Albanian Journal of Mathematics

Për një Shqipëri të shkencës dhe kulturës.

VOLUME 9, 2015

www.albanian-j-math.com

ALBANIAN JOURNAL OF MATHEMATICS
Volume 9, Number 1, Pages 3–29
ISSN: 1930-1235; (**2015**)

SIEGEL FUNCTIONS, MODULAR CURVES, AND SERRE'S UNIFORMITY PROBLEM

Harris B. Daniels
Department of Mathematics
Amherst College Box 2239
P.O. 5000
Amherst, MA 01002-5000
Email: hdaniels@amherst.edu

Abstract. Serre's uniformity problem asks whether there exists a bound k such that for any $p > k$, the Galois representation associated to the p-torsion of an elliptic curve $E/\mathbb{Q}$ is surjective independent of the choice of E. Serre showed that if this representation is not surjective, then it has to be contained in either a Borel subgroup, the normalizer of a split Cartan subgroup, the normalizer of a non-split Cartan subgroup, or one of a finite list of "exceptional" subgroups. We will focus on the case when the image is contained in the normalizer of a split Cartan subgroup. In particular, we will show that the only elliptic curves whose Galois representation at 11 is contained in the normalizer of a split Cartan have complex multiplication. To prove this we compute $X_s^+(11)$ using modular units, use the methods of Poonen and Schaefer to compute its Jacobian, and then use the method of Chabauty and Coleman to show that the only points on this curve correspond to CM elliptic curves.

1. Introduction

It is a classical result that the points of an elliptic curve E over a number field K (a smooth projective genus one curve with at least one K-rational point) can be given the structure of an abelian group. In fact, it is known from the Mordell-Weil theorem, that this group is finitely generated. Therefore, we have that

$$E(K) \cong E_{\text{tor}}(K) \times \mathbb{Z}^{r_K}$$

where $E_{\text{tor}}(K)$ is the torsion subgroup of $E(K)$ and $r = r_K$ is the rank of $E(K)$. There are many interesting questions about the rank of an elliptic curve that are still open, but the focus of this paper is on the torsion part of $E(K)$.

Let p be a prime number, and let $E[p]$ be the $\mathbb{F}_p$-vector space of p-torsion points on $E(\overline{K})$, where $\overline{K}$ is a fixed algebraic closure of K. The natural Galois action of $\text{Gal}(\overline{K}/K)$ on $E[p]$ induces a Galois representation $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}(E[p])$, and if we choose a $\mathbb{Z}/p\mathbb{Z}$-basis of $E[p]$, then we obtain a Galois representation $\rho_{E,p}$:

2010 *Mathematics Subject Classification.* Primary 14H52; Secondary 11F80.
Key words and phrases. Elliptic Curves, Modular Curves, Galois Representations.

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. The image of $\rho_{E,p}$ was extensively studied by Serre in [15].

Theorem 1.1. [15] *If E is an elliptic curve over $\mathbb{Q}$ that does not have complex multiplication, then there exists a constant $C_E > 0$ such that for every prime $p > C_E$, the mod-p Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is surjective.*

Serre asked the next natural question: can the constant C_E be chosen independently of E?

Question 1.2 (Serre's Uniformity Problem, [15], §4.3)**.** Does there exist a constant $C > 0$ such that $\rho_{E,p}$ is surjective for all $p > C$ and all E without complex multiplication?

In [15], Serre also shows that there are five possible cases for what the image of $\rho_{E,p}$ could be. There is an $\mathbb{F}_p$-basis of $E[p]$ such that one of the following happens:

(1) $\rho_{E,p}$ is surjective;
(2) The image of $\rho_{E,p}$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$;
(3) The image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$;
(4) The image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$;
(5) The image of $\rho_{E,p}$ is contained in one of a finite list of "exceptional" subgroups.

