2016

Binary Quartic Forms over Fp

Daniel Thomas Kamenetsky
University of South Carolina

Binary Quartic Forms over $\mathbb{F}_p$

by

Daniel Thomas Kamenetsky

Bachelor of Arts
Hamilton College 2011

Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Arts in

Mathematics

College of Arts and Sciences

University of South Carolina

2016

Accepted by:

Frank Thorne, Director of Thesis

Michael Filaseta, Reader

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

Acknowledgments

I would like to thank my advisor, Dr. Frank Thorne, whose enthusiasm for the study of mathematics is unparalleled. I would also like to thank my parents for supporting me and encouraging me to choose my own path.

Thank you to Ed, who was there for the highs and the lows of my graduate school journey and will now be a lifelong friend. And to Emily, my partner and best friend, I could not have done this without you.

Abstract

Let V_p denote the five dimensional vector space of binary quartic forms over the finite field $\mathbb{F}_p$, with p a prime greater than 3. There is a natural action of the group $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p. This action partitions V_p into orbits, the number of which increases with p. In this thesis, we determine explicitly, for a given p, the number of orbits under the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p. Moreover, we determine the size of each orbit and the general structure of the forms each orbit contains. We also introduce an application of understanding these orbits to the study of the Fourier transforms of certain functions over V_p that are of interest in algebraic number theory. We include two appendices with preliminary work towards extending key results from existing work on binary cubic forms to the case of binary quartic forms.

Table of Contents

List of Tables

Chapter 1

Introduction

The study of integral binary quadratic, cubic and quartic forms relies on understanding certain group actions. The group $\mathrm{GL}_2(\mathbb{Z})$ acts on such forms by linear substitution of variable. In the case of integral quadratic and cubic forms, this action has a unique polynomial invariant called the discriminant; that is, any other polynomial invariant for the action can be expressed as a polynomial in the discriminant. For quartic forms, two unique polynomial invariants are necessary to generate all others. This distinction creates a roadblock when attempting to extend results about quadratic and cubic forms to the quartic case. Recently in [1], Bhargava and Shankar overcame this challenge and applied their results on counting binary quartic forms having bounded invariants in their proof that the average rank of elliptic curves over $\mathbb{Q}$, when ordered by their heights, is bounded. Their work indicates a strong potential for interesting applications of the further study of binary quartic forms and the relevant group actions, not only over the integers, but also over finite fields.

Integral binary quadratic forms are well understood due to the seminal work of Gauss in *Disquisitiones Arithmeticae* and the contributions of many others over the last two centuries. Of particular interest in algebraic number theory is the connection between $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of irreducible integral binary quadratic forms and the class numbers of quadratic fields.

Also with motivation from applications in algebraic number theory, integral binary cubic forms have been studied extensively. Delone and Faddeev showed that there is a bijection between the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible integral binary

cubic forms and the set of isomorphism classes of cubic rings. This correspondence together with an asymptotic formula for the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible integral binary cubic forms with fixed discriminant, proved by Davenport, led to Davenport and Heilbronn providing an asymptotic formula for the number of cubic fields, up to isomorphism, with bounded discriminant. Roberts later conjectured the existence of a second main term in the Davenport-Heilbronn theorem, which has been proved independently by Taniguchi and Thorne [7] and Bhargava, Shankar, and Tsimerman [2]. The work of Bhargava, Shankar, and Tsimerman draws from classical geometry of numbers techniques, which they extend by finding ways to count points in fundamental domains with complicated cuspidal regions. On the other hand, Taniguchi and Thorne build off of the theory of Shintani zeta functions. One of the ingredients in their proof is the computation of certain cubic Gauss sums that appear in the functional equations for these zeta functions; controlling the Gauss sums leads to good error terms in the sieve methods that they use. Interesting questions arise when one looks at analogous sums in the case of binary quartic forms. We investigate one sum of interest, and we take the first step towards an explicit formula. We overcome a key hurdle that is not present in the cubic case; in particular, we classify the orbits of the natural action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on the space of binary quartic forms over $\mathbb{F}_p$.

1.1 The Fourier Transform of a Function on the Space of Cubic Forms and Motivating Examples

Let p be a prime greater than three, and let W_p denote the four dimensional vector space of binary cubic forms over the finite field $\mathbb{F}_p$. We express an element $f \in W_p$ in the form

$$f(x, y) = a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3,$$

and we identify the 4-tuple $a = (a_1, a_2, a_3, a_4) \in \mathbb{F}_p^4$ with f. The group $\mathrm{GL}_2(\mathbb{F}_p)$ naturally acts on W_p. An element $\gamma \in \mathrm{GL}_2(\mathbb{F}_p)$ acts on $f(x, y)$ by

$$\gamma \cdot f(x, y) = \frac{1}{\det(\gamma)} f((x, y) \cdot \gamma).$$

One consequence of including the scalar $1/(\det(\gamma))$ is that

$$\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \cdot f(x, y) = cf(x, y).$$

Let $f \in W_p$. We say that $[\alpha : \beta] \in \mathbb{P}^1(\mathbb{F}_q)$, with q a power of p, is a root of f if $f(\alpha, \beta) = 0$. Table 1.1 shows a partition of W_p into sets corresponding to conditions on the roots of a given form. It is straightforward to compute the number of elements in each set by considering the number of possibilities for each root and accounting for scaling. The cardinalities are given in the table so that they suggest the intuitive counting argument. For our purposes, it is important to note that the sets $W_p(0)$, $W_p(1^3)$, $W_p(1^21)$, $W_p(111)$, $W_p(21)$, and $W_p(3)$ are the orbits of the action of $\mathrm{GL}_2(\mathbb{F}_p)$ on W_p [6].

Table 1.1 A partition of W_p

Set notation	Description	Cardinality
$W_p(0)$	The form 0	1
$W_p(111)$	Set of forms with three distinct roots in $\mathbb{P}^1(\mathbb{F}_p)$	$\binom{p+1}{3}(p-1)$
$W_p(1^21)$	Set of forms with a double root in $\mathbb{P}^1(\mathbb{F}_p)$ and one other distinct root in $\mathbb{P}^1(\mathbb{F}_p)$	$(p+1)p(p-1)$
$W_p(1^3)$	Set of forms with a triple root in $\mathbb{P}^1(\mathbb{F}_p)$	$(p+1)(p-1)$
$W_p(21)$	Set of forms with a conjugate pair of roots in $\mathbb{P}^1(\mathbb{F}_{p^2})$ and one other distinct root in $\mathbb{P}^1(\mathbb{F}_p)$	$\frac{p^2-p}{2}(p+1)(p-1)$
$W_p(3)$	Set of forms with a triple of conjugate roots in $\mathbb{P}^1(\mathbb{F}_{p^3})$	$\frac{p^3-p}{3}(p-1)$

In what remains of this section, we provide the details of an argument from the work of Bhargava, Shankar, and Tsimerman in [2] and a result of Taniguchi and Thorne in [6], both of which demonstrate an application of the Fourier transform of certain functions on W_p.

We begin with section 9.4 of [2], in which the authors work through an equidistribution argument that allows them to determine the main term for the weighted count of irreducible integral binary cubic forms having bounded discriminant, where each form is weighted by the number of its roots in $\mathbb{P}_1(\mathbb{Z}/n\mathbb{Z})$. A key component of the argument is finding a pointwise bound for the Fourier transform of the function $w_p : W_p \to \mathbb{C}$, which given a form f as its input, outputs the number of roots in $P^1(\mathbb{F}_p)$.

Let $\widehat{W_p}$ be the space of additive characters $\chi : W_p \to \mathbb{C}^\times$. Then the Fourier transform $\widehat{w_p}$ of w_p is given by

$$\widehat{w_p}(\chi) = p^{-4} \sum_{f \in W_p} w_p(f)\overline{\chi}(f).$$

Since W_p is a finite abelian group isomorphic to $\mathbb{F}_p^4$, the dual group $\widehat{W_p}$ is also isomorphic to $\mathbb{F}_p^4$, and we can list the characters explicitly by identifying them with elements of W_p. First, we define a bilinear form:

$$[f, g] = a_4b_1 - \frac{1}{3}a_3b_2 + \frac{1}{3}a_2b_3 - a_1b_4,$$

where $f \in W_p$ and $g \in W_p$ are identified with $(a_1, a_2, a_3, a_4) \in \mathbb{F}_p^4$ and $(b_1, b_2, b_3, b_4) \in \mathbb{F}_p^4$, respectively. Recall that p is a prime greater than three, and so, 3 is invertible. We choose this alternating form as opposed to the usual dot product because it has the property that given $\gamma \in \mathrm{GL}_2(\mathbb{F}_p)$,

$$[\gamma \cdot f, g] = \det(\gamma)[f, \gamma^{-1} \cdot g], \tag{1.1}$$

which will be relevant when we move to the work of Taniguchi and Thorne [6]. Next, we define a complex-valued bilinear map, which allows us to identify the elements of

W_p with the elements of $\widehat{W_p}$:

$$\langle f, g\rangle_p = \exp\left(\frac{2\pi i}{p}[f, g]\right).$$

For each g in W_p, $\langle -, g\rangle_p$ defines the corresponding character in $\widehat{W_p}$. For example, the form 0 is identified with the trivial character $\langle -, 0\rangle_p$, which maps all of W_p to 1. We can now express the Fourier transform $\widehat{w_p}$ as a function on W_p:

$$\widehat{w_p}\,(g) = p^{-4} \sum_{f \in W_p} w_p(f)\langle f, g\rangle_p.$$

To bound the Fourier transform of w_p pointwise, Bhargava, Shankar and Tsimerman address $\widehat{w_p}(0)$ and $\widehat{w_p}(g)$ with $g \neq 0$ separately. First, we observe that

$$\widehat{w_p}\,(0) = p^{-4} \sum_{f \in W_p} w_p(f).$$

Moreover, we have that $w_p(0) = p + 1$; $w_p(f) = 3$ if $f \in W_p(111)$, $w_p(f) = 2$ if $f \in W_p(1^21)$; $w_p(f) = 1$ if $f \in W_p(1^3)$ or $f \in W_p(21)$; $w_p(f) = 0$ if $f \in W_p(3)$. Hence, from Table 1.1, we have that

$$\widehat{w_p}\,(0) = p^{-4}\left(p + 1 + 3\,|W_p(111)| + 2\left|W_p(1^21)\right| + \left|W_p(1^3)\right| + |W_p(21)|\right) = 1 + p^{-1}.$$

Next, we consider $\widehat{w_p}(g)$ where $g \neq 0$. We have that

$$\begin{aligned}\widehat{w_p}\,(g) &= p^{-4} \sum_{f \in W_p} w_p(f)\langle f, g\rangle_p \\ &= p^{-4} \sum_{f:\langle f,g\rangle_p = 1} w_p(f) + p^{-4} \sum_{f:\langle f,g\rangle_p \neq 1} w_p(f)\langle f, g\rangle_p.\end{aligned}$$

Note that $\langle f, g\rangle_p = 1$ if and only if $[f, g] = 0$. If $0 \neq (b_1, b_2, b_3, b_4) \in \mathbb{F}_p^4$ is fixed, then at least one of b_1, b_2, b_3, b_4, which we denote by b, is nonzero. For any of the p^3 choices for the three a_i paired with the $b_j \neq b$ in the equation $a_4b_1 - \frac{1}{3}a_3b_2 + \frac{1}{3}a_2b_3 - a_1b_4 = 0$, the a_i corresponding to b is uniquely determined by the equation. Hence, there are p^3 choices for f, with $g \neq 0$, such that $[f, g] = 0$, and therefore, such that $\langle f, g\rangle_p = 1$. Moreover, we have seen that $w_p(0) = p + 1$ and that $w_p(f) \leq 3$ when $f \neq 0$. Thus,

$$\sum_{f:\langle f,g\rangle_p = 1} w_p(f) \leq 3(p^3 - 1) + (p + 1) = 3p^3 + p - 2.$$

Next, note that multiplying f by a scalar $c \in \mathbb{F}_p^\times$ does not impact the roots of f, and so, $w_p(cf) = w_p(f)$. So,

$$\sum_{c\in\mathbb{F}_p^\times} w_p(cf)\langle cf, g\rangle_p = w_p(f) \sum_{c\in\mathbb{F}_p^\times} \langle cf, g\rangle_p = w_p(f) \sum_{c\in\mathbb{F}_p^\times} \exp\left(\frac{2\pi i c}{p}[f, g]\right) = -w_p(f).$$

Moreover, for any $c \in \mathbb{F}_p^\times$, if $\langle f, g\rangle_p \neq 1$, then $\langle cf, g\rangle_p \neq 1$, and so, for any $c \in \mathbb{F}_p^\times$, the set of forms f such that $\langle f, g\rangle_p \neq 1$ is the same as the set of forms f such that $\langle cf, g\rangle_p \neq 1$. It now follows that

$$\begin{aligned}\sum_{f:\langle f,g\rangle_p\neq 1} w_p(f)\langle f, g\rangle_p &= \frac{1}{p-1} \sum_{c\in\mathbb{F}_p^\times} \sum_{f:\langle f,g\rangle_p\neq 1} w_p(cf)\langle cf, g\rangle_p \\ &= \frac{1}{p-1} \sum_{f:\langle f,g\rangle_p\neq 1} \sum_{c\in\mathbb{F}_p^\times} w_p(cf)\langle cf, g\rangle_p \\ &= -\frac{1}{p-1} \sum_{f:\langle f,g\rangle_p\neq 1} w_p(f),\end{aligned}$$

and also, since $w_p(f) \leq 3$ when $f \neq 0$,

$$\frac{1}{p-1} \sum_{f:\langle f,g\rangle_p\neq 1} w_p(f) \leq \frac{3}{p-1}(p^4 - p^3) = 3p^3.$$

Thus,

$$\widehat{w_p}\,(g) = p^{-4} \sum_{f:\langle f,g\rangle_p=1} w_p(f) + p^{-4} \sum_{f:\langle f,g\rangle_p\neq 1} w_p(f)\langle f, g\rangle_p \ll p^{-1}$$

uniformly for $g \neq 0$.

Whereas bounding the Fourier transform of w_p is sufficient for Bhargava, Shankar, and Tsimerman to move forward with their equidistribution argument, Taniguchi and Thorne find explicit formulas for the Fourier transforms of certain functions relevant to their work. One example is the function $\phi_p : W_p \to \mathbb{C}$ defined as the characteristic function of those $f \in W_p$ with $\Delta(f) = 0$, where $\Delta(f)$ denotes the discriminant of the binary cubic form f. We can express the Fourier transform $\widehat{\phi_p}$ of ϕ_p as a function on W_p as we did with $\widehat{w_p}$ above:

$$\widehat{\phi_p}\,(g) = p^{-4} \sum_{f\in W_p} \phi_p(f)\langle f, g\rangle_p.$$

We then have the following result:

Proposition 1.1. (Taniguchi-Thorne) The Fourier transform of ϕ_p is given by

$$\widehat{\phi_p}(g) = \begin{cases} p^{-1} + p^{-2} - p^{-3} & \text{if } g = 0 \\ p^{-2} - p^{-3} & \text{if } \Delta(g) \neq 0, g \neq 0 \cdot \\ -p^{-3} & \text{if } \Delta(g) = 0 \end{cases}$$

Proof. Let $G = \mathrm{GL}_2(\mathbb{F}_p)$, and let $g \in W_p$. We will express the sum

$$S = \sum_{a_1 \in \mathbb{F}_p} \sum_{a_2 \in \mathbb{F}_p} \sum_{\gamma \in G} \langle \gamma \cdot (a_1 x^3 + a_2 x^2 y), g \rangle_p$$

in two different ways.

