Journal der mathematiſchen Ablehnungen

Paper No.33 (2015)

A general representation theory for constructing groups of permutation polynomials

Chris Castillo and Robert S. Coulter

Department of Mathematical Sciences, University of Delaware

AMS Subject class: 11T06, 12E10, 20C99

Keywords: finite field, permutation polynomial, regular representation, equivalent representations

Note: This is a personal preprint; for correct page numbering and references please see the original paper, the proper citation for which is:

C. Castillo and R.S. Coulter, *A general representation theory for constructing groups of permutation polynomials*, Finite Fields Appl. **35** (2015), 172–203.

Abstract

Using the left regular action of a group on itself, we develop a general representation theory for constructing groups of permutation polynomials. As an application of the method, we compute polynomial representations of several abelian and nonabelian groups, and we determine the equivalence classes of the groups of polynomials we construct. In particular, when the size of the group is equal to the size of the field in which the group is represented, all non-identity representation polynomials are necessarily fixed-point free permutation polynomials.

§ 1. Introduction

We begin by fixing some notation. Throughout, we will let $q = p^n$ for some prime p and let $\mathbb{F}_q$ denote the finite field of order q. The multiplicative group of $\mathbb{F}_q$ will be denoted $\mathbb{F}_q^\times = \langle\zeta\rangle$ for some fixed, but arbitrary, primitive element ζ of $\mathbb{F}_q$. We will be concerned with elements of $\mathbb{F}_q[X]$, the ring of polynomials over $\mathbb{F}_q$ in the indeterminate X. Any function $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial $f \in \mathbb{F}_q[X]$, for example, via the interpolation formula

$$f(X) = \sum_{x\in\mathbb{F}_q} \left(1 - (X-x)^{q-1}\right)\varphi(x).$$

This representation is unique if one restricts the degree of the polynomials to less than q; polynomials in $\mathbb{F}_q[X]$ with degree less than q are called *reduced*. If, under evaluation, a polynomial $f \in \mathbb{F}_q[X]$ induces a bijection on $\mathbb{F}_q$, then we call $f(X)$ a *permutation polynomial* over $\mathbb{F}_q$.

This paper is motivated by two problems concerning permutation polynomials. The first problem is to find new classes of permutation polynomials (problem P2 in [9]). Permutation polynomials are a central object of study in finite field theory, and determining whether a given polynomial is a permutation polynomial is a non-trivial task. Hermite [8] proved the initial results over prime fields, introducing the criterion that now bears his name, and Dickson [6] expanded these to arbitrary finite fields. While it is a simple exercise to show that the monomial X^k is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$, much less simple is the result by Matthews [11] that the "all-ones" polynomial $h_k(X) = 1 + X + X^2 + \cdots + X^k$ is a permutation polynomial over $\mathbb{F}_q$ (of odd characteristic) if and only if $k \equiv 1 \pmod{p(q-1)}$. The reader who is interested in the basic theory of permutation polynomials is referred to Chapter 7 of [10], which is a standard reference in the field.

The second problem is concerned with representation theory and the structure of permutation polynomials. A *representation* is a homomorphism $G \to \mathrm{Sym}(S)$ of a group G into the group of symmetries of some object S. When G is finite and S is a set of cardinality $|G|$, the representation is called a *permutation representation*. In this paper, we will investigate a certain type of permutation representation. Taking the set S to be the underlying set of a finite field $\mathbb{F}_q$, we can consider $\mathrm{Sym}(S)$ to be the set of reduced permutation polynomials over $\mathbb{F}_q$. Since two reduced permutation polynomials can be composed and reduced modulo $X^q - X$ to produce another, it is natural to investigate the types of permutation groups that can be represented by certain permutation polynomials.

There are several other results describing groups of permutation polynomials with relatively simple polynomial generators. For example, Carlitz [4] showed the full symmetric group on q letters can be generated by X^{q-2} and all linear polynomials in $\mathbb{F}_q[X]$, while Wells determined polynomial generators for several small-index subgroups of S_q in [15]. Additionally, Wan and Lidl [14], in the course of proving when polynomials of the form $X^r f(X^s)$ were permutation polynomials, also determined that they have the group structure of a generalized wreath product.

We are interested specifically in whether it is possible to represent given groups of order roughly q by permutation polynomials over $\mathbb{F}_q$. This is possible in the loosest sense via a consideration of the standard proof of Cayley's Theorem, so we focus on the question of whether some groups can be represented by permutation polynomials that are aesthetically pleasing in some way. For example, it is easy to see that the elementary abelian group of order q can be represented by the set of (permutation) polynomials $\{X + a : a \in \mathbb{F}_q\}$, while the cyclic group of order $q - 1$ can be represented by $\{aX : a \in \mathbb{F}_q^\times\}$. These linear polynomials are as simple as can possibly be achieved; in general, the form of the permutation polynomials representing a given group will be significantly more complicated.

In Section 3, we describe a method for constructing permutation polynomials representing a given finite group G and prove in Theorem 3.3 that the resulting group of polynomials is indeed isomorphic to G. This method is based on the aforementioned proof of Cayley's Theorem, which in turn relies on the left regular action of G on itself and an assignation σ between the elements of G and the elements of $\mathbb{F}_q$. Generally speaking, one can make this assignment arbitrarily, and using interpolation produce many groups of permutation polynomials representing G. However, almost certainly a random assignation will result in unpredictable forms for the representation polynomials, lacking any sort of aesthetic. Our approach to producing permutation polynomials with a better aesthetic, that is, with relatively few terms or easily-described coefficients, is to preserve as much of the structure of G as possible in the assignation; we introduce the notions of "preserved subgroup" and "hemimorphism" to make more precise this concept of preservation of structure. In particular, we prove in Theorem 3.7 that the restriction of σ to the preserved subgroup is a group homomorphism. One interesting property of our method is that in the case when $|G| = q$, all permutation polynomials not representing the identity are fixed point free; we know of no other method for constructing permutation polynomials where this is guaranteed. Section 3 also addresses, via quasiequivalence of representations, when two groups of permutation polynomials produced by this method are essentially the same.

As applications of the general theory, we represent several families of groups by polynomials. Representations of cyclic groups which preserve some of the group structure in the additive group of $\mathbb{F}_q$ are considered in Section 4, and representations of cyclic groups which preserve some of the group structure in the multiplicative group $\mathbb{F}_q^\times$ are considered in Section 5. We also consider polynomial representations of dihedral groups in Section 6.1 and certain Hamiltonian groups in Section 6.2. New classes of permutation polynomials produced by our approach are given in Theorems 4.1, 4.3, 4.5, 5.1, 5.2, and 5.3, and Corollary 4.7. Theorems 6.1 and 6.4 exhibit families of permutation polynomials which, while already known, are shown to possess a nice group structure. In most cases, the forms obtained look somewhat complicated.

However, they still have either relatively few non-zero terms or a very simple description of the coefficients of each term; for example, we obtain permutation binomials for the Hamiltonian groups we consider. We also determine a new set of polynomial generators for $GL(\mathbb{F}_{p^2})$ in Theorem 4.9.

§ 2. Useful lemmas

Before developing the theory, we give several formulae which we will use in subsequent sections to simplify computations. Proofs are omitted as they are elementary and the results listed are standard.

Lemma 2.1. *Let $x \in \mathbb{F}_q^\times$, and recall that $h_k(X) = 1 + X + X^2 + \cdots + X^k$. Then*

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

Lemma 2.2. *Let $x \in \mathbb{F}_q$ and let $r, t \in \{1, 2, \dots, q-1\}$ such that $(q-1) \mid rt$. Then*

$$\sum_{s=0}^{t-1} (x^r)^s = \begin{cases} t, & x^r = 1, \\ 0, & x^r \neq 1. \end{cases}$$

Lemma 2.3. *For any finite field $\mathbb{F}_q$, we have*

$$\sum_{x \in \mathbb{F}_q} x^d = \begin{cases} 0, & \text{if } d = 0 \text{ or } (q-1) \nmid d, \\ -1, & \text{if } d \neq 0 \text{ and } (q-1) \mid d. \end{cases}$$

§ 3. A general theory for polynomial representation of groups

In this section, we define a method of constructing permutation polynomials which represent the left regular action of a group G on (the underlying set of) a field $\mathbb{F}_q$. We also examine several ways in which group structure can be reflected in field structure and when two representations are effectively the same.

§ 3.1. Constructing polynomial representations of groups

Let G be a group of order $|G| \leq q$ and associate elements of G with elements of $\mathbb{F}_q$ according to an injective function $\sigma \colon G \to \mathbb{F}_q$. In general, we choose σ to preserve some of the group structure, though this is not necessary for the basic theory. Define the binary operation $* \colon G \times \mathbb{F}_q \to \mathbb{F}_q$ by

$$g * x := \begin{cases} \sigma\big(g \cdot \sigma^{-1}(x)\big), & x \in \operatorname{Im}(\sigma), \\ x, & x \notin \operatorname{Im}(\sigma), \end{cases}$$

for all $g \in G$ and all $x \in \mathbb{F}_q$. Note that $*$ is essentially the left regular action of G on itself. Indeed, the field is first relabeled by the group according to σ so that G then acts naturally on itself (while fixing any field element not corresponding to a group element). The following lemma is therefore easy to verify.

Lemma 3.1. *The binary operation $*$ defines an action of G on $\mathbb{F}_q$.*

The action $*$ of each $g \in G$ on $\mathbb{F}_q$ defines a permutation φ_g of $\mathbb{F}_q$. Interpolating will thus produce a reduced (permutation) polynomial $f_g \in \mathbb{F}_q[X]$ which represents φ_g and hence also represents the action of g on $\mathbb{F}_q$. Explicitly, we compute $f_g(X)$ according to the formula

$$f_g(X) = \sum_{x \in \mathbb{F}_q} \left(1 - (X - x)^{q-1}\right)(g * x).$$

Often the representation will rely on a collection Z of parameters, and we will write $f_g^{[Z]}(X)$ as an indication of the dependence of the representation on these parameters. For $g \in G$, we call the permutation polynomial $f_g(X)$ (or $f_g^{[Z]}(X)$) the *representation polynomial* of g as it represents the left regular action of G on itself, under composition modulo $X^q - X$. We shall prove this claim forthwith after noting some properties of representation polynomials. In computations, we will denote the composition of a polynomial $f(X)$ with itself k times, reduced modulo $X^q - X$, by $f(X)^{[k]}$.

Lemma 3.2. *Representation polynomials are permutation polynomials which possess the following properties.*

1. *The composition of two representation polynomials, reduced modulo $X^q - X$, is again a representation polynomial. In fact,*
$$\big(f_{g_1} \circ f_{g_2}\big)(X) = f_{g_1 g_2}(X).$$
2. *The composition of the representation of g with itself k times, reduced modulo $X^q - X$, is the representation of g^k. Explicitly,*
$$f_g(X)^{[k]} = f_{g^k}(X),$$
and in particular, $\big(f_g(X)\big)^{[-1]} = f_{g^{-1}}(X)$.
3. *If $g \neq e$, then $f_g(X)$ fixes precisely the elements of $\mathbb{F}_q \setminus \mathrm{Im}(\sigma)$. In particular, f_g fixes no point of $\mathbb{F}_q$ when $|G| = q$.*
4. *The constant term of $f_g(X)$ is $g * 0$. In particular, the constant term is $\sigma(g)$ when $\sigma(e) = 0$.*

Proof. Let $x \in \mathbb{F}_q$ and $g_1, g_2 \in G$. Then $g_1 * (g_2 * x) = (g_1 g_2) * x$ since $*$ defines a group action, so $f_{g_1}(f_{g_2}(X)) = f_{g_1 g_2}(X)$. Applying induction easily gives the second statement.

It follows immediately from the definition of the action $*$ that every element of G fixes $\mathbb{F}_q \setminus \mathrm{Im}(\sigma)$ pointwise. If the action of some $g \in G$ fixed an element $x \in \mathrm{Im}(\sigma)$, then we would have

$$x = g * x = \sigma(g \cdot \sigma^{-1}(x)),$$

and applying σ^{-1} to both sides yields $\sigma^{-1}(x) = g \cdot \sigma^{-1}(x)$. Since σ is injective, the element g acts as the identity of G, hence must be the identity of G, proving the third statement.