Serre showed the exceptional groups, as in case (5) above, are not subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for p greater than 13. The uniformity question in case (2) was proven by Mazur [11] where he showed that if p is greater than 37, and E does not have CM, then the image of $\rho_{E,p}$ cannot be contained in a Borel subgroup. Bilu, Parent, and Bilu, Parent, and Rebolledo [3] (also using results of Momose [12]) have shown that if $p \geq 11$, $p \neq 13$, and E is not CM, then case (3) cannot occur. This just leaves the case when the image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartain subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In this case, the arguments used by Mazur [11], and Bilu and Parent [2], fail and a different tactic must be taken. The focus of this paper is on the split case for the case of $p = 11$.

Theorem 1.3 (Theorem 5.5, Corollary 5.6)**.** *Any elliptic curve defined over $\mathbb{Q}$ whose associated Galois representation at 11 has image contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z})$ has complex multiplication.*

As mentioned above, Theorem 1.3 has already been proven. It is the simplest case of [13, Theorem 1.1] and in fact was probably even known before that. Here, the main goal is to prove the result by analyzing completely the arithmetic of the modular curve, $X_s^+(11)$, that parametrizes elliptic curves over $\mathbb{Q}$ with $\rho_{E,11}$ having split Cartan image. In the proof of Parent, the author shows a bound on the height of the j-invariant of any elliptic curve in the split case (3) above, and then run an exhaustive calculation that proves that none of the curves up to that bound have split Cartan image and are not CM, therefore proving the desired result. Our methods work directly on $X_s^+(11)$, in that we calculate all the rational points on $X_s^+(11)$, and in doing so, we compute the structure of the jacobian of the modular curve, and determine its rational points.

More concretely, the main theorem of this article is the following.

Theorem 1.4. *Let X be the modular curve $X_s^+(11)$ and let J be its associated jacobian variety. Then:*

(1) *X has a model $y^2 = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1$, and the j-map $X \to \mathbb{P}^1(\mathbb{Q})$ can be calculated explicitly.*

(2) *$X(\mathbb{Q})$ contains exactly 6 points, two of which are points at infinity ∞_+ and ∞_-, and one is a cusp $(0, -1)$. The points, together with the j-invariant of the elliptic curve associated to each non-cuspidal point are given in the following table:*

P	$(0, 1)$	$(0, -1)$	$(1, 2)$	$(1, -2)$	∞_+	∞_-
$j(P)$	8000	*cusp*	-3375	16581375	-884736	-88473600

(3) *$J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$. The torsion subgroup of $J(\mathbb{Q})$ is generated by $[(0, 1) - \infty_-]$, while $[\infty_+ - \infty_-]$ is a generator of infinite order.*

Another main goal of this paper is to illustrate several important techniques in the computation of rational points on (hyperelliptic) curves. First, a model for $X = X_s^+(11)$ is computed using Siegel functions and modular units and compute the j-map that gives the j-invariant of the elliptic curve associated to each non-cuspidal point on the curve. The method used to compute a model for X should readily generalize to other modular curves of prime level. In order to be able to apply the method of Chabauty and Coleman to find a bound on the number of rational points on X, we first need to determine the rank of the jacobian variety (in particular, one needs to show that the rank of $J(\mathbb{Q})$ less than the genus of X, which is 2). The jacobian is studied by performing a 2-descent via the methods of Poonen, Schaefer, and Stoll, that allows us to determine the structure of $J(\mathbb{Q})$, and in particular show that the free rank is 1, less than the genus of X, as desired. The method of Chabauty and Coleman now produces a bound of 8 rational points on X, but a naive search for points only yields the 6 points listed in Theorem 1.4. Finally, we find several automorphisms of $X(\mathbb{Q})$ that allows us to conclude that if there was an additional point beyond the 6 we list, then there would be at least 10 points on X, contradicting the bound of 8. Hence, the ones we list are all the rational points on X.