As a_1 and a_2 vary, we obtain the form 0 when $a_1 = a_2 = 0$, $p-1$ forms in the orbit $W_p(1^3)$ when $a_1 \in \mathbb{F}_p^\times$ and $a_2 = 0$, and $p(p-1)$ forms in the orbit $W_p(1^2 1)$ when $a_1 \in \mathbb{F}_p$ and $a_2 \in \mathbb{F}_p^\times$. So, instead of summing over G, we can sum over the orbits $W_p(0)$, $W_p(1^3)$, and $W_p(1^2 1)$. Note that $\sum_{f \in W_p(0)} \langle f, g \rangle_p = 1$. Hence,

$$\begin{aligned} S &= |G| + (p-1)\frac{|G|}{|W_p(1^3)|} \sum_{f \in W_p(1^3)} \langle f, g \rangle_p + p(p-1)\frac{|G|}{|W_p(1^2 1)|} \sum_{f \in W_p(1^2 1)} \langle f, g \rangle_p \\ &= |G| \left(1 + \frac{1}{p+1} \sum_{f \in W_p(1^3)} \langle f, g \rangle_p + \frac{1}{p+1} \sum_{f \in W_p(1^2 1)} \langle f, g \rangle_p \right). \end{aligned}$$

On the other hand, from property (1.1), we have that

$$\langle \gamma \cdot (a_1 x^3 + a_2 x^2 y), g \rangle_p = \exp\left(\frac{2\pi i}{p} \det(\gamma)[a_1 x^3 + a_2 x^2 y, \gamma^{-1} \cdot g] \right).$$

Hence,

$$S = \sum_{\gamma \in G} \sum_{a_1 \in \mathbb{F}_p} \sum_{a_2 \in \mathbb{F}_p} \exp\left(\frac{2\pi i}{p} \det(\gamma)[a_1 x^3 + a_2 x^2 y, \gamma \cdot g] \right).$$

If $\gamma \cdot g(x, y) = b_1 x^3 + b_2 x^2 y + b_3 x y^2 + b_4 y^3$, then

$$[a_1 x^3 + a_2 x^2 y, \gamma \cdot g] = \frac{1}{3} a_2 b_3 - a_1 b_4.$$

So, by orthogonality relations, $S = 0$ unless there is some $\gamma \in G$ such that $\gamma \cdot g(x, y)$ can be expressed in the form $b_1 x^3 + b_2 x^2 y$, in which case

$$\exp\left(\frac{2\pi i}{p} \det(\gamma)[a_1 x^3 + a_2 x^2 y, \gamma \cdot g] \right) = 1.$$

If $g \in W_p(0)$, then $\gamma \cdot g$ is in this form, namely with $b_1 = b_2 = 0$. If $g \in W_p(1^3)$, then there are $(p-1)|G|/|W_p(1^3)|$ choices for γ such that $\gamma \cdot g(x,y)$ is in this form, namely such that $b_1 \in \mathbb{F}_p^\times$ and $b_2 = 0$. If $g \in W_p(1^21)$, then there are $p(p-1)|G|/|W_p(1^21)|$ choices for γ such that $\gamma \cdot g(x,y)$ is in this form, namely such that $b_1 \in \mathbb{F}_p$ and $b_2 \in \mathbb{F}_p^\times$. Otherwise, $[0,1]$ is not a double root of $\gamma \cdot g(x,y)$, and so, $\gamma \cdot g(x,y)$ cannot be expressed in the form $b_1x^3 + b_2x^2y$. Thus,

$$S = \begin{cases} |G|p^2 & \text{if } g \in W_p(0) \\ (p-1)\frac{|G|}{|W_p(1^3)|}p^2 & \text{if } g \in W_p(1^3) \\ p(p-1)\frac{|G|}{|W_p(1^21)|}p^2 & \text{if } g \in W_p(1^21) \\ 0 & \text{otherwise.} \end{cases}$$

Combining the two expressions for S and dividing through by $|G|$, we have

$$1 + \frac{1}{p+1}\sum_{f \in W_p(1^3)} \langle f, g\rangle_p + \frac{1}{p+1}\sum_{f \in W_p(1^21)} \langle f, g\rangle_p = \begin{cases} p^2 & \text{if } g \in W_p(0) \\ \frac{1}{p+1}p^2 & \text{if } g \in W_p(1^3) \\ \frac{1}{p+1}p^2 & \text{if } g \in W_p(1^21) \\ 0 & \text{otherwise,} \end{cases}$$

and so,

$$\sum_{f \in W_p(1^3)} \langle f, g\rangle_p + \sum_{f \in W_p(1^21)} \langle f, g\rangle_p = \begin{cases} p^3 + p^2 - p - 1 & \text{if } g \in W_p(0) \\ p^2 - p - 1 & \text{if } g \in W_p(1^3) \text{ or } g \in W_p(1^21) \\ -p - 1 & \text{otherwise.} \end{cases}$$

Finally, since $\Delta(f) = 0$ if and only if f has a repeated root, we have

$$\begin{aligned}
\widehat{\phi_p}(g) &= \frac{1}{p^4} \sum_{f \in W_p} \phi_p(f) \langle f, g \rangle_p \\
&= \frac{1}{p^4} \left(\sum_{f \in W_p(0)} \langle f, g \rangle_p + \sum_{f \in W_p(1^3)} \langle f, g \rangle_p + \sum_{f \in W_p(1^2 1)} \langle f, g \rangle_p \right) \\
&= \begin{cases} p^{-1} + p^{-2} - p^{-3} & \text{if } g = 0 \\ p^{-2} - p^{-3} & \text{if } \Delta(g) \neq 0, g \neq 0 \\ -p^{-3} & \text{if } \Delta(g) = 0. \end{cases}
\end{aligned}$$

□

Proposition 1.1 serves as the primary motivating example for our work.

1.2 The Space of Binary Quartic Forms over $\mathbb{F}_p$

We now shift our focus to binary quartic forms. Let V_p denote the five dimensional vector space of binary quartic forms over the finite field $\mathbb{F}_p$, with p a prime greater than 3. We express an element $f \in V_p$ in the form

$$f(x, y) = a_1 x^4 + a_2 x^3 y + a_3 x^2 y^2 + a_4 x y^3 + a_5 y^4,$$

and we identify the 5-tuple $a = (a_1, a_2, a_3, a_4, a_5) \in \mathbb{F}_p^5$ with f. As in the cubic case, the group $\mathrm{GL}_2(\mathbb{F}_p)$ naturally acts on V_p. An element $\gamma \in \mathrm{GL}_2(\mathbb{F}_p)$ acts on $f(x, y)$ by linear substitution of variable:

$$\gamma \cdot f(x, y) = f((x, y) \cdot \gamma).$$

The group $\mathrm{GL}_1(\mathbb{F}_p)$ also naturally acts on V_p by scalar multiplication. We will consider the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p given by

$$(c, \gamma) \cdot f(x, y) = c f((x, y) \cdot \gamma).$$

In the cubic case, we partitioned W_p into sets corresponding to conditions on the roots of a given form. An analogous partition of V_p is given in Table 1.2. It is again

straightforward to compute the number of elements in each set by considering the number of possibilities for each root and accounting for scaling. Does this partition correspond to the orbits of the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p? Unfortunately, the answer is no, but it does provide a starting point. Before exploring the orbits further, we use the final section of Chapter 1 to introduce the function on V_p that we would like to study.

1.3 The Fourier Transform of a Function on the Space of Quartic Forms

Our goal is to find a result similar to Proposition 1.1 in the quartic case. We begin by redefining $\Delta(f)$ to be the discriminant of the binary quartic form f, and let ν_p be the characteristic function of those $f \in V_p$ with $\Delta(f) = 0$. Next, we define the Fourier transform $\widehat{\nu_p}$ of ν_p as we did in the cubic case. Let $\widehat{V_p}$ be the space of additive characters $\chi : V_p \to \mathbb{C}^\times$. Then the Fourier transform $\widehat{\nu_p}$ of ν_p is given by

$$\widehat{\nu_p}(\chi) = p^{-5} \sum_{f \in V_p} \nu_p(f)\overline{\chi}(f).$$

Since V_p is a finite abelian group isomorphic to $\mathbb{F}_p^5$, the dual group $\widehat{V_p}$ is also isomorphic to $\mathbb{F}_p^5$, and we can list the characters explicitly by identifying them with elements of V_p. We define a different bilinear form for the quartic case:

$$[f, g] = a_5 b_1 - \frac{1}{4} a_4 b_2 + \frac{1}{6} a_3 b_3 - \frac{1}{4} a_2 b_4 + a_1 b_5,$$

where $f \in V_p$ and $g \in V_p$ are identified with $(a_1, a_2, a_3, a_4, a_5) \in \mathbb{F}_p^5$ and $(b_1, b_2, b_3, b_4, b_5) \in \mathbb{F}_p^5$, respectively. Recall that p is a prime greater than three, and so, 4 and 6 are invertible. We choose this alternating form because it has a property similar to property (1.1), namely, that given $\gamma \in \mathrm{GL}_2(\mathbb{F}_p)$,

$$[(c, \gamma) \cdot f, g] = (\det \gamma)^4 [f, (c, \gamma^{-1}) \cdot g]. \tag{1.2}$$

Table 1.2 A partition of V_p

Set notation	Description	Cardinality
$V_p(0)$	The form 0	1
$V_p(1111)$	Set of forms with four distinct roots in $\mathbb{P}^1(\mathbb{F}_p)$	$\binom{p+1}{4}(p-1)$
$V_p(1^211)$	Set of forms with a double root in $\mathbb{P}^1(\mathbb{F}_p)$ and two other distinct roots in $\mathbb{P}^1(\mathbb{F}_p)$	$(p+1)\binom{p}{2}(p-1)$
$V_p(1^21^2)$	Set of forms with two distinct double roots in $\mathbb{P}^1(\mathbb{F}_p)$	$\binom{p+1}{2}(p-1)$
$V_p(1^31)$	Set of forms with a triple root in $\mathbb{P}^1(\mathbb{F}_p)$ and one other distinct root in $\mathbb{P}^1(\mathbb{F}_p)$	$(p+1)(p)(p-1)$
$V_p(1^4)$	Set of forms with one root in $\mathbb{P}^1(\mathbb{F}_p)$ repeated four times	$(p+1)(p-1)$
$V_p(211)$	Set of forms with a conjugate pair of roots in $\mathbb{P}^1(\mathbb{F}_{p^2})$ and two distinct roots in $\mathbb{P}^1(\mathbb{F}_p)$	$\frac{p^2-p}{2}\binom{p+1}{2}(p-1)$
$V_p(21^2)$	Set of forms with a conjugate pair of roots in $\mathbb{P}^1(\mathbb{F}_{p^2})$ and one double root in $\mathbb{P}^1(\mathbb{F}_p)$	$\frac{p^2-p}{2}(p+1)(p-1)$
$V_p(22)$	Set of forms with two distinct conjugate pairs of roots in $\mathbb{P}^1(\mathbb{F}_{p^2})$	$\binom{\frac{p^2-p}{2}}{2}(p-1)$
$V_p(2^2)$	Set of forms with a conjugate pair of roots in $\mathbb{P}^1(\mathbb{F}_{p^2})$ repeated two times	$\frac{p^2-p}{2}(p-1)$
$V_p(31)$	Set of forms with a triple of conjugate roots in $\mathbb{P}^1(\mathbb{F}_{p^3})$ and one root in $\mathbb{P}^1(\mathbb{F}_p)$	$\frac{p^3-p}{3}(p+1)(p-1)$
$V_p(4)$	Set of forms with four conjugate roots in $\mathbb{P}^1(\mathbb{F}_{p^4})$	$\frac{p^4-p^2}{4}(p-1)$

It is straightforward to verify this property by expanding both sides of the equation. As in the cubic case, we define a complex-valued bilinear map, which allows us to identify the elements of V_p with the elements of $\widehat{V_p}$:

$$\langle f, g\rangle_p = \exp\left(\frac{2\pi i}{p}[f,g]\right).$$

For each g in V_p, $\langle -, g\rangle_p$ defines the corresponding character in $\widehat{V_p}$. We can now express the Fourier transform $\widehat{\nu_p}$ as a function on V_p:

$$\widehat{\nu_p}\,(g) = p^{-5} \sum_{f \in V_p} \nu_p(f)\langle f, g\rangle_p.$$

Given $g \in V_p$, we want an explicit formula for $\widehat{\nu_p}$. In the proof of Proposition 1.1, we exploit the fact that $W_p(0)$, $W_p(1^3)$, and $W_p(1^2 1)$ are orbits under the action of $\mathrm{GL}_2(\mathbb{F}_p)$ on W_p. We will show in Chapter 2 that analogously, each of the sets $V_p(0)$, $V_p(1^4)$, $V_p(1^3 1)$, $V_p(1^2 1^2)$, $V_p(2^2)$, $V_p(1^2 11)$, and $V_p(21^2)$ are orbits under the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p. Since $\Delta(f) = 0$ if and only if f has a repeated root, we have that

$$\begin{aligned} p^5 \widehat{\nu}_p(g) &= \sum_{f \in V_p} \nu_p(f)\langle f, g\rangle_p \\ &= \sum_{f \in V_p(0)} \langle f, g\rangle_p + \sum_{f \in V_p(1^4)} \langle f, g\rangle_p + \sum_{f \in V_p(1^3 1)} \langle f, g\rangle_p + \sum_{f \in V_p(1^2 1^2)} \langle f, g\rangle_p \\ &\quad + \sum_{f \in V_p(1^2 11)} \langle f, g\rangle_p + \sum_{f \in V_p(21^2)} \langle f, g\rangle_p + \sum_{f \in V_p(2^2)} \langle f, g\rangle_p. \end{aligned}$$

Let $G = \mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$. We can compute sums over a single orbit by choosing a representative from the orbit and summing over the elements of G. For example,

$$\frac{|G|}{|V_p(1^4)|} \sum_{f \in V_p(1^4)} \langle f, g\rangle_p = \sum_{(c,\gamma) \in G} \langle (c,\gamma) \cdot x^4, g\rangle_p = \sum_{(c,\gamma) \in G} \exp\left(2\pi i (\det \gamma)^4 [x^4, (c,\gamma) \cdot g]/p\right),$$

where the last equality follows from property (1.2). In order to exploit orthogonality relations, we might instead consider the following equations, again using property (1.2):

$$\begin{aligned} |G| \sum_{f \in V_p(0)} \langle f, g\rangle_p + (p-1)\frac{|G|}{|V_p(1^4)|} \sum_{f \in V_p(1^4)} \langle f, g\rangle_p & \\ = \sum_{a \in \mathbb{F}_p} \sum_{(c,\gamma) \in G} \langle (c,\gamma) \cdot a x^4, g\rangle_p & \\ = \sum_{a \in \mathbb{F}_p} \sum_{(c,\gamma) \in G} \exp\left(2\pi i (\det \gamma)^4 [a x^4, (c,\gamma) \cdot g]/p\right) & \\ = \sum_{(c,\gamma) \in G} \sum_{a \in \mathbb{F}_p} \exp\left(2\pi i (\det \gamma)^4 [a x^4, (c,\gamma) \cdot g]/p\right). & \end{aligned}$$

Now, if $(c,\gamma)\cdot g = b_1x^4 + b_2x^3y + b_3x^2y^2 + b_4xy^3 + b_5y^4$ for a fixed g, then

$$\sum_{a\in\mathbb{F}_p} \exp\left(2\pi i(\det\gamma)^4[ax^4,(c,\gamma)\cdot g]/p\right) = \sum_{a\in\mathbb{F}_p} \exp\left(2\pi i(\det\gamma)^4 ab_5/p\right) = \begin{cases} 0 & \text{if } b_5 \neq 0 \\ p & \text{if } b_5 = 0. \end{cases}$$

Since we have that $\sum_{f\in V_p(0)}\langle f,g\rangle_p = 1$, we have reduced the problem of computing $\sum_{f\in V_p(1^4)}\langle f,g\rangle_p$ to the question of how many binary quartic forms over $\mathbb{F}_p$ in a given orbit under the action of G have 0 as the coefficient of the y^4 term.

We can see from this example that we might be able to adapt the general strategy used in the proof of Proposition 1.1 to the quartic case. Unlike in the proof of Proposition 1.1, however, we now need to compute multiple sums, some of which require detailed analysis of the distribution of certain coefficients in a given orbit. While this work is largely outside the scope of this thesis, some preliminary results are included in the appendices, and in the remaining two chapters, we complete a key first step towards solving the problem by classifying the orbits of the natural action of $\mathrm{GL}_1(\mathbb{F}_p)\times\mathrm{GL}_2(\mathbb{F}_p)$ on the space of binary quartic forms over $\mathbb{F}_p$.

Chapter 2

The Orbits of the Action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p Containing Forms with Repeated Roots

This chapter and the one that follows are organized so that the simplest cases appear first and the most complicated cases appear last. The techniques used as we progress through the different cases require more and more machinery, which we develop along the way.

First, we establish notation and conventions for discussing the roots of a form $f \in V_p$, which are elements of $\mathbb{P}^1(\mathbb{F}_q)$, with q a power of p. There is a bijection between $\mathbb{P}^1(\mathbb{F}_q)$ and $\mathbb{F}_q \cup \{\infty\}$, where ∞, called the point at infinity, satisfies the conditions $0^{-1} = \infty$ and $x \cdot \infty = \infty$ if $0 \neq x \in \mathbb{F}_q$. More precisely, we define $\varphi : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{F}_q \cup \{\infty\}$ by $\varphi([\alpha : \beta]) = \alpha\beta^{-1}$. Since for any $\lambda \in \mathbb{F}_q^\times$, $\lambda\alpha(\lambda\beta)^{-1} = \alpha\beta^{-1}$, φ is well-defined. The inverse of φ is given by the map $\varphi^{-1} : \mathbb{F}_q \cup \{\infty\} \to \mathbb{P}^1(\mathbb{F}_q)$ defined by $\varphi^{-1}(\alpha) = [\alpha : 1]$ if $\alpha \neq \infty$ and $\varphi^{-1}(\infty) = [1 : 0]$.

Now, consider the map $\psi_1 : \mathbb{P}^1(\mathbb{F}_q) \times \mathrm{PGL}_2(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$, with q a power of p, defined by

$$\psi_1\left([\alpha : \beta], \overline{\gamma}\right) = [r\alpha + s\beta : t\alpha + u\beta],$$

where

$$\overline{\gamma} = \left\{ \lambda \begin{pmatrix} r & t \\ s & u \end{pmatrix} : \lambda \in \mathbb{F}_q^\times \right\}.$$

This map defines a right group action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$. We can define a right action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_q)$ in the same way.

Next consider the map $\psi_2 : (\mathbb{F}_q \cup \{\infty\}) \times \mathrm{PGL}_2(\mathbb{F}_q) \to \mathbb{F}_q \cup \{\infty\}$ defined by

$$\psi_2(\alpha, \overline{\gamma}) = (r\alpha + s)(t\alpha + u)^{-1},$$

when $\alpha \neq \infty$, and $\psi_2(\infty, \overline{\gamma}) = rt^{-1}$, with $\overline{\gamma}$ as above. This map defines a right group action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $\mathbb{F}_q \cup \{\infty\}$. Again, we can analogously define a right action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{F}_q \cup \{\infty\}$.

