$;*
(2) *$Q = 7$ and $\alpha^{24} + \alpha^{18} + 4\alpha^{12} + 2 = 0$;*
(3) *$Q = 3$ and $\alpha^{12} + \alpha^{10} + \alpha^4 + 1 = 0$; or*
(4) *$Q = 2$ and $\alpha \neq 1$.*

The number of elements $\alpha \in \mathbb{F}_{Q^3}^*$ having the stated properties is $Q^2 - 1$, 24, 12 and 6 in cases (1)–(4). For $\alpha \in \mathbb{F}_{Q^2}^*$, the polynomial $x^{Q+3} + \alpha x^2$ permutes $\mathbb{F}_{Q^2}$ if and only if $Q = 2$ and $\alpha \neq 1$.

Proof. First assume $\alpha \in \mathbb{F}_{Q^3}^*$. By Theorem 1.1, $x^{Q^2+Q+2} + \alpha x$ permutes $\mathbb{F}_{Q^3}$ if and only if $g_\alpha(x) := x(x+\alpha)(x+\alpha^Q)(x+\alpha^{Q^2})$ permutes $\mathbb{F}_Q$. By Lemma 2.2, the latter condition never occurs if Q is odd, except possibly when $Q \in \{3, 7\}$. Since it is easy to verify the result directly for $Q \leq 7$, we assume henceforth that Q is even and $Q > 2$. In this case, g_α permutes $\mathbb{F}_Q$ if and only if $\alpha + \alpha^Q + \alpha^{Q^2} = 0$ and g_α has no nonzero roots in $\mathbb{F}_Q$, and one easily checks that the latter condition follows from the former since $\alpha \neq 0$.

Now assume $\alpha \in \mathbb{F}_{Q^2}^*$. As above, $x^{Q+3} + \alpha x^2$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(2, Q+1) = 1$ and $g_\alpha(x) := x^2(x+\alpha)(x+\alpha^Q)$ permutes $\mathbb{F}_Q$. The first condition says that Q is even, so if $Q > 2$ then Lemma 2.2 implies that α is not in $\mathbb{F}_Q$ and g_α has no degree-three term, which cannot both occur. Finally, the result is clear when $Q = 2$. □

Finally, using degree-5 permutation polynomials over $\mathbb{F}_Q$ yields the following result.

Corollary 2.5. *Pick any prime power Q, and any $\alpha \in \mathbb{F}_{Q^2}^*$. The polynomial $x^{2Q+3} + \alpha x$ permutes $\mathbb{F}_{Q^2}$ if and only if one of the following holds:*

(1) *$Q \equiv \pm 2 \pmod 5$ and $\alpha^{2Q-2} - 3\alpha^{Q-1} + 1 = 0$;*
(2) *$Q = 5^n$ and either $\alpha^{Q-1} = -1$ or $\alpha^{(Q-1)/2} = -1$;*
(3) *$Q = 13$ and $\alpha^{12} - 3\alpha^6 + 1 = 0$;*
(4) *$Q = 5$ and $\alpha^4 - \alpha^2 + 1 = 0$; or*
(5) *$Q = 3$ and either $\alpha = 1$ or $\alpha^2 = -1$.*

The number of elements $\alpha \in \mathbb{F}_{Q^2}$ having the stated properties is $2Q - 2$ in case (1), $3(Q-1)/2$ in case (2), and 12, 4 and 3 in cases (3), (4) and (5).

Proof. By Theorem 1.1, $x^{2Q+3} + \alpha x$ permutes $\mathbb{F}_{Q^2}$ if and only if $g_\alpha(x) := x(x^2+\alpha)(x^2+\alpha^Q)$ permutes $\mathbb{F}_Q$. The result is easy to verify if $Q \leq 13$, so we assume throughout that $Q > 13$.