The paper is organized as follows. In Section 2 Siegel functions, and modular units are defined. In Section 3 we construct a model for $X_s^+(11)$ using modular units built out of Siegel functions, and in Section 3.5 we go on to compute the j-map. The 2-descent on the jacobian variety is described in Section 4. Finally, the method of Chabauty and Coleman is summarized in Section 5 and Theorem 1.3 is proved in Section 5.4.

1.1. **Acknowledgments.** Much of the contents of this paper were originally written in partial fulfillment of the requirements for the degree of doctor of philosophy at the University of Connecticut in 2013. Without the help and guidance of my thesis advisor, Álvaro Lozano-Robledo, this paper would not have been possible.

2. Klein Forms, Siegel Functions, and Modular Units

2.1. **Klein Forms and Siegel Functions.** In this Section we follow the notation and terminology laid out in Section 1 and 2 of Chapter 2 of [10]. In these sections, the authors give explicit methods for computing units in the function field of the modular curve $X(N)$. These functions are units because they only have poles and zeros at the cusps, and so when we consider the functions only on the non-cuspidal points, they are invertible. Before diving in, we need to recall the definition of what it means to be modular for a given congruence subgroup.

Definition 2.1. *A modular function for a congruence subgroup* Γ *is a meromorphic function on the compact Riemann surface* $\Gamma\backslash\mathscr{H}^*$.

Often, modular functions are considered as meromorphic functions on $\mathscr{H}^*$ that are invariant under the action of Γ. From this perspective a modular function for Γ is a function that satisfies the following conditions:

(1) $f(\tau)$ is invariant under the Γ. That is, $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma$;
(2) $f(\tau)$ is meromorphic in $\mathscr{H}$;
(3) $f(\tau)$ is meromorphic at the cusps.

Let L be a lattice in the complex plane and let $\mathfrak{f}(z, L)$ be the Klein form attached to L (see [10]). This is a function which takes a complex variable z and a lattice L as its arguments. These functions are homogeneous of degree 1; that is to say that $\mathfrak{f}(\lambda z, \lambda L) = \lambda\mathfrak{f}(z, L)$ for $\lambda \in \mathbb{C}$.

Let $W = \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} \in \mathbb{C}^2$ such that $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. Take $L = L(W) = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and let $z = z(\mathbf{a}, w) = a_1\omega_1 + a_2\omega_2$ with $\mathbf{a} = (a_1, a_2) \in \mathbb{R}^2$. Now, we can create a new function that takes as its arguments a vector $\mathbf{a} \in \mathbb{R}^2$ instead of $z \in \mathbb{C}$ and a vector $W \in \mathbb{C}^2$ whose entries are linearly independent over $\mathbb{R}$ by $\mathfrak{f}_{\mathbf{a}}(W) = \mathfrak{f}(z, L)$. In [10, Chapter 2], the authors show that these functions have the following properties:

K0. $\mathfrak{f}_{\mathbf{a}}(\lambda W) = \lambda\mathfrak{f}_{\mathbf{a}}(W)$.
K1. For $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $\mathfrak{f}_{\mathbf{a}}(\alpha W) = \mathfrak{f}_{\mathbf{a}\alpha}(W)$.
K2. If $\mathbf{b} = (b_1, b_2) \in \mathbb{Z}^2$, then $f_{\mathbf{a}+\mathbf{b}}(W) = \varepsilon(\mathbf{a}, \mathbf{b})\mathfrak{f}_{\mathbf{a}}(W)$, where

$$\varepsilon(\mathbf{a}, \mathbf{b}) = (-1)^{b_1b_2+b_1+b_2}e^{-\pi i(b_1a_2-b_2a_1)}.$$