We claim that $\mathbb{P}^1(\mathbb{F}_q)$ and $\mathbb{F}_q \cup \{\infty\}$ are isomorphic as $\mathrm{PGL}_2(\mathbb{F}_q)$-sets (or $\mathrm{PGL}_2(\mathbb{F}_p)$-sets). Indeed, with $\overline{\gamma}$ as above, we have that

$$\begin{aligned}\varphi([\alpha : \beta] \cdot \overline{\gamma}) &= \varphi([r\alpha + s\beta : t\alpha + u\beta]) = (r\alpha + s\beta)(t\alpha + u\beta)^{-1} \\ &= \beta^{-1}(r\alpha + s\beta)(t\alpha + u\beta)^{-1}\left(\beta^{-1}\right)^{-1} = (r\alpha\beta^{-1} + s)(t\alpha\beta^{-1} + u)^{-1} \\ &= \left(\alpha\beta^{-1}\right) \cdot \overline{\gamma} = \varphi([\alpha : \beta]) \cdot \overline{\gamma},\end{aligned}$$

and also that

$$\begin{aligned}\varphi^{-1}(\alpha \cdot \overline{\gamma}) &= \varphi^{-1}\left((r\alpha + s)(t\alpha + u)^{-1}\right) = [(r\alpha + s)(t\alpha + u)^{-1} : 1] \\ &= [r\alpha + s : t\alpha + u] = [\alpha : 1] \cdot \overline{\gamma} = \varphi^{-1}(\alpha) \cdot \overline{\gamma}\end{aligned}$$

when $\alpha \neq \infty$, and

$$\varphi^{-1}(\infty \cdot \overline{\gamma}) = \varphi^{-1}\left(rt^{-1}\right) = [rt^{-1} : 1] = [r : t] = [1 : 0] \cdot \overline{\gamma} = \varphi^{-1}(\infty) \cdot \overline{\gamma}.$$

Hence, we will use the actions defined by ψ_1 and ψ_2 interchangeably depending on the setting.

2.1 Case 1: Orbits with a One-Term Representative

We begin our study of the orbits by showing explicitly that the orbits are at least as refined as the partition of V_p into the sets $V_p(\sigma)$ given in Table 1.2. We will make use of the following observation. If

$$\overline{\gamma} = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_p)$$

and $\alpha \cdot \overline{\gamma} = \beta$, with $\alpha, \beta \in \mathbb{F}_q \cup \infty$, then, since $\mathbb{F}_q$ has characteristic p,

$$\alpha^p \cdot \overline{\gamma} = (r\alpha^p + s)(t\alpha^p + u)^{-1} = \Big((r\alpha + s)(t\alpha + u)^{-1}\Big)^p = (\alpha \cdot \overline{\gamma})^p = \beta^p.$$

Applying this fact repeatedly, we have that if $\alpha \cdot \overline{\gamma} = \beta$, then $\alpha^{p^n} \cdot \overline{\gamma} = \beta^{p^n}$ for any $n \in \mathbb{Z}^+$. It follows that if $\alpha \cdot \overline{\gamma} = \beta$ and $\alpha^{p^n} = \alpha$ for some $n \in \mathbb{Z}^+$, then

$$\beta^{p^n} = \alpha^{p^n} \cdot \overline{\gamma} = \alpha \cdot \overline{\gamma} = \beta.$$

Proposition 2.1. Let $f \in V_p(\sigma_1)$ and $g \in V_p(\sigma_2)$ with $\sigma_1 \neq \sigma_2$. Then f and g are not in the same orbit under the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$.

Proof. Let $f \in V_p(\sigma_1)$ and $g \in V_p(\sigma_2)$ with $\sigma_1 \neq \sigma_2$. Let $[\alpha_1; \alpha_2], [\alpha_3; \alpha_4], [\alpha_5; \alpha_6]$, $[\alpha_7; \alpha_8] \in \mathbb{P}^1(\mathbb{F}_{q_1})$ be the roots of f, and let $[\beta_1; \beta_2], [\beta_3; \beta_4], [\beta_5; \beta_6], [\beta_7; \beta_8] \in \mathbb{P}^1(\mathbb{F}_{q_2})$ be the roots of g, where q_1 and q_2 are the appropriate powers of p. We have that

$$f(x, y) = a(\alpha_2 x - \alpha_1 y)(\alpha_4 x - \alpha_3 y)(\alpha_6 x - \alpha_5 y)(\alpha_8 x - \alpha_7 y)$$

and that

$$g(x, y) = b(\beta_2 x - \beta_1 y)(\beta_4 x - \beta_3 y)(\beta_6 x - \beta_5 y)(\beta_8 x - \beta_7 y)$$

for some $a, b \in \mathbb{F}_p^\times$.

Assume that there exists $(c, \gamma) \in \mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ such that $(c, \gamma) \cdot f = g$, where

$$\gamma = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Then

$$\begin{aligned} g(x, y) &= [(c, \gamma) \cdot f](x, y) \\ &= ca(\alpha_2(rx + sy) - \alpha_1(tx + uy)) \cdots (\alpha_8(rx + sy) - \alpha_7(tx + uy)) \\ &= ca((-\alpha_1 t + \alpha_2 r)x - (\alpha_1 u - \alpha_2 s)y) \cdots ((-\alpha_7 t + \alpha_8 r)x - (\alpha_7 u - \alpha_8 s)y). \end{aligned}$$

So, for each $j \in \{1, 3, 5, 7\}$, there is a unique $i \in \{1, 3, 5, 7\}$ such that

$$[\beta_j; \beta_{j+1}] = [\alpha_i u - \alpha_{i+1} s; -\alpha_i t + \alpha_{i+1} r] = [\alpha_i; \alpha_{i+1}] \cdot \overline{\gamma},$$

where

$$\overline{\gamma} = \left\{ \begin{pmatrix} u & -t \\ -s & r \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_p).$$

Hence, f and g have the same number of distinct roots. Moreover, since $\mathbb{P}^1(\mathbb{F}_q)$ and $\mathbb{F}_q \cup \{\infty\}$ are isomorphic as $\mathrm{PGL}_2(\mathbb{F}_p)$-sets, we have shown that there exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that for each $j \in \{1,3,5,7\}$, there is a unique $i \in \{1,3,5,7\}$ such that $\alpha_i \alpha_{i+1}^{-1} \cdot \overline{\gamma} = \beta_j \beta_{j+1}^{-1}$. Hence, if $\left(\alpha_i \alpha_{i+1}^{-1}\right)^{p^n} = \alpha_i \alpha_{i+1}^{-1}$, then for the corresponding j, $\left(\beta_j \beta_{j+1}^{-1}\right)^{p^n} = \beta_j \beta_{j+1}^{-1}$ for any $n \in \mathbb{Z}^+$. Therefore, f and g have the same number of roots in each extension of $\mathbb{F}_p$. But then f and g are both in $V_p(\sigma)$ for some σ, which is a contradiction. $\square$

Since $|V_p(0)| = 1$, it follows immediately from Proposition 2.1 that $V_p(0)$ is an orbit of the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p. To determine how the sets $V_p(\sigma)$, with $\sigma \in \{1^4, 1^3 1, 1^2 1^2\}$, break down into orbits under this action, we consider a representative from each set and compute the size of its stabilizer. We recall that $|\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)| = (p-1)(p^2-1)(p^2-p)$.

First, we claim that $V_p(1^4)$ is a single orbit. Since $x^4 \in V_p(1^4)$ and $|V_p(1^4)| = p^2 - 1$, it suffices to show that the size of the stabilizer of x^4 is $(p-1)(p^2-p)$. Suppose that there exists $(c, \gamma) \in \mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ such that $(c, \gamma) \cdot x^4 = x^4$, where

$$\gamma = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Then

$$x^4 = c\left(r^4 x^4 + 4r^3 s x^3 y + 6r^2 s^2 x^2 y^2 + 4r s^3 x y^3 + s^4 y^4\right).$$

Hence, $s = 0$, and for each of the $p-1$ nonzero choices of r, there is a unique choice for c such that $cr^4 = 1$. Moreover, the only restriction on the second column of γ is that the columns of γ must be linearly independent, and so, for each choice of r, there are $p^2 - p$ ways to assign t and u. Thus, there are indeed $(p-1)(p^2-p)$ distinct elements $(c, \gamma) \in \mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ such that $(c, \gamma) \cdot x^4 = x^4$.

We show similarly that $V_p(1^31)$ is a single orbit of the action of $\mathrm{GL}_1(\mathbb{F}_p)\times\mathrm{GL}_2(\mathbb{F}_p)$ on V_p. Since $x^3y \in V_p(1^31)$ and $|V_p(1^31)| = p(p^2-1)$, it suffices to show that the size of the stabilizer of x^3y is $(p-1)^2$. Suppose that there exists $(c,\gamma) \in \mathrm{GL}_1(\mathbb{F}_p)\times\mathrm{GL}_2(\mathbb{F}_p)$ such that $(c,\gamma)\cdot x^3y = x^3y$, where

$$\gamma = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Then

$$x^3y = c\left(r^3tx^4 + r^2(ru+3st)x^3y + 3rs(ru+st)x^2y^2 + s^2(3ru+st)xy^3 + s^3uy^4\right).$$

Since $r^2(ru+3st) = 1$, $r \neq 0$. Then, since $r^3t = 0$, $t = 0$. Since $\gamma \in \mathrm{GL}_2(\mathbb{F}_p)$, $u \neq 0$, and so, $s^3u = 0$ implies that $s = 0$. So, the number of distinct elements $(c,\gamma) \in \mathrm{GL}_1(\mathbb{F}_p)\times\mathrm{GL}_2(\mathbb{F}_p)$ such that $(c,\gamma)\cdot x^3y = x^3y$ is the number of distinct ways to assign c, r, and u such that $cr^3u = 1$, which is $(p-1)^2$.

Next, we show that $V_p(1^21^2)$ is a single orbit. Since $x^2y^2 \in V_p(1^21^2)$ and $|V_p(1^21^2)| = \frac{1}{2}p(p^2-1)$, it suffices to show that the size of the stabilizer of x^2y^2 is $2(p-1)^2$. Suppose that there exists $(c,\gamma) \in \mathrm{GL}_1(\mathbb{F}_p)\times\mathrm{GL}_2(\mathbb{F}_p)$ such that $(c,\gamma)\cdot x^2y^2 = x^2y^2$, where

$$\gamma = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Then

$$x^2y^2 = c[r^2t^2x^4 + 2rt(ru+st)x^3y + (r^2u^2 + 4rstu + s^2t^2)x^2y^2$$
$$+ 2su(ru+st)xy^3 + s^2u^2y^4)].$$

Since $\gamma \in \mathrm{GL}_2(\mathbb{F}_p)$, $r^2t^2 = 0$, and $s^2u^2 = 0$, either $r = u = 0$ or $s = t = 0$. In the former case, we count the number of distinct ways to assign c, s, and t such that $cs^2t^2 = 1$, which is $(p-1)^2$. In the latter case, we count the number of distinct ways to assign c, r, and u such that $cr^2u^2 = 1$, which is again $(p-1)^2$. Thus, there are indeed $2(p-1)^2$ distinct elements $(c,\gamma) \in \mathrm{GL}_1(\mathbb{F}_p)\times\mathrm{GL}_2(\mathbb{F}_p)$ such that $(c,\gamma)\cdot x^2y^2 = x^2y^2$.

So far, we have relied on the existence of a simple representative in each set, but this approach does not generalize well. Instead, we will exploit properties of the action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$, which we develop in the next section.

2.2 The Action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$ and the Cross Ratio

The results in this section are essential to continuing our general strategy for classifying the orbits, which is to compute the size of the stabilizer of a representative form $f \in V_p(\sigma)$.

Lemma 2.2. *Let $\overline{\gamma} \in PGL_2(\mathbb{F}_q)$ such that $\overline{\gamma}$ is not the identity. Then $\overline{\gamma}$ is in the stabilizer of at most two elements of $\mathbb{F}_q \cup \{\infty\}$.*

Proof. Let

$$\overline{\gamma} = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_q)$$

such that $\overline{\gamma}$ is not the identity, and let $\alpha \in \mathbb{F}_q \cup \{\infty\}$. Then $\overline{\gamma}$ is in the stabilizer of α if and only if $\alpha(t\alpha+u) = r\alpha+s$. Either the quadratic equation $tx^2+(u-r)x-s=0$ has at most two solutions, or $t=s=0$ and $u=r$. Since $\overline{\gamma}$ is not the identity, the latter case yields a contradiction. Hence, $\overline{\gamma}$ is in the stabilizer of at most two elements of $\mathbb{F}_q \cup \{\infty\}$. □

Proposition 2.3. The action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $F_q \cup \{\infty\}$ is simply triply transitive.

Proof. To show that the action is triply transitive, it suffices to show that for any three distinct points $\alpha_1, \alpha_2, \alpha_3 \in F_q \cup \{\infty\}$, there exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that $\alpha_1 \cdot \overline{\gamma} = 1$, $\alpha_2 \cdot \overline{\gamma} = 0$, and $\alpha_3 \cdot \overline{\gamma} = \infty$. Indeed, we can take

$$\overline{\gamma} = \left\{ \begin{pmatrix} \alpha_1-\alpha_3 & \alpha_1-\alpha_2 \\ -\alpha_2(\alpha_1-\alpha_3) & -\alpha_3(\alpha_1-\alpha_2) \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_q)$$

so that

$$\begin{aligned}\alpha_1 \cdot \overline{\gamma} &= ((\alpha_1-\alpha_3)\alpha_1-\alpha_2(\alpha_1-\alpha_3))((\alpha_1-\alpha_2)\alpha_1-\alpha_3(\alpha_1-\alpha_2))^{-1}\\ &= (\alpha_1^2-\alpha_3\alpha_1-\alpha_2\alpha_1+\alpha_2\alpha_3)(\alpha_1^2-\alpha_2\alpha_1-\alpha_3\alpha_1+\alpha_3\alpha_2)^{-1}=1,\end{aligned}$$

and also,

$$\alpha_2 \cdot \overline{\gamma} = ((\alpha_1-\alpha_3)\alpha_2-\alpha_2(\alpha_1-\alpha_3))((\alpha_1-\alpha_2)\alpha_2-\alpha_3(\alpha_1-\alpha_2))^{-1}=0,$$

and lastly,

$$\alpha_3 \cdot \overline{\gamma} = ((\alpha_1-\alpha_3)\alpha_3-\alpha_2(\alpha_1-\alpha_3))((\alpha_1-\alpha_2)\alpha_3-\alpha_3(\alpha_1-\alpha_2))^{-1}=\infty.$$

Now, let $\alpha_1, \alpha_2, \alpha_3$ be three distinct points in $\mathbb{F}_q \cup \{\infty\}$ and assume that there exist $\overline{\gamma_1}, \overline{\gamma_2} \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that $\alpha_i \cdot \overline{\gamma_1} = \alpha_i \cdot \overline{\gamma_2}$ for $i = 1, 2, 3$. Then $\overline{\gamma_2} \circ \overline{\gamma_1}^{-1}$ is in the stabilizer of α_i for $i = 1, 2, 3$. By Lemma 2.2, $\overline{\gamma_2} \circ \overline{\gamma_1}^{-1}$ is the identity, and so, $\overline{\gamma_1} = \overline{\gamma_2}$. Thus, the action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $F_q \cup \{\infty\}$ is simply triply transitive. $\square$

Let $\overline{\gamma}$ be as in the proof above. Note that the action of $\overline{\gamma}$ on $\alpha_4 \in \mathbb{F}_q \cup \{\infty\}$ is given by

$$\begin{aligned}\alpha_4 \cdot \overline{\gamma} &= ((\alpha_1-\alpha_3)\alpha_4-\alpha_2(\alpha_1-\alpha_3))((\alpha_1-\alpha_2)\alpha_4-\alpha_3(\alpha_1-\alpha_2))^{-1}\\ &= (\alpha_1\alpha_4-\alpha_3\alpha_0-\alpha_2\alpha_1+\alpha_2\alpha_3)(\alpha_1\alpha_4-\alpha_2\alpha_4-\alpha_3\alpha_1+\alpha_3\alpha_2)^{-1}\\ &= ((\alpha_4-\alpha_2)(\alpha_1-\alpha_3))((\alpha_4-\alpha_3)(\alpha_1-\alpha_2))^{-1}\\ &= \frac{(\alpha_4-\alpha_2)(\alpha_1-\alpha_3)}{(\alpha_4-\alpha_3)(\alpha_1-\alpha_2)}.\end{aligned}$$

The last expression is, by definition, the cross ratio of the four ordered points α_1, α_2, α_3, α_4. The order of the points is significant. For example, if

$$\frac{(\alpha_4-\alpha_2)(\alpha_1-\alpha_3)}{(\alpha_4-\alpha_3)(\alpha_1-\alpha_2)} = C,$$

then the cross ratio of the four ordered points $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ is

$$\frac{(\alpha_1-\alpha_3)(\alpha_2-\alpha_4)}{(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)} = \frac{C}{C-1},$$

The cross ratio and its properties have been studied extensively and are well-understood. One property, which can be found in Section 1.11 of [4], is that if the cross ratio of the four ordered points α_1, α_2, α_3, α_4 is C, then the cross ratio of these four points in a different order is one of the following :

$$C, \frac{1}{C}, 1-C, \frac{1}{1-C}, \frac{C}{C-1}, \frac{C-1}{C}.$$

Moreover, if the four ordered points are distinct, then the cross ratio is not 0, 1 or ∞. In Chapter 3, we study the orbits of the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p containing forms with four distinct roots, and the cross ratio plays an important role.

While Proposition 2.3 focuses on the action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on $\mathbb{F}_q \cup \{\infty\}$, with q a power of p, it also leads to a useful result about the action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on $\mathbb{F}_q \cup \{\infty\}$. We have seen that if $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ and $\alpha \cdot \overline{\gamma} = \beta$, with $\alpha, \beta \in \mathbb{F}_q$, then $\alpha^p \cdot \overline{\gamma} = \beta^p$. The following proposition shows that for any element of $\mathrm{PGL}_2(\mathbb{F}_q)$ that has this property when acting on three distinct points in $\mathbb{F}_q \cup \{\infty\}$, there is an element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts in the same way on those three points.

Proposition 2.4. Let $\alpha_1, \alpha_2, \alpha_3$ and $\beta_1, \beta_2, \beta_3$ be two sets of three distinct ordered points in $F_q \cup \{\infty\}$, with q a power of p. There exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that for each $i \in \{1,2,3\}$, $\alpha_i \cdot \overline{\gamma} = \beta_i$ if and only if there exists $\overline{\gamma}' \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that for each $i \in \{1,2,3\}$, $\alpha_i \cdot \overline{\gamma}' = \beta_i$ and $\alpha_i^p \cdot \overline{\gamma}' = \beta_i^p$.