To prove the fourth statement, note first that for a fixed $x \in \mathbb{F}_q$ and any $y \in \mathbb{F}_q$,

$$(y - x)^{q-1} = \begin{cases} 1, & y \neq x, \\ 0, & y = x, \end{cases}$$

and hence $1 - (y - x)^{q-1}$ is nonzero precisely when $y = x$. Thus,

$$f_g(0) = \sum_{x \in \mathbb{F}_q} \left(1 - (0 - x)^{q-1}\right)(g * x) = \left(1 - (0 - 0)^{q-1}\right)(g * 0) = g * 0.$$

Moreover, when $\sigma(e) = 0$ we have

$$g * 0 = \sigma\left(g \cdot \sigma^{-1}(0)\right) = \sigma(g \cdot e) = \sigma(g). \qquad \square$$

Note that statement 1 above shows that the map defined by $g \mapsto f_g$ is a homomorphism, that is, representation polynomials indeed describe the representation

$$G \to \mathrm{Sym}(\mathbb{F}_q) \hookrightarrow \mathbb{F}_q[X]/(X^q - X).$$

Moreover, this representation is faithful since distinct group elements produce distinct permutations of $\mathbb{F}_q$, and hence distinct representation polynomials. We shall denote the set of representation polynomials of G by $\Gamma = \big\{f_g(X) : g \in G\big\}$; when the representation polynomials depend on a parameter set Z, we will accordingly denote the set of representation polynomials by $\Gamma^{[Z]}$.

Theorem 3.3. *The set Γ of representation polynomials of a group G forms a group isomorphic to G under composition modulo $X^q - X$.*

Proof. The first two statements of Lemma 3.2 show that Γ is closed and possesses mutliplicative inverses. We claim $f_e(X)$ acts as the identity for Γ. Indeed, since $*$ is a group action, we have $e * x = x$ for all $x \in \mathbb{F}_q$. Thus $f_e(X) = X$ as desired, and we have shown that Γ is a group. As noted above, the first statement in Lemma 3.2 shows that Γ behaves under composition and reduction precisely as the group G itself does, hence $\Gamma \cong G$. □

§ 3.2. Preserving group structure in field structure

The motivation for developing the method just described is to produce new families of permutation polynomials (which happen to be endowed with a group structure inherited from the construction). The previous theorem guarantees that we indeed produce groups of permutation polynomials, but it is not clear whether they will come from families of permutation polynomials which are already known. Our intuition is that choosing σ to preserve some of the group structure will lead to the most visually appealing families of permutation polynomials, that is those with simply-described coefficients, relatively few terms, etc. We make this precise as follows.

Typically, we construct σ so that the images of some of the group elements in the field maintain their group structure even under the field arithmetic; that is, by "preserving structure" we mean that σ restricts to a homomorphism on some subset of G. The requirement that σ be injective means that σ can be a homomorphism only if G is an elementary abelian p-group (for a representation into the additive group of $\mathbb{F}_q$) or a cyclic group of order dividing $q-1$ (for a representation into the multiplicative group of $\mathbb{F}_q$). Thus, we do not expect σ to be a homomorphism itself, but rather to behave like a homomorphism only on some portion of the group.

We will write $\mathbb{F}_q^+$ for the additive group of $\mathbb{F}_q$ and $\mathbb{F}_q^\times$ for the multiplicative group of $\mathbb{F}_q$. It will often be convenient to treat the theory for both of these groups at once, so we will write $\mathbb{F}_q^\star$ to denote either $\mathbb{F}_q^+$ or $\mathbb{F}_q^\times$, with $\star$ representing the appropriate group operation in computations. Accordingly, for any $a_1, \dots, a_k \in \mathbb{F}_q$ and any nonnegative integers $\delta_1, \dots, \delta_k$ we define

$$\bigstar_{i=1}^{k} a_i\delta_i := \big(\underbrace{a_1 \star a_1 \star \cdots \star a_1}_{\delta_1 \text{ times}}\big) \star \cdots \star \big(\underbrace{a_k \star a_k \star \cdots \star a_k}_{\delta_k \text{ times}}\big),$$

and we let id* denote the identity of $\mathbb{F}_q^\star$, so that id$^+ = 0$ and id$^\times = 1$. In what follows, we consider only functions σ which satisfy $\sigma(e) = \text{id}^\star$, and we will call σ and its corresponding representation *additive* (respectively, *multiplicative*) if $\sigma(e) = 0$ (respectively, if $\sigma(e) = 1$). In either case, we refer to such a function σ as an *assignation*; we will only consider representations for which σ is an assignation. Note that an assignation cannot simultaneously be both additive and multiplicative, so we will restrict ourselves to considering only the appropriate operation as being denoted by $\star$ instead of both operations simultaneously.

By itself, an assignation indicates that a small amount of structure has already been preserved, namely, that there is a natural algebraic correspondence between the identities of the group and the field. We think of this as a sort of local preservation of structure; the following theorem tells us something about the structure preserved at a global level.

Lemma 3.4. *Let σ and σ' be two assignations of a group G. If $\sigma(G)$ and $\sigma'(G)$ are both subgroups of $\mathbb{F}_q^\star$, then $\sigma(G) \cong \sigma'(G)$.*

Proof. Since the assignations are injective by definition, we have that $|\sigma(G)| = |\sigma'(G)| = |G|$.

Suppose first that σ and σ' are additive assignations. The subgroups of $\mathbb{F}_q^+$ are elementary abelian p-groups, and since $|\sigma(G)| = |\sigma'(G)|$, $\sigma(G)$ and $\sigma'(G)$ are elementary abelian p-groups of the same order. Therefore they are isomorphic.

If σ and σ' are multiplicative assignations, then $\sigma(G) \cong C_{|G|}$ and $\sigma'(G) \cong C_{|G|}$ since the cyclic group C_m has a unique (cyclic) subgroup C_d for each divisor d of m. Thus $\sigma(G)$ and $\sigma'(G)$ are isomorphic in this case as well. □

It will prove useful to define a measure of how much structure an assignation preserves. Given an assignation $\sigma\colon G \to \mathbb{F}_q^\star$, we call the set

$$P^\star(G,\sigma) = \{g \in G : \forall\ x \in \sigma(G),\ g * x = \sigma(g) \star x\}$$

preserved subset of the assignation. We remark that since $g * x = \sigma\left(g \cdot \sigma^{-1}(x)\right)$, for $g \in P^\star(G,\sigma)$ we have

$$\sigma\left(g \cdot \sigma^{-1}(x)\right) = \sigma(g) \star x = \sigma(g) \star \sigma\left(\sigma^{-1}(x)\right)$$

for all $x \in \sigma(G)$, that is, σ behaves like a homomorphism on the preserved subset. We will see shortly that this is, in fact, the case: the preserved subset $P^\star(G,\sigma)$ is a group and the restriction of σ to it is indeed a homomorphism from $P^\star(G,\sigma)$ into $\mathbb{F}_q^\star$.

Lemma 3.5. *Let $g \in G$ and let $\sigma\colon G \to \mathbb{F}_q^\star$ be an assignation. Then for some $c \in \mathbb{F}_q$ and all $x \in \sigma(G)$, $g * x = c \star x$ if and only if $c = \sigma(g)$ and $g \in P^\star(G,\sigma)$.*

Proof. Suppose $g * x = c \star x$ for some $c \in \mathbb{F}_q$ and all $x \in \sigma(G)$. Then in particular, $g * \mathsf{id}^\star = c \star \mathsf{id}^\star = c$. Since

$$g * \mathsf{id}^\star = \sigma\left(g \cdot \sigma^{-1}(\mathsf{id}^\star)\right) = \sigma(g \cdot e) = \sigma(g),$$

we have that $c = \sigma(g)$. Thus $g * x = \sigma(g) \star x$ for all $x \in \sigma(G)$, and hence $g \in P^\star(G,\sigma)$.

On the other hand, for $g \in P^\star(G,\sigma)$ we have $g * x = \sigma(g) \star x$ for all $x \in \sigma(G)$ by definition. Taking $c = \sigma(g)$ completes the proof. □

Corollary 3.6. *Let $\sigma\colon G \to \mathbb{F}_q$ be an assignation and suppose $\sigma(G) = \mathbb{F}_q^\star$. Then the linear polynomial $c \star X$ is a representation polynomial if and only if $c = \sigma(g)$ for some $g \in P^\star(G,\sigma)$.*

From the above corollary, we see that there is a correspondence, via linear representation polynomials, between group elements on which σ behaves like a homomorphism and linear representation polynomials. This correspondence indicates that the preserved subset is indeed a decent measure of the amount of structure preserved by the assignation; the next result will make this statement precise.

Theorem 3.7. *Let $\sigma\colon G \to \mathbb{F}_q^\star$ be an assignation. Then the preserved subset $P^\star(G,\sigma)$ is an abelian subgroup of G, and the restriction $\sigma\big|_{P^\star(G,\sigma)}\colon P^\star(G,\sigma) \to \mathbb{F}_q^\star$ is a homomorphism.*

Proof. Let $g, h \in P^\star(G,\sigma)$. Since $*$ defines a group action, for all $x \in \sigma(G)$ we have

$$gh * x = g * (h * x) = \sigma(g) \star (\sigma(h) \star x) = (\sigma(g) \star \sigma(h)) \star x.$$

In particular, taking $x = \mathsf{id}^\star$ yields $gh * \mathsf{id}^\star = (\sigma(g) \star \sigma(h)) \star \mathsf{id}^\star = \sigma(g) \star \sigma(h)$. But we also have

$$gh * \mathsf{id}^\star = \sigma\left(gh \cdot \sigma^{-1}(\mathsf{id}^\star)\right) = \sigma(gh \cdot e) = \sigma(gh),$$

and hence $\sigma(gh) = \sigma(g) \star \sigma(h)$ for all $g, h \in P^\star(G,\sigma)$. Then for any $x \in \sigma(G)$, we now have

$$gh * x = (\sigma(g) \star \sigma(h)) \star x = \sigma(gh) * x,$$

which shows that $gh \in P^\star(G,\sigma)$. Therefore $P^\star(G,\sigma)$ is closed. Moreover, for all $x \in \sigma(G)$,

$$e * x = x = \mathsf{id}^\star \star x = \sigma(e) \star x$$

shows that $e \in P^\star(G,\sigma)$, and hence $P^\star(G,\sigma)$ is indeed a group.

That $P^\star(G,\sigma)$ is abelian follows immediately from the commutativity of $\mathbb{F}_q^\star$ since

$$\sigma(gh) = \sigma(g) \star \sigma(h) = \sigma(h) \star \sigma(g) = \sigma(hg)$$

for all $g, h \in P^\star(G,\sigma)$. □

In light of this theorem, we shall refer to $P^\star(G,\sigma)$ as the *preserved subgroup* from now on.

Since the restriction of an assignation is a homomorphism on the preserved subgroup, we can preserve the most group structure by constructing assignations which are homomorphisms on large subgroups of G; that is, those for which many representation polynomials are linear (by Corollary 3.6). The intuition is that by preserving more structure, the remaining representation polynomials will also have a relatively nice form.

One very strong way to preserve structure is by defining the assignation as follows. Fix a presentation $G = \langle a_1, \ldots, a_k \mid R_1, \ldots, R_j \rangle$ with generators $a_1, \ldots, a_k$ and relations $R_1, \ldots, R_j$. We say that an assignation $\sigma\colon G \to \mathbb{F}_q^\star$ is a *hemimorphism* if for all $g = \prod_{i=1}^k a_i^{\delta_i} \in G$, we have

$$\sigma(g) = \sigma\left(\prod_{i=1}^{k} a_i^{\delta_i}\right) = \mathop{\bigstar}_{i=1}^{k} \sigma(a_i)\delta_i.$$

In general, σ is a hemimorphism if each element of $\sigma(G)$ is uniquely representable as a sum or product (as appropriate to the type of assignation) of images of generators of G. Thus a hemimorphism behaves like a homomorphism with respect to a product of generators of G, though not (in general) with respect to products of arbitrary elements of G.

In addition to representations which are hemimorphisms, we will also be interested in multiplicative representations of cyclic groups which are nearly hemimorphisms, in the following sense. For a cyclic group $G = \langle g \rangle$ such that $(|G|-1) \mid (q-1)$, we say that a multiplicative assignation $\sigma\colon G \to \mathbb{F}_q^\times$ *preserves a long cycle* if $\sigma(g)$ is a generator of the subgroup of $\mathbb{F}_q^\times$ of order $\frac{q-1}{|G|-1}$ and $g * x = \sigma(g)\,x$ for all but two values of $x \in \sigma(G)$. Note that this is a weakening of the condition from the definition of preserved subgroup, which requires that $g * x = \sigma(g)\,x$ for *all* $x \in \sigma(G)$. The "long cycle" that is preserved is the cyclic group $\langle \sigma(g) \rangle \le \mathbb{F}_q^\times$ of order $|G|-1$, with the element 0 inserted to extend it artificially to a cycle of length $|G|$. In computations, the exceptional elements will be indicated by the parameter z, so that $g * \sigma(g^{z-1}) = 0$ and $g * 0 = \sigma(g^z)$. Thus the action of g on $\mathbb{F}_q^\times$ is described by the cycle

$$\left(\sigma(g), \sigma(g^2), \ldots, \sigma(g^{z-1}), 0, \sigma(g^z), \ldots, \sigma(g^{|G|-1})\right).$$

Note that when σ preserves a long cycle, the preserved subgroup $P^\times(G,\sigma)$ is necessarily trivial.

