Finding Nice Permutation Polynomials over Finite Fields

By Karl Wallulis

A MTH 501 – Mathematical Literature Project

Under the direction of Dr. John Caughman IV

2nd Reader: Dr. Derek Garton

Submitted in partial fulfillment of the requirements for the degree of

Masters of Science in Mathematics
Portland State University
Fariborz Maseeh Department of Mathematics & Statistics

June 16, 2017
Introduction.

A polynomial over a finite field $\mathbb{F}_q$ is defined to be a permutation polynomial if it permutes the elements of the field. Permutation polynomials were first studied by Betti, Mathieu and Hermite as a way of representing permutations. In this mathematical literature project, we work through a 2008 paper by Michael E. Zieve [1] that describes a set of necessary and sufficient conditions under which a specific family of polynomials over a finite field $\mathbb{F}_q$ of the form $f(x) = x^r h_k(x^v)^t$ permutes the field, where $h_k(x) := x^{k-1} + x^{k-2} + \cdots + 1$ and $r, k, v$ and $t$ are positive integers. These results coincide with those of previous authors in special cases, but with simpler proofs.

§1 Families of “nice” permutation polynomials.

Recent attention has been focused on finding permutation polynomials of “nice” forms. Akbary, Q. Wang and L. Wang [2, 3] studied binomials in $\mathbb{F}_q$ of the form $f(x) = x^u + x^r$, with the condition that $d := \gcd(q - 1, u - r)$ satisfies $(q - 1)/d \in \{3, 5, 7\}$. They found necessary and sufficient conditions for such polynomials to permute $\mathbb{F}_q$. However, their proofs contained “lengthy calculations involving coefficients of Chebyshev polynomials, lacunary sums of binomial coefficients, determinants of circulant matrices […] among other things” (Zieve pg. 1). Their proofs also required completely different arguments in each of the aforementioned cases.

More recently, Zieve proved a set of necessary and sufficient conditions for a more general family of functions $f(x) = x^r h_k(x^v)^t$ to be permutation polynomials (where $h_k(x) := x^{k-1} + x^{k-2} + \cdots + 1$ and $r, k, v$ and $t$ are positive integers). Note that this family
contains as a subset the family of polynomials \( f(x) = x^u + x^r \), with \( k = 2 \) and \( v = u - r \).

First, the main result (using the notation \( s := \gcd(q - 1, v) \), \( d := (q - 1)/s \), and \( e := v/s \)):

**Proposition 1.1** (Zieve pg. 2) Let \( f(x) = x^r h_k(x^v)^t \), where \( h_k(x) := x^{k-1} + x^{k-2} + \ldots + 1 \) and \( r, k, v \) and \( t \) are positive integers. Then \( f \) permutes \( \mathbb{F}_q \) if and only if all of the following conditions hold:

1. \( \gcd(r, s) = \gcd(d, k) = 1 \)
2. \( \gcd(d, 2r + vt(k - 1)) \leq 2 \)
3. \( k^{st} \equiv (-1)^{(d+1)(r+1)} \) (mod \( p \))
4. \( g(x) := x^r \left( \frac{1-x^{ke}}{1-x^e} \right)^{st} \) is injective on \( \mu_d \setminus \mu_1 \)
5. \( (-1)^{(d+1)(r+1)} \notin g(\mu_d \setminus \mu_1) \)

where, for any positive integer \( i \), the symbol \( \mu_i \) denotes the set of \( i \)th roots of unity.

Conditions 4 and 5 are obviously more complicated than the first three. In the cases \( d \in \{3, 5, 7\} \), if just the first three conditions hold, a corollary allows us to determine whether \( f(x) \) permutes the field from a simpler set of conditions:

**Corollary 1.3** (Zieve pg. 2) Suppose the first three conditions of Proposition 1.1 hold, and \( d \) is an odd prime. Pick \( \omega \in \mathbb{F}_q \) of order \( d \).