First suppose $Q \not\equiv 0 \pmod 5$. By Lemma 2.2, g_α permutes $\mathbb{F}_Q$ if and only if $Q \equiv \pm 2 \pmod 5$ and $g_\alpha(x) = x^5 + \beta x^3 + 5^{-1}\beta^2 x$ for some $\beta \in \mathbb{F}_Q^*$, or equivalently $(x+\alpha)(x+\alpha^Q) = x^2 + \beta x + 5^{-1}\beta^2$. If this last equality holds then

$$\alpha^{Q-1} + \alpha^{1-Q} = \frac{(\alpha^Q + \alpha)^2}{\alpha^{Q+1}} - 2 = \frac{\beta^2}{5^{-1}\beta^2} - 2 = 5 - 2 = 3,$$

so that $\alpha^{2Q-2} - 3\alpha^{Q-1} + 1 = 0$. Conversely, if $\alpha \in \mathbb{F}_{Q^2}^*$ satisfies $\alpha^{2Q-2} - 3\alpha^{Q-1} + 1 = 0$, then $(\alpha^Q + \alpha)^2 = 5\alpha^{Q+1}$, so $\beta := \alpha^Q + \alpha$ satisfies $(x+\alpha)(x+\alpha^Q) = x^2 + \beta x + 5^{-1}\beta^2$. Here $\beta \in \mathbb{F}_Q$, and further $\beta \neq 0$ since otherwise we would have $\alpha^{Q-1} = 1$ so that $\alpha^{2Q-2} - 3\alpha^{Q-1} + 1 = -1$ is nonzero. In case $Q \not\equiv 0 \pmod 5$, it remains only to show that the polynomial $x^{2Q-2} - 3x^{Q-1} + 1$ has $2Q-2$ roots in $\mathbb{F}_{Q^2}^*$. It suffices to show that $x^2 - 3x + 1$ is irreducible over $\mathbb{F}_Q$, since then the roots of this polynomial in $\mathbb{F}_{Q^2}$ are γ and γ^Q; since the product of the roots is 1, it follows that $\gamma^{Q+1} = 1$, so that γ has $(Q-1)$ distinct $(Q-1)$-th roots in $\mathbb{F}_{Q^2}^*$. Thus, we need only show that $x^2 - 3x + 1$ is irreducible over $\mathbb{F}_Q$. To this end, write $Q = p^j$ with p prime; since $Q \equiv \pm 2 \pmod 5$, we see that j is odd and $p \equiv \pm 2 \pmod 5$. Since j is odd, irreducibility of $x^2 - 3x + 1$ over $\mathbb{F}_Q$ is equivalent to irreducibility over $\mathbb{F}_p$. The latter irreducibility is clear if $p = 2$, so assume p is odd. Then $x^2 - 3x + 1$ is irreducible over $\mathbb{F}_p$ if and only if its discriminant (namely 5) is a nonsquare in $\mathbb{F}_p$, which by quadratic reciprocity is the same as requiring that p is a nonsquare in $\mathbb{F}_5$, which indeed is the case since $p \equiv \pm 2 \pmod 5$.

Now suppose $Q \equiv 0 \pmod 5$. Note that if $g_\alpha(x)$ has a term of degree 3, then $g_\alpha(x+\mu)$ has a term of degree 2 for any $\mu \in \mathbb{F}_Q^*$. Thus, Lemma 2.2 implies that g_α permutes $\mathbb{F}_Q$ if and only if either

(1) $\alpha + \alpha^Q = 0$ and $-\alpha^{Q+1}$ is not a fourth power in $\mathbb{F}_Q$, or
(2) $(x+\alpha)(x+\alpha^Q) = x^2 + 2\beta x + \beta^2$ for some nonsquare $\beta \in \mathbb{F}_Q$.

In the first case, since $\alpha^{Q-1} = -1$, we have $\alpha \notin \mathbb{F}_Q$ and $-\alpha^{Q+1} = \alpha^2$, so $-\alpha^{Q+1}$ is a nonsquare in $\mathbb{F}_Q$ and hence is not a fourth power. In the second case, the equality $(x+\alpha)(x+\alpha^Q) = (x+\beta)^2$ occurs just when $\alpha = \beta$. □

3. Complete permutation polynomials

In this section we use the results of the previous section to construct complete permutation polynomials.

Corollary 3.1. *Pick $\alpha \in \mathbb{F}_Q^*$, and put $q = Q^m$ where m and s are positive integers with $\gcd(m, Q-1) = 1$. Then $f(x) := \alpha x^{1+s(q-1)/(Q-1)}$ is a complete permutation polynomial over $\mathbb{F}_q$ if and only if*

(1) $\gcd(1 + s(q-1)/(Q-1), Q-1) = 1$ *and*
(2) $\alpha x^{ms+1} + x$ *permutes* $\mathbb{F}_Q$.