§ 3.3. Equivalence of representations

It is of interest to know when various polynomial representations of a given group are essentially the same; that is, when they act in the same way on the underlying set. For a given group G, suppose the assignations σ and σ' are either both additive or both multiplicative, and let their corresponding groups of representation polynomials be denoted $\Gamma = \{f_g(X) : g \in G\}$ and $\Gamma' = \{f'_g(X) : g \in G\}$, respectively. We say that Γ and Γ' are *quasiequivalent* if there exist group automorphisms $\psi\colon G \to G$ and $\alpha\colon \mathbb{F}_q^\star \to \mathbb{F}_q^\star$ such that

$$f_g(X) = (\alpha^{-1} \circ f'_{\psi(g)} \circ \alpha)(X)$$

for all $g \in G$. If ψ is the identity automorphism, then Γ and Γ' are said to be *equivalent*. We remark that our definition follows Aschbacher [1, p. 9], which requires that α be an isomorphism in the category containing the structure on which the group G acts. Thus we require that α be a *group isomorphism* of $\mathbb{F}_q^\star$; a more general definition used elsewhere in the literature requires only that α be a *bijection* of $\mathbb{F}_q$ (cf. [7, p. 17]). Note that any $\alpha \in \operatorname{Aut}\mathbb{F}_q^\times$ is given by a function $\alpha(x) = x^a$ for some $(a, q-1) = 1$, and hence we can naturally consider α to be defined on $\mathbb{F}_q$ by specifying $\alpha(0) = 0$.

We now prove a very useful result giving a condition for two representations to be quasiequivalent.

Theorem 3.8. *Let $\sigma\colon G \to \mathbb{F}_q^\star$ and $\sigma'\colon G \to \mathbb{F}_q^\star$ be two assignations. The representations Γ and Γ' corresponding to σ and σ', respectively, are quasiequivalent if and only if there exist $\alpha \in \operatorname{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \operatorname{Aut}(G)$ such that $\sigma = \alpha^{-1} \circ \sigma' \circ \psi$.*

Proof. Suppose Γ and Γ' are equivalent. Then there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ such that $f_g(x) = \alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right)$ for all $g \in G$ and all $x \in \mathbb{F}_q$. In particular, taking $x = \mathsf{id}^\star \in \sigma(G)$, we obtain

$$f_g(x) = f_g(\mathsf{id}^\star) = \sigma\left(g \cdot \sigma^{-1}(\mathsf{id}^\star)\right) = \sigma(g \cdot e) = \sigma(g)$$

on the one hand, and

$$\begin{aligned}\alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right) &= \alpha^{-1}\left(f'_{\psi(g)}(\alpha(\mathsf{id}^\star))\right)\\ &= \alpha^{-1}\left(f'_{\psi(g)}(\mathsf{id}^\star)\right)\\ &= \alpha^{-1}\left(\sigma'\left(\psi(g)\cdot(\sigma')^{-1}(\mathsf{id}^\star)\right)\right)\\ &= \alpha^{-1}\left(\sigma'(\psi(g)\cdot e)\right)\\ &= \alpha^{-1}\left(\sigma'(\psi(g))\right)\end{aligned}$$

on the other. Thus, $\sigma(g) = (\alpha^{-1}\circ\sigma'\circ\psi)(g)$ for all $g \in G$, and we see that $\sigma = \alpha^{-1}\circ\sigma'\circ\psi$.

Now suppose that there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ satisfying $\sigma = \alpha^{-1}\circ\sigma'\circ\psi$. If $x \in \sigma(G)$, then for all $g \in G$ we have

$$\begin{aligned}f_g(x) &= \sigma\left(g\cdot\sigma^{-1}(x)\right)\\ &= \alpha^{-1}\left(\sigma'\left(\psi\left(g\cdot\psi^{-1}\left((\sigma')^{-1}(\alpha(x))\right)\right)\right)\right)\\ &= \alpha^{-1}\left(\sigma'\left(\psi(g)\cdot\psi\left(\psi^{-1}\left((\sigma')^{-1}(\alpha(x))\right)\right)\right)\right)\\ &= \alpha^{-1}\left(\sigma'\left(\psi(g)\cdot(\sigma')^{-1}(\alpha(x))\right)\right)\\ &= \alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right).\end{aligned}$$

Now let $x \in \mathbb{F}_q \setminus \sigma(G)$ so that $f_g(x) = x$. If $\alpha(x) \in \sigma'(G)$, then $\alpha(x) = \sigma'(g)$ for some $g \in G$. Writing $g' = \psi^{-1}(g)$, we have

$$x = \alpha^{-1}\left(\sigma'(g)\right) = \alpha^{-1}\left(\sigma'(\psi(g'))\right) = \sigma(g'),$$

a contradiction. Thus $\alpha(x) \notin \sigma'(G)$ whenever $x \notin \sigma(G)$. Then

$$\alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right) = \alpha^{-1}\left(\alpha(x)\right) = x,$$

and hence $f_g(x) = \alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right)$ for all $x \notin \sigma(G)$. We conclude that $f_g(X) = \alpha^{-1}\left(f'_{\psi(g)}(\alpha(X))\right)$, so that Γ and Γ' are quasiequivalent. □

For hemimorphisms, we can significantly strengthen the statement of the previous theorem. We omit the proof as it is a simple computation using the definition of hemimorphism to show that the hypotheses satisfy the theorem.

Theorem 3.9. *Let $G = \langle a_1, \ldots, a_k \mid R_1, \ldots, R_j\rangle$ be a group with two hemimorphisms σ and σ'. The representations Γ and Γ' corresponding to σ and σ', respectively, are quasiequivalent if and only if there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ such that $\sigma(a_i) = \alpha^{-1}(\sigma'(\psi(a_i)))$ for each $1 \le i \le k$.*

We actually know more about additive hemimorphisms, as demonstrated by the next two corollaries. Recall that $\mathbb{F}_q^+$, as an elementary abelian p-group, can be considered as an n-dimensional vector space over $\mathbb{F}_p$, and that any two vector subspaces of the same dimension are isomorphic.

Corollary 3.10. *Let $G = \langle a_1, \ldots, a_k \mid R_1, \ldots, R_j\rangle$ be a group with two additive hemimorphisms σ and σ', and suppose $\sigma(G)$ and $\sigma'(G)$ are both vector subspaces of $\mathbb{F}_q$ of the same dimension. Then the representations Γ and Γ' corresponding to σ and σ', respectively, are equivalent.*

Since we can consider $\mathbb{F}_q^+$ as a vector space over $\mathbb{F}_p$, we have $\mathrm{Aut}(\mathbb{F}_q^+) \cong GL(\mathbb{F}_q)$, so every automorphism of $\mathbb{F}_q^+$ can be represented by a linear map. We will describe $GL(\mathbb{F}_q)$ by polynomials of the form

$$L(X) = \sum_{i=0}^{n-1} \ell_i X^{p^i}$$

where $\ell_i \in \mathbb{F}_q$. Berlekamp [2, Chapter 11] called such polynomials *linearized polynomials*. It is an easy exercise to show that they indeed behave linearly over $\mathbb{F}_p$, that is

$$L(aX + b) = aL(X) + L(b)$$

for any $a \in \mathbb{F}_p$ and any $b \in \mathbb{F}_q$. Vaughan [13] showed that the algebra of linear transformations of $\mathbb{F}_q$ (considered as a vector space over $\mathbb{F}_p$) is isomorphic to the algebra of all linearized polynomials in $\mathbb{F}_q[X]$. For our purposes, we only require the fact, established by Dickson [6], that the elements from the set of *invertible* linear transformations of $\mathbb{F}_q$ (i.e. from the set $GL(\mathbb{F}_q)$) are in bijective correspondence with elements from the set of linearized permutation polynomials satisfying one of the following equivalent conditions:

1. $\begin{vmatrix} \ell_0 & \ell_{n-1}^p & \ell_{n-2}^{p^2} & \cdots & \ell_1^{p^{n-1}} \\ \ell_1 & \ell_0^p & \ell_{n-1}^{p^2} & \cdots & \ell_2^{p^{n-1}} \\ \ell_2 & \ell_1^p & \ell_0^{p^2} & \cdots & \ell_3^{p^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \ell_{n-1} & \ell_{n-2}^p & \ell_{n-3}^{p^2} & \cdots & \ell_0^{p^{n-1}} \end{vmatrix} \neq 0;$
2. The unique root of $L(X)$ in $\mathbb{F}_q$ is 0.

(Bottema [3] and Carlitz [5] showed *a fortiori* that $GL(\mathbb{F}_q)$ is isomorphic to the group of invertible linearized polynomials over $\mathbb{F}_q$; see [10, p. 382] for further historical information.) Therefore each element of $GL(\mathbb{F}_q)$ can be represented by a unique reduced linearized (permutation) polynomial $L(X) \in \mathbb{F}_q[X]$.

Corollary 3.11. *Let $L(X) \in \mathbb{F}_q[X]$ denote the polynomial representation of the element of $GL(\mathbb{F}_q)$ which corresponds to the change of basis of $\mathbb{F}_q$ from $[\beta_i]$ to $[\gamma_i]$. Then the following formula holds:*

$$f_g^{[\beta_i]}(X) = L(X)^{[-1]} \circ f_g^{[\gamma_i]}(X) \circ L(X).$$

Unlike the additive representation of cyclic groups where all polynomial representations are equivalent (see Section 4), in general there are several inequivalent multiplicative representations among assignations which preserve a long cycle. Explicitly, consider a cyclic group $G = \langle g \rangle$ with $(|G| - 1) \mid (q - 1)$. Let $z \in \{1, 2, \ldots, |G| - 1\}$ and choose a generator ξ of $\langle \sigma(g) \rangle \leq \mathbb{F}_q^\times$. Define $\sigma \colon G \to \mathbb{F}_q$ by $\sigma(g^d) = \xi^d$ for $z - (|G| - 1) \leq d \leq z - 1$ and $\sigma(g^z) = 0$ so that σ preserves a long cycle and the action of g describes the cycle $(\xi, \xi^2, \ldots, \xi^{z-1}, 0, \xi^z, \ldots, \xi^{|G|-1})$ in $\mathbb{F}_q$. The representation group will be denoted $\Gamma^{[\xi;z]}$ to emphasize the dependence of the representation on both ξ and z. For more detail on the computations in the proof below, see the representations of C_p and C_q in Section 5.

In what follows, given $\alpha_a \in \mathrm{Aut}\,\mathbb{F}_q^\times$ we will consider $1 \leq a \leq q - 1$ to be the representative of the corresponding residue class modulo $q - 1$, so that the condition $(a, q - 1) = 1$ means that a^{-1} is well-defined as the multiplicative inverse of a in the ring $\mathbb{Z}/(q - 1)\mathbb{Z}$. Similarly, any automorphism of G is of the form $\psi_j(x) = x^j$ for j satisfying $(j, |G|) = 1$, since G is cyclic.

Theorem 3.12. *Let G be a cyclic group such that $(|G| - 1)m = q - 1$ for some integer m, and consider assignations that preserve a long cycle, as described above. Then for $a, a' \in \{1, 2, \ldots, q - 1 : (a, q - 1) = 1\}$ and $z, z' \in \{1, 2, \ldots, |G| - 1\}$, the polynomial representations $\Gamma^{[\zeta^{ma};z]}$ and $\Gamma^{[\zeta^{ma'};z']}$ of G are:*

1. *equivalent for $z = z'$ and any a and a';*

2. *quasiequivalent whenever* $z' \equiv 1 - z \pmod{|G|-1}$*; or*

3. *not quasiequivalent whenever* $z' \not\equiv 1 - z \pmod{|G|-1}$.

Proof. We begin by proving the equivalence statement. Let $z \in \{1, 2, \dots, |G|-1\}$ and $\alpha_a \in \operatorname{Aut} \mathbb{F}_q^\times$, and note that $\alpha_a^{-1} = \alpha_{a^{-1}}$. That $\Gamma^{[\zeta^m;z]}$ and $\Gamma^{[\zeta^{ma};z]}$ are equivalent follows immediately since direct calculation shows

$$f_{g^j}^{[\zeta^m;z]}(x) = f_g^{[\zeta^m;z]}(x)^{[j]} = (\alpha_a^{-1} \circ f_g^{[(\zeta^m)^a;z]} \circ \alpha_a)(x)^{[j]} = (\alpha_a^{-1} \circ f_{g^j}^{[\zeta^{ma};z]} \circ \alpha_a)(x)$$

for each $x \in \mathbb{F}_q$ and each $j \in \{1, 2, \dots, |G|\}$.