1. If
   \[ (*) \quad \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \in \mu_{st} \text{ for every } \zeta \in \mu_d \setminus \mu_1 \]
   Then \( f \) permutes \( \mathbb{F}_q \).
2. If \( d = 3 \) then \( f \) always permutes \( \mathbb{F}_q \).
3. If \( d = 5 \) then \( f \) permutes \( \mathbb{F}_q \) if and only if \( (*) \) holds.
4. If \( d = 7 \) then \( f \) permutes \( \mathbb{F}_q \) if and only if either \( (*) \) holds or there exists \( \epsilon \in \{-1, 1\} \) such that
   \[
   \left( \frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}} \right)^{st} = \omega^{2\epsilon(2r+(k-1)vt)i}
   \]
   for every \( i \in \{1, 2, 4\} \).
Before diving into the proofs, it will serve to go through a worked example in detail. The field $\mathbb{F}_{16}$ should be simple enough to allow for computations by hand but rich enough to demonstrate the complexity of the algebra. Line (2) of Corollary 1.3 gives us a great foothold for finding a permutation polynomial within this field: we simply need positive integers $r, v, k$ and $t$ satisfying $d = 3$ and meeting the first three conditions of Proposition 1.1. Since $q = 16$, we must have $d = 15/s = 3$, so $s = 5$. As $s = \gcd(15, v)$, we can choose $v = 5$. Choosing $r = 4$, $k = 5$ and $t = 1$ satisfies Conditions 1-3 of Proposition 1.1, as $\gcd(4, 5) = \gcd(3, 5) = 1, \gcd(3, 2(4) + 5(4)) = \gcd(3, 28) \leq 2$ and $5^5 = (-1)^{20} \pmod{2}$. Our chosen polynomial is therefore

$$f(x) = x^4 h_5(x^5) = x^4(x^{20} + x^{15} + x^{10} + x^5 + 1)$$

which we hope to see permute the elements of the field $\mathbb{F}_{16}$.

Now that we have defined our polynomial, if we are to find its image in $\mathbb{F}_{16}$ we need a characterization of the field that allows for straightforward evaluation of polynomials. It is a basic result of abstract algebra that every finite field is a finite extension of a prime field $\mathbb{F}_p$, $p$ a prime, with $\mathbb{F}_p \approx \mathbb{Z}_p$. Therefore, $\mathbb{F}_{16}$ is an extension of degree 4 over the prime field $\mathbb{F}_2 \approx \mathbb{Z}_2$. This finite extension can be obtained by taking the quotient of $\mathbb{Z}_2[x]$ by the ideal generated by an irreducible polynomial $p(x)$ of degree 4 in $\mathbb{Z}_2[x]$. The polynomial $p(x) = x^4 + x + 1$ meets these conditions, therefore $\mathbb{F}_{16} \approx \mathbb{Z}_2[x] / \langle p(x) \rangle$. The elements of $\mathbb{F}_{16}$ can then be expressed as the sixteen distinct residue classes under division of polynomials in $\mathbb{Z}_2[x]$ by $p(x)$, which means every element corresponds bijectively to a polynomial of degree less than 4 in $\mathbb{Z}_2[x]$. 
Even using this representation, evaluating $f(x)$ would still be a chore – consider evaluating 

$$f(x^3 + x + 1) = (x^3 + x + 1)^4 \left( (x^3 + x + 1)^{20} + (x^3 + x + 1)^{15} + \cdots + 1 \right)$$

by hand. To further simplify matters, we make use of the fact that the nonzero elements of a finite field comprise a cyclic multiplicative subgroup $\mathbb{F}_q^*$, and we can therefore express all nonzero elements of $\mathbb{F}_{16}$ as powers of any generator $\beta$ of this group. It so happens that in $\mathbb{F}_{16}$, the element $\beta := x + <p(x)>$ is a generator of the group, and we have

\[
\begin{align*}
\beta^2 &= x^2 \\
\beta^4 &= x + 1 \\
\beta^5 &= x^2 + x \\
\beta^6 &= x^3 + x^2 \\
\beta^8 &= x^2 + 1 \\
\beta^{10} &= x^2 + x + 1 \\
\beta^{11} &= x^3 + x^2 + x \\
\beta^{12} &= x^3 + x^2 + x + 1 \\
\beta^{13} &= x^3 + x^2 + 1 \\
\beta^{14} &= x^3 + 1 \\
\beta^{15} &= 1
\end{align*}
\]

(all mod $<p(x)>$).

This representation of the elements of $\mathbb{F}_{16}$ permits straightforward evaluation of our polynomial $f(x) = x^4 h_5(x^5) = x^4(x^{20} + x^{15} + x^{10} + x^5 + 1)$ by hand. For example,

\[
\begin{align*}
\beta^7 &= x^4 \\
f(x^3 + x + 1) &= f(\beta^7) = (\beta^7)^4((\beta^7)^{20} + (\beta^7)^{15} + \cdots + 1) \\
&= \beta^{28}(\beta^{140} + \beta^{105} + \beta^{70} + \beta^{35} + 1) = \beta^{13}(\beta^5 + 1 + \beta^{10} + \beta^5 + 1) \\
&= \beta^{13}(\beta^{10}) = \beta^8 = x^2 + 1
\end{align*}
\]

It is no coincidence that $f(\beta^7) = \beta^{15-7}$. This polynomial has the interesting property that $f(\beta^k) = \beta^{15-k}$ over $\mathbb{F}_{16}$ (the motivated reader can verify this using similar computations as above for the other elements of $\mathbb{F}_{16}^*$). This, together with the fact that $f(0) = 0$, proves that $f(x)$ is indeed a permutation polynomial over $\mathbb{F}_{16}$, as we hoped.
§2  An important preliminary lemma.