Proof. Let $\alpha_1, \alpha_2, \alpha_3$ and $\beta_1, \beta_2, \beta_3$ be two sets of three distinct ordered points in $F_q \cup \{\infty\}$, with q a power of p. First, suppose that there exists

$$\overline{\gamma} = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_p)$$

such that for each $i \in \{1,2,3\}$, $\alpha_i \cdot \overline{\gamma} = \beta_i$. Let

$$\overline{\gamma}' = \left\{ \lambda \begin{pmatrix} r & t \\ s & u \end{pmatrix} : \lambda \in \mathbb{F}_q^\times \right\} \in \mathrm{PGL}_2(\mathbb{F}_q).$$

Since for each $i \in \{1,2,3\}$, $\alpha_i \cdot \overline{\gamma} = \beta_i$, we have that $\alpha_i \cdot \overline{\gamma}' = \beta_i$. Moreover, since for each $i \in \{1,2,3\}$, $\alpha_i^p \cdot \overline{\gamma} = \beta_i^p$, we also have that $\alpha_i^p \cdot \overline{\gamma}' = \beta_i^p$.

Next, suppose that there exists $\overline{\gamma}' \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that for each $i \in \{1,2,3\}$, $\alpha_i \cdot \overline{\gamma}' = \beta_i$ and $\alpha_i^p \cdot \overline{\gamma}' = \beta_i^p$. If γ' is a representative matrix in $\overline{\gamma}'$, then γ' has at least one nonzero entry. Scaling by the inverse of this entry, we have

$$\overline{\gamma}' = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\}$$

where at least one of r, s, t, u is equal to 1. Let

$$\overline{\gamma}_p = \left\{ \begin{pmatrix} r^p & t^p \\ s^p & u^p \end{pmatrix} \right\}.$$

We have that $\beta_i^p = \alpha_i^p \cdot \overline{\gamma}'$ for $i = 1,2,3$, but also, since $\mathbb{F}_q$ has characteristic p,

$$\beta_i^p = (\alpha_i \cdot \overline{\gamma}')^p = \left((r\alpha_i + s)(t\alpha_i + u)^{-1}\right)^p = (r^p\alpha_i^p + s^p)(t^p\alpha_i^p + u^p)^{-1} = \alpha_i^p \cdot \overline{\gamma}_p$$

for $i = 1,2,3$. Hence, $\overline{\gamma}'$ and $\overline{\gamma}_p$ act in the same way on the three distinct points $\alpha_1^p, \alpha_2^p, \alpha_3^p$. By Proposition 2.3, $\overline{\gamma}'$ and $\overline{\gamma}_p$ are equal as elements of $\mathrm{PGL}_2(\mathbb{F}_q)$; that is

$$\lambda \begin{pmatrix} r & t \\ s & u \end{pmatrix} = \begin{pmatrix} r^p & t^p \\ s^p & u^p \end{pmatrix}.$$

Since one of r, s, t, u is 1, $\lambda = 1$, and hence, $r, s, t, u \in \mathbb{F}_p$. Therefore, there exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ that acts as $\overline{\gamma}'$ on the α_i, namely

$$\overline{\gamma} = \left\{ \lambda \begin{pmatrix} r & t \\ s & u \end{pmatrix} : \lambda \in \mathbb{F}_p^\times \right\}.$$

□

2.3 Case 2: Other Orbits of Forms with Repeated Roots

We now establish a connection between the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on two forms f and g in the same set $V_p(\sigma)$ and the action of $\mathrm{PGL}_2(\mathbb{F}_p)$ on their roots in $\mathbb{P}^1(\mathbb{F}_q)$,

with q the appropriate power of p. This, in turn, allows us to make use of the results from the previous section.

Proposition 2.5. Let $f, g \in V_p(\sigma)$ for some fixed σ. Let $[\alpha_1;\alpha_2], [\alpha_3;\alpha_4], [\alpha_5;\alpha_6], [\alpha_7;\alpha_8] \in \mathbb{P}^1(\mathbb{F}_q)$ be the roots of f, and let $[\beta_1;\beta_2], [\beta_3;\beta_4], [\beta_5;\beta_6], [\beta_7;\beta_8] \in \mathbb{P}^1(\mathbb{F}_q)$ be the roots of g, where q is the appropriate power of p. There exists (c,γ) in $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ such that $(c,\gamma)\cdot f = g$ if and only if there exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that for each $j \in \{1,3,5,7\}$, there is a unique $i \in \{1,3,5,7\}$ such that

$$[\alpha_i;\alpha_{i+1}]\cdot\overline{\gamma} = [\beta_j;\beta_{j+1}].$$

Proof. Let $f, g \in V_p$. Let $[\alpha_1;\alpha_2], [\alpha_3;\alpha_4], [\alpha_5;\alpha_6], [\alpha_7;\alpha_8] \in \mathbb{P}^1(\mathbb{F}_q)$ be the roots of f, and let $[\beta_1;\beta_2], [\beta_3;\beta_4], [\beta_5;\beta_6], [\beta_7;\beta_8] \in \mathbb{P}^1(\mathbb{F}_q)$ be the roots of g. We have that

$$f(x,y) = a(\alpha_2 x - \alpha_1 y)(\alpha_4 x - \alpha_3 y)(\alpha_6 x - \alpha_5 y)(\alpha_8 x - \alpha_7 y)$$

and that

$$g(x,y) = b(\beta_2 x - \beta_1 y)(\beta_4 x - \beta_3 y)(\beta_6 x - \beta_5 y)(\beta_8 x - \beta_7 y)$$

for some $a, b \in \mathbb{F}_p^\times$.

First, suppose that there exists $(c,\gamma) \in \mathrm{GL}_1(\mathbb{F}_p)\times\mathrm{GL}_2(\mathbb{F}_p)$ such that $(c,\gamma)\cdot f = g$, where

$$\gamma = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Then

$$\begin{aligned} g(x,y) &= [(c,\gamma)\cdot f](x,y) \\ &= ca(\alpha_2(rx+sy) - \alpha_1(tx+uy))\cdots(\alpha_8(rx+sy) - \alpha_7(tx+uy)) \\ &= ca((-\alpha_1 t + \alpha_2 r)x - (\alpha_1 u - \alpha_2 s)y)\cdots((-\alpha_7 t + \alpha_8 r)x - (\alpha_7 u - \alpha_8 s)y). \end{aligned}$$

Let

$$\overline{\gamma} = \left\{ \begin{pmatrix} u & -t \\ -s & r \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_p).$$

Then for each $j \in \{1,3,5,7\}$, there is a unique $i \in \{1,3,5,7\}$ such that

$$[\alpha_i; \alpha_{i+1}] \cdot \overline{\gamma} = [\alpha_i u - \alpha_{i+1} s; -\alpha_i t + \alpha_{i+1} r] = [\beta_j; \beta_{j+1}].$$

Next, suppose that there exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that for each $j \in \{1,3,5,7\}$, there is a unique $i \in \{1,3,5,7\}$ such that

$$[\alpha_i; \alpha_{i+1}] \cdot \overline{\gamma} = [\beta_j; \beta_{j+1}],$$

where

$$\overline{\gamma} = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_p).$$

Then $[\beta_j; \beta_{j+1}] = [r\alpha_i + s\alpha_{i+1}; t\alpha_i + u\alpha_{i+1}]$, and hence, for each $j \in \{1,3,5,7\}$, there is a unique $i \in \{1,3,5,7\}$ such that

$$(\beta_j, \beta_{j+1}) = c_j(r\alpha_i + s\alpha_{i+1}, t\alpha_i + u\alpha_{i+1})$$

for some $c_j \in \mathbb{F}_q^\times$. So,

$$\begin{aligned} g(x,y) &= b(\beta_2 x - \beta_1 y)(\beta_4 x - \beta_3 y)(\beta_6 x - \beta_5 y)(\beta_8 x - \beta_7 y) \\ &= c_1 c_3 c_5 c_7 b((t\alpha_1 + u\alpha_2)x - (r\alpha_1 + s\alpha_2)y) \cdots ((t\alpha_7 + u\alpha_8)x - (r\alpha_7 + s\alpha_8)y) \\ &= c_1 c_3 c_5 c_7 b(\alpha_2(ux - sy) - \alpha_1(-tx + ry)) \cdots (\alpha_8(ux - sy) - \alpha_7(-tx + ry)) \\ &= c_1 c_3 c_5 c_7 b a^{-1}[(1, \gamma) \cdot f](x,y), \end{aligned}$$

where

$$\gamma = \begin{pmatrix} u & -t \\ -s & r \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Since $g \in V_p$ and $(1, \gamma) \cdot f \in V_p$, $c = c_1 c_3 c_5 c_7 b a^{-1} \in \mathbb{F}_p$. Moreover, $(c, \gamma) \cdot f = g$. $\square$

An important consequence of Proposition 2.5 is that given $f \in V_p(\sigma)$, for each element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as a permutation on the roots of f, there are $p-1$ elements of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ that fix f, and these are the only elements that fix f. So, rather than compute the size of the stabilizer of f with respect to the action of

$\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$, we can count the number of elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation on the roots of f. It is important to observe that not all permutations of the roots of f can be realized as an element of $\mathrm{PGL}_2(\mathbb{F}_p)$; in order for an element of $\mathrm{PGL}_2(\mathbb{F}_p)$ to act as a permutation of the roots, the permutation must satisfy the condition that if $\alpha \to \beta$, then $\alpha^p \to \beta^p$. Let N be the number of elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation of the roots of f. Then the size of the stabilizer of f with respect to the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ is $N(p-1)$. Again, we recall that $|\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)| = (p-1)(p^2-1)(p^2-p)$.

Let $f \in V_p(2^2)$, and recall that $|V_p(2^2)| = \frac{1}{2}p(p-1)^2$. We will show that $V_p(2^2)$ is a single orbit by showing that there are $2(p+1)$ elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation on the roots of f. We denote the roots of f by α and α^p. By Proposition 2.3, for each $\beta \in \mathbb{F}_{p^2}$ such that $\beta \neq \alpha$ and $\beta \neq \alpha^p$, there is a unique element $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_{p^2})$ such that $\overline{\gamma} \cdot \alpha = \alpha$, $\overline{\gamma} \cdot \alpha^p = \alpha^p$, and $\overline{\gamma} \cdot 0 = \beta$. Since $0^p = 0$, by Proposition 2.4, there exists $\overline{\gamma}' \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that $\overline{\gamma}' \cdot \alpha = \alpha^p$, $\overline{\gamma}' \cdot \alpha^p = \alpha$, and $\overline{\gamma}' \cdot 0 = \beta$ if and only if $\beta^p = \beta$. So, there are $p+1$ elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as the permutation of α and α^p given by $\alpha \mapsto \alpha$ and $\alpha^p \mapsto \alpha^p$. By an analogous argument, there are $p+1$ elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as the permutation of α and α^p given by $\alpha \mapsto \alpha^p$ and $\alpha^p \mapsto \alpha$.

Next, let $f \in V_p(1^2 11)$, and recall that $|V_p(1^2 11)| = \frac{1}{2}(p+1)p(p-1)^2$. We will show that $V_p(1^2 11)$ is a single orbit by showing that there are 2 elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation on the roots of f. We denote the roots of f by α_1, α_2, and α_3, where α_1 is the double root. Any element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that in acting as a permutation of the roots, changes the double root of f corresponds to a collection of elements of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ that do not fix f. Hence, there are only two permutations of the roots to consider. The first is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, and $\alpha_3 \to \alpha_3$. The second is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_3$, and $\alpha_3 \to \alpha_2$. By Proposition 2.3, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as each of these permutations.

Finally, let $f \in V_p(21^2)$, and recall that $|V_p(21^2)| = \frac{1}{2}(p+1)p(p-1)^2$. We will show that $V_p(1^211)$ is a single orbit by showing that there are 2 elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation on the roots of f. We denote the roots of f by α_1, α_2, and α_2^p, where α_1 is the double root. Since $\alpha_1^p = \alpha_1$, there are no elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation that sends α_1 to α_2. Hence, there are only two permutations of the roots to consider. The first is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, and $\alpha_2^p \to \alpha_2^p$. The second is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2^p$, and $\alpha_2^p \to \alpha_2$. By Proposition 2.3, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_{p^2})$ that acts as each of these permutations, and by Proposition 2.4, each has a corresponding element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts in the same way.

We have now shown that each of $V_p(0)$, $V_p(1^4)$, $V_p(1^31)$, $V_p(1^21^2)$, $V_p(2^2)$, $V_p(1^211)$, and $V_p(21^2)$ is single orbit under the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p.

Chapter 3

The Orbits of the Action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p Containing Forms with Four Distinct Roots

In order to extend our strategy of counting the number of elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation of the roots of a form f to the case where f has four distinct roots, we need to build upon Proposition 2.3 and Proposition 2.4. We do this by considering the cross ratio of the roots.

Proposition 3.1. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\beta_1, \beta_2, \beta_3, \beta_4$ be two sets of ordered points in $\mathbb{F}_q \cup \{\infty\}$. Then the two ordered sets have the same cross ratio if and only if there exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that $\alpha_i \cdot \overline{\gamma} = \beta_i$, $i = 1, 2, 3, 4$. Moreover, this $\overline{\gamma}$ is unique.

Proof. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\beta_1, \beta_2, \beta_3, \beta_4$ be two sets of ordered points in $\mathbb{F}_q \cup \{\infty\}$. First, suppose that $\alpha_i \cdot \overline{\gamma} = \beta_i$, $i = 1, 2, 3, 4$, for some

$$\overline{\gamma} = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_q).$$

Then $\beta_i = (r\alpha_i + s)(t\alpha_i + u)^{-1}$, and hence,

$$\begin{aligned} \beta_i - \beta_j &= [(r\alpha_i + s)(t\alpha_j + u) - (r\alpha_j + s)(t\alpha_i + u)](t\alpha_i + u)^{-1}(t\alpha_j + u)^{-1} \\ &= (ru - st)(\alpha_i - \alpha_j)((t\alpha_i + u)(t\alpha_j + u))^{-1}. \end{aligned}$$

So,

$$\frac{(\beta_1 - \beta_3)(\beta_2 - \beta_4)}{(\beta_1 - \beta_4)(\beta_2 - \beta_3)} = \frac{(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)}{(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)}.$$

Next, suppose that the two sets of ordered points have the same cross ratio. Then

$$\frac{(\beta_1 - \beta_3)(\beta_2 - \beta_4)}{(\beta_1 - \beta_4)(\beta_2 - \beta_3)} = C = \frac{(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)}{(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)}.$$

By Proposition 2.3, there exists a unique $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that $\alpha_i \cdot \overline{\gamma} = \beta_i$, $i = 2, 3, 4$. We have already shown that the two sets of ordered points $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\alpha_1 \cdot \overline{\gamma}, \alpha_2 \cdot \overline{\gamma}, \alpha_3 \cdot \overline{\gamma}, \alpha_4 \cdot \overline{\gamma}$ have the same cross ratio. Hence,

$$\frac{(\alpha_1 \cdot \overline{\gamma} - \beta_3)(\beta_2 - \beta_4)}{(\alpha_1 \cdot \overline{\gamma} - \beta_4)(\beta_2 - \beta_3)} = \frac{(\alpha_1 \cdot \overline{\gamma} - \alpha_3 \cdot \overline{\gamma})(\alpha_2 \cdot \overline{\gamma} - \alpha_4 \cdot \overline{\gamma})}{(\alpha_1 \cdot \overline{\gamma} - \alpha_4 \cdot \overline{\gamma})(\alpha_2 \cdot \overline{\gamma} - \alpha_3 \cdot \overline{\gamma})} = C.$$

So, $\alpha_1 \cdot \overline{\gamma}$ and β_1 both satisfy the linear equation

$$((\beta_2 - \beta_4) - C(\beta_2 - \beta_3))x = \beta_3(\beta_2 - \beta_4) - C\beta_4(\beta_2 - \beta_3),$$

and thus, $\alpha_1 \cdot \overline{\gamma} = \beta_1$. □

The proof of the following proposition is almost identical to the proof of Proposition 2.4 but it relies on Proposition 3.1 instead of Proposition 2.3.

Proposition 3.2. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\beta_1, \beta_2, \beta_3, \beta_4$ be two sets of three distinct ordered points in $F_q \cup \{\infty\}$, with q a power of p. There exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that for each $i \in \{1, 2, 3, 4\}$, $\alpha_i \cdot \overline{\gamma} = \beta_i$ if and only if there exists $\overline{\gamma}' \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that for each $i \in \{1, 2, 3, 4\}$, $\alpha_i \cdot \overline{\gamma}' = \beta_i$ and $\alpha_i^p \cdot \overline{\gamma}' = \beta_i^p$.

Proof. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and $\beta_1, \beta_2, \beta_3, \beta_4$ be two sets of three distinct ordered points in $F_q \cup \{\infty\}$, with q a power of p. First, suppose that there exists

$$\overline{\gamma} = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\} \in \mathrm{PGL}_2(\mathbb{F}_p)$$

such that for each $i \in \{1, 2, 3, 4\}$, $\alpha_i \cdot \overline{\gamma} = \beta_i$. Let

$$\overline{\gamma}' = \left\{ \lambda \begin{pmatrix} r & t \\ s & u \end{pmatrix} : \lambda \in \mathbb{F}_q^\times \right\} \in \mathrm{PGL}_2(\mathbb{F}_q).$$

Since for each $i \in \{1, 2, 3, 4\}$, $\alpha_i \cdot \overline{\gamma} = \beta_i$, we have that $\alpha_i \cdot \overline{\gamma}' = \beta_i$. Moreover, since for each $i \in \{1, 2, 3, 4\}$, $\alpha_i^p \cdot \overline{\gamma} = \beta_i^p$, we also have that $\alpha_i^p \cdot \overline{\gamma}' = \beta_i^p$.