Proof. By Corollary 1.3 with $r = 1$ and $h(x) = \alpha x^s + 1$, we see that $f(x) + x$ permutes $\mathbb{F}_q$ if and only if $g(x) := x^n(\alpha x^s + 1)$ permutes $\mathbb{F}_Q$, where $mn \equiv 1 \pmod{Q-1}$. Since $\gcd(m, Q-1) = 1$, the polynomial x^m permutes $\mathbb{F}_Q$, so $g(x)$ permutes $\mathbb{F}_Q$ if and only if $g(x^m) = x^{mn}(\alpha x^{ms} + 1)$ permutes $\mathbb{F}_Q$. Since $mn \equiv 1 \pmod{Q-1}$, this last condition says that $x(\alpha x^{ms} + 1)$ permutes $\mathbb{F}_Q$. Next, $f(x)$ permutes $\mathbb{F}_q$ if and only if $1 + s(q-1)/(Q-1)$ is coprime to $q-1$; since this number is clearly coprime to $(q-1)/(Q-1)$, it suffices to ensure that it is coprime to $Q-1$. □

One can use Corollary 3.1 to exhibit many families of complete permutation polynomials, by using the various known families of permutation binomials over $\mathbb{F}_Q$. We give only one instance of this, which suffices to answer the open problem in [14].

Corollary 3.2. *If Q is a power of 4, and $\alpha \in \mathbb{F}_Q$ is not a cube, then $\alpha x^{(Q+1)(Q+2)/2+1}$ is a complete permutation polynomial over $\mathbb{F}_{Q^2}$.*

Proof. We apply Corollary 3.1 with $m = 2$ and $s = Q/2 + 1$. Since $1 + s(Q+1) = 4 + (s+1)(Q-1)$ is coprime to $Q-1$, it follows that $\alpha x^{1+s(Q+1)}$ is a complete permutation polynomial over $\mathbb{F}_{Q^2}$ if and only if $\alpha x^{Q+3} + x$ permutes $\mathbb{F}_Q$. This polynomial induces the same function on $\mathbb{F}_Q$ as does $\alpha x^4 + x$. In particular, this function is a homomorphism from the additive group of $\mathbb{F}_Q$ to itself, so it is bijective if and only if its kernel is trivial, which is the case since α is not a cube in $\mathbb{F}_Q$. □

Remark 3.3. The open problem in [14] asked whether there exist complete permutation polynomials over $\mathbb{F}_{2^{2^e}}$. The previous corollary provides complete permutation polynomials more generally over every field $\mathbb{F}_{2^{4d}}$. As noted above, one can produce many further complete permutation polynomials as consequences of Corollary 3.1.

The rest of the results in this section use the permutation polynomials from Corollaries 2.3, 2.4 and 2.5 to produce complete permutation polynomials.

Corollary 3.4. *For $\alpha \in \mathbb{F}_{Q^2}^*$ and $\beta \in \mathbb{F}_Q$, the polynomial $f(x) := \alpha x^{Q+2} + \beta x$ is a complete permutation polynomial over $\mathbb{F}_{Q^2}$ if and only if one of the following holds:*

(1) $Q \equiv 5 \pmod 6$ *and* α^{Q-1} *has order* 6*;*
(2) $Q \equiv 2 \pmod 6$ *and* α^{Q-1} *has order* 3*; or*
(3) $Q \equiv 0 \pmod 3$ *and* $\alpha^{Q-1} = -1$.

Proof. At least one polynomial in $\{f(x), f(x)+x\}$ has terms of degrees $Q+2$ and 1, so by Corollary 2.3 if $f(x)$ is a complete permutation polynomial then $Q \not\equiv 1 \pmod 3$. Conversely, suppose that $Q \not\equiv 1 \pmod 3$. It follows that αx^{Q+2} permutes $\mathbb{F}_{Q^2}$: for, this is equivalent to requiring $\gcd(Q+2, Q^2-1) = 1$, and $\gcd(Q+2, Q^2-1)$ divides $\gcd(Q^2-4, Q^2-1) = \gcd(3, Q-1) = 1$. Each of $f(x)$ and $f(x)+x$ has the form $\alpha x^{Q+2} + \gamma x$ with $\gamma \in \mathbb{F}_Q$, and at least one of them has $\gamma \in \mathbb{F}_Q^*$. Since $\alpha x^{Q+2} + \gamma x$ permutes $\mathbb{F}_{Q^2}$ if and only if $x^{Q+2} + \gamma\alpha^{-1}x$ permutes $\mathbb{F}_{Q^2}$, and $(\gamma\alpha^{-1})^{Q-1} = \alpha^{1-Q}$, the result now follows from Corollary 2.3. □