We begin with a preliminary lemma that defines an auxiliary polynomial of great use in the proof of the main proposition. We show that the question of whether \( f(x) \) permutes \( \mathbb{F}_q \) can be reduced to whether this auxiliary polynomial permutes the \( d \)th roots of unity \( \mu_d \) of \( \mathbb{F}_q \).

**Lemma 2.1** (Zieve pg. 3)  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. \( \gcd(r, (q - 1)/d) = 1 \)
2. \( x^r h(x)^{(q - 1)/d} \) permutes \( \mu_d \)

**Proof.**  Let (a) denote the statement “\( f(x) \) permutes \( \mathbb{F}_q \)” Zieve proves that (a) \( \leftrightarrow (1) \cap (2) \) by showing that (a) implies (1) and that (1) implies the equivalence of (a) and (2). The underlying logic ought to be made explicit:

1. \( a \rightarrow 1 \)
2. \( \text{If } 1, a \leftrightarrow 2 \)
   a. \( \therefore a \rightarrow 2 \)
   b. \( \therefore a \rightarrow 1 \land 2 \)
3. \( \therefore 1 \land 2 \rightarrow a \)
4. \( \therefore a \leftrightarrow 1 \land 2 \)

We need to show that if \( f(x) \) permutes \( \mathbb{F}_q \) then \( \gcd(r, (q - 1)/d) = 1 \). Let \( s := (q - 1)/d \). Assume that \( f(x) \) permutes \( \mathbb{F}_q \) and assume by way of contradiction that \( \gcd(r, s) = g > 1 \). We can then write \( r = r' g, s = s' g \) (\( r', s' \in \mathbb{Z}^+ \)). For \( \zeta \in \mu_s \), we have

\[
f(\zeta x) = (\zeta x)^r h((\zeta x)^s) = \zeta^r x^r h(x^s) = \zeta^r f(x)
\]

Choose \( \zeta^{s'} \) with \( \zeta \) primitive, so that \( \zeta^{s'} \neq 1 \). We have
\[ f(\zeta^s x) = (\zeta^s)^r f(x) = (\zeta^s)^{r' g} f(x) = (\zeta^s g)^{r' f}(x) = (\zeta^s r') f(x) = f(x), \]
so \( f(x) \) fails to permute \( \mathbb{F}_q \), a contradiction.

We must now show that if \( \gcd(r, s) = 1 \), then \( f(x) \) permutes \( \mathbb{F}_q \) if and only if
\[ g(x) := x^r h(x)^s \] permutes \( \mu_d \) and then the proof will be complete. To show this, Zieve first argues that if \( \gcd(r, s) = 1 \), then the values of \( f \) on \( \mathbb{F}_q \) consist of all the \( s \)th roots of the values of \( f(x)^s = x^{rs} h(x^s)^s \) (pg. 3). To see why this is the case, pick a nonzero value in the range of \( f(x)^s = x^{rs} h(x^s)^s \). We have \( x = \beta^k \) for a generator \( \beta \) of \( \mathbb{F}_q^* \). If we can show that the set
\[ \Gamma := \{ f(\beta^{k+nd}), n \in \{1, 2, \ldots, s\} \} \]
consists of \( s \) distinct elements in the range of \( f(x) \) and that for all \( n \), \( f(\beta^{k+nd})^s = f(\beta^k)^s \), then we are done.

Recall that \( d = (q - 1)/s \), so \( x^{sd} = x^{q-1} = 1 \) for all \( x \in \mathbb{F}_q \). We have
\[ f(\beta^{k+nd}) = (\beta^{k+nd})^r h((\beta^{k+nd})^s) = \beta^{kr} (\beta^{dr})^n h(\beta^{ks}) \]
The order of \( \beta^{dr} \) in \( \mathbb{F}_q \) is
\[ \frac{q - 1}{\gcd(dr, q - 1)} = \frac{q - 1}{d \gcd(r, s)} = \frac{q - 1}{d} = s \]
Therefore, each of the elements of \( \Gamma \) are distinct. Finally, we have
\[ f(\beta^{k+nd})^s = (\beta^{k+nd})^{rs} h((\beta^{k+nd})^s)^s = (\beta^k)^{rs} (h(\beta^{ks}))^s = f(\beta^k)^s \]
and we’re done.