Next, suppose that there exists $\overline{\gamma}' \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that for each $i \in \{1,2,3,4\}$, $\alpha_i \cdot \overline{\gamma}' = \beta_i$ and $\alpha_i^p \cdot \overline{\gamma}' = \beta_i^p$. If γ' is a representative matrix in $\overline{\gamma}'$, then γ' has at least one nonzero entry. Scaling by the inverse of this entry, we have

$$\overline{\gamma}' = \left\{ \begin{pmatrix} r & t \\ s & u \end{pmatrix} \right\}$$

where at least one of r, s, t, u is equal to 1. Let

$$\overline{\gamma}_p = \left\{ \begin{pmatrix} r^p & t^p \\ s^p & u^p \end{pmatrix} \right\}.$$

We have that $\beta_i^p = \alpha_i^p \cdot \overline{\gamma}'$ for $i = 1,2,3,4$, but also, since $\mathbb{F}_q$ has characteristic p,

$$\beta_i^p = (\alpha_i \cdot \overline{\gamma}')^p = \left((r\alpha_i + s)(t\alpha_i + u)^{-1}\right)^p = (r^p\alpha_i^p + s^p)(t^p\alpha_i^p + u^p)^{-1} = \alpha_i^p \cdot \overline{\gamma}_p$$

for $i = 1,2,3,4$. Hence, $\overline{\gamma}'$ and $\overline{\gamma}_p$ act in the same way on the three distinct points $\alpha_1^p, \alpha_2^p, \alpha_3^p$. By Proposition 3.1, $\overline{\gamma}'$ and $\overline{\gamma}_p$ are equal as elements of $\mathrm{PGL}_2(\mathbb{F}_q)$; that is

$$\lambda \begin{pmatrix} r & t \\ s & u \end{pmatrix} = \begin{pmatrix} r^p & t^p \\ s^p & u^p \end{pmatrix}.$$

Since one of r, s, t, u is 1, $\lambda = 1$, and hence, $r, s, t, u \in \mathbb{F}_p$. Therefore, there exists $\overline{\gamma} \in \mathrm{PGL}_2(\mathbb{F}_p)$ that acts as $\overline{\gamma}'$ on the α_i, namely

$$\overline{\gamma} = \left\{ \lambda \begin{pmatrix} r & t \\ s & u \end{pmatrix} : \lambda \in \mathbb{F}_p^\times \right\}.$$

□

As before, we let N be the number of elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation of the roots of f so that, by Proposition 2.5, the size of the stabilizer of f with respect to the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ is $N(p-1)$. We recall that $|\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)| = (p-1)(p^2-1)(p^2-p)$.

3.1 Case 1: Orbits of Forms with Four Conjugate Roots in $\mathbb{P}^1(\mathbb{F}_{p^4})$

The results in this section, which then motivate the results in subsequent sections, are largely based on the work of H. R. Brahana in [3]. While his work was done in a different setting many years ago, it provides a framework from which to build our argument.

Let $f \in V_p(4)$, and recall that $|V_p(4)| = \frac{1}{4}p^2(p+1)(p-1)^2$. We will show that $V_p(4)$ is partitioned into one orbit of size $\frac{1}{4}p(p+1)(p-1)^2$ and $\frac{p-1}{2}$ orbits of size $\frac{1}{2}p(p+1)(p-1)^2$ by showing that there are either 2 or 4 elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation on the roots of f depending on the cross ratio of the roots. We denote the roots of f by α, α^p, α^{p^2}, and α^{p^3}. We need only to consider permutations of the roots where if $\alpha \to \beta$ then $\alpha^p \to \beta^p$, of which there are four. The first is given by $\alpha \to \alpha$, $\alpha^p \to \alpha^p$, $\alpha^{p^2} \to \alpha^{p^2}$, and $\alpha^{p^3} \to \alpha^{p^3}$. The second is given by $\alpha \to \alpha^p$, $\alpha^p \to \alpha^{p^2}$, $\alpha^{p^2} \to \alpha^{p^3}$, and $\alpha^{p^3} \to \alpha$. The third is given by $\alpha \to \alpha^{p^2}$, $\alpha^p \to \alpha^{p^3}$, $\alpha^{p^2} \to \alpha$, and $\alpha^{p^3} \to \alpha^p$. The fourth is given by $\alpha \to \alpha^{p^3}$, $\alpha^p \to \alpha$, $\alpha^{p^2} \to \alpha^p$, and $\alpha^{p^3} \to \alpha^{p^2}$.

It follows immediately from Proposition 3.1 and Proposition 3.2 that there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as the permutation given by $\alpha \to \alpha$, $\alpha^p \to \alpha^p$, $\alpha^{p^2} \to \alpha^{p^2}$, and $\alpha^{p^3} \to \alpha^{p^3}$. Let C be the cross ratio of of the ordered points α, α^p, α^{p^2}, and α^{p^3}. Then

$$\frac{(\alpha^{p^2}-\alpha)(\alpha^{p^3}-\alpha^p)}{(\alpha^{p^2}-\alpha^p)(\alpha^{p^3}-\alpha)} = \frac{(\alpha-\alpha^{p^2})(\alpha^p-\alpha^{p^3})}{(\alpha-\alpha^{p^3})(\alpha^p-\alpha^{p^2})} = C.$$

That is, the cross ratio of of the ordered points α^{p^2}, α^{p^3}, α, and α^p is also C. By Proposition 3.1, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_{p^4})$ that acts as the permutation given by $\alpha \to \alpha^{p^2}$, $\alpha^p \to \alpha^{p^3}$, $\alpha^{p^2} \to \alpha$, and $\alpha^{p^3} \to \alpha^p$, and by Proposition 3.2, there is a corresponding element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts in the same way. Hence there are at least 2 elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation on the roots of f.

For the remaining two permutations, note that

$$\frac{(\alpha^p - \alpha^{p^3})(\alpha^{p^2} - \alpha)}{(\alpha^p - \alpha)(\alpha^{p^2} - \alpha^{p^3})} = \frac{(\alpha^{p^3} - \alpha^p)(\alpha - \alpha^{p^2})}{(\alpha^{p^3} - \alpha^{p^2})(\alpha - \alpha^p)} = \frac{C}{C-1}.$$

and that $C = C/(C-1)$ if and only if $C = 0$ or $C = 2$. Since the four roots of f are distinct, $C \neq 0$. So, by Proposition 3.1 and Proposition 3.2, for each of the remaining permutations, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as that permutation if and only if $C = 2$. Hence, the size of the stabilizer of f is $4(p-1)$ if the cross ratio of the roots of f is 2 and $2(p-1)$ otherwise. The corresponding orbit having f as a representative has size $\frac{1}{4}p(p+1)(p-1)^2$ or $\frac{1}{2}p(p+1)(p-1)^2$, respectively. Suppose that there are m orbits of the former size and k orbits of the latter size. Then

$$\frac{1}{4}p^2(p+1)(p-1)^2 = \frac{m}{4}p(p+1)(p-1)^2 + \frac{k}{2}p(p+1)(p-1)^2,$$

and hence, $2k + m = p$.

If $m > 1$, then there exist forms $f, g \in V_p(4)$ such that for each form the cross ratio of the roots, when ordered as α, α^p, α^{p^2}, and α^{p^3}, is 2 but also f and g are in distinct orbits. But then by Proposition 3.1 and Proposition 3.2 there exists a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that maps the roots of f to the roots of g, and so, by Proposition 2.5 there exists an element of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ that maps f to g, which is a contradiction. Hence $m \leq 1$. Since p is odd, $m = 1$ and $k = (p-1)/2$.

Hence, we conclude that for the case of $V_p(4)$, there is one orbit of size $\frac{1}{4}p(p+1)(p-1)^2$, and there are $(p-1)/2$ orbits of size $\frac{1}{2}p(p+1)(p-1)^2$.

3.2 Case 2: Orbits of Forms with a Conjugate Pair of Roots in $\mathbb{P}^1(\mathbb{F}_{p^2})$ and Two Distinct Roots in $\mathbb{P}^1(\mathbb{F}_p)$

The argument for determining how $V_p(211)$ is partitioned into orbits is very similar to the argument for $V_p(4)$ in the previous section. First, let $f \in V_p(211)$, and recall that $|V_p(211)| = \frac{1}{4}p^2(p+1)(p-1)^2$. We denote the roots of f by α_1, α_2, α_3, and α_3^p.

We need only to consider permutations of the roots where if $\alpha \to \beta$ then $\alpha^p \to \beta^p$, of which there are again four. The first is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_3$, and $\alpha_3^p \to \alpha_3^p$. The second is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_3$, and $\alpha_3^p \to \alpha_3^p$. The third is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_3^p$, and $\alpha_3^p \to \alpha_3$. The fourth is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_3^p$, and $\alpha_3^p \to \alpha_3$.

As with $V_p(4)$, it follows immediately that there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as the permutation given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_3$, and $\alpha_3^p \to \alpha_3^p$. Let C be the cross ratio of of the ordered points α_1, α_2, α_3, and α_3^p. Then

$$\frac{(\alpha_2 - \alpha_3^p)(\alpha_1 - \alpha_3)}{(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3^p)} = \frac{(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3^p)}{(\alpha_1 - \alpha_3^p)(\alpha_2 - \alpha_3)} = C.$$

That is, the cross ratio of of the ordered points α_2, α_1, α_3^p, and α_3 is also C. By Proposition 3.1, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_{p^2})$ that acts as the permutation given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_3^p$, and $\alpha_3^p \to \alpha_3$, and by Proposition 3.2, there is a corresponding element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts in the same way. Hence there are at least 2 elements of $\mathrm{PGL}_2(\mathbb{F}_p)$ that act as a permutation on the roots of f.

For the remaining two permutations, note that

$$\frac{(\alpha_1 - \alpha_3^p)(\alpha_2 - \alpha_3)}{(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3^p)} = \frac{(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3^p)}{(\alpha_2 - \alpha_3^p)(\alpha_1 - \alpha_3)} = \frac{1}{C}.$$

and that $C = 1/C$ if and only if $C = 1$ or $C = -1$. Since the four roots of f are distinct, $C \neq 1$. So, by Proposition 3.1 and Proposition 3.2, for each of the remaining permutations, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as that permutation if and only if $C = -1$. Hence, the size of the stabilizer of f is $4(p-1)$ if the cross ratio of the roots of f is -1 and $2(p-1)$ otherwise. The corresponding orbit having f as a representative has size $\frac{1}{4}p(p+1)(p-1)^2$ or $\frac{1}{2}p(p+1)(p-1)^2$, respectively. Suppose that there are m orbits of the former size and k orbits of the latter size. Then

$$\frac{1}{4}p^2(p+1)(p-1)^2 = \frac{m}{4}p(p+1)(p-1)^2 + \frac{k}{2}p(p+1)(p-1)^2,$$

and hence, $2k + m = p$. By the same argument used for the case of $V_p(4)$, we have $m \leq 1$. Since p is odd, we again have that $m = 1$ and $k = (p-1)/2$.

In conclusion, for the case of $V_p(211)$, there is one orbit of size $\frac{1}{4}p(p+1)(p-1)^2$, and there are $(p-1)/2$ orbits of size $\frac{1}{2}p(p+1)(p-1)^2$.

3.3 Case 3: Orbits of Forms with Two Distinct Conjugate Pairs of Roots in $\mathbb{P}^1(\mathbb{F}_{p^2})$

In this section, we address the case of $V_p(22)$; we can draw from our work in the previous two cases. Let $f \in V_p(22)$, and recall that $|V_p(22)| = \frac{1}{8}(p-2)p(p+1)(p-1)^2$. We denote the roots of f by α_1, α_1^p, α_2, and α_2^p. As before, we need only to consider permutations of the roots where if $\alpha \to \beta$ then $\alpha^p \to \beta^p$. In this case, there are eight such permutations, which we break into two sets of four. For the first set, the first permutation is given by $\alpha_1 \to \alpha_1$, $\alpha_1^p \to \alpha_1^p$, $\alpha_2 \to \alpha_2$, and $\alpha_2^p \to \alpha_2^p$. The second is given by $\alpha_1 \to \alpha_1^p$, $\alpha_1^p \to \alpha_1$, $\alpha_2 \to \alpha_2^p$, and $\alpha_2^p \to \alpha_2$. The third is given by $\alpha_1 \to \alpha_2$, $\alpha_1^p \to \alpha_2^p$, $\alpha_2 \to \alpha_1$, and $\alpha_2^p \to \alpha_1^p$. The fourth is given by $\alpha_1 \to \alpha_2^p$, $\alpha_1^p \to \alpha_2$, $\alpha_2 \to \alpha_1^p$, and $\alpha_2^p \to \alpha_1$. We saw that the ordered points α_1^p, α_1, α_2^p, and α_2 and the ordered points α_2, α_2^p, α_1, and α_1^p have the same cross ratio as the ordered points α_1, α_1^p, α_2, and α_2^p in the arguments for cases $V_p(211)$ and $V_p(4)$, respectively. Similarly, if the cross ratio for the ordered points α_1, α_1^p, α_2, and α_2^p is C, then

$$\frac{(\alpha_2^p - \alpha_1^p)(\alpha_2 - \alpha_1)}{(\alpha_2^p - \alpha_1)(\alpha_2 - \alpha_1^p)} = \frac{(\alpha_1 - \alpha_2)(\alpha_1^p - \alpha_2^p)}{(\alpha_1 - \alpha_2^p)(\alpha_1^p - \alpha_2)} = C.$$

That is, the cross ratio of of the ordered points α_2^p, α_2, α_1^p, and α_1 is also C. Hence, by Proposition 3.1 and Proposition 3.2, for each of the permutations in this first set, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as that permutation.

For the second set, the first permutation is given by $\alpha_1 \to \alpha_1$, $\alpha_1^p \to \alpha_1^p$, $\alpha_2 \to \alpha_2^p$, and $\alpha_2^p \to \alpha_2$. The second is given by $\alpha_1 \to \alpha_1^p$, $\alpha_1^p \to \alpha_1$, $\alpha_2 \to \alpha_2$, and $\alpha_2^p \to \alpha_2^p$. The third is given by $\alpha_1 \to \alpha_2$, $\alpha_1^p \to \alpha_2^p$, $\alpha_2 \to \alpha_1^p$, and $\alpha_2^p \to \alpha_1$. The fourth is given by $\alpha_1 \to \alpha_2^p$, $\alpha_1^p \to \alpha_2$, $\alpha_2 \to \alpha_1$, and $\alpha_2^p \to \alpha_1^p$. If the cross ratio of the ordered points α_1, α_1^p, α_2, and α_2^p is C, then, as we saw in the case of $V_p(211)$, the ordered points

α_1, α_1^p, α_2^p, and α_2 and the ordered points α_1^p, α_1, α_2, and α_2^p have cross ratio $1/C$. Similarly,

$$\frac{(\alpha_2 - \alpha_1^p)(\alpha_2^p - \alpha_1)}{(\alpha_2 - \alpha_1)(\alpha_2^p - \alpha_1^p)} = \frac{(\alpha_2^p - \alpha_1)(\alpha_2 - \alpha_1^p)}{(\alpha_2^p - \alpha_1^p)(\alpha_2 - \alpha_1)} = \frac{1}{C}.$$

That is, the ordered points α_2, α_2^p, α_1^p, and α_1 and the ordered points α_2^p, α_2, α_1, and α_1^p have cross ratio $1/C$ as well. Hence, by Proposition 3.1 and Proposition 3.2, for each of the permutations in the second set, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as that permutation if and only $C = -1$.

So, the size of the stabilizer of f is $8(p-1)$ if the cross ratio of the roots of f is -1 and $4(p-1)$ otherwise. The corresponding orbit having f as a representative has size $\frac{1}{8}p(p+1)(p-1)^2$ or $\frac{1}{4}p(p+1)(p-1)^2$, respectively. Suppose that there are m orbits of the former size and k orbits of the latter size. Then

$$\frac{1}{8}(p-2)p(p+1)(p-1)^2 = \frac{m}{8}p(p+1)(p-1)^2 + \frac{k}{4}p(p+1)(p-1)^2,$$

and hence, $2k + m = p - 2$. By the same argument used for the case of $V_p(4)$, we have $m \leq 1$. Since p is odd, $m = 1$ and $k = (p-3)/2$.

Thus, for the case of $V_p(22)$, there is one orbit of size $\frac{1}{8}p(p+1)(p-1)^2$, and there are $(p-3)/2$ orbits of size $\frac{1}{4}p(p+1)(p-1)^2$.