Now let $z, z' \in \{1, 2, \dots, |G|-1\}$ and consider two representations of G with distinct parameters z and z'. In light of the equivalence statement just proved, it will suffice to consider representations which both use the fixed parameter $\xi = \zeta^m$. Suppose the representations $f_g^{[\xi;z]}(X)$ and $f_{g^j}^{[\xi;z']}(X)$ are quasiequivalent so that $f_g^{[\xi;z]}(X) = (\alpha_a^{-1} \circ f_{g^j}^{[\xi;z']} \circ \alpha_a)(X)$ for some $\alpha_a \in \operatorname{Aut} \mathbb{F}_q^\times$ and $\psi_j \in \operatorname{Aut} G$. We will show that $\Gamma^{[\xi^a;z]}$ and $\Gamma^{[\xi^{a'};z']}$ are quasiequivalent only when $z' \equiv z \pmod{|G|-1}$ by determining several conditions that a and j must satisfy.

First, $f_g^{[\xi;z]}(0) = \xi^z$, and

$$\alpha_a^{-1}\left(f_{g^j}^{[\xi;z']}(\alpha_a(0))\right) = \alpha_{a^{-1}}\left(f_{g^j}^{[\xi;z']}(0)\right) = \alpha_{a^{-1}}\left(\xi^{z'+j-1}\right) = \xi^{a^{-1}(z'+j-1)},$$

so we must have $z \equiv a^{-1}(z'+j-1) \pmod{\frac{q-1}{m}}$, or equivalently,

$$z' \equiv az - j + 1 \pmod{\tfrac{q-1}{m}}. \tag{1}$$

Next, $f_g^{[\xi;z]}(\xi^{z-1}) = 0$, and

$$\alpha_a^{-1}\left(f_{g^j}^{[\xi;z']}\left(\alpha_a(\xi^{a^{-1}(z'-j)})\right)\right) = \alpha_{a^{-1}}\left(f_{g^j}^{[\xi;z']}(\zeta^{z'-j})\right) = \alpha_{a^{-1}}(0) = 0,$$

so we must also have $z - 1 \equiv a^{-1}(z'-j) \pmod{\frac{q-1}{m}}$, or equivalently,

$$z' \equiv az - a + j \pmod{\tfrac{q-1}{m}}. \tag{2}$$

Subtracting congruences (1) from congruence (2) gives the condition

$$a + 1 \equiv 2j \pmod{\tfrac{q-1}{m}}. \tag{3}$$

Continuing, $f_g^{[\xi;z]}(1) = \xi$, and

$$f_{g^j}^{[\xi;z']}(1) = \begin{cases} \xi^j, & j \le z'-1, \\ 0, & j = z', \\ \xi^{j-1}, & j \ge z'+1. \end{cases}$$

Since $\alpha_a(1) = 1$, we also have

$$\alpha_a^{-1}\left(f_{g^j}^{[\xi;z']}(\alpha_a(1))\right) = \begin{cases} \xi^{ja^{-1}}, & j \le z'-1, \\ 0, & j = z', \\ \xi^{(j-1)a^{-1}}, & j \ge z'+1. \end{cases}$$

This leads to three cases: $j = z'$, $j \le z'-1$, and $j \ge z'+1$. In the first case, when $j = z'$, we must have $\xi = 0$, which is impossible since $\xi = \zeta^m \in \mathbb{F}_q^\times$.

The second case $j \leq z' - 1$ implies $\xi = \xi^{ja^{-1}}$, or $a \equiv j \pmod{\frac{q-1}{m}}$. Substituting this into congruence (3), we obtain $a + 1 \equiv 2a \pmod{\frac{q-1}{m}}$, or $a \equiv 1 \pmod{\frac{q-1}{m}}$. Thus $j \equiv 1 \pmod{\frac{q-1}{m}}$ as well, and hence $z \equiv z' \pmod{\frac{q-1}{m}}$ follows from congruence (1). But this means $z = z'$, contradicting the assumption that z and z' are distinct.

Finally, when $j \geq z' + 1$, we must have $\xi = \xi^{(j-1)a^{-1}}$, or equivalently, $a \equiv j - 1 \pmod{\frac{q-1}{m}}$. Substituting this expression into congruence (3), we obtain the congruence $(j-1) + 1 \equiv 2j \pmod{\frac{q-1}{m}}$, or $j \equiv 0 \pmod{|G| - 1}$. Since $j \in \{1, 2, \ldots, |G|\}$, this means $j = |G| - 1$ and $a \equiv (|G| - 1) - 1 \equiv -1 \pmod{|G| - 1}$. Substituting back into (1), we find that $z' \equiv 1 - z \pmod{|G| - 1}$, proving case (2) and completing the proof. □

§ 4. Additive representations of cyclic groups

In this section we construct additive representations of cyclic p-groups in $\mathbb{F}_q^+$. Each assignation we use is a hemimorphism and the images of the group are always subgroups of $\mathbb{F}_q^+$; therefore all representations of a given group will be equivalent by Corollary 3.10. Although we do not do so here, the theory we develop can be used to build additive representations of direct products of cyclic p-groups, $C_{p^{n_1}} \times \cdots \times C_{p^{n_k}}$ with $n_1 + \cdots + n_k \leq n$, which are all equivalent.

§ 4.1. Representation of C_p

Let $C_p = \langle g \rangle$ and choose arbitrary $\beta \in \mathbb{F}_q^\times$. Define $\sigma \colon C_p \to \mathbb{F}_q$ by $\sigma(g^k) = k\beta$, so that the action of g describes the cycle $(0, \beta, 2\beta, \ldots, (p-1)\beta)$ in $\mathbb{F}_q$. This is a hemimorphism, and

$$g^k * \ell\beta = \sigma\left(g^k \cdot \sigma^{-1}(\ell\beta)\right) = \sigma\left(g^k \cdot g^\ell\right) = \sigma(g^{k+\ell}) = (k+\ell)\beta = k\beta + \ell\beta = \sigma(g^k) + \ell\beta$$

shows that the preserved subgroup $P^+(C_p, \sigma)$ is the group C_p itself. Since $\sigma(C_p) = \langle \beta \rangle$ is a subgroup of $\mathbb{F}_q^+$, it follows from Corollary 3.10 that all additive representations of C_p are equivalent.

Theorem 4.1. *Let $\beta \in \mathbb{F}_q^\times$. Then the polynomial representing the element g^k of C_p in $\mathbb{F}_q^+$ is*

$$f_{g^k}^{[\beta]}(X) = X + k\beta h_{\lfloor \frac{q-2}{p-1} \rfloor}((\beta^{-1}X)^{p-1}).$$

Proof. As we saw above, the action of g^k on $x \in \mathbb{F}_q$ is

$$g^k * x = \begin{cases} x + k\beta, & x \in \langle \beta \rangle, \\ x, & \text{otherwise.} \end{cases}$$

Interpolating, we obtain

$$\begin{aligned} f_{g^k}^{[\beta]}(X) &= \sum_{x \in \mathbb{F}_q} \left(1 - (X-x)^{q-1}\right)(g^k * x) \\ &= \left(\sum_{x \in \mathbb{F}_q \setminus \langle \beta \rangle} \left(1 - (X-x)^{q-1}\right)(x)\right) + \left(\sum_{x \in \langle \beta \rangle} \left(1 - (X-x)^{q-1}\right)(x + k\beta)\right) \\ &= \left(\sum_{x \in \mathbb{F}_q} \left(1 - (X-x)^{q-1}\right)(x)\right) \\ &\qquad + \left(\sum_{x \in \langle \beta \rangle} \left(\left(1 - (X-x)^{q-1}\right)(x + k\beta) - \left(1 - (X-x)^{q-1}\right)(x)\right)\right) \end{aligned}$$

$$
\begin{aligned}
&= X + \sum_{i=0}^{p-1} \left(1-(X-i\beta)^{q-1}\right)(k\beta) \\
&= X + k\beta(1-X^{q-1}) + k\beta\sum_{i=1}^{p-1}\left(1-X^{q-1}-h_{q-2}((i\beta)^{-1}X)\right) \\
&= X + \left(k\beta(1-X^{q-1})\sum_{i=0}^{p-1}1\right) - \left(k\beta\sum_{i=1}^{p-1}h_{q-2}((i\beta)^{-1}X)\right) \\
&= X + 0 - k\beta\sum_{i=1}^{p-1}\sum_{k=0}^{q-2} i^{-k}(\beta^{-1}X)^k \\
&= X - k\beta\sum_{k=0}^{q-2}(\beta^{-1}X)^k\sum_{i=1}^{p-1}i^{-k} \\
&= X - k\beta\sum_{k=0}^{\lfloor\frac{q-2}{p-1}\rfloor}(\beta^{-1}X)^{(p-1)k}(-1) \\
&= X + k\beta h_{\lfloor\frac{q-2}{p-1}\rfloor}\left((\beta^{-1}X)^{p-1}\right),
\end{aligned}
$$

where we used Lemma 2.1 to get from the fourth to the fifth line, and Lemma 2.3 was used to simplify the inner sum on the third-to-last line. □

We remark that this proof is typical in that it consists of a list of simplifications to the interpolation of a given action. These computations are routine, and will be omitted in the future.

§ 4.2. Representation of C_q

Let $C_q = \langle g\rangle$ and fix a basis $[\beta_i] = [\beta_0, \beta_1, \dots, \beta_{n-1}]$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. Define the bijection $\sigma\colon C_q \to \mathbb{F}_q$ by

$$\sigma(g^k) = \sigma\left(g^{\sum_{i=0}^{n-1}\kappa_i p^i}\right) = \sum_{i=0}^{n-1}\kappa_i\beta_i.$$

In summary, we rewrite the exponent k of a general element g^k of C_q p-adically, and then assign the digit in the i-th position as the coefficient of the i-th basis element of $\mathbb{F}_q$. As we will see shortly, the form of the representation polynomial reflects where there are p-adic carries when adding 1 and $\sum_{i=0}^{n-1}\kappa_i p^i$. Thus it will be convenient to define the family of affine subspaces

$$\mathcal{F}_j^{[\beta_i]} = \left\{\sum_{i=0}^{j-1}(p-1)\beta_i + \sum_{i=j}^{n-1}\delta_i\beta_i : \delta_i \in \mathbb{F}_p\right\}$$

of $\mathbb{F}_q$ over $\mathbb{F}_p$ for $1 \le j \le n-1$, which will correspond to where these carries occur. Note that since $\mathcal{F}_j^{[\beta_i]}$ is an affine linear subspace of dimension $n-j$ over $\mathbb{F}_p$, it has order p^{n-j}.

While the above form of assignation will be most useful in the following computations, it will be easier to see that σ is a hemimorphism if we consider a slight variation. To that end, let C_q have the presentation

$$\langle a_1, \dots, a_n \mid a_i a_j = a_j a_i \text{ for all } i, a_i^p = a_{i+1} \text{ for } i \le n-1, a_n^p = 1\rangle\,.$$

By taking $a_i = g^{p^{i-1}}$, we see that this presentation in fact describes C_q. The assignation σ then becomes

$$\sigma(g^k) = \sigma\left(g^{\sum_{i=0}^{n-1}\kappa_i p^i}\right) = \sigma\left(\prod_{i=0}^{n-1}\left(g^{p^i}\right)^{\kappa_i}\right) = \sigma\left(\prod_{i=0}^{n-1}a_{i+1}^{\kappa_i}\right) = \sum_{i=0}^{n-1}\kappa_i\beta_i.$$

Using this second form of the assignation, it is clear that σ is a hemimorphism.