With that important fact established, the rest of the proof is straightforward. It is at this point that we first use the important auxiliary polynomial \( g(x) \). We see that the values
of $f(x)^s$ consist of $f(0) = 0$ and all the values of $g(x) = x^r h(x)^s$ on $(\mathbb{F}_q^*)^s$. It follows that if $g(x)$ permutes the elements of $(\mathbb{F}_q^*)^s = \mu_d$, then the range of $f(x)$, which consists of all of the $s$th roots of the elements in the range of $g(x)$, will be all of $\mathbb{F}_q$. And if $g(x)$ fails to permute $\mu_d$, then $f(x)$ will consist only of the set of $s$th roots of a proper subset of $\mu_d$, and consequently will not permute $\mathbb{F}_q$. \hfill \Box$

Returning to our worked example of $f(x) = x^4 h_5(x^5)$ in $\mathbb{F}_{16}$, where $h_5(x) = x^4 + x^3 + \cdots + 1$, we hope to have

$$g(x) = x^4(x^4 + x^3 + \cdots + 1)^5$$

permute $\mu_3 = \{1, \beta^5, \beta^{10}\}$. We have $g(1) = (1 + 1 + 1 + 1 + 1)^5 = 1$, $g(\beta^5) = \beta^{20} (\beta^{20} + \beta^{15} + \beta^{10} + \beta^5 + 1)^5 = \beta^5 (\beta^5 + 1 + \beta^{10} + \beta^5 + 1)^5 = \beta^5 (\beta^{10})^5 = \beta^{55} = \beta^{10}$, and

$g(\beta^{10}) = \beta^{60} (\beta^{40} + \beta^{30} + \beta^{20} + \beta^{10} + 1)^5 = \beta^{10} (\beta^{10} + 1 + \beta^{10} + \beta^5 + 1)^5 = \beta^{10} (\beta^5)^5 = \beta^{35} = \beta^5$.

The auxiliary polynomial $g(x)$ proves to be a useful tool for producing simple results. For the next two propositions, we use the notation $f(x) = x^r h_k(x^v)^t$ (where $h_k(x) := x^{k-1} + x^{k-2} + \cdots + 1$ and $r, k, v$ and $t$ are positive integers) and $s := \gcd(q - 1, v)$, $d := (q - 1)/s$, $e := v/s$.

**Proposition 3.1** (Zieve pg. 4) If $d = 1$ then $f(x)$ permutes $\mathbb{F}_q$ if and only if $\gcd(k, p) = \gcd(r, s) = 1$. If $d = 2$ then $f(x)$ permutes $\mathbb{F}_q$ if and only if $\gcd(k, 2) = \gcd(r, s) = 1$ and $k^s = (-1)^{r+1} \pmod{p}$.

*Proof.* These results follow easily from Lemma 2.1. Note that $g(x)$ is obtained from $f(x)$ by replacing $h_k(x^{q-1/d})$ with $h_k(x^{(q-1)/d})$. Given the above definition of $f(x)$, we then have $g(x) = x^r h_k(x^e)^t$. If $d = 1$, then $\mu_d = \mu_1 = \{1\}$, so we only need $\gcd(r, s) = 1$ and
Wallulis 9

\[ g(1) = 1. \] But we have

\[ g(1) = (1)^r (1 + 1 + \cdots + 1)^{st} = k^{st} = k^{(q-1)t} \]

(note that \( d = 1 \) implies \( s = q - 1 \), so \( g(x) \) permutes \( \mu_d \) if and only if \( \gcd(k, p) = 1 \).

If \( d = 2 \), then \( g(x) \) acts on \( \mu_2 = \{-1, 1\} \). We still have \( g(1) = k^{st} \), and we also have

\[ g(-1) = (-1)^r h_k (-1^e)^{st} = (-1)^r ((-1^e)^{k-1} + \cdots + 1)^{st} \]

This implies that \( k \) must be odd (otherwise \( g(-1) = 0 \)), and consequently \( g(-1) = (-1)^r \),
which in turn forces \( g(1) = k^{st} \) to be \( (-1)^{r+1} \) (mod \( p \)).

\[ \Box \]

§3 Main proposition and two useful corollaries.