Corollary 3.5. *For* $\alpha \in \mathbb{F}_{Q^3}^*$ *and* $\beta \in \mathbb{F}_Q$*, the polynomial* $f(x) := \alpha x^{Q^2+Q+2} + \beta x$ *is a complete permutation polynomial over* $\mathbb{F}_{Q^3}$ *if and only if one of the following holds:*

(1) Q *is even and* $\alpha^{Q^2} + \alpha^{Q^2-Q+1} + \alpha = 0$*;*
(2) $Q = 7$ *and* $2\alpha^{24} + 4\alpha^{12} + \alpha^6 + 1 = 0$ *and* $\beta \notin \{0, -1\}$*;*
(3) $Q = 3$ *and* $\alpha^{12} + \alpha^8 + \alpha^2 + 1 = 0$ *and* $\beta = 1$*; or*
(4) $Q = 2$ *and* $\alpha \neq 1$.

Proof. This follows from Corollary 2.4 in the same way that Corollary 3.4 followed from Corollary 2.3. All that is required is to determine when $\gcd(Q^2+Q+2, Q^3-1) = 1$. Note that this gcd is even when Q is odd, so we may assume that Q is even. Now $\gcd(Q^2+Q+2, Q^3-1)$ divides $(Q^2+Q+2)(Q-1) - (Q^3-1) = Q-1$ and hence divides $Q^2+Q+2-(Q-1)(Q+2) = 4$, so $\gcd(Q^2+Q+2, Q^3-1) = 1$ when Q is even. □

Corollary 3.6. *For* $\alpha \in \mathbb{F}_{Q^2}^*$ *and* $\beta \in \mathbb{F}_Q$*, the polynomial* $\alpha x^{2Q+3} + \beta x$ *is a complete permutation polynomial over* $\mathbb{F}_{Q^2}$ *if and only if one of the following holds:*

(1) $Q \equiv \pm 2 \pmod 5$ *and* $\alpha^{2Q-2} - 3\alpha^{Q-1} + 1 = 0$*;*
(2) $Q = 5^n$ *and* $\alpha^{Q-1} = -1$*;*
(3) $Q = 5^n$ *and* $\beta^{(Q-1)/2}, (\beta+1)^{(Q-1)/2} \in \{0, -\alpha^{(Q-1)/2}\}$*;*
(4) $Q = 13$ *and* $\alpha^{12} - 3\alpha^6 + 1 = 0$ *and* $\beta \in \{0, 3, -4, -1\}$*;*
(5) $Q = 13$ *and* $\alpha^{12} + 3\alpha^6 + 1 = 0$ *and* $\beta \in \{5, 6, 7\}$*;*
(6) $Q = 5$ *and* $\alpha^4 - \alpha^2 + 1 = 0$ *and* $\beta \in \{0, -1\}$*;*
(7) $Q = 5$ *and* $\alpha^4 + \alpha^2 + 1 = 0$ *and* $\beta = 2$*;*
(8) $Q = 3$ *and* $\alpha^2 = -1$*; or*
(9) $Q = 3$ *and* $\alpha + \beta = 1$.

Proof. This follows from Corollary 2.5 using the same argument as in the proof of Corollary 3.4. Again, it suffices to determine when $\gcd(2Q+3, Q^2-1) = 1$. Note that $\gcd(2Q+3, Q^2-1)$ equals $\gcd(2Q+3, Q+1) \cdot \gcd(2Q+3, Q-1)$, and since $2Q+3 = 2(Q+1)+1$ and $2Q+3 = 2(Q-1)+5$ we see that $\gcd(2Q+3, Q^2-1) = 1$ if and only if $Q \not\equiv 1 \pmod 5$. □

Remark 3.7. Many further families of complete permutation polynomials can be constructed using the same methods as above. For instance, since the inverse of a complete permutation polynomial is again a complete permutation polynomial, one can use the inverses of the complete permutation polynomials constructed above. These inverses take an especially simple form in case the polynomial itself is a monomial.

4. Mutually orthogonal latin squares

In this section we explain how the permutation polynomials constructed in this paper can be used to produce complete sets of mutually orthogonal latin squares, and consequently to produce projective planes.