Lemma 4.2. *We have $P^+(C_q,\sigma)=\langle a_n\rangle=\langle g^{p^{n-1}}\rangle$, and $P^+(C_q,\sigma)$ is represented by the linear polynomials $X+\kappa_{n-1}\beta_{n-1}$ for $\kappa_{n-1}\in\mathbb{F}_p$.*

Proof. Let $k=\sum_{i=0}^{n-1}\kappa_i p^i\in\{0,1,\ldots,q-1\}$ and let $x=\sum_{i=0}^{n-1}\lambda_i\beta_i\in\mathbb{F}_q$. The elements of $P^+(C_q,\sigma)$ will be precisely those elements $g^k\in C_q$ for which $g^k * x=\sigma(g^k)+x$ for all $x\in\mathbb{F}_q$. Using the above computations, we have

$$\begin{aligned} g^k * x &= \sigma(g\cdot\sigma^{-1}(x)) \\ &= \sigma\left(\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i}\right)\cdot\sigma^{-1}\left(\sum_{i=0}^{n-1}\lambda_i\beta_i\right)\right) \\ &= \sigma\left(\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i}\right)\cdot\left(\prod_{i=0}^{n-1} a_{i+1}^{\lambda_i}\right)\right), \end{aligned}$$

and

$$\begin{aligned} \sigma(g^k)+x &= \left(\sum_{i=0}^{n-1}\kappa_i\beta_i\right)+\left(\sum_{i=0}^{n-1}\lambda_i\beta_i\right) \\ &= \sum_{i=0}^{n-1}(\kappa_i+\lambda_i)\beta_i \\ &= \sigma\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i+\lambda_i}\right). \end{aligned}$$

Thus $g^k * x=\sigma(g^k)+x$ if and only if $\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i}\right)\cdot\left(\prod_{i=0}^{n-1} a_{i+1}^{\lambda_i}\right)=\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i+\lambda_i}$. The latter statement occurs if and only if there are no p-adic carries when adding $\sum_{i=0}^{n-1}\kappa_i p^i$ and $\sum_{i=0}^{n-1}\lambda_i p^i$ for any $x\in\mathbb{F}_q$; that is, when $\kappa_i+\lambda_i\le p-1$ for all $0\le i\le n-2$ and any choice of λ_i. In particular, we may choose $x=\sum_{i=0}^{n-1}(p-1)\beta_i$, and hence it is clear that we must have $\kappa_i=0$ for all $0\le i\le n-2$. Therefore,

$$P^+(C_q,\sigma)=\{g^{\kappa_{n-1}p^{n-1}}:\kappa_{n-1}\in\mathbb{F}_p\}=\langle g^{p^{n-1}}\rangle=\langle a_n\rangle,$$

proving the first claim, and by Corollary 3.6, we have

$$f^{[\beta_i]}_{g^{\kappa_{n-1}p^{n-1}}}(X)=\sigma(g^{\kappa_{n-1}p^{n-1}})+X=X+\kappa_{n-1}\beta_{n-1},$$

proving the second one. □

We now determine the polynomial generator of C_q in the additive representation. To obtain this, we only need to keep track of carries from the first position; the representation of a general element is much more complex since multiple carries need to be accounted for simultaneously.

Theorem 4.3. *The permutation polynomial representing the additive action of g on $\mathbb{F}_q$ is*

$$f_g^{[\beta_i]}(X)=X+\beta_0-\sum_{j=1}^{n-1}\beta_j\sum_{x\in\mathcal{F}_j^{[\beta_i]}}h_{q-2}(x^{-1}X).$$

Proof. For an element $x\in\mathbb{F}_q$, we will write $x=\sum_{i=0}^{n-1}\lambda_i\beta_i$. Let us assume that $\lambda_0=\cdots=\lambda_{j-1}=p-1$ and $\lambda_j<p-1$, so that j is the position of lowest index where there is not a p-adic carry when adding 1 to $\sum_{i=0}^{n-1}\lambda_i p^i$. Then the action of g on x is

$$g * x=\sigma\left(g\cdot\sigma^{-1}\left(\sum_{i=0}^{n-1}\lambda_i\beta_i\right)\right)=\sigma\left(g\cdot g^{\sum_{i=0}^{n-1}\lambda_i p^i}\right)=\sigma\left(g^{1+\sum_{i=0}^{n-1}\lambda_i p^i}\right)$$

$$= \sum_{i=0}^{j}(1+\lambda_i)\beta_i + \sum_{i=j+1}^{n-1}\lambda_i\beta_i = \sum_{i=0}^{n-1}\lambda_i\beta_i + \sum_{i=0}^{j}\beta_i = x + \beta_0 + \sum_{i=1}^{j}\beta_i.$$

Interpolating then gives the desired result. □

Corollary 4.4. *The coefficient of the X^k term of $f_g^{[\beta_i]}(X)$ is*

$$-\sum_{j=1}^{n-1}\beta_j \sum_{x\in\mathcal{F}_j^{[\beta_i]}} x^{q-1-k}.$$

The general form of the representation polynomial of g^k, for $k = \sum_{i=0}^{n-1}\kappa_i p^i$, is:

$$f_{g^k}^{[\beta_i]}(X) = X + \sum_{i=0}^{n-1}\kappa_i\beta_i - \sum_{i=0}^{n-1}\left(\sum_{x\in\mathcal{B}_i} h_{q-2}(x^{-1}X)\right)\beta_i$$

where

$$\mathcal{B}_i = \left\{\sum_{i=0}^{n-1}\lambda_i\beta_i \in \mathbb{F}_q : \sum_{i=0}^{n-1}\lambda_i p^i + \sum_{i=0}^{n-1}\kappa_i p^i \text{ has a base-}p\text{ carry at } p^i\right\}.$$

Based on computational evidence, we suspect there is a correspondence between the degree of the representation polynomial and the order of the element of C_q that it represents.

Conjecture 1. *The degree of $f_{g^k}^{[\beta_i]}(X)$ is $p^n - \frac{p^{n+1}}{o(g^k)}$ when $o(g^k) > p$.*

---

§ 4.3. Representation of C_{p^2} in $\mathbb{F}_{p^2}$

For C_{p^2}, there is only one carry to keep track of, and hence we can explicitly compute the form of the representation polynomial of any element of C_{p^2}. Since Lemma 4.2 gives the form of representation polynomial for elements of the subgroup of C_{p^2} of order p, with the following theorem we have described the entire group $\Gamma^{[\beta_0,\beta_1]}$ of representation polynomials of C_{p^2}. Recall that the additive representation groups of C_{p^2} in $\mathbb{F}_{p^2}$ are equivalent by Corollary 3.10.

Theorem 4.5. *The representation polynomial of $g^{\kappa_0+\kappa_1 p}$ for $\kappa_0 \neq 0$ is given by*

$$f_{g^{\kappa_0+\kappa_1 p}}^{[\beta_0,\beta_1]}(X) = X + \kappa_0\beta_0 + \kappa_1\beta_1 - \beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1}\sum_{\lambda_1=0}^{p-1} h_{p^2-2}\left((\lambda_0\beta_0+\lambda_1\beta_1)^{-1}X\right).$$

Proof. Let $x = \lambda_0\beta_0 + \lambda_1\beta_1 \in \mathbb{F}_{p^2}$. Then the action of $g^{\kappa_0+\kappa_1 p} \in C_{p^2}$ on x is

$$\begin{aligned}
g^{\kappa_0+\kappa_1 p} * x &= \sigma\left(g^{\kappa_0+\kappa_1 p}\cdot\sigma^{-1}(\lambda_0\beta_0+\lambda_1\beta_1)\right)\\
&= \sigma\left(g^{\kappa_0+\kappa_1 p}\cdot g^{\lambda_0+\lambda_1 p}\right)\\
&= \sigma\left(g^{(\kappa_0+\lambda_0)+(\kappa_1+\lambda_1)p}\right)\\
&= \begin{cases}(\kappa_0+\lambda_0)\beta_0+(\kappa_1+\lambda_1)\beta_1, & \kappa_0+\lambda_0 < p,\\ (\kappa_0+\lambda_0)\beta_0+(\kappa_1+\lambda_1+1)\beta_1, & \kappa_0+\lambda_0 \geq p,\end{cases}\\
&= \begin{cases}(\lambda_0\beta_0+\lambda_1\beta_1)+(\kappa_0\beta_0+\kappa_1\beta_1), & \kappa_0+\lambda_0 < p,\\ (\lambda_0\beta_0+\lambda_1\beta_1)+(\kappa_0\beta_0+\kappa_1\beta_1)+\beta_1, & \kappa_0+\lambda_0 \geq p,\end{cases}\\
&= \begin{cases}x+(\kappa_0\beta_0+\kappa_1\beta_1), & \lambda_0 < p-\kappa_0,\\ x+(\kappa_0\beta_0+\kappa_1\beta_1)+\beta_1, & \lambda_0 \geq p-\kappa_0.\end{cases}
\end{aligned}$$

Interpolation gives the desired result. □

Lemma 4.6. *The leading term of* $f^{[\beta_0,\beta_1]}_{g^{\kappa_0+\kappa_1 p}}(X)$ *is* $\kappa_0\beta_1^p X^{p^2-p}$ *when* $\kappa_0 \neq 0$.

Proof. Using Lemmas 2.1 and 2.3 to simplify the representation polynomial of $g^{\kappa_0+\kappa_1 p}$ (with $\kappa_0 \neq 0$) from the previous theorem, we obtain

$$\begin{aligned} f^{[\beta_0,\beta_1]}_{g^{\kappa_0+\kappa_1 p}}(X) &= X + \kappa_0\beta_0 + \kappa_1\beta_1 - \beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\lambda_1=0}^{p-1} h_{p^2-2}\left((\lambda_0\beta_0+\lambda_1\beta_1)^{-1}X\right) \\ &= X + \kappa_0\beta_0 + \kappa_1\beta_1 - \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\substack{0\le k<p^2-1 \\ p-1\mid k}} (X-\lambda_0\beta_0)^k \beta_1^{p^2-k}(-1), \end{aligned}$$

Since there are only linear and constant terms outside the double sum on the right, the leading term of $f^{[\beta_0,\beta_1]}_{g^{\kappa_0+\kappa_1 p}}(X)$ must occur inside the sum. In particular, the highest power of X comes from the leading term of $(X-\lambda_0\beta_0)^k$ for the largest value of k, and this occurs when $k = p^2-p$. Therefore, the leading term is

$$-\sum_{\lambda_0=p-\kappa_0}^{p-1} X^k \beta_1^{p^2-k}(-1) = \kappa_0 X^{p^2-p}\beta_1^{p^2-(p^2-p)} = \kappa_0\beta_1^p X^{p^2-p}. \qquad \square$$

Corollary 4.7. *The polynomials* $X \pm X^{p-1}h_{p-1}(X^{p-1})$ *are permutation polynomials over* $\mathbb{F}_{p^2}$.

Proof. Recall that the composition of permutation polynomials is again a permutation polynomial. To prove the corollary, one easily checks that

$$f^{[\beta_0,\beta_1]}_{g^{(p-1)+\kappa_1 p}}(X) = X - \beta_0 + \kappa_1\beta_1 - \beta_1(\beta_1^{-1}X)^{p-1}h_{p-1}\big((\beta_1^{-1}X)^{p-1}\big),$$

from which it follows that

$$(X+\beta_0)\circ f^{[\beta_0,1]}_{g^{p-1}}(X) = X - X^{p-1}h_{p-1}(X^{p-1})$$

and

$$(X+\beta_0)\circ f^{[\beta_0,-1]}_{g^{p-1}}(X) = X + X^{p-1}h_{p-1}(X^{p-1})$$

are also permutation polynomials. □

The corollary may also be proved directly, independent of the fact that these polynomials arise as representation polynomials of a particular group. Indeed,

$$x + ax^{p-1}h_{p-1}(x^{p-1}) = \begin{cases} x, & x\in\mathbb{F}_p, \\ x-a, & x\in\mathbb{F}_{p^2}\setminus\mathbb{F}_p, \end{cases}$$

which shows that $X + aX^{p-1}h_{p-1}(x^{p-1})$ is a permutation polynomial for any $a\in\mathbb{F}_p$.

Lemma 4.8. *The representation polynomial* $f^{[\beta_0,\beta_1]}_g(X)$ *is conjugate to*

1. $f^{[r\beta_0,r\beta_1]}_g(X)$ *by* rX *for any* $r\in\mathbb{F}_{p^2}^\times$;
2. $f^{[\beta_0+s\beta_1,\beta_1]}_g(X)$ *by* $M_s(X) = \frac{1}{\beta_0^p\beta_1-\beta_0\beta_1^p}\Big(s\beta_1^2X^p + (\beta_0^p\beta_1 - \beta_0\beta_1^p - s\beta_1^{p+1})X\Big)$ *for any* $s\in\mathbb{F}_p$;
3. $f^{[t\beta_0,\beta_1]}_g(X)$ *by* $N_t(X) = \frac{1}{\beta_0^{p-1}-\beta_1^{p-1}}\Big((t-1)X^p + (\beta_0^{p-1} - t\beta_1^{p-1})X\Big)$ *for any* $t\in\mathbb{F}_p^\times$.

Proof. It follows from Corollary 3.11 that to show

$$L(X)^{[-1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ L(X) = f_g^{[\beta_0',\beta_1']}(X)$$

for a linearized polynomial $L(X)$, it will suffice to verify that $L(\beta_0) = \beta_0'$ and $L(\beta_1) = \beta_1'$. This computation is straightforward. □

Theorem 4.9. *Let $\rho \in \mathbb{F}_{p^2}^\times$ be primitive and let $\psi, \tau \in \mathbb{F}_p$ with τ primitive. Then the polynomials ρX, $M_\psi(X)$, and $N_\tau(X)$ (as defined in Lemma 4.8) generate a group of permutation polynomials isomorphic to $GL(\mathbb{F}_{p^2})$.*

Proof. Recall that the elements of the group $GL(\mathbb{F}_{p^2})$ are precisely the linearized polynomials which produce a change of basis of $f_g^{[\beta_0,\beta_1]}(X)$ upon conjugation. We will show that any change of basis can be accomplished by composition of (conjugations by) ρX, $M_\psi(X)$, and $N_\tau(X)$, demonstrating that they indeed generate a group of polynomials under composition modulo $X^q - X$ which is isomorphic to $GL(\mathbb{F}_{p^2})$.