We are finally ready for the main result. I will deviate slightly from Zieve's version for reasons explained in a subsequent remark.

**Proposition.** \( f \) permutes \( \mathbb{F}_q \) if and only if all of the following conditions hold:

1. \( \gcd(r, s) = \gcd(d, k) = 1 \)
2. \( k^{st} \equiv (-1)^{(d+1)(r+1)} \) (mod \( p \))
3. \( g(x) := x^r \left( \frac{1 - x^{ke}}{1 - x^e} \right)^{st} \) is injective on \( \mu_d \setminus \mu_1 \)
4. \( (-1)^{(d+1)(r+1)} \notin g(\mu_d \setminus \mu_1) \)

**Proof.** \( f \) permutes \( \mathbb{F}_q \) \( \Rightarrow \) (1) – (4)

We established in Lemma 2.1 that \( f \) permutes \( \mathbb{F}_q \) if and only if \( \gcd(r, s) = 1 \) and

\( \hat{g}(x) := x^r h_k (x^e)^{st} \) permutes \( \mu_d \). Assume throughout that \( \gcd(r, s) = 1 \) and \( \hat{g}(x) \) permutes \( \mu_d \). We will show that \( \gcd(d, k) = 1 \) and (2) – (4) must hold. For \( \zeta \in \mu_d \setminus \mu_1 \), we have

\[ \hat{g}(x) = \zeta^r \left( \frac{1 - \zeta^{ke}}{1 - \zeta^e} \right)^{st}. \]
If $\zeta \in \mu_{ke}$, then $\hat{g}(\zeta) = 0$. So for $\hat{g}$ to permute $\mu_{d}$, we need $\gcd(d, k) = 1$. To see why, assume by way of contradiction that $\gcd(d, k) = m > 1$; we can then write $d = md', k = mk'$. For a primitive $\zeta \in \mu_{d}$, we see that

$$\hat{g}(\zeta^{dr}) = \left( \frac{1 - \zeta^{md'ke}}{1 - \zeta^e} \right)^{st} = \left( \frac{1 - \zeta^{dk'e}}{1 - \zeta^e} \right)^{st} = 0$$

so $\hat{g}$ does not permute $\mu_{d}$, a contradiction.

Recall that $\hat{g}(1) = k^{st}$. Since $\hat{g}$ permutes $\mu_{d}$, we have

$$\prod_{\zeta \in \mu_{d}} \hat{g}(\zeta) = \prod_{\zeta \in \mu_{d}} e^{i \frac{2 \pi k \zeta}{d}} = e^{i \frac{2 \pi}{d} \sum_{k=1}^{d} \frac{2 \pi k}{d}} = e^{i \frac{2 \pi}{d} \frac{d+1}{2}} = e^{i \pi (d+1)} = (-1)^{d+1}$$

Additionally,

$$\prod_{\zeta \in \mu_{d}} \hat{g}(\zeta) = k^{st} \prod_{\zeta \in \mu_{d} \setminus \mu_1} \zeta^{r} \left( \frac{1 - \zeta^{ke}}{1 - \zeta^e} \right)^{st}$$

Since $\gcd(d, k) = 1$, for all $\zeta \in \mu_{d}$, $0 < i < j < d - 1$, $\zeta^{ik} = \zeta^{jk} \Rightarrow \zeta^{(j-i)k} = 1 \Rightarrow i = j$, so $\zeta^{k}$ permutes $\mu_{d}$, therefore

$$\prod_{\zeta \in \mu_{d} \setminus \mu_1} \left( \frac{1 - \zeta^{ke}}{1 - \zeta^e} \right)^{st} = 1.$$ 

Therefore, we have $(-1)^{d+1} = k^{st} (-1)^{(d+1) r}$, so $k^{st} = (-1)^{(d+1)(r+1)}$.

Finally, (3) and (4) follow from the fact that $\hat{g}(x)$ permutes $\mu_{d}$ and $\hat{g}(1) = k^{st} = (-1)^{(d+1)(r+1)}$. 