We begin by recalling the definitions. A *latin square* of order n is an $n \times n$ matrix with entries from an n-element set S, such that each element of S occurs exactly once in each row and each column. Two such squares $L_1 = [\alpha_{ij}]$ and $L_2 = [\beta_{ij}]$ which have the same set S are called *orthogonal* if every ordered pair in $S \times S$ occurs as $(\alpha_{ij}, \beta_{ij})$ for some i, j. A set of pairwise orthogonal latin squares is called a set of mutually orthogonal latin squares (MOLS). Any set of MOLS of order n has cardinality at most $n-1$, and a set of $n-1$ MOLS of order n is called a *complete* set of MOLS of order n. A classical argument of Bose [2] shows that a complete set of MOLS of order n can be used to produce a projective plane of order n (see also [4, Thm. 5.2.2]).

We will always take S to be the finite field $\mathbb{F}_q$, and we will label the rows and columns of our latin squares by the elements of $\mathbb{F}_q$. In this case, a permutation polynomial f over $\mathbb{F}_q$ corresponds to the latin square whose ij-th entry is $i+f(j)$, and the latin squares corresponding to two permutation polynomials f, g are orthogonal if and only if $f-g$ is a permutation polynomial. Via this correspondence, the following consequences of Corollaries 2.3, 2.4 and 2.5 exhibit complete sets of mutually orthogonal latin squares of order q.

Corollary 4.1. *Let Q be a prime power with $Q \not\equiv 1 \pmod 3$, and let α be any fixed element of $\mathbb{F}_{Q^2}$ for which α^{Q-1} has order either 6 (if $Q \equiv 5 \pmod 6$) or 3 (if $Q \equiv 0 \pmod 2$) or 2 (if $Q \equiv 0 \pmod 3$).*

Then the set of all polynomials $\beta x^{Q+2} + \alpha\gamma x$ *with* $\beta, \gamma \in \mathbb{F}_Q$*, where at least one of* β, γ *is nonzero, corresponds to a complete set of* $Q^2 - 1$ *MOLS of order* Q^2*.*

Corollary 4.2. *Let* Q *be a power of* 2*. Then the set of all polynomials* $\beta x^{Q^2+Q+2} + \alpha x$ *with* $\beta \in \mathbb{F}_Q$ *and* $\alpha^{Q^2} + \alpha^Q + \alpha = 0$*, where at least one of* α, β *is nonzero, corresponds to a complete set of* $Q^3 - 1$ *MOLS of order* Q^3*.*

Corollary 4.3. *Let* Q *be a prime power which is congruent mod* 5 *to either* 0, 2, *or* -2*, and let* α *be any fixed element of* $\mathbb{F}_{Q^2}$ *for which* $\alpha^{2Q-2} - 3\alpha^{Q-1} + 1 = 0$*. Then the set of all polynomials* $\beta x^{2Q+3} + \alpha\gamma x$ *with* $\beta, \gamma \in \mathbb{F}_Q$*, where at least one of* β, γ *is nonzero, corresponds to a complete set of* $Q^2 - 1$ *MOLS of order* Q^2*.*

5. The results of Xu, Cao, Tu, Zeng and Hu

In this section we show how our results imply all three main results in [15], as well as three of the four main results in [12]. We note that the proofs in [12] and [15] involve lengthy computations based on a completely different method than the one in the present note.

The first main result of [15] is [15, Thm. 3.1], which follows from the special case of Corollary 3.4 in which $\beta = 0$ and $Q = 3^j$ with j odd. Note that Corollary 3.4 exhibits complete permutation polynomials for every prime power Q such that $Q \not\equiv 1 \pmod 3$.

Likewise, [12, Thm. 1] follows from the special case of Corollary 3.5 in which $\beta = 0$ and $Q = 2^j$ with $\gcd(j, 3) = 1$. Note that Corollary 3.5 exhibits complete permutation polynomials whenever Q is a power of 2.

Next, [15, Thm. 2] and [15, Thm. 3.3] follow from the special cases of Corollary 3.6 in which $\beta = 0$ and either $Q = 2^j$ or $Q = 3^j$. Note that Corollary 2.5 exhibits complete permutation polynomials for every prime power Q which is congruent to 0, 2 or 3 (mod 5).