Let the basis $[\beta_0, \beta_1]$ be fixed and the basis $[\gamma_0, \gamma_1]$ be arbitrary. We first show that there are unique $r \in \mathbb{F}_{p^2}^\times$, $s \in \mathbb{F}_p$, and $t \in \mathbb{F}_p^\times$ for which the basis $[\gamma_0, \gamma_1]$ can be rewritten as $[r(t\beta_0 + s\beta_1), r\beta_1]$. Since we must have $r\beta_1 = \gamma_1$, r is uniquely determined. That there are unique s and t for which $t\beta_0 + s\beta_1 = r^{-1}\gamma_0$ follows at once since the right-hand side may be written as a unique $\mathbb{F}_p$-linear combination of the basis elements β_0 and β_1. Thus the bases $[r(t\beta_0 + s\beta_1), r\beta_1]$ and $[\gamma_0, \gamma_1]$ are the same.

Now write $r = \rho^{\kappa_1}$, $s = \kappa_2\psi$, and $t = \tau^{\kappa_3}$. Then

$$(\rho X)^{[-\kappa_1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ (\rho X)^{[\kappa_1]} = (\rho X)^{[-(\kappa_1-1)]} \circ f_g^{[\rho\beta_0,\rho\beta_1]}(X) \circ (\rho X)^{[\kappa_1-1]},$$

and inductively, we have

$$(\rho X)^{[-\kappa_1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ (\rho X)^{[\kappa_1]} = f_g^{[\rho^{\kappa_1}\beta_0,\rho^{\kappa_1}\beta_1]}(X) = f_g^{[r\beta_0,r\beta_1]}(X).$$

Thus conjugation by $(\rho X)^{[\kappa_1]}$ changes the basis of representation from $[\beta_0, \beta_1]$ to $[r\beta_0, r\beta_1]$. This change of basis is accomplished by a unique linearized polynomial, so we conclude that $(\rho X)^{[\kappa_1]} = rX$. It follows similarly that $M_\psi(X)^{[\kappa_2]} = M_s(X)$ and $N_\tau(X)^{[\kappa_3]} = N_t(X)$.

Finally, the computation

$$\begin{aligned}
(rX)^{[-1]} \circ M_s(X)^{[-1]} \circ N_t(X)^{[-1]} &\circ f_g^{[\beta_0,\beta_1]}(X) \circ N_t(X) \circ M_s(X) \circ (rX) \\
&= (rX)^{[-1]} \circ M_s(X)^{[-1]} \circ f_g^{[t\beta_0,\beta_1]}(X) \circ M_s(X) \circ (rX) \\
&= (rX)^{[-1]} \circ f_g^{[t\beta_0+s\beta_1,\beta_1]}(X) \circ (rX) \\
&= f_g^{[r(t\beta_0+s\beta_1),r(\beta_1)]}(X) \\
&= f_g^{[\gamma_0,\gamma_1]}(X)
\end{aligned}$$

shows that conjugation by $L_{r,s,t}(X) = N_t(X) \circ M_s(X) \circ (rX)$ changes the basis of the representation from $[\beta_0, \beta_1]$ to $[r(t\beta_0 + s\beta_1), r\beta_1]$. As r, s, and t vary, the latter basis runs over all bases of $\mathbb{F}_{p^2}^+$ over $\mathbb{F}_p$, and hence the set $\{L_{r,s,t}(X) : r \in \mathbb{F}_{p^2}^\times, s \in \mathbb{F}_p, t \in \mathbb{F}_p^\times\}$ produces all changes of basis of $\mathbb{F}_{p^2}^+$ over $\mathbb{F}_p$; that is, this set is in fact a group isomorphic to $GL(\mathbb{F}_{p^2})$. □

Corollary 4.10. *Let $[\beta_0, \beta_1]$ and $[\gamma_0, \gamma_1]$ be two bases of $\mathbb{F}_{p^2}^+$ over $\mathbb{F}_p$. Then there exist unique $r \in \mathbb{F}_{p^2}^\times$, $s \in \mathbb{F}_p$, and $t \in \mathbb{F}_p^\times$ such that*

$$f_g^{[\gamma_0,\gamma_1]}(X) = L(X)^{[-1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ L(X),$$

where $L(X) = L_{r,s,t}(X) = N_t(X) \circ M_s(rX)$.

§ 5. Multiplicative representations of cyclic groups

In this section, we construct multiplicative representations of several families of cyclic groups, some whose order divides $q-1$ and others with order a power of p.

§ 5.1. Representation of C_m for $m \mid (q-1)$

Let $C_m = \langle g \rangle$ for some $m \mid (q-1)$ and choose $z \in \{1, 2, \ldots, m-1\}$ such that $(z, m) = 1$. Writing $\xi = \left(\zeta^{\frac{q-1}{m}}\right)^z$, define $\sigma \colon C_p \to \mathbb{F}_q$ by $\sigma(g^k) = \xi^k$ so that the action of g describes the cycle $(\xi, \xi^2, \ldots, \xi^m = 1)$ in $\mathbb{F}_q$. This defines a hemimorphism with preserved subgroup $P^\times(C_m, \sigma) = C_m$ since

$$g^k * \xi^\ell = \sigma\left(g^k \cdot \sigma^{-1}(\xi^\ell)\right) = \sigma\left(g^k \cdot g^\ell\right) = \sigma(g^{k+\ell}) = \xi^{k+\ell} = \xi^k \xi^\ell = \sigma(g^k)\xi^\ell,$$

and hence $g^k * x = \sigma(g^k)\xi^\ell$ holds for all $g^k \in C_m$ and all $\xi^\ell \in \sigma(C_m)$.

Theorem 3.9 shows that all representations of C_m in $\mathbb{F}_q^\times$ are equivalent. Indeed, the presentation of C_m has a single generator which is mapped to a generator of the (unique) subgroup of $\mathbb{F}_q^\times$ of order $(q-1)/m$. Since there exists an automorphism of $\mathbb{F}_q^\times$ mapping any generator of this subgroup to any other, the conditions of the theorem are satisfied.

Theorem 5.1. *Let $z \in \{1, 2, \ldots, m-1\}$ such that $(z, m) = 1$ and define $\xi = \left(\zeta^{\frac{q-1}{m}}\right)^z$. Then the polynomial representing the element g^k of C_m in $\mathbb{F}_q^\times$ is*

$$f_{g^k}^{[\xi;z]}(X) = X + (\xi^k - 1)Xh_{\lfloor \frac{q-2}{m} \rfloor}(X^m).$$

Proof. The action of g^k on $x \in \mathbb{F}_q$ is

$$g^k * x = \begin{cases} \xi^k x, & x \in \langle \xi \rangle, \\ x, & x \in \mathbb{F}_q \setminus \langle \xi \rangle. \end{cases}$$

The result follows from interpolation. □

§ 5.2. Representations of C_p and C_q

We will now construct representations of the cyclic p-groups C_p and C_q that preserve a long cycle. Thus Theorem 3.12 shows that all representations with a fixed value of the parameter z are equivalent, and those with differing values of z are not quasiequivalent.

Let $C_p = \langle g \rangle$ and choose $z \in \{1, 2, \ldots, p-1\}$. Writing $\xi = \zeta^{\frac{q-1}{p-1}}$, define $\sigma \colon C_p \to \mathbb{F}_q$ by

$$\sigma(g^k) = \begin{cases} \xi^k, & 1 \le k \le z-1, \\ 0, & k = z, \\ \xi^{k-1}, & z+1 \le k \le p, \end{cases}$$

so that the action of g describes the cycle $(\xi, \xi^2, \ldots, \xi^{z-1}, 0, \xi^z, \ldots, \xi^{p-1})$ in $\mathbb{F}_q$. In particular, σ preserves a long cycle in C_p.

Theorem 5.2. *Let $z \in \{1, 2, \ldots, p-1\}$ and define $\xi = \zeta^{\frac{q-1}{p-1}}$. Then the polynomial representing the generator g of C_p in $\mathbb{F}_q^\times$ is*

$$f_g^{[\xi;z]}(X) = X + (\xi - 1)Xh_{\lfloor \frac{q-2}{p-1} \rfloor}(X^{p-1}) + \xi^z h_{q-2}(\xi^{1-z}X).$$

Proof. The action of g on $x \in \mathbb{F}_q$ is

$$g * x = \begin{cases} x, & x \notin \langle \xi \rangle \cup \{0\}, \\ 0, & x = \xi^{z-1}, \\ \xi^z, & x = 0, \\ \xi x, & x \in \langle \xi \rangle \setminus \{\xi^{z-1}\}, \end{cases}$$

and interpolating, we obtain the desired result. □

Let $C_q = \langle g \rangle$, choose a generator ξ of $\mathbb{F}_q^\times$, and choose $z \in \{1, 2, \ldots, q-1\}$. Define the bijection $\sigma \colon C_q \to \mathbb{F}_q$ by

$$\sigma\left(g^k\right) = \begin{cases} \xi^k, & 1 \le k \le z-1, \\ 0, & k = z, \\ \xi^{k-1}, & z+1 \le k \le q. \end{cases}$$

For $z+1 \le k \le q$, we have $g^{k-q} = g^k$, hence

$$\sigma\left(g^{k-q}\right) = \sigma\left(g^k\right) = \xi^{k-1} = \xi^{k-1-(q-1)} = \xi^{k-q};$$

that is, $\sigma\left(g^k\right) = \xi^k$ for $z+1-q \le k \le 0$. Therefore, we can rewrite the bijection as

$$\sigma\left(g^k\right) = \begin{cases} \xi^k, & z+1-q \le k \le z-1, \\ 0, & k = z, \end{cases}$$

and it is clear that σ preserves a long cycle.

Theorem 5.3. *The polynomial representing the multiplicative action of g on $\mathbb{F}_q$ is*

$$f_g^{[\xi;z]}(X) = \xi X + \xi^z h_{q-2}(\xi^{1-z}X),$$

and the polynomial representing the multiplicative action of g^k on $\mathbb{F}_q$ for $2 \le k \le q-1$ is

$$f_{g^k}^{[\xi;z]}(X) = \xi^k X + \xi^z h_{q-2}(\xi^{k-z}X) + (\xi^k - \xi^{k-1}) \sum_{i=1}^{k-1} h_{q-2}(\xi^{k-z}X)\xi^{z-i}.$$

Proof. The action of g on $0 \in \mathbb{F}_q$ is

$$g * 0 = \sigma\left(g \cdot \sigma^{-1}(0)\right) = \sigma\left(g \cdot g^z\right) = \sigma\left(g^{z+1}\right) = \sigma\left(g^{z+1-q}\right) = \xi^{z+1-q},$$

while for $z+1-q \le \ell \le z-1$,

$$g * \xi^\ell = \sigma\left(g \cdot \sigma^{-1}(\xi^\ell)\right) = \sigma\left(g \cdot g^\ell\right) = \sigma\left(g^{\ell+1}\right) = \begin{cases} \xi^{\ell+1}, & z+1-q \le \ell \le z-2, \\ 0, & \ell = z-1. \end{cases}$$

For $2 \le k \le q-1$, the action of g^k on $\mathbb{F}_q$ is

$$g^k * 0 = \sigma\left(g^k \cdot \sigma^{-1}(0)\right) = \sigma\left(g^k \cdot g^z\right) = \sigma\left(g^{z+k}\right) = \sigma\left(g^{z+k-q}\right) = \xi^{z+k-q} = \xi^{z+k-1},$$

while for $1 \le k + \ell \le q-1$,

$$\begin{aligned} g^k * \xi^\ell &= \sigma\left(g^k \cdot \sigma^{-1}(\xi^\ell)\right) = \sigma\left(g^k \cdot g^\ell\right) = \sigma\left(g^{k+\ell}\right) \\ &= \begin{cases} \xi^{k+\ell}, & 1 \le k+\ell \le z-1, \\ 0, & k+\ell = z, \\ \xi^{k+\ell-1}, & z+1 \le k+\ell \le q-1, \end{cases} \end{aligned}$$

$$= \begin{cases} \xi^{k+\ell}, & 1-k \leq \ell \leq z-k-1, \\ 0, & \ell = z-k, \\ \xi^{k+\ell-1}, & z-k+1 \leq \ell \leq q-1-k. \end{cases}$$

But for $z \leq \ell \leq q-1-k$, we have

$$\sigma\left(g^{k+\ell-q}\right) = \sigma\left(g^{k+\ell}\right) = \xi^{k+\ell-1} = \xi^{k+\ell-1-(q-1)} = \xi^{k+\ell-q},$$

so $g^k * \xi^\ell = \xi^{k+\ell}$ when $z-(q-1) \leq \ell \leq -k$. Therefore,

$$g^k * \xi^\ell = \begin{cases} \xi^{k+\ell}, & z+1-q \leq \ell \leq z-k-1, \\ 0, & \ell = z-k, \\ \xi^{k+\ell-1}, & z-k+1 \leq \ell \leq z-1. \end{cases}$$

Finally, interpolation yields the desired polynomials. □

We remark that it is straightforward to prove directly that each representation polynomial $f_g^{[\xi;z]}(X) = \xi X + \xi^z h_{q-2}(\xi^{1-z}X)$ is in fact a permutation polynomial. First, observe that

$$h_{q-2}(x) = \begin{cases} 1, & x = 0, \\ -1, & x = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Consequently, it can be seen that

$$f_g^{[\xi;z]}(x) = \begin{cases} \xi^z, & x = 0, \\ 0, & x = \xi^{z-1}, \\ \xi x, & \text{otherwise,} \end{cases}$$

from which the permutation behavior of $f_g^{[\xi;z]}(X)$ is clear. Of course, Theorem 5.3 tells us more than this.