Wallulis 10
For $\zeta \in \mu_d \setminus \mu_1$, we have

$$\left[\frac{1 - \zeta^{ke}}{1 - \zeta^e}\right]^{st} \in \mu_d$$

(since $\gcd(d, k) = \gcd(d, e) = 1$) and $(\mathbb{F}_q^*)^s = \mu_d$. From (2), we have $\hat{g}(1) = k^{st} = (-1)^{(d+1)(r+1)}(mod\ p)$, so $\hat{g}(1) \in \mu_d$. Therefore $\hat{g}(x) := x^r h_k(x^e)^{st}$ maps $\mu_d$ into $\mu_d$, so that bijectivity is equivalent to injectivity. From (3) and (4), we have

$$g(x) := x^r \left[\frac{1 - x^{ke}}{1 - x^e}\right]^{st}$$

is injective on $\mu_d \setminus \mu_1$ and $\hat{g}(1) \notin g(\mu_d \setminus \mu_1)$, so $\hat{g}$ is injective and therefore bijective on $\mu_d$.

Since $\gcd(r, s) = 1$, $f$ permutes $\mathbb{F}_q$ by Lemma 2.1. \qed

**Remark.** Zieve put an extra condition (pg. 4) that I believe to be superfluous and only included as an aid in the corollaries:

$$\gcd(d, 2r + vt(k - 1) \leq 2$$

This is a necessary condition for $g$ to permute $\mu_d$ (and therefore for $f$ to permute $\mathbb{F}_q$), but it is implied by condition (3), which gives injectivity of $g(x)$ on $\mu_d \setminus \mu_1$.

**Proof.** As $\hat{g}(x)$ permutes $\mu_d$, we must have $g(\zeta) \neq g(1/\zeta)$ if $\zeta \neq (1/\zeta)$. But

$$\hat{g}(\zeta) = \frac{\zeta^r}{\zeta^{2r}} \left[\frac{1 - \zeta^{ke}}{1 - \zeta^e}\right]^{st} = \zeta^{-r} \left[\frac{(\zeta^{-ke} - 1)\zeta^e}{1 - \zeta^e}\right]^{st} = \zeta^{-r} \left[\frac{1 - \zeta^{-ke}}{1 - \zeta^{-e}}\right]^{st} = \hat{g}(1/\zeta).$$
Therefore, if \( g(\zeta) \neq g(1/\zeta) \), then \( \zeta^{2r+est(k-1)} \neq 1 \). Let \( m = 2r + est(k - 1) \). Assume by way of contradiction that \( \gcd(d, m) = g > 2 \). We can then write \( m = m'g \) and \( d = d'g \) for \( m' < m, d' < d \). For a primitive \( \zeta \in \mu_d \), we clearly have \( \zeta^{d'} \neq \zeta^{-d'} \) (since \( g > 2 \)). But

\[
(\zeta^{d'})^m = (\zeta^{d'})^{mg} = (\zeta^{d'}g)^{mr} = (\zeta^d)^{mr} = 1
\]

Therefore \( g(\zeta^{d'}) = g(1/\zeta^{d'}) \), a contradiction. Thus, \( \gcd(d, 2r + vt(k - 1)) \leq 2 \). \( \square \)

The next two corollaries follow logically from Zieve's version of Proposition 3.2, so I will reproduce it here for the sake of the reader:

**Proposition 3.2** (Zieve pg. 4) \( f \) permutes \( \mathbb{F}_q \) if and only if all of the following conditions hold:

1. \( \gcd(r, s) = \gcd(d, k) = 1 \)
2. \( \gcd(d, 2r + vt(k - 1)) \leq 2 \)
3. \( k^{st} \equiv (-1)^{(d+1)(r+1)} \pmod{p} \)
4. \( g(x) := x^r \left( \frac{1-x^{ke}}{1-x^e} \right)^{st} \) is injective on \( \mu_d \setminus \mu_1 \)
5. \( (-1)^{(d+1)(r+1)} \notin g(\mu_d \setminus \mu_1) \)

The first three conditions of Proposition 3.2 can be easily checked, while the last two require significantly more work. The work is simplified if \( d \) is an odd prime (even more so if it is a small one). In this case, we have a corollary that assumes the first three conditions of Proposition 3.2 and identifies a polynomial \( \chi(x) = nx + \theta(x^2) \in \mathbb{F}_d[x] \) that permutes \( \mathbb{F}_d \) if and only if \( f \) permutes \( \mathbb{F}_q \).