The third main result of [15] is an immediate consequence of the following result from our previous paper [19, Cor. 5.3] (which itself is a simple consequence of Lemma 2.1):

Lemma 5.1. *Let* Q *be a prime power, let* r *and* d *be positive integers, and let* β *be a* $(Q+1)$*-th root of unity in* $\mathbb{F}_{Q^2}$*. Then* $x^{r+d(Q-1)} + \beta^{-1}x^r$ *permutes* $\mathbb{F}_{Q^2}$ *if and only if all of the following hold:*

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

By restricting to the case $r = 1$, we obtain the following complete permutation polynomials from this result:

Corollary 5.2. *Let Q be a prime power, let d be a positive integer, and let β be a $(Q+1)$-th root of unity in $\mathbb{F}_{Q^2}$. Then $\beta x^{1+d(Q-1)}$ is a complete permutation polynomial over $\mathbb{F}_{Q^2}$ if and only if all of the following hold:*

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

By restricting to the special case that $2d \mid (Q+1)$, we obtain a stronger version of [15, Thm. 3.5]. By restricting to the special case that Q is even and $d = Q/4 + 1$, we obtain a stronger version of [12, Thm. 3].

The results in this paper do not imply [12, Thm. 4]. That result was proved by using a particular case of a generalization of Lemma 2.1 from [1]. Whereas the proof of Lemma 2.1 involves the multiplicative group of $\mathbb{F}_q$, the proof of [12, Thm. 4] involves instead the additive group of $\mathbb{F}_q$. It would be good to understand the general class of all permutation polynomials which can be produced by variants of the method used to prove [12, Thm. 4].

References

[1] A. Akbary, D. Ghioca and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* **17** (2011), 51–67. 12

[2] R. C. Bose, On the application of the properties of Galois fields to the construction of hyper-Graeco-Latin squares, *Sankhyā* **3** (1938), 323–338. 10

[3] L. Carlitz and D. R. Hayes, Permutations with coefficients in a subfield, *Acta Arith.* **21** (1972), 131–135. 3

[4] J. Dénes and A. D. Keedwell, Latin Squares and their Applications, Academic Press, New York, 1974. 10

[5] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.* **11** (1896/97), 65–120. 4

[6] R. J. Friedlander, B. Gordon and M. D. Miller, On a group sequencing problem of Ringel, in: Proceedings of the Ninth Southeastern Conference on Combinatorics, Graph Theory, and Computing, 307–321, Utilitas Math., Winnipeg, 1978. 1

[7] R. J. Friedlander, B. Gordon and P. Tannenbaum, Partitions of groups and complete mappings, *Pacific J. Math.* **92** (1981), 283–293. 1

[8] H. B. Mann, The construction of orthogonal latin squares, *Ann. Math. Statist.* **13** (1942), 418–423. 1
[9] A. M. Masuda and M. E. Zieve, Permutation binomials over finite fields, *Trans. Amer. Math. Soc.* **361** (2009), 4169–4180. 3
[10] H. Niederreiter and K. H. Robinson, Bol loops of order pq, *Math. Proc. Cambride Philos. Soc.* **89** (1981), 241–256. 1
[11] L. J. Paige, Neofields, *Duke Math. J.* **16** (1949), 39–60. 1
[12] Z. Tu, X. Zeng and L. Hu, Several classes of complete permutation polynomials, *Finite Fields Appl.* **25** (2014), 182–193. 3, 11, 12
[13] T. J. Tucker and M. E. Zieve, Permutation polynomials, curves without points, and Latin squares, preprint, 2000. 3, 5
[14] B. Wu and D. Lin, On constructing complete permutation polynomials over finite fields of even characteristic, arXiv:1310.4358v2 [math.NT], 29 Oct 2013. 3, 8
[15] G. Xu, X. Cao, Z. Tu, X. Zeng and L. Hu, Complete permutation polynomials over finite fields of odd characteristic, arXiv:1312.0930v1 [math.NT], 1 Dec 2013. 3, 11, 12
[16] M. E. Zieve, Some families of permutation polynomials over finite fields, *Internat. J. Number Theory* **4** (2008), 851–857. 3
[17] M. E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, *Proc. Amer. Math. Soc.* **137** (2009), 2209–2216. 3
[18] M. E. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, in *Additive Number Theory*, Springer (2010), 355–359. 3
[19] M. E. Zieve, Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$, arXiv:1310.0776v2 [math.NT], 7 Oct 2013. 3, 11

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

Mathematical Sciences Center, Tsinghua University, Beijing 100084, China

E-mail address: zieve@umich.edu
URL: www.math.lsa.umich.edu/∼zieve/