§ 6. Multiplicative representations of nonabelian groups

In this section, we use hemimorphisms to construct polynomial representations of certain dihedral and Hamiltonian groups. In both cases, the preserved subgroup $P^\star(G,\sigma)$ is a large (index 2) subgroup of G, and accordingly half of the polynomials in the representation group Γ are linear by Corollary 3.6.

§ 6.1. Representation of dihedral groups of order $q-1$

Suppose $q-1 = 2m$ for some $m \in \mathbb{N}$ and consider the dihedral group of order $2m$ with presentation

$$D_{2m} = \left\langle r, t \mid r^m = t^2 = rtrt = 1 \right\rangle.$$

Let ρ be a generator of $\langle \zeta^2 \rangle$, let τ be a generator of $\langle \zeta \rangle = \mathbb{F}_q^\times$, and define $\sigma\colon D_{2m} \to \mathbb{F}_q$ by $\sigma(r^k t^\varepsilon) = \rho^k \tau^\varepsilon$ for all $k \in \{0,1,\ldots,m-1\}$ and all $\varepsilon \in \{0,1\}$. By construction, σ is a hemimorphism.

Let $x = \rho^\ell \tau^\varepsilon \in \mathbb{F}_q^\times$. Then the action of r^k on x is

$$\begin{aligned} r^k * x &= \sigma\left(r^k \cdot \sigma^{-1}(\rho^\ell \tau^\varepsilon)\right) = \sigma\left(r^k \cdot r^\ell t^\varepsilon\right) = \sigma\left(r^{k+\ell} t^\varepsilon\right) \\ &= \rho^{k+\ell}\tau^\varepsilon = \rho^k \cdot \rho^\ell \tau^\varepsilon = \rho^k x = \sigma(r^k)x, \end{aligned}$$

which shows that $\langle r \rangle \leq P^\times(D_{2m},\sigma)$. In fact, we have $P^\times(D_{2m},\sigma) = \langle r \rangle$ since $\langle r \rangle \cong C_m$ is a maximal cyclic subgroup of D_{2m}.

Theorem 6.1. *The polynomial representing r^k is*

$$f_{r^k}^{[\rho,\tau]}(X) = \rho^k X,$$

and the polynomial representing t is

$$f_t^{[\rho,\tau]} = \tau X^{q-2}.$$

Proof. By Corollary 3.6, it is clear that $f_{r^k}^{[\rho,\tau]}(X) = \sigma(r^k)X = \rho^k X$.

Note that $t^\varepsilon = t^{-\varepsilon}$, so that the action of t on $x = \rho^\ell \tau^\varepsilon \in \mathbb{F}_q^\times$ is

$$t * x = \sigma\left(t \cdot \sigma^{-1}(\rho^\ell \tau^\varepsilon)\right) = \sigma\left(t \cdot r^\ell t^\varepsilon\right) = \sigma\left(r^{-\ell} t \cdot t^{-\varepsilon}\right) = \sigma\left(r^{-\ell} t^{1-\varepsilon}\right) = \rho^{-\ell}\tau^{1-\varepsilon}.$$

We interpolate to obtain

$$\begin{aligned}
f_t^{[\rho,\tau]}(X) &= \sum_{x \in \mathbb{F}_q^\times} \left(1 - (X-x)^{q-1}\left(t * x\right)\right. \\
&= \sum_{\ell=0}^{m-1} \left[\left(1 - (X-\rho^\ell)^{q-1}\right)(\rho^{-\ell}\tau) + \left(1 - (X-\rho^\ell\tau)^{q-1}\right)(\rho^{-\ell})\right] \\
&= \sum_{\ell=0}^{m-1} \left[\left(1 - X^{q-1} - h_{q-2}\left((\rho^\ell)^{-1}X\right)\right)\rho^{-\ell}\tau + \left(1 - X^{q-1} - h_{q-2}\left((\rho^\ell\tau)^{-1}X\right)\right)\rho^{-\ell}\right] \\
&= \left(\sum_{\ell=0}^{m-1}(1-X^{q-1})(\rho^{-\ell} + \rho^{-\ell}\tau)\right) - \left(\sum_{\ell=0}^{m-1}\rho^{-\ell}\left[\tau h_{q-2}(\rho^{-\ell}X) + h_{q-2}(\rho^{-\ell}\tau^{-1}X)\right]\right) \\
&= \left((1-X^{q-1})\sum_{x \in \mathbb{F}_q^\times} x\right) - \left(\sum_{\ell=0}^{m-1}\rho^{-\ell}\sum_{k=0}^{q-2}\left[\tau(\rho^{-\ell})^k + (\rho^{-\ell}\tau^{-1})^k\right]X^k\right) \\
&= 0 - \sum_{\ell=0}^{m-1}\rho^{-\ell}\sum_{k=0}^{q-2}\rho^{-\ell k}(\tau + \tau^{-k})X^k \\
&= -\sum_{k=0}^{q-2}(\tau + \tau^{-k})X^k \sum_{\ell=0}^{m-1}\rho^{-\ell(k+1)},
\end{aligned}$$

where the third line follows from Lemma 2.1. The innermost sum on the last line simplifies to

$$\sum_{\ell=0}^{m-1}\left(\rho^{-(k+1)}\right)^\ell = \begin{cases} m, & \rho^{-(k+1)} = 1, \\ 0, & \rho^{-(k+1)} \neq 1, \end{cases}$$

by Lemma 2.2. Since $o(\rho) = m$, we have $\rho^{-(k+1)} = 1$ when $m \mid (k+1)$, and hence either $k = m-1$ or $k = 2m-1$ as $0 \leq k \leq q-2 = 2m-1$.

It will be helpful at this point to perform several auxiliary computations. Since $2m = q-1$, we have that $\tau^{-m} = \tau^m$. Thus $o(\tau^m) = 2$ shows that τ^m is the unique element of $\mathbb{F}_q^\times$ of order 2, that is, $\tau^{-m} = -1$. Additionally, $\tau^{-2m} = (\tau^{-1})^{q-1} = 1$.

Continuing the computation of $f_t^{[\rho,\tau]}(X)$, we have

$$\begin{aligned}
f_t^{[\rho,\tau]}(X) &= -\sum_{k=0}^{q-2}(\tau + \tau^{-k})X^k \sum_{\ell=0}^{m-1}\rho^{-\ell(k+1)} \\
&= -m(\tau + \tau^{1-m})X^{m-1} - m(\tau + \tau^{1-2m})X^{2m-1} \\
&= -m\tau\left[(1 + \tau^{-m})X^{m-1} + (1 + \tau^{-2m})X^{2m-1}\right]
\end{aligned}$$

$$\begin{aligned}&= -m\tau\left[(1+(-1))X^{m-1} + (1+1)X^{2m-1}\right]\\ &= -2m\tau X^{2m-1}.\end{aligned}$$

Since $2m = q-1 \equiv -1 \pmod{p}$, we conclude that $f_t^{[\rho,\tau]}(X) = \tau X^{q-2}$. □

Corollary 6.2. *The polynomial representing $r^k t^\varepsilon \in D_{2m}$ is*

$$f_{r^k t^\varepsilon}^{[\rho,\tau]}(X) = \begin{cases}\rho^k X, & \text{when } \varepsilon = 0,\\ \rho^k \tau X^{q-2}, & \text{when } \varepsilon = 1.\end{cases}$$

Theorem 6.3. *Any two hemimorphisms representing D_{2m} are quasiequivalent. If we let σ and σ' be two such hemimorphisms with parameters ρ, τ and ρ', τ', repsectively, then writing $\rho = \tau^d$ and $\rho' = (\tau')^{d'}$, we have that σ and σ' are equivalent if and only if $d = d'$.*

Proof. Without loss of generality, we may fix the assignation σ to be

$$\sigma(r) = \rho = \zeta^2, \quad \sigma(t) = \tau = \zeta.$$

Now let σ' be defined by

$$\sigma'(r) = \rho' = (\zeta^y)^2, \quad \sigma'(t) = \tau' = \zeta^z$$

for some $(y, 2m) = (z, 2m) = 1$ (so that ζ^y and ζ^z are generators of $\mathbb{F}_q^\times$). By Theorem 3.9, to prove that σ and σ' are quasiequivalent, it will suffice to show that there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ and $\psi \in \mathrm{Aut}(D_{2m})$ such that

$$\sigma(r) = \alpha^{-1}\left(\sigma'(\psi(r))\right), \quad \sigma(t) = \alpha^{-1}\left(\sigma'(\psi(t))\right).$$

To this end, define the number s to be the least positive integer satisfying $s \equiv y^{-1}z \pmod{2m}$; we know that y is invertible modulo $2m$ since $(y, 2m) = 1$. Note that s is also invertible modulo $2m$, since y and z are, and hence that s is odd. We claim that the functions α and ψ defined by $\alpha(x) = x^z$ and $\psi(x) = x^s$, respectively, satisfy the above equations.

First, we verify that α and ψ are automorphisms of the appropriate groups. That $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ is clear since $(z, 2m) = (z, q-1) = 1$. Thus if we can show that $\psi(r)$ and $\psi(t)$ satisfy the same relations as r and t, respectively, then $\psi(r)$ and $\psi(t)$ will be generators for a group isomorphic to D_{2m}; that is, ψ will be an automorphism of D_{2m}.

Since s is invertible modulo $2m$, it is also invertible modulo m. Hence $\psi(r) = r^s$ is also a generator of $\langle r\rangle$, and so has order m. Moreover, $\psi(t)$ has order two since $\psi(t) = t^s = t$ as s is odd. Finally,

$$\psi(r)\psi(t)\psi(r)\psi(t) = r^s t^s r^s t^s = r^s(tr^s t) = r^s(r^{-s}) = 1$$

shows that $\psi(t)$ and $\psi(r)$ satisfy all the necessary relations, so $\psi \in \mathrm{Aut}(D_{2m})$.

Now it remains to verify that the conditions of Theorem 3.9 are satisfied. Note that

$$ysz^{-1} \equiv y(y^{-1}z)z^{-1} \equiv 1 \pmod{2m}$$

and $\alpha^{-1}(x) = \alpha(x)^{[-1]} = x^{z^{-1}}$. Then

$$\alpha^{-1}\left(\sigma'(\psi(r))\right) = \alpha^{-1}\left(\sigma'(r^s)\right) = \left((\zeta^{2y})^s\right)^{z^{-1}} = \zeta^2 = \sigma(r)$$

and

$$\alpha^{-1}\left(\sigma'(\psi(t))\right) = \alpha^{-1}\left(\sigma'(t)\right) = (\zeta^z)^{z^{-1}} = \zeta = \sigma(t),$$

as desired.