**Corollary 3.3** (Zieve pg. 5) Suppose the first three conditions of Proposition 3.2 hold, and \( d \) is an odd prime. Pick \( \omega \in \mathbb{F}_q \) of order \( d \). Then \( f \) permutes \( \mathbb{F}_q \) if and only if there exists \( \theta \in \mathbb{F}_d[x] \) with \( \theta(0) = 0 \) and \( \deg(\theta) < (d - 1)/2 \) such that \((2r + (k - 1)vt)x + \theta(x^2)\) permutes \( \mathbb{F}_q \) and, for every \( i \) with \( 0 < i < d/2 \), we have

\[
\omega^{\theta(i^2)} = \left( \frac{\omega^l \omega^{-l} e - \omega^{-l} e}{\omega^l e - \omega^{-l} e} \right)^{st}.
\]
Proof. Our focus will be on \( g(\zeta^2), \zeta \in \mu_d \setminus \mu_1, \) with \( g(x) \) defined as earlier. As a preliminary step, we show that squaring permutes \( \mu_d \) if \( d \) is odd. As \( \mu_d \) is a cyclic group of order \( (d - 1) \), we have \( \mu_d = \{1, \beta, \beta^2, ..., \beta^{d-1}\} \) for a primitive \( \beta \in \mu_d \). Assume by way of contradiction that squaring does not permute \( \mu_d \); then \( \beta^{2a} = \beta^{2b} \) for some \( a \) and \( b, 0 \leq a < b < d \). Then \( \beta^{2(b-a)} = 1 \Rightarrow d \mid (b - a) \) (as \( d \) is odd), a contradiction.

Since squaring permutes \( \mu_d \), condition (4) of Proposition 3.2 is equivalent to injectivity of \( g(\zeta^2) \) on \( \mu_d \setminus \mu_1 \). For \( \zeta \in \mu_d \setminus \mu_1 \), we have \( g(\zeta^2) = \zeta^{2r} \left( \frac{1-\zeta^{2ke}}{1-\zeta^{2e}} \right)^{st} \). But

\[
\left( \frac{1 - \zeta^{2ke}}{(1 - \zeta^{2e})(\zeta^{e(k-1)})} \right) = \left( \frac{1 - \zeta^{2ke}}{\zeta^{e(k-1)} - \zeta^{e(k+1)}} \right) = \left( \frac{1 - \zeta^{2ke}}{\zeta^{ke}(\zeta^{-e} - \zeta^{e})} \right) = \left( \frac{\zeta^{-ke} - \zeta^{ke}}{\zeta^{-e} - \zeta^{e}} \right)
\]

So

\[
(a) \quad g(\zeta^2) = \zeta^{2r+est(k-1)} \left( \frac{\zeta^{ke} - \zeta^{-ke}}{\zeta^{-e} - \zeta^{e}} \right)^{st}
\]

For \( i \in \mathbb{Z} \setminus d\mathbb{Z} \), let \( \psi(i) \) be the unique element of \( \mathbb{Z}/d\mathbb{Z} \) such that

\[
(b) \quad \omega^{\psi(i)} = \left( \frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}} \right)^{st}
\]

Which is guaranteed to exist and be unique since \( \gcd(d, ke) = 1 \) and \( \omega \) has order \( d \). If we let \( \psi(i) = 0 \) for \( i \in d\mathbb{Z} \), then \( \psi \) induces a map from \( \mathbb{Z}/d\mathbb{Z} \) to itself, with the properties \( \psi(-i) = \psi(i) \) and \( g(\omega^{2i}) = \omega^{i(2r+st(k-1))} \) (Zieve pg. 5). We have \( \psi(-i) = \psi(i) \) because \( \left( \frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}} \right) = -\left( \frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}} \right) \), and by (a) and (b),

\[
g(\omega^{2i}) = \omega^{2r+est(k-1)} \omega^{\psi(i)} = \omega^{i(2r+st(k-1))} \psi(i)
\]

Observe that Conditions (4) and (5) of Proposition 3.2, which guarantee that \( \tilde{g} \) permutes
If \( d \), are equivalent to the bijectivity of the map \( \chi : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \) given by \( \chi(i) = ni + \psi(i) \) (with \( n := 2r + (k - 1)vt \)). Since \( \psi(-i) = \psi(i) \), we must have a \( \theta(i^2) \in \mathbb{F}_d[x] \) of degree less than \( (d - 1)/2 \) (since \( i \) is of order \( (d - 1) \) with \( \theta(i^2) = \psi(i) \), and \( \theta(0) = 0 \). This completes the proof. \( \square \)