3.4 Case 4: Orbits of Forms with a Triple of Conjugate Roots in $\mathbb{P}^1(\mathbb{F}_{p^3})$ and One Root in $\mathbb{P}^1(\mathbb{F}_p)$

The next case is $V_p(31)$. Let $f \in V_p(31)$; recall that $|V_p(31)| = \frac{1}{3}p(p+1)^2(p-1)^2$. We denote the roots of f by α_1, α_2, α_2^p, and $\alpha_2^{p^2}$. As before, we need only to consider permutations of the roots where if $\alpha \to \beta$ then $\alpha^p \to \beta^p$, of which there are three. The first is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, $\alpha_2^p \to \alpha_2^p$, and $\alpha_2^{p^2} \to \alpha_2^{p^2}$. The second is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2^p$, $\alpha_2^p \to \alpha_2^{p^2}$, and $\alpha_2^{p^2} \to \alpha_2$. The third is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2^{p^2}$, $\alpha_2^p \to \alpha_2$, and $\alpha_2^{p^2} \to \alpha_2^p$. It follows immediately from Proposition 3.1 and Proposition 3.2 that there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as the

permutation given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, $\alpha_2^p \to \alpha_2^p$, and $\alpha_2^{p^2} \to \alpha_2^{p^2}$. Let C be the cross ratio of the ordered points α, α^p, α^{p^2}, and α^{p^3}. Then for the remaining two permutations, we have that

$$\frac{(\alpha_1 - \alpha_2^{p^2})(\alpha_2^p - \alpha_2)}{(\alpha_1 - \alpha_2)(\alpha_2^p - \alpha_2^{p^2})} = \frac{1}{1-C}$$

and that

$$\frac{(\alpha_1 - \alpha_2)(\alpha_2^p - \alpha_2^{p^2})}{(\alpha_1 - \alpha_2^{p^2})(\alpha_2^p - \alpha_2)} = \frac{C-1}{C}.$$

That is, the cross ratio of of the ordered points α_1, α_2^p, $\alpha_2^{p^2}$, and α_2 is $1/(1-C)$, and the cross ratio of of the ordered points α_1, $\alpha_2^{p^2}$, α_2, and α_2^p is $(C-1)/C$. Moreover, $C = 1/(1-C)$ if and only if $C = (C-1)/C$ if and only if $C^2 - C + 1 = 0$. Completing the square, we have that $C^2 - C + 1 = 0$ if and only if $(2(C-1/2))^2 = -3$, which has no solution when $p \equiv -1 \pmod 3$ and the two solutions $(1+\sqrt{-3})/2$ and $(1-\sqrt{-3})/2$ when $p \equiv 1 \pmod 3$.

So, the size of the stabilizer of f is $(p-1)$ when $p \equiv -1 \pmod 3$, in which case the size of the corresponding orbit having f as a representative is $p(p+1)(p-1)^2$. Hence, if $p \equiv -1 \pmod 3$, then $V_p(31)$ is partitioned into $(p+1)/3$ orbits of size $p(p+1)(p-1)^2$.

On the other hand, suppose that $p \equiv 1 \pmod 3$. Then by Proposition 3.1 and Proposition 3.2, for each of the the second and third permutations above, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as that permutation if and only if either $C = (1+\sqrt{-3})/2$ or $C = (1-\sqrt{-3})/2$. So, the size of the stabilizer of f is $3(p-1)$ if the cross ratio of the roots of f is either $(1+\sqrt{-3})/2$ or $(1-\sqrt{-3})/2$ and $(p-1)$ otherwise, and the corresponding orbit having f as a representative has size $\frac{1}{3}p(p+1)(p-1)^2$ or $p(p+1)(p-1)^2$, respectively. Suppose that there are m orbits of the former size and k orbits of the latter size. Then

$$\frac{1}{3}p(p+1)^2(p-1)^2 = \frac{m}{3}p(p+1)(p-1)^2 + kp(p+1)(p-1)^2,$$

and hence, $3k + m = p + 1$.

If $m > 2$, then there exist forms $f, g \in V_p(31)$ such that f and g are in distinct orbits and either the cross ratio of the roots of each form, when ordered as α_1, α_2, α_2^p, and $\alpha_2^{p^2}$, is $(1+\sqrt{-3})/2$ or the cross ratio of the roots of each form, when ordered as α_1, α_2, α_2^p, and $\alpha_2^{p^2}$, is $(1-\sqrt{-3})/2$. In either case, by Proposition 3.1 and Proposition 3.2 there exists a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that maps the roots of f to the roots of g, and so, by Proposition 2.5 there exists an element of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ that maps f to g, which is a contradiction. Hence $m \leq 2$. Since $p \equiv 1 \pmod 3$, $m = 2$ and $k = (p-1)/3$.

So, we conclude that for the case of $V_p(31)$, there are two orbits of size $\frac{1}{3}p(p+1)(p-1)^2$ and $(p-1)/3$ orbits of size $p(p+1)(p-1)^2$ when $p \equiv 1 \pmod 3$. On the other hand, there are $(p+1)/3$ orbits of size $p(p+1)(p-1)^2$ when $p \equiv -1 \pmod 3$.

3.5 Case 5: Orbits of Forms with Four Distinct Roots in $\mathbb{P}^1(\mathbb{F}_p)$

The final case is $V_p(1111)$, where all roots are in $\mathbb{F}_p$. Let $f \in V_p(1111)$, and recall that $|V_p(1111)| = \frac{1}{24}(p-2)p(p+1)(p-1)^2$. We denote the roots of f by α_1, α_2, α_3, and α_4. Unlike in all previous cases, all of the possible 24 permutations of the roots satisfy the condition that if $\alpha \to \beta$ then $\alpha^p \to \beta^p$. Let C be the cross ratio of the ordered points α_1, α_2, α_3, and α_4. We break the permutations into six sets of four based on the cross ratios of their outputs in terms of C.

The first set of permutations preserve the cross ratio C. The first permutation in this set is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_3$, and $\alpha_4 \to \alpha_4$. The second is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_4$, and $\alpha_4 \to \alpha_3$. The third is given by $\alpha_1 \to \alpha_3$, $\alpha_2 \to \alpha_4$, $\alpha_3 \to \alpha_1$, and $\alpha_4 \to \alpha_2$. The fourth is given by $\alpha_1 \to \alpha_4$, $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_2$, and $\alpha_4 \to \alpha_1$. It follows immediately from Proposition 3.1 and Proposition 3.2 that there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as each of the permutations in the first set.

The second set of permutations change the cross ratio to $1/C$. The first permutation in this set is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_4$, and $\alpha_4 \to \alpha_3$. The second is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_3$, and $\alpha_4 \to \alpha_4$. The third is given by $\alpha_1 \to \alpha_3$, $\alpha_2 \to \alpha_4$, $\alpha_3 \to \alpha_2$, and $\alpha_4 \to \alpha_1$. The fourth is given by $\alpha_1 \to \alpha_4$, $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_1$, and $\alpha_4 \to \alpha_2$. As we showed in the case of $V_p(211)$, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as each permutation in the second set if and only if $C = -1$.

The third set of permutations change the cross ratio to $C/(C-1)$. The first permutation in this set is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_4$, $\alpha_3 \to \alpha_3$, and $\alpha_4 \to \alpha_2$. The second is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_4$, and $\alpha_4 \to \alpha_1$. The third is given by $\alpha_1 \to \alpha_3$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_1$, and $\alpha_4 \to \alpha_4$. The fourth is given by $\alpha_1 \to \alpha_4$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_2$, and $\alpha_4 \to \alpha_3$. As we showed in the case of $V_p(4)$, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as each permutation in the set group if and only if $C = 2$.

The fourth set of permutations change the cross ratio to $1 - C$. The first permutation in this set is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_2$, and $\alpha_4 \to \alpha_4$. The second is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_4$, $\alpha_3 \to \alpha_1$, and $\alpha_4 \to \alpha_3$. The third is given by $\alpha_1 \to \alpha_3$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_4$, and $\alpha_4 \to \alpha_2$. The fourth is given by $\alpha_1 \to \alpha_4$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_3$, and $\alpha_4 \to \alpha_1$. We have not addressed a permutation from this group in previous cases, but it is similar to the second and third groups. Note that $C = 1 - C$ if and only if $C = 1/2$. Hence, by Proposition 3.1 and Proposition 3.2 there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as each of the permutations in the fourth set if and only if $C = 1/2$.

The fifth set of permutations change the cross ratio to $1/(1-C)$. The first permutation in this set is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_4$, and $\alpha_4 \to \alpha_2$. The second is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_4$, $\alpha_3 \to \alpha_3$, and $\alpha_4 \to \alpha_1$. The third is given by $\alpha_1 \to \alpha_3$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_2$, and $\alpha_4 \to \alpha_4$. The fourth is given by $\alpha_1 \to \alpha_4$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_1$, and $\alpha_4 \to \alpha_3$. As we showed in the case of $V_p(31)$, there is a

unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as each permutation in the fifth set if and only if $C = (1+\sqrt{-3})/2$ or $C = (1-\sqrt{-3})/2$.

The sixth set of permutations change the cross ratio to $(C-1)/C$. The first permutation in this set is given by $\alpha_1 \to \alpha_1$, $\alpha_2 \to \alpha_4$, $\alpha_3 \to \alpha_2$, and $\alpha_4 \to \alpha_3$. The second is given by $\alpha_1 \to \alpha_2$, $\alpha_2 \to \alpha_3$, $\alpha_3 \to \alpha_1$, and $\alpha_4 \to \alpha_4$. The third is given by $\alpha_1 \to \alpha_3$, $\alpha_2 \to \alpha_2$, $\alpha_3 \to \alpha_4$, and $\alpha_4 \to \alpha_1$. The fourth is given by $\alpha_1 \to \alpha_4$, $\alpha_2 \to \alpha_1$, $\alpha_3 \to \alpha_3$, and $\alpha_4 \to \alpha_2$. As we showed in the case of $V_p(31)$, there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as each permutation in the sixth set if and only if $C = (1+\sqrt{-3})/2$ or $C = (1-\sqrt{-3})/2$.

So, the size of the stabilizer of f is $12(p-1)$ if the cross ratio of the roots of f is $(1+\sqrt{-3})/2$ or $(1-\sqrt{-3})/2$, the size of the stabilizer of f is $8(p-1)$ if the cross ratio of the roots of f is -1, 2, or $1/2$, and the size of the stabilizer of f is $4(p-1)$ otherwise. The corresponding orbit having f as a representative has size $\frac{1}{12}p(p+1)(p-1)^2$, $\frac{1}{8}p(p+1)(p-1)^2$, or $\frac{1}{4}p(p+1)(p-1)^2$, respectively. Suppose that there are m orbits of the first size, k orbits of the second size, and n orbits of the third size. Then

$$\frac{1}{24}(p-2)p(p+1)(p-1)^2 = \frac{m}{12}p(p+1)(p-1)^2 + \frac{k}{8}p(p+1)(p-1)^2 + \frac{n}{4}p(p+1)(p-1)^2,$$

and hence, $2m+3k+6n = p-2$.

By the same argument used for the case of $V_p(31)$, we have $m \leq 2$. Moreover, since $p > 3$, $p-2 \not\equiv 1 \pmod 3$, and hence, $m \neq 2$. It is worth examining a more intuitive argument for why $m \neq 2$ in this case whereas we had $m = 2$ in the case of $V_p(31)$. We know that we cannot have forms $f, g \in V_p(1111)$ such that f and g are in distinct orbits but also the cross ratio of the roots of each form, when ordered as α_1, α_2, α_3, and α_4, is $(1+\sqrt{-3})/2$. Assume, however, that the forms f and g are in distinct orbits where the cross ratio of the roots of f, when ordered as α_1, α_2, α_3, and α_4, is $(1+\sqrt{-3})/2$, and the cross ratio of the roots of g, when ordered as β_1, β_2, β_3, and β_4, is $(1-\sqrt{-3})/2$. Noting that if $C = (1+\sqrt{-3})/2$, then

$1/(1-C) = (C-1)/C = (1+\sqrt{-3})/2$ and $1-C = C/(C-1) = 1/C = (1-\sqrt{-3})/2$, we see that the roots of g , when ordered as β_2, β_1, β_3, and β_4, for example, have cross ratio $(1+\sqrt{-3})/2$. By Proposition 3.1 and Proposition 3.2 there is a unique element of $\mathrm{PGL}_2(\mathbb{F}_p)$ that acts as the permutation given by $\alpha_1 \to \beta_2$, $\alpha_2 \to \beta_1$, $\alpha_3 \to \beta_3$, and $\alpha_4 \to \beta_4$. So, by Proposition 2.5 there exists an element of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ that maps f to g, which is a contradiction. This argument breaks down in the case of $V_p(31)$ because any map that does not satisfy the condition that if $\alpha \to \beta$ then $\alpha^p \to \beta^p$ cannot be realized as the action of an element of $\mathrm{PGL}_2(\mathbb{F}_p)$ on the roots. Suppose that $f, g \in V_p(31)$ such that the cross ratio of the roots of f when ordered as α_1, α_2, α_2^p, and $\alpha_2^{p^2}$, is $(1+\sqrt{-3})/2$, and the cross ratio of the roots of g, when ordered as β_1, β_2, β_2^p, and $\beta_2^{p^2}$, is $(1-\sqrt{-3})/2$. We cannot rearrange the roots of g so that we simultaneously have that the cross ratio is $(1+\sqrt{-3})/2$ and that there is a map from the roots of f to the roots of g satisfying that if $\alpha \to \beta$ then $\alpha^p \to \beta^p$.

Returning to the case of $V_p(1111)$, we see that since $3k+6n \equiv 0 \pmod 3$, $m = 0$ when $p \equiv -1 \pmod 3$, and $m = 1$ when $p \equiv 1 \pmod 3$. Moreover, if $m = 0$, then $p-2 = 3k+6n$, and if $m = 1$, then $p-2 = 2+3k+6n$. In either case, since p is odd, we conclude that k is also odd. We claim that $k = 1$.

The only other case to consider is the case where there are three orbits, with representatives f, g, h, of size $\frac{1}{8}p(p+1)(p-1)^2$ such that the cross ratio of the roots of f, when ordered as α_1, α_2, α_3, and α_4, is 2, the cross ratio of the roots of g, when ordered as β_1, β_2, β_3, and β_4, is -1, and the cross ratio of the roots of h, when ordered as δ_1, δ_2, δ_3, and δ_4, is $1/2$. Noting that if $C = 2$, then $C/(C-1) = 2$, $1/(1-C) = 1-C = -1$ and $1/C = (C-1)/C = 1/2$, we see that the roots of g, when ordered as β_4, β_2, β_3, and β_1, for example, have cross ratio 2 and that the roots of h, when ordered as δ_2, δ_1, δ_3, and δ_4, for example, have cross ratio 2 as well. It now follows from Proposition 3.1, Proposition 3.2 and Proposition 2.5 that f, g, and h lie in the same orbit, and so, this case never happens.

Hence, we conclude that for the case of $V_p(1111)$, there is one orbit of size $\frac{1}{12}p(p+1)(p-1)^2$, one orbit of size $\frac{1}{8}p(p+1)(p-1)^2$, and there are $(p-7)/6$ orbits of size $\frac{1}{4}p(p+1)(p-1)^2$ when $p \equiv 1 \pmod 3$. On the other hand, there is one orbit of size $\frac{1}{8}p(p+1)(p-1)^2$ and there are $(p-5)/6$ orbits of size $\frac{1}{4}p(p+1)(p-1)^2$ when $p \equiv -1 \pmod 3$.

We have thus completely classified the orbits of the action of $\mathrm{GL}_1(\mathbb{F}_p) \times \mathrm{GL}_2(\mathbb{F}_p)$ on V_p. There is still much work to be done towards achieving our goal to find a result similar to Proposition 1.1 in the quartic case. Ideas for the next steps, along with some preliminary results, are included in the appendices.

Bibliography

[1] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242.

[2] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math. **193** (2013), no. 2, 439–499.

[3] H. R. Brahana, *Note on irreducible quartic congruences*, Trans. Amer. Math. Soc. **38** (1935), no. 2, 395–400.

[4] J. W. P. Hirschfeld, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1998.

[5] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[6] Takashi Taniguchi and Frank Thorne, *Orbital L-functions for the space of binary cubic forms*, Canad. J. Math. **65** (2013), no. 6, 1320–1383.

[7] ———, *Secondary terms in counting functions for cubic fields*, Duke Math. J. **162** (2013), no. 13, 2451–2508.

Appendix A

Outline of Strategy to Compute an Explicit Formula for $\widehat{\phi}_p(g)$

This appendix is intended to provide a rough sketch of future work. It has not been rigorously checked.

The next step of our general strategy is to consider collections of binary quartic forms over $\mathbb{F}_p$ of a given shape, such as ax^4, all of which have a repeated root. Table A.1 shows some key examples.

Table A.1 Count of forms of a given shape in each orbit

Shape of form	# in $V_p(0)$	# in $V_p(1^4)$	# in $V_p(1^31)$	# in $V_p(1^21^2)$	# in $V_p(1^211)$	# in $V_p(21^2)$	# in $V_p(2^2)$
0	1	0	0	0	0	0	0
a_1x^4	1	$p-1$	0	0	0	0	0
a_2x^3y	1	0	$p-1$	0	0	0	0
$a_3x^2y^2$	1	0	0	$p-1$	0	0	0
$a_1x^4+a_2x^3y$	1	$p-1$	$p(p-1)$	0	0	0	0
$a_1x^4+a_3x^2y^2$	1	$p-1$	0	$p-1$	$\frac{1}{2}(p-1)^2$	$\frac{1}{2}(p-1)^2$	0
$a_2x^3y+a_3x^2y^2$	1	0	$p-1$	$p-1$	$(p-1)^2$	0	0
$a_1x^4+a_2x^3y+a_3x^2y^2$	1	$p-1$	$p(p-1)$	$p(p-1)$	$\frac{1}{2}p(p-1)^2$	$\frac{1}{2}p(p-1)^2$	0
$kx^2(x^2-ay^2)$	p	$p-1$	0	0	$\frac{1}{2}(p-1)^2$	$\frac{1}{2}(p-1)^2$	0
$k(x^2-ay^2)^2$	p	$p-1$	0	$\frac{1}{2}(p-1)^2$	0	0	$\frac{1}{2}(p-1)^2$

We also note the sizes of the relevant stabalizers:

$$|G| = (p+1)(p)(p-1)^3; \quad \frac{|G|}{|V_p(1^4)|} = p(p-1)^2; \quad \frac{|G|}{|V_p(1^31)|} = (p-1)^2;$$
$$\frac{|G|}{|V_p(1^21^2)|} = 2(p-1)^2; \frac{|G|}{|V_p(1^211)|} = 2(p-1);$$
$$\frac{|G|}{|V_p(21^2)|} = 2(p-1); \quad \frac{|G|}{|V_p(2^2)|} = 2(p+1)(p-1).$$

Recall that we want to find an explicit formula for $\widehat{\phi}_p(g)$, and we know that

$$\begin{aligned} p^5\widehat{\phi}_p(g) &= \sum_{f\in V_p} \phi_p(f)\langle f,g\rangle_p \\ &= \sum_{f\in V_p(0)} \langle f,g\rangle_p + \sum_{f\in V_p(1^4)} \langle f,g\rangle_p + \sum_{f\in V_p(1^31)} \langle f,g\rangle_p + \sum_{f\in V_p(1^21^2)} \langle f,g\rangle_p \\ &\quad + \sum_{f\in V_p(1^211)} \langle f,g\rangle_p + \sum_{f\in V_p(21^2)} \langle f,g\rangle_p + \sum_{f\in V_p(2^2)} \langle f,g\rangle_p. \end{aligned}$$

So, we want to express the sums over the seven orbits containing forms with repeated roots in terms of sums of the form $\sum_{\text{coeff. of } f} \sum_{(c,\gamma)\in G} \langle (c,\gamma)\cdot f, g\rangle_p$, where f is chosen from the left-most column of Table A.1. Table A.2 shows the relationships between these two types of sums.