For the assignations σ and σ' to be equivalent, we require that we can choose ψ to be the identity, that is, $s = 1$. Consider the more-general case where σ is defined by

$$\sigma(r) = \rho = \tau^d, \quad \sigma(t) = \tau,$$

and σ' is defined by

$$\sigma'(r) = \rho' = (\tau')^{d'} = \tau^{zd'}, \quad \sigma'(t) = \tau' = \tau^{z}.$$

Let $\alpha \in \operatorname{Aut}(\mathbb{F}_q^\times)$ be defined by $\alpha(x) = x^a$. In order to satisfy the conditions of Theorem 3.9, we require that

$$\tau = \sigma(t) = \alpha^{-1}\left(\sigma'(t)\right) = \alpha^{-1}\left(\tau^{z}\right) = \tau^{za^{-1}},$$

which shows that we must have $a \equiv z \pmod{2m}$. Thus $\alpha(x) = x^z$, and indeed $\alpha \in \operatorname{Aut}(\mathbb{F}_q^\times)$ since $(z, 2m) = 1$. Furthermore, the theorem also requires that

$$\tau^{d} = \sigma(r) = \alpha^{-1}\left(\sigma'(r)\right) = \alpha^{-1}\left(\tau^{zd'}\right) = \tau^{zd'z^{-1}} = \tau^{d'}.$$

Therefore σ and σ' define equivalent representations if and only if $d = d'$. □

§ 6.2. Representation of certain Hamiltonian groups of order $q - 1$

Hamiltonian groups are defined to be those nonabelian groups in which every subgroup is normal. A finite Hamiltonian group must be isomorphic to a direct product of a quaternion group of order 8, an elementary abelian 2-group, and an abelian group of odd order; see [12, pp. 143–145] for a proof. We will not consider the representation of Hamiltonian groups generally, but rather those of the following type.

Suppose $q - 1 = 8m$ for some odd $m \in \mathbb{N}$ and let H_{8m} be the Hamiltonian group of order $8m$ which is a direct product of the quaternion group and a cyclic group of odd order with presentation

$$H_{8m} = Q \times O = \left\langle i, j \mid i^2 = j^2 = -1, (-1)^2 = 1, ji = -ij \right\rangle \times \langle g \mid g^m = 1 \rangle.$$

Let ρ be a generator of $\langle \zeta^2 \rangle$, let τ be a generator of $\langle \zeta \rangle$, and define $\sigma\colon H_{8m} \to \mathbb{F}_q$ by $\sigma(i^\delta j^\varepsilon g^k) = \rho^{m\delta + 4k}\tau^\varepsilon$ for all $\delta \in \{0, 1, 2, 3\}$, all $\varepsilon \in \{0, 1\}$, and all $k \in \{0, 1, \ldots, m-1\}$. By construction, σ is a hemimorphism.

Let $x = \rho^{m\gamma + 4\ell}\tau^\varepsilon \in \mathbb{F}_q^\times$. Then the action of $i^\delta g^k$ on x is

$$\begin{aligned} i^\delta g^k * x &= \sigma\left(i^\delta g^k \cdot \sigma^{-1}(\rho^{m\gamma+4\ell}\tau^\varepsilon)\right) = \sigma\left(i^\delta g^k \cdot i^\gamma j^\varepsilon g^\ell\right) = \sigma\left(i^{\delta+\gamma} j^\varepsilon g^{k+\ell}\right) \\ &= \rho^{m(\delta+\gamma)+4(k+\ell)}\tau^\varepsilon = \rho^{m\delta+4k} \cdot \rho^{m\gamma+4\ell}\tau^\varepsilon = \rho^{m\delta+4k}x = \sigma(i^\delta g^k)x, \end{aligned}$$

which shows that $\langle i, g \rangle \le P^\times(H_{8m}, \sigma)$. In fact, we have $P^\times(H_{8m}, \sigma) = \langle i, g \rangle$ since $\langle i, g \rangle \cong C_{4m}$ is a maximal cyclic subgroup of H_{8m}.

Theorem 6.4. *The polynomial representing $i^\delta g^k$ is*

$$f_{i^\delta g^k}^{[\rho,\tau]}(X) = \rho^{m\delta+4k}X,$$

and the polynomial representing j is

$$f_j^{[\rho,\tau]}(X) = 2^{-1}\tau\left[(1 - \tau^{-2-2m})X^{2m+1} + (1 + \tau^{-2-2m})X^{6m+1}\right].$$

Proof. By Corollary 3.6, it is clear that $f_{i^\delta g^k}^{[\rho,\tau]}(X) = \sigma(i^\delta g^k)X = \rho^{m\delta+4k}X$.

The action of j on $x = \rho^{m\gamma+4\ell}\tau^\varepsilon \in \mathbb{F}_q^\times$ is

$$\begin{aligned} j * \rho^{m\gamma+4\ell}\tau^\varepsilon &= \sigma\left(j \cdot \sigma^{-1}(\rho^{m\gamma+4\ell}\tau^\varepsilon)\right) = \sigma\left(j \cdot i^\gamma j^\varepsilon g^\ell\right) \\ &= \begin{cases} \sigma\left(i^{-\gamma} j g^\ell\right), & \varepsilon = 0, \\ \sigma\left(i^{2-\gamma} g^\ell\right), & \varepsilon = 1, \end{cases} \\ &= \begin{cases} \rho^{-m\gamma+4\ell}\tau, & \varepsilon = 0, \\ \rho^{m(2-\gamma)+4\ell}, & \varepsilon = 1. \end{cases} \end{aligned}$$

Interpolation proceeds in a similar to the proof of Theorem 6.1, and yields the desired result. □

Corollary 6.5. *The polynomial representing* $i^\delta j^\varepsilon g^k \in H_{8m}$ *is*

$$f^{[\rho,\tau]}_{i^\delta j^\varepsilon g^k}(X) = \begin{cases} \rho^{m\delta+4k}X, & \textit{when } \varepsilon = 0, \\ 2^{-1}\rho^{m\delta+4k}\tau\left[(1-\tau^{-2-2m})X^{2m+1} + (1+\tau^{-2-2m})X^{6m+1}\right], & \textit{when } \varepsilon = 1. \end{cases}$$

Theorem 6.6. *Any two hemimorphisms representing* H_{8m} *are quasiequivalent. If we let* σ *and* σ' *be two such hemimorphisms with parameters* ρ, τ *and* ρ', τ', *repsectively, then writing* $\rho = \tau^d$ *and* $\rho' = (\tau')^{d'}$, *we have that* σ *and* σ' *are equivalent if and only if* $d \equiv d' \pmod{4m}$.

Proof. Without loss of generality, we may fix the assignation σ to be

$$\sigma(i) = \rho^m = \zeta^{2m}, \quad \sigma(j) = \tau = \zeta, \quad \sigma(g) = \rho^4 = \zeta^8.$$

Now let σ' be defined by

$$\sigma'(i) = (\rho')^m = (\zeta^y)^{2m}, \quad \sigma'(j) = \tau' = \zeta^z, \quad \sigma'(g) = (\rho')^4 = (\zeta^y)^8$$

for some $(y, 8m) = (z, 8m) = 1$ (so that ζ^y and ζ^z are generators of $\mathbb{F}_q^\times$). By Theorem 3.9, to prove that σ and σ' are quasiequivalent, it will suffice to show that there exist $\alpha \in \operatorname{Aut}(\mathbb{F}_q^\times)$ and $\psi \in \operatorname{Aut}(D_{2m})$ such that

$$\sigma(i) = \alpha^{-1}\left(\sigma'(\psi(i))\right), \quad \sigma(j) = \alpha^{-1}\left(\sigma'(\psi(j))\right), \quad \sigma(g) = \alpha^{-1}\left(\sigma'(\psi(g))\right).$$

We claim that the functions α and ψ, defined as follows, satisfy the above equations. Define the function α by $\alpha(x) = x^z$. Let s be the least positive integer satisfying $s \equiv y^{-1}z \pmod{8m}$; we know that y is invertible modulo $8m$ since $(y, 8m) = 1$. Now let ψ to be the homomorphism defined by $\psi(i) = i^s$, $\psi(j) = j$, and $\psi(g) = g^s$.

First, we verify that α and ψ are automorphisms of the appropriate structures. That $\alpha \in \operatorname{Aut}(\mathbb{F}_q^\times)$ is clear since $(z, 8m) = (z, q-1) = 1$. Note that s is invertible modulo $8m$ since $(y, 8m) = (z, 8m) = 1$. Thus, in particular, s is invertible modulo m and modulo 4, and hence $\psi(i)$ and $\psi(g)$ are generators of $\langle i \rangle$ and $\langle g \rangle = O$, respectively. Certainly ψ induces an automorphism of O, and moreover, ψ also induces an automorphism of Q since $\operatorname{Aut}(Q) \cong S_{24}$, and hence there exists an automorphism of Q which maps i to $i^s = i^{\pm 1}$ and fixes j. Therefore $\psi \in \operatorname{Aut}(H_{8m})$.

It remains to verify that the conditions of Theorem 3.9 are satisfied. Note that

$$ysz^{-1} \equiv y(y^{-1}z)z^{-1} \equiv 1 \pmod{8m}$$

and $\alpha^{-1}(x) = \alpha(x)^{[-1]} = x^{z^{-1}}$. Then

$$\alpha^{-1}\left(\sigma'(\psi(i))\right) = \alpha^{-1}\left(\sigma'(i^s)\right) = \left((\zeta^{2my})^s\right)^{z^{-1}} = \zeta^{2m} = \sigma(i),$$

$$\alpha^{-1}\left(\sigma'(\psi(j))\right) = \alpha^{-1}\left(\sigma'(j)\right) = (\zeta^z)^{z^{-1}} = \zeta = \sigma(j),$$

and

$$\alpha^{-1}\left(\sigma'(\psi(g))\right) = \alpha^{-1}\left(\sigma'(g^s)\right) = \left((\zeta^{8y})^s\right)^{z^{-1}} = \zeta^8 = \sigma(g),$$

as desired.

For the assignations σ and σ' to be equivalent, we require that we can choose ψ to be the identity, that is, $s = 1$. Consider the more-general case where σ is defined by

$$\sigma(i) = \rho^m = \tau^{md}, \quad \sigma(j) = \tau, \quad \sigma(g) = \rho^4 = z^{4d},$$

and σ' is defined by

$$\sigma'(i) = (\rho')^m = \left((\tau')^{d'}\right)^m = \tau^{md'z}, \quad \sigma'(j) = \tau' = \tau^z, \quad \sigma(g) = (\rho')^4 = \left((\tau')^{d'}\right) = \tau^{4d'z}.$$

Let $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ be defined by $\alpha(x) = x^a$. In order to satisfy the conditions of Theorem 3.9, we require that

$$\tau = \sigma(t) = \alpha^{-1}\left(\sigma'(t)\right) = \alpha^{-1}\left(\tau^z\right) = \tau^{za^{-1}},$$

which shows that we must have $a \equiv z \pmod{8m}$. Thus $\alpha(x) = x^z$, and indeed $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ since $(z, 8m) = 1$. Furthermore, the theorem also requires that

$$\tau^{md} = \sigma(i) = \alpha^{-1}\left(\sigma'(i)\right) = \alpha^{-1}\left(\tau^{md'z}\right) = \tau^{md'zz^{-1}} = \tau^{md'}$$

and

$$\tau^{4d} = \sigma(g) = \alpha^{-1}\left(\sigma'(g)\right) = \alpha^{-1}\left(\tau^{4d'z}\right) = \tau^{4d'zz^{-1}} = \tau^{4d'}.$$

From the first equation, we have $md \equiv md' \pmod 4$, and hence $d \equiv d' \pmod 4$ (since m is odd); similarly, we have $d \equiv d' \pmod m$ since the second equation implies $4d \equiv 4d' \pmod m$. Thus we conclude that σ and σ' define equivalent representations if and only if $d \equiv d' \pmod{4m}$. □

References

[1] M. Aschbacher, *Finite Group Theory*, Cambridge: Cambridge University Press, 1986.

[2] E.R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw Hill, 1968.

[3] O. Bottema, *On the Betti-Mattieu group*, Nieuw Arch. Wisk. (2)**16** no. 4 (1930), 46–50.

[4] L. Carlitz, *Permutations in a finite field*, Proc. Amer. Math. Soc. **4** (1953), 538.

[5] ______, *A note on the Betti-Mattieu group*, Portugal. Math. **22** (1963), 121–125.

[6] 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** (1897), 65–120, 161–183.

[7] J.D. Dixon and B. Mortimer, *Permutation Groups*, New York: Springer, 1996.

[8] C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57** (1863), 750–757.

[9] R. Lidl and G.L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly **95** (1988), 243–246.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge: Cambridge University Press, 1997.

[11] R. Matthews, *Permutation properties of the polynomials $1 + x + \cdots + x^k$ over a finite field*, Proc. Amer. Math. Soc. **120** (1994), 47–51.

[12] D.J.S. Robinson, *A Course in the Theory of Groups*, second edition, New York: Springer, 1996.

[13] T.P. Vaughan, *Polynomials and linear transformations over finite fields*, J. reine angew. Math. **262** (1974), 179–206.

[14] D. Wan and R. Lidl, *Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure*, Mh. Math. **112** (1991), 149–163.

[15] C. Wells, *Generators for groups of permutation polynomials over finite fields*, Acta Sci. Math. Szeged **29** (1968), 167–176.