We first reduced the question of whether a polynomial \( f \in \mathbb{F}_q[x] \) permutes \( \mathbb{F}_q \) to whether a related polynomial permutes the smaller group \( \mu_d \). Corollary 3.3 now allows to consider only whether the related polynomial \( \chi = ni + \theta(i^2) \) permutes \( \mathbb{F}_q \). As earlier, considering small values of \( d \) gives us simple and useful results. Let \( \tilde{\theta} \) denote \( \theta/n \). For \( d = 3 \) and \( d = 5 \), only the trivial \( \tilde{\theta} = 0 \) gives us bijectivity of \( \chi \), as proven by Betti in 1851 [4]. For \( d = 7 \), bijectivity of \( \chi \) holds if and only if \( \tilde{\theta} = \mu x^2 \) where \( \mu \in \{0, 2, -2\} \), proven by Hermite in 1863 [5]. For \( d = 11 \), “there are 25 possibilities for \( \tilde{\theta} \), but these comprise just five classes modulo the equivalence \( \tilde{\theta}(x) \sim \tilde{\theta}(\alpha^2 x)/\alpha \) with \( \alpha \in \mathbb{F}_d^* \)” (Zieve pg. 6). We collect these results in a final corollary.

**Corollary 3.4** (Zieve pg. 6) Suppose the first three conditions of Proposition 3.2 hold, and \( d \) is an odd prime. Pick \( \omega \in \mathbb{F}_q \) of order \( d \).

(a) If
\[
(*) \quad \frac{\xi^k - \xi^{-k}}{\xi - \xi^{-1}} \in \mu_{st} \text{ for every } \xi \in \mu_d \setminus \mu_1
\]
then \( f \) permutes \( \mathbb{F}_q \).

(b) If \( d = 3 \) then \( f \) always permutes \( \mathbb{F}_q \).

(c) If \( d = 5 \) then \( f \) permutes \( \mathbb{F}_q \) if and only if \( (*) \) holds.

(d) If \( d = 7 \) then \( f \) permutes \( \mathbb{F}_q \) if and only if either \( (*) \) holds or there exists \( \epsilon \in \{-1, 1\} \) such that
\[
\left( \frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}} \right)^{st} = \omega^{2\epsilon(2r + (k - 1)vt)i}
\]
for every \( i \in \{1, 2, 4\} \).

(e) If \( d = 11 \) then \( f \) permutes \( \mathbb{F}_q \) if and only if either \( (*) \) holds or there is some \( \psi \in \mathcal{C} \) such that
For every $i \in (\mathbb{F}^{11}_1)^2$, where $C$ is the union of the sets $\{mi : m \in \{\pm 3, \pm 5\}\}$, $\{5m^3i^3 + m^7i^3 - 2mi^2 - 4m^5i : m \in \mathbb{F}^{11}_1\}$, and $\{4m^3i^4 + m^7i^3 - 2mi^2 - 5m^5i : m \in \mathbb{F}^{11}_1\}$.

**Proof.** Recall that for $d \in \{3, 5\}$, only the trivial $\theta = 0$ meets the conditions of Corollary 3.3. Therefore, we have

$$\omega^{\theta(i^2)} = 1 = \left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st}$$

which gives us condition (*):

$$\frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} \in \mu_{st}$$

for every $\zeta \in \mu_d \setminus \mu_1$. So for $d = 5$, $f$ permutes $\mathbb{F}_q$ if and only if (*) holds.

For $d = 3$, Condition (1) of Proposition 3.2 gives us $\gcd(d, k) = 1 \Rightarrow k \equiv \pm 1 \pmod{3}$ so $(\zeta^k - \zeta^{-k}) = \pm (\zeta - \zeta^{-1})$. As $q - 1 = sd$, either $q$ or $s$ is even. If $s$ is even, then $(\zeta^k - \zeta^{-k})^s = (\zeta - \zeta^{-1})^s$, so (*) holds. If $q$ is even, then $p = 2$, so $(\zeta^k - \zeta^{-k}) \equiv (\zeta - \zeta^{-1}) \pmod{2}$, and again (*) holds. Therefore, if $d = 3$, $f$ permutes $\mathbb{F}_q$.

For $d = 7$, we must have $\theta = \mu x^2$ where $\mu \in \{0, 2n, -2n\}$. From Corollary 3.3, we therefore must have

$$\omega^{\theta(i^2)} = \omega^{2\epsilon(2r+(k-1)v)t_i^4} = \left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st}$$

for $(i^2 | i \in \mathbb{Z}/7\mathbb{Z}) = \{1, 2, 4\}$. But in $\mathbb{F}_7$, $1^4 \equiv 1, 2^4 \equiv 2, \text{ and } 4^4 \equiv 4$, so we can write

$$\omega^{2\epsilon(2r+(k-1)v)t_i} = \left(\frac{\omega^{ike} - \omega^{-ike}}{\omega^{ie} - \omega^{-ie}}\right)^{st}$$

The case $d = 11$ is treated similarly. □
References