Table A.2 Expressing $\sum_{\text{coeff. of } f} \sum_{(c,\gamma)\in G} \langle (c,\gamma)\cdot f, g\rangle_p$ in terms of sums over the orbits

f	copies of $\sum_{f\in V_p(0)} \langle f,g\rangle_p$	copies of $\sum_{f\in V_p(1^4)} \langle f,g\rangle_p$	copies of $\sum_{f\in V_p(1^31)} \langle f,g\rangle_p$	copies of $\sum_{f\in V_p(1^21^2)} \langle f,g\rangle_p$	copies of $\sum_{f\in V_p(1^211)} \langle f,g\rangle_p$	copies of $\sum_{f\in V_p(21^2)} \langle f,g\rangle_p$	copies of $\sum_{f\in V_p(2^2)} \langle f,g\rangle_p$
0	$p(p+1)(p-1)^3$	0	0	0	0	0	0
a_1x^4	$p(p+1)(p-1)^3$	$p(p-1)^3$	0	0	0	0	0
a_2x^3y	$p(p+1)(p-1)^3$	0	$(p-1)^3$	0	0	0	0
$a_3x^2y^2$	$p(p+1)(p-1)^3$	0	0	$2(p-1)^3$	0	0	0
$a_1x^4+a_2x^3y$	$p(p+1)(p-1)^3$	$p(p-1)^3$	$p(p-1)^3$	0	0	0	0
$a_1x^4+a_3x^2y^2$	$p(p+1)(p-1)^3$	$p(p-1)^3$	0	$2(p-1)^3$	$(p-1)^3$	$(p-1)^3$	0
$a_2x^3y+a_3x^2y^2$	$p(p+1)(p-1)^3$	0	$(p-1)^3$	$2(p-1)^3$	$2(p-1)^3$	0	0
$a_1x^4+a_2x^3y+a_3x^2y^2$	$p(p+1)(p-1)^3$	$p(p-1)^3$	$p(p-1)^3$	$2p(p-1)^3$	$p(p-1)^3$	$p(p-1)^3$	0
$kx^2(x^2-ay^2)$	$p^2(p+1)(p-1)^3$	$p(p-1)^3$	0	0	$(p-1)^3$	$(p-1)^3$	0
$k(x^2-ay^2)^2$	$p^2(p+1)(p-1)^3$	$p(p-1)^3$	0	$(p-1)^4$	0	0	$(p+1)(p-1)^3$

Next, we use Table A.2 to choose a collection of sums that are equivalent, up to

a factor in terms of p, to $\widehat{\phi}_p(g)$. One option is the following:

$$\begin{aligned}
&(p+1)(p)(p-1)^3p^5\widehat{\phi}_p(g)\\
&\qquad = p\sum_{k\in\mathbb{F}_p}\sum_{a\in\mathbb{F}_p}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot(k(x^2-ay^2)^2),g\rangle_p\\
&\qquad\quad - p\sum_{a_1\in\mathbb{F}_p}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot a_1x^4,g\rangle_p\\
&\qquad\quad - p^2\sum_{a_3\in\mathbb{F}_p}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot a_3x^2y^2,g\rangle_p\\
&\qquad\quad + (p+1)\sum_{a_1\in\mathbb{F}_p}\sum_{a_2\in\mathbb{F}_p}\sum_{a_3\in\mathbb{F}_p}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot(a_1x^4+a_2x^3y+a_3x^2y^2),g\rangle_p.
\end{aligned}$$

The last step is finding explicit formulas for these sums of the form $\sum_{\text{coeff. of } f}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot f,g\rangle_p$. The challenge is to determine how often the sum is nonzero. Conditions for each choice of f under which the sum $\sum_{\text{coeff. of } f}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot f,g\rangle_p$ is nonzero are provided in Table A.3.

Table A.3 Conditions on the coefficients of f such that $\sum_{\text{coeff. of } f}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot f,g\rangle_p\neq 0$

f	$[f,(c,\gamma)\cdot g]$	condition for $\sum_{\text{coeff. of } f}\sum_{(c,\gamma)\in G}\langle(c,\gamma)\cdot f,g\rangle_p\neq 0$
a_1x^4	a_1b_5	$b_5=0$
a_2x^3y	$-\frac{1}{4}a_2b_4$	$b_4=0$
$a_3x^2y^2$	$\frac{1}{6}a_3b_3$	$b_3=0$
$a_1x^4+a_2x^3y$	$-\frac{1}{4}a_2b_4+a_1b_5$	$b_4=0$ and $b_5=0$
$a_1x^4+a_3x^2y^2$	$\frac{1}{6}a_3b_3+a_1b_5$	$b_3=0$ and $b_5=0$
$a_2x^3y+a_3x^2y^2$	$\frac{1}{6}a_3b_3-\frac{1}{4}a_2b_4$	$b_3=0$ and $b_4=0$
$a_1x^4+a_2x^3y+a_3x^2y^2$	$\frac{1}{6}a_3b_3-\frac{1}{4}a_2b_4+a_1b_5$	$b_3=0$ and $b_4=0$ and $b_5=0$
$kx^2(x^2-ay^2)$	$-\frac{1}{6}kab_3+ab_5$	$b_3=0$ and $b_5=0$, or $b_3\neq 0$
$k(x^2-ay^2)^2$	$ka^2b_1-\frac{1}{6}2kab_3+kb_5$	$b_1=0$ and $b_3=0$ and $b_5=0$, or $b_1=0$ and $b_3\neq 0$, or $b_1\neq 0$ and $\left(-\frac{1}{6}2b_3\right)^2-4b_1b_5$ is a square or zero

Appendix B

Counting the Number of Forms in Each Orbit Where the x^2y^2 Coefficient is 0

This appendix includes only rough arguments and has not been rigorously checked.

Let $f(x,y) := a_1x^4+a_2x^3y+a_3x^2y^2+a_4xy^3+a_5y^4$, where $a_i \in \mathbb{F}_p$ for $i = 1,2,3,4,5$ with p a prime greater than 3. Then f factors completely over $\overline{\mathbb{F}_p}$:

$$f(x,y) = (\alpha_1x - \beta_1y)(\alpha_2x - \beta_2y)(\alpha_3x - \beta_3y)(\alpha_4x - \beta_4y),$$

$\alpha_i, \beta_i \in \overline{\mathbb{F}_p}$ for $i = 1,2,3,4$. The roots of f are elements of $\mathbb{P}^1\left(\overline{\mathbb{F}_p}\right)$, which we denote by $[\beta_i : \alpha_i]$ for $i = 1,2,3,4$. Note that $\alpha_i = 0$ for some i if and only if y is a factor of $f(x,y)$, and similarly, $\beta_i = 0$ for some i if and only if x is a factor of $f(x,y)$.

Consider the collection of forms f with $a_3 = 0$, which we denote by $\mathcal{C}_{a_3=0}$. Clearly, the form $f(x,y) = 0$ is in $\mathcal{C}_{a_3=0}$, and so, $|V_p(0) \cap \mathcal{C}_{a_3=0}| = |V_p(0)| = 1$. We want to determine the size of $V_p(\sigma) \cap \mathcal{C}_{a_3=0}$, where

$$\sigma \in \{1111, 1^211, 1^21^2, 1^31, 1^4, 211, 21^2, 22, 2^2, 31, 4\}.$$

First, we consider $V_p(1^4) \cap \mathcal{C}_{a_3=0}$, which clearly contains the $p-1$ forms a_1x^4, $0 \neq a_1 \in \mathbb{F}_p$, and the $p-1$ forms a_5y^4, $0 \neq a_5 \in \mathbb{F}_p$. Any other element of $V_p(1^4)$ can be expressed as $a_1(x - \beta_1y)^4$ with $0 \neq a_1, \beta_1 \in \mathbb{F}_p$, but then $a_3 = 6a_1\beta_1^2 \neq 0$. So,

$$|V_p(1^4) \cap \mathcal{C}_{a_3=0}| = 2p - 2.$$

Next, we look at $V_p(1^31) \cap \mathcal{C}_{a_3=0}$, which clearly contains the $p-1$ forms a_2x^3y, $0 \neq a_2 \in \mathbb{F}_p$, and the $p-1$ forms a_4xy^3, $0 \neq a_4 \in \mathbb{F}_p$, as well as the $(p-1)^2$ forms

$a_1x^3(x-\beta_1 y)$ with $0 \neq a_1, \beta_1 \in \mathbb{F}_p$, and the $(p-1)^2$ forms $-a_5y^3(\alpha_1 x - y)$ with $0 \neq a_5, \alpha_1 \in \mathbb{F}_p$. Any other element of $V_p(1^31)$ can be expressed as $a_1x(x+\beta_1 y)^3$ with $0 \neq a_1, \beta_1 \in \mathbb{F}_p$, $-a_5y(\alpha_1 x - y)^3$ with $0 \neq a_5, \alpha_1 \in \mathbb{F}_p$ or $a_1(x-\beta_1 y)^3(x-\beta_2 y)$ with $0 \neq a_1, \beta_1, \beta_2 \in \mathbb{F}_p$, $\beta_1 \neq \beta_2$, so that $a_3 = 3a_1\beta_1^2 \neq 0$, $a_3 = 3a_5\alpha_1^2 \neq 0$ or $a_3 = 3a_1\beta_1(\beta_2+\beta_1)$, respectively. We see that among these cases only the $(p-1)^2$ forms $a_1(x-\beta_1 y)^3(x+\beta_1 y)$ have $a_3 = 0$. Hence,

$$|V_p(1^31) \cap \mathcal{C}_{a_3=0}| = 2(p-1) + 3(p-1)^2 = 3p^2 - 4p + 1.$$

Now, condsider both $V_p(1^21^2) \cap \mathcal{C}_{a_3=0}$ and $V_p(2^2) \cap \mathcal{C}_{a_3=0}$. First, note that if $f \in \mathcal{C}_{a_3=0}$, then x^2 is a factor of $f(x,y)$ if and only if x^3 is a factor of $f(x,y)$, and similarly, y^2 is a factor of $f(x,y)$ if and only if y^3 is a factor of $f(x,y)$. Hence, any element of $(V_p(1^21^2) \cup V_p(2^2)) \cap \mathcal{C}_{a_3=0}$ can be expressed as $a_1(x-\beta_1 y)^2(x-\beta_2 y)^2$ with $0 \neq a_1 \in \mathbb{F}_p$ and β_1, β_2 either distinct nonzero elements of $\mathbb{F}_p$ or conjugates in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. In this case, $a_3 = a_1(\beta_1^2 + 4\beta_1\beta_2 + \beta_2^2)$. Completing the square, we see that $\beta_1^2 + 4\beta_1\beta_2 + \beta_2^2 = 0$ if and only if $\beta_1 = (-2 \pm \sqrt{3})\beta_2$. If $p \equiv 1 \pmod{12}$ or $p \equiv 11 \pmod{12}$, then $-2 \pm \sqrt{3} \in \mathbb{F}_p$, and if $p \equiv 5 \pmod{12}$ or $p \equiv 7 \pmod{12}$, then $-2 \pm \sqrt{3}$ are conjugates in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. In the former case, for each of the $p-1$ choices for β_2, β_1 is determined up to the choice between $-2+\sqrt{3}$ and $-2-\sqrt{3}$. But also, swapping β_1 and β_2 does not change the form. So, there are $p-1$ choices for the roots and $p-1$ choices for a_1. Hence,

$$|V_p(1^21^2) \cap \mathcal{C}_{a_3=0}| = \begin{cases} p^2+2p+1 & \text{if } p \equiv 1 \pmod{12} \text{ or } p \equiv 11 \pmod{12} \\ 0 & \text{otherwise.} \end{cases}$$

In the latter case, note that $u + v\sqrt{3} = (-2+\sqrt{3})(u - v\sqrt{3})$ if and only if $u = -v$, and $u + v\sqrt{3} = (-2-\sqrt{3})(u - v\sqrt{3})$ if and only if $u = v$. So, there are $p-1$ choices for a conjugate pair $\beta_1 = u + v\sqrt{3}$ and $\beta_2 = u - v\sqrt{3}$ in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ satisfying each of the equations $\beta_1 = (-2 \pm \sqrt{3})\beta_2$. But again, swapping β_1 and β_2 does not change the

form, and there are $p-1$ choices for a_1. Hence,

$$|V_p(2^2) \cap \mathcal{C}_{a_3=0}| = \begin{cases} p^2+2p+1 & \text{if } p \equiv 5 \pmod{12} \text{ or } p \equiv 7 \pmod{12} \\ 0 & \text{otherwise.} \end{cases}$$

Next, we consider $V_p(1^2 11) \cap \mathcal{C}_{a_3=0}$, which clearly contains the forms $a_2(x-\beta_1 y)^2(x-\beta_2 y)(y)$ with $0 \neq \beta_1, \beta_2 \in \mathbb{F}_p$, $\beta_1 \neq \beta_2$. For these forms, $a_3 = -a_2(2\beta_1+\beta_2)$. If we set $a_3 = 0$, and we choose a_2 and β_1, then β_2 is determined. Hence, there are $(p-1)^2$ forms $a_2(x-\beta_1 y)^2(x-\beta_2 y)(y)$ in $V_p(1^2 11) \cap \mathcal{C}_{a_3=0}$. Recall that if $f \in \mathcal{C}_{a_3=0}$, then x^2 is a factor of $f(x,y)$ if and only if x^3 is a factor of $f(x,y)$, and similarly, y^2 is a factor of $f(x,y)$ if and only if y^3 is a factor of $f(x,y)$. Hence, any other element of $V_p(1^2 11) \cap \mathcal{C}_{a_3=0}$ can be expressed as $a_1(x-\beta_1 y)^2(x-\beta_2 y)(x-\beta_3 y)$ with $0 \neq a_1, \beta_1 \in \mathbb{F}_p$ and β_2, β_3 distinct elements of $\mathbb{F}_p$ not equal to β_1. In this case, $a_3 = a_1(\beta_1^2 + 2(\beta_2+\beta_3)\beta_1 + \beta_2\beta_3)$. We want to count all combinations of $a_1, \beta_1, \beta_2, \beta_3$ such that $a_3 = 0$ and then subtract any combinations that produce a form outside of $V_p(1^2 11)$. By completing the square, we see that $\beta_1^2 + 2(\beta_2+\beta_3)\beta_1 + \beta_2\beta_3 = 0$ if and only if $(\beta_1+\beta_2+\beta_3)^2 - (\beta_2^2+\beta_2\beta_3+\beta_3^2) = 0$. Completing the square again, we have equivalently that

$$(\beta_1+\beta_2+\beta_3)^2 - \left(\beta_2 + \frac{1}{2}\beta_3\right)^2 = \frac{3}{4}\beta_3^2,$$

which we rewrite as

$$\left(\beta_1 + 2\beta_2 + \frac{3}{2}\beta_3\right)\left(\beta_1 + \frac{1}{2}\beta_3\right) = \frac{3}{4}\beta_3^2.$$

Now, if $\beta_3 = 0$, then either $\beta_1 = 0$ and β_2 can be any element of $\mathbb{F}_p$ or $\beta_1 = -2\beta_2$. Since there are $p-1$ choice for a_1, we have accounted for $2p(p-1)$ combinations of $a_1, \beta_1, \beta_2, \beta_3$ such that $a_3 = 0$. If $\beta_3 \neq 0$, we have

$$\left(2\frac{\beta_1}{\beta_3} + 4\frac{\beta_2}{\beta_3} + 3\right)\left(2\frac{\beta_1}{\beta_3} + 1\right) = 3.$$

If for a fixed choice of $0 \neq \beta_3 \in \mathbb{F}_p$, we choose $\beta_1 \in \mathbb{F}_p$ so that $\left(2\frac{\beta_1}{\beta_3}+1\right) = k \neq 0$, then β_2 is uniquely determined by the above equation. With the $p-1$ choices for a_1,

this accounts for an additional $(p-1)^3$ combinations of $a_1, \beta_1, \beta_2, \beta_3$ such that $a_3 = 0$. Since either $\beta_3 = 0$ or $\beta_3 \neq 0$, no other combinations exist. Since, swapping β_2 and β_3 does not change the form, we have

$$\frac{2p(p-1) + (p-1)^3}{2}$$

forms $a_1(x - \beta_1 y)^2(x - \beta_2 y)(x - \beta_3 y)$ with $a_3 = 0$; however, we have included forms that do not satisfy the conditions $0 \neq \beta_1$, $\beta_2 \neq \beta_3$, $\beta_1 \neq \beta_2$, and $\beta_1 \neq \beta_3$. In particular, we have included the $p-1$ forms $a_1 x^4$ in $V_p(1^4) \cap \mathcal{C}_{a_3=0}$, which correspond to the case $\beta_1 = \beta_2 = \beta_3 = 0$. We have included the $(p-1)^2$ forms $a_1 x^3(x - \beta y)$ in $V_p(1^3 1) \cap \mathcal{C}_{a_3=0}$; these forms correspond to the equivalent cases $\beta_1 = \beta_2 = 0$, $\beta_3 \neq 0$ and $\beta_1 = \beta_3 = 0$, $\beta_2 \neq 0$. Note that $\beta_1 = \beta_2 = 0$, $\beta_3 \neq 0$ corresponds to the case $k = 1$. We have also included the $(p-1)^2$ forms $a_1(x - \beta y)^3(x + \beta y)$ in $V_p(1^3 1) \cap \mathcal{C}_{a_3=0}$; these forms correspond to the cases $\beta_1 = \beta_2$, $\beta_1 = -\beta_3$ when $k = -1$ and $\beta_1 = \beta_3$, $\beta_1 = -\beta_2$ when $k = 3$. Lastly, if $p \equiv 1 \pmod{12}$ or $p \equiv 11 \pmod{12}$, then we have included the $(p-1)^2$ forms $a_1(x - \beta_1 y)^2(x - \beta_2 y)^2$ in $V_p(1^2 1^2) \cap \mathcal{C}_{a_3=0}$, which correspond to the case $\beta_2 = \beta_3$ when $k = -3 \pm 2\sqrt{3}$. So, if $p \equiv 1 \pmod{12}$ or $p \equiv 11 \pmod{12}$, then there are

$$\frac{2p(p-1) + (p-1)^3}{2} - (p-1) - 3(p-1)^2 = \frac{(p-5)(p-1)^2}{2}$$

forms $a_1(x - \beta_1 y)^2(x - \beta_2 y)(x - \beta_3 y)$ in $V_p(1^2 11) \cap \mathcal{C}_{a_3=0}$ with $0 \neq a_1, \beta_1 \in \mathbb{F}_p$ and β_2, β_3 distinct elements of $\mathbb{F}_p$ not equal to β_1. If $p \equiv 5 \pmod{12}$ or $p \equiv 7 \pmod{12}$, then there are

$$\frac{2p(p-1) + (p-1)^3}{2} - (p-1) - 2(p-1)^2 = \frac{(p-3)(p-1)^2}{2}.$$

Thus, adding in the $(p-1)^2$ forms $a_2(x - \beta_1 y)^2(x - \beta_2 y)(y)$ discussed above,

$$|V_p(1^2 11) \cap \mathcal{C}_{a_3=0}| = \begin{cases} \dfrac{p^3 - 5p^2 + 7p - 3}{2} & \text{if } p \equiv 1 \pmod{12} \text{ or } p \equiv 11 \pmod{12} \\ \dfrac{p^3 - 3p^2 + 3p - 1}{2} & \text{otherwise.} \end{cases}$$

Next, we consider $V_p(21^2) \cap \mathcal{C}_{a_3=0}$. Any element of $V_p(21^2) \cap \mathcal{C}_{a_3=0}$ can be expressed as

$$a_1(x-\beta_1 y)^2(x-(u+v\sqrt{n})y)(x-(u-v\sqrt{n})y)$$

with $u \in \mathbb{F}_p$, $0 \neq a_1, \beta_1, v \in \mathbb{F}_p$, and n not a square modulo p. In this case, $a_3 = a_1(\beta_1^2 + 4u\beta_1 + u^2 - nv^2)$. Completing the square, we see that $a_3 = 0$ if and only if

$$\beta_1 = -2u \pm \sqrt{3u^2 + nv^2}.$$

Let $0 \neq r \in \mathbb{F}_p$, and let $N_p(q(u,v) = r)$ denote the number of solutions $(u,v) \in \mathbb{F}_p$ to the equation $q(u,v) = r$. We follow the classical approach given in the third section of Chapter 8 in [5]. For a fixed n in $\mathbb{F}_p$,

$$\begin{aligned}
N_p(3u^2+nv^2=r) &= \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=r}} N_p(u^2=a)N_p(v^2=b) \\
&= \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=r}} \left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right) \\
&= \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=r}} 1 + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=r}} \left(\frac{a}{p}\right) + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=r}} \left(\frac{b}{p}\right) + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=r}} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \\
&= \sum_{a\in\mathbb{F}_p} 1 + \sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right) + \sum_{b\in\mathbb{F}_p} \left(\frac{b}{p}\right) + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=r}} \left(\frac{ab}{p}\right) \\
&= p + 0 + 0 + \sum_{a\in\mathbb{F}_p} \left(\frac{a(r-3a)n^{-1}}{p}\right) \\
&= p + \sum_{\substack{a\in\mathbb{F}_p \\ a\neq 0, 3^{-1}r}} \left(\frac{a(r-3a)n^{-1}}{p}\right) \\
&= p + \sum_{\substack{a\in\mathbb{F}_p \\ a\neq 0, 3^{-1}r}} \left(\frac{a(r-3a)^{-1}n}{p}\right) \\
&= p + \sum_{\substack{k\in\mathbb{F}_p \\ k\neq 0, -3^{-1}n}} \left(\frac{k}{p}\right) = p - \left(\frac{-3^{-1}n}{p}\right) = p - \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{n}{p}\right).
\end{aligned}$$

For the case $r = 0$, the result changes:

$$\begin{aligned}
N_p(3u^2 + nv^2 = 0) &= \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=0}} N_p(u^2 = a)N_p(v^2 = b) \\
&= \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=0}} \left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right) \\
&= \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=0}} 1 + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=0}} \left(\frac{a}{p}\right) + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=0}} \left(\frac{b}{p}\right) + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=0}} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \\
&= \sum_{a\in\mathbb{F}_p} 1 + \sum_{a\in\mathbb{F}_p} \left(\frac{a}{p}\right) + \sum_{b\in\mathbb{F}_p} \left(\frac{b}{p}\right) + \sum_{\substack{a,b\in\mathbb{F}_p \\ 3a+nb=0}} \left(\frac{ab}{p}\right) \\
&= p + 0 + 0 + \sum_{a\in\mathbb{F}_p} \left(\frac{-3n^{-1}a^2}{p}\right) \\
&= p + 0 + 0 + \sum_{\substack{a\in\mathbb{F}_p \\ a\neq 0}} \left(\frac{-3n}{p}\right) = p + (p-1)\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{n}{p}\right).
\end{aligned}$$

For each of the $\dfrac{p-1}{2}$ choices for a nonzero square $r \in \mathbb{F}_p$, there are $N_p(3u^2+nv^2 = r)$ pairs (u, v), with n not a square modulo p, each having two corresponding choices for β_1 such that $a_3 = 0$. If 3 is a square modulo p, then we have to subtract the extraneous pairs $(u, v) = \left(\sqrt{\dfrac{r}{3}}, 0\right)$ and $(u, v) = \left(-\sqrt{\dfrac{r}{3}}, 0\right)$, which do not yield forms in $V_p(21^2)$. We also have $N_p(3u^2+nv^2 = 0)$ pairs (u, v) each having one corresponding choice of β_1 such that $a_3 = 0$, but we have to subtract the extraneous pair $(0, 0)$, which does not yield a form in $V_p(21^2)$. Moreover, the solutions (u, v) and $(u, -v)$ yield the same form, and there are $p - 1$ choices for a_1. Hence,

$$\begin{aligned}
&|V_p(21^2) \cap \mathcal{C}_{a_3=0}| \\
&\quad = \left(\frac{p-1}{2} \cdot \frac{N_p(3u^2 + nv^2 = r) - \left(\left(\frac{3}{p}\right) + 1\right)}{2} \cdot 2 + \frac{N_p(3u^2 + nv^2 = 0) - 1}{2}\right)(p-1) \\
&\quad = \begin{cases} \dfrac{p^3 - 3p^2 + 3p - 1}{2} & \text{if } p \equiv 1 \pmod{12} \text{ or } p \equiv 11 \pmod{12} \\ \dfrac{p^3 - p^2 - p + 1}{2} & \text{otherwise.} \end{cases}
\end{aligned}$$

Next, we consider $V_p(211) \cap \mathcal{C}_{a_3=0}$, which clearly contains the forms

$$a_2(x - \beta_1 y)(x - (u + v\sqrt{n})y)(x - (u - v\sqrt{n})y))(y)$$

with $u \in \mathbb{F}_p$, $0 \neq a_1, \beta_1, v \in \mathbb{F}_p$, and n not a square modulo p. For these forms, $a_3 = -a_2(2u + \beta_1)$. If we set $a_3 = 0$, and we choose a_2 and u, then β_1 is determined. There is no restriction on the choice of v except that taking v or $-v$ yield the same form. Hence, there are $\dfrac{p(p-1)^2}{2}$ forms

$$a_2(x - \beta_1 y)(x - (u + v\sqrt{n})y)(x - (u - v\sqrt{n})y))(y)$$

in $V_p(211) \cap \mathcal{C}_{a_3=0}$. Any other element of $V_p(211) \cap \mathcal{C}_{a_3=0}$ can be expressed as

$$a_1(x - \beta_1 y)(x - \beta_2 y)(x - (u + v\sqrt{n})y)(x - (u - v\sqrt{n})y)$$

with $u \in \mathbb{F}_p$, $0 \neq a_1, \beta_1, \beta_2, v \in \mathbb{F}_p$, and n not a square modulo p. In this case,

$$a_3 = a_1(u^2 - nv^2 + 2u(\beta_1 + \beta_2) + \beta_1\beta_2).$$

By completing the square, we see that $u^2 + 2(\beta_1 + \beta_2)u + \beta_1\beta_2 - nv^2 = 0$ if and only if

$$(u + \beta_1 + \beta_2)^2 - (\beta_1^2 + \beta_1\beta_2 + \beta_2^2) - nv^2 = 0.$$

Completing the square again, we have equivalently that

$$(u + \beta_1 + \beta_2)^2 - \left(\beta_1 + \frac{1}{2}\beta_2\right)^2 - \frac{3}{4}\beta_2^2 - nv^2 = 0.$$

Solving for u, we have

$$u = \frac{1}{2}\left(-2(\beta_1 + \beta_2) \pm \sqrt{(2\beta_1 + \beta_2)^2 + 3\beta_2^2 + n(2v)^2}\right).$$

Let $0 \neq r \in \mathbb{F}_p$, and let $N_p(q(u, v) = r)$ denote the number of solutions $(u, v) \in \mathbb{F}_p$ to the equation $q(u, v) = r$. Then, for a fixed n in $\mathbb{F}_p$,

$$
\begin{aligned}
&N_p((2\beta_1+\beta_2)^2+3\beta_2^2+n(2v)^2=r)\\
&\quad=\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}} N_p((2\beta_1+\beta_2)^2=a)N_p(\beta_2^2=b)N_p((2v)^2=c)\\
&\quad=\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}} \left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right)\left(1+\left(\frac{c}{p}\right)\right)\\
&\quad=\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}} 1+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}}\left(\frac{a}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}}\left(\frac{b}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}}\left(\frac{c}{p}\right)\\
&\qquad+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}}\left(\frac{ab}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}}\left(\frac{ac}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}}\left(\frac{bc}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}}\left(\frac{abc}{p}\right)\\
&\quad=p^2+0+0+0+\sum_{c\neq r}\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=r-c}}\left(\frac{ab}{p}\right)+\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=0}}\left(\frac{ab}{p}\right)+\sum_{nb\neq r}\sum_{\substack{a,c\in\mathbb{F}_p\\3a+c=r-nb}}\left(\frac{ac}{p}\right)\\
&\qquad+\sum_{\substack{a,c\in\mathbb{F}_p\\3a+c=0}}\left(\frac{ac}{p}\right)+\sum_{3a\neq r}\sum_{\substack{b,c\in\mathbb{F}_p\\nb+c=r-3a}}\left(\frac{bc}{p}\right)+\sum_{\substack{b,c\in\mathbb{F}_p\\nb+c=0}}\left(\frac{bc}{p}\right)\\
&\qquad+\sum_{c\neq r}\left(\frac{c}{p}\right)\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=r-c}}\left(\frac{ab}{p}\right)+\left(\frac{r}{p}\right)\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=0}}\left(\frac{ab}{p}\right)\\
&\quad=p^2+(p-1)\left(-\left(\frac{-3n}{p}\right)\right)+(p-1)\left(\frac{-3n}{p}\right)+(p-1)\left(-\left(\frac{-3}{p}\right)\right)\\
&\qquad+(p-1)\left(\frac{-3}{p}\right)+(p-1)\left(-\left(\frac{-n}{p}\right)\right)+(p-1)\left(\frac{-n}{p}\right)\\
&\qquad-\left(\frac{r}{p}\right)\left(-\left(\frac{-3n}{p}\right)\right)+\left(\frac{r}{p}\right)(p-1)\left(\frac{-3n}{p}\right)\\
&\quad=p^2+\left(\frac{r}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{n}{p}\right)p.
\end{aligned}
$$

For the case $r=0$, the result changes:

$$
\begin{aligned}
&N_p((2\beta_1+\beta_2)^2+3\beta_2^2+n(2v)^2=0)\\
&\quad=\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=r}} N_p((2\beta_1+\beta_2)^2=a)N_p(\beta_2^2=b)N_p((2v)^2=c)\\
&\quad=\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}} \left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{b}{p}\right)\right)\left(1+\left(\frac{c}{p}\right)\right)\\
&\quad=\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}} 1+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}}\left(\frac{a}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}}\left(\frac{b}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}}\left(\frac{c}{p}\right)\\
&\qquad+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}}\left(\frac{ab}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}}\left(\frac{ac}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}}\left(\frac{bc}{p}\right)+\sum_{\substack{a,b,c\in\mathbb{F}_p\\3a+nb+c=0}}\left(\frac{abc}{p}\right)\\
&\quad=p^2+0+0+0+\sum_{c\neq 0}\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=-c}}\left(\frac{ab}{p}\right)+\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=0}}\left(\frac{ab}{p}\right)+\sum_{nb\neq 0}\sum_{\substack{a,c\in\mathbb{F}_p\\3a+c=-nb}}\left(\frac{ac}{p}\right)\\
&\qquad+\sum_{\substack{a,c\in\mathbb{F}_p\\3a+c=0}}\left(\frac{ac}{p}\right)+\sum_{3a\neq 0}\sum_{\substack{b,c\in\mathbb{F}_p\\nb+c=-3a}}\left(\frac{bc}{p}\right)+\sum_{\substack{b,c\in\mathbb{F}_p\\nb+c=0}}\left(\frac{bc}{p}\right)\\
&\qquad+\sum_{c\neq 0}\left(\frac{c}{p}\right)\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=-c}}\left(\frac{ab}{p}\right)+\sum_{\substack{a,b\in\mathbb{F}_p\\3a+nb=0}}\left(\frac{0}{p}\right)\\
&\quad=p^2+(p-1)\left(-\left(\frac{-3n}{p}\right)\right)+(p-1)\left(\frac{-3n}{p}\right)+(p-1)\left(-\left(\frac{-3}{p}\right)\right)\\
&\qquad+(p-1)\left(\frac{-3}{p}\right)+(p-1)\left(-\left(\frac{-n}{p}\right)\right)+(p-1)\left(\frac{-n}{p}\right)\\
&\qquad0\cdot\left(-\left(\frac{-3n}{p}\right)\right)+0\\
&\quad=p^2.
\end{aligned}
$$

For each of the $\dfrac{p-1}{2}$ choices for a nonzero square $r\in\mathbb{F}_p$, there are $N_p((2\beta_1+\beta_2)^2+3\beta_2^2+n(2v)^2=r)$ triples (β_1,β_2,v), with n not a square modulo p, each having two corresponding choices for u such that $a_3=0$. We have to subtract the $N_p((2\beta_1+\beta_2)^2+3\beta_2^2=r)$ extraneous triples $(\beta_1,\beta_2,0)$, which do not yield forms in $V_p(211)$. We also have $N_p((2\beta_1+\beta_2)^2+3\beta_2^2+n(2v)^2=0)$ pairs (β_1,β_2,v) each having one corresponding choice of u such that $a_3=0$, but we have to subtract the

$N_p((2\beta_1+\beta_2)^2+3\beta_2^2=0)$ extraneous triples with $v=0$ that do not yield a form in $V_p(211)$. Note that we are including the case where $\beta_1=\beta_2$. Moreover, β_1 and β_2 are interchangable as are the pairs (u,v) and $(u,-v)$, and there are $p-1$ choices for a_1. Hence,

$$\begin{aligned}
|V_p(211)\cap\mathcal{C}_{a_3=0}| &= (p-1)\cdot\frac{p-1}{2}\cdot\frac{N_p((2\beta_1+\beta_2)^2+3\beta_2^2+n(2v)^2=r)}{4}\cdot 2\\
&\quad-(p-1)\cdot\frac{p-1}{2}\cdot\frac{N_p((2\beta_1+\beta_2)^2+3\beta_2^2=r)}{4}\cdot 2\\
&\quad+(p-1)\frac{N_p((2\beta_1+\beta_2)^2+3\beta_2^2+n(2v)^2=0)}{4}\\
&\quad-(p-1)\frac{N_p((2\beta_1+\beta_2)^2+3\beta_2^2=0)}{4}\\
&\quad-\frac{1}{2}|V_p(21^2)\cap\mathcal{C}_{a_3=0}|+\frac{1}{2}p(p-1)^2\\
&=\begin{cases}\dfrac{p^4-2p^3+2p^2-2p+1}{4} & \text{if } p\equiv 1 \pmod{12}\\[2ex] \dfrac{p^3-3p^2+3p-1}{4} & \text{if } p\equiv 5 \pmod{12}\\[2ex] \dfrac{p^3-3p^2+3p-1}{4} & \text{if } p\equiv 7 \pmod{12}\\[2ex] \dfrac{p^3-p^2-p+1}{4} & \text{if } p\equiv 11 \pmod{12}.\end{cases}
\end{aligned}$$

The cases of $V_p(31)$ and $V_p(4)$ remain open.