K3. If $\alpha \in \Gamma(N)$, and $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$ such that the denominators of a_1 and a_2 divide N, then

$$\mathfrak{f}_{\mathbf{a}}(\alpha W) = \mathfrak{f}_{\mathbf{a}\alpha}(W) = \varepsilon_{\mathbf{a}}(\alpha)\mathfrak{f}_{\mathbf{a}}(W)$$

where $\varepsilon_{\mathbf{a}}(\alpha)$ is a $2N$th root of unity. If we let $\mathbf{a} = \left(\frac{r}{N}, \frac{2}{N}\right)$, $\varepsilon(\alpha)$ is given by

$$\varepsilon_{\mathbf{a}}(\alpha) = -(-1)^{\left(\frac{a-1}{N}r+\frac{c}{N}s+1\right)\left(\frac{b}{N}r+\frac{d-1}{N}s+1\right)}e^{2\pi i(br^2+(b-1)rs-cs^2)2N^2}.$$

Definition 2.2. *For* $\alpha = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *and* $\tau \in \mathscr{H}$, *let* $j(\alpha, \tau)$ *be the factor of automorphy given by*

$$j(\alpha, \tau) = c\tau + d.$$

The Klein functions may be considered as functions on the upper half plane, as follows: let $\tau \in \mathscr{H}$ and define $\mathfrak{f}_{\mathbf{a}}(\tau) = \mathfrak{f}_{\mathbf{a}}(W_\tau)$, where $W_\tau = \begin{pmatrix}\tau\\ 1\end{pmatrix}$.

Proposition 2.3. *For* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$

$$\mathfrak{f}_{\mathbf{a}\alpha}(\tau) = j(\alpha, \tau)\mathfrak{f}_{\mathbf{a}}(\alpha\tau).$$

Proof: Using properties **K0** and **K1** we see that for

$$\mathfrak{f}_{\mathbf{a}\alpha}(\tau) = \mathfrak{f}_{\mathbf{a}\alpha}(W_\tau) = \mathfrak{f}_{\mathbf{a}}(\alpha W_\tau) = \mathfrak{f}_{\mathbf{a}}\left(\begin{pmatrix}a\tau + b\\ c\tau + d\end{pmatrix}\right) = \mathfrak{f}_{\mathbf{a}}\left((c\tau + d)\begin{pmatrix}\frac{a\tau+b}{c\tau+d}\\ 1\end{pmatrix}\right) = j(\alpha, \tau)\mathfrak{f}_{\mathbf{a}}(\alpha\tau).$$

■

Definition 2.4. *The Siegel function associated to* $\mathbf{a} \in \mathbb{R}^2$, $g_{\mathbf{a}}(\tau)$, *is a function on* $\mathscr{H}$ *defined by*

$$g_{\mathbf{a}}(\tau) = \mathfrak{f}_{\mathbf{a}}(\tau)\eta(\tau)^2,$$

where $\eta(\tau)^2 = q^{\frac{1}{12}} \prod_{n=1}^{\infty}(1-q^n)^2$ *is the Dedekind eta function and* $q = e^{2\pi i\tau}$.

Notice that property **K2** says that if we are normalizing our functions to have leading coefficient 1, then $\mathbf{a} \in \mathbb{R}^2$ only matters modulo $\mathbb{Z}$. That is, we can actually take $\mathbf{a} \in (\mathbb{R}/\mathbb{Z})^2$. In fact, for the rest of the paper we are going to restrict ourselves, for the sake of simplicity, to considering functions where $\mathbf{a} \in (\mathbb{Q}/\mathbb{Z})^2$.

Before we continue, let us recall a theorem about the Dedekind eta function.

Proposition 2.5. [1, page 51] *If* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, *then*

$$\eta(\alpha\tau) = \xi(\alpha) \cdot \sqrt{j(\alpha,\tau)}\eta(\tau),$$

where $\xi(\alpha)$ *is a* 24*th root of unity.*

Remark 2.6. The observant reader might ask about how the square root above is chosen and whether the choice depend on τ. We will ignore this question for now and see in the proof of 2.8 that this ambiguity can be ignored.

For our purposes, we will only be interested in $\mathbf{a} = (a_1, a_2) \in (\mathbb{Q}/\mathbb{Z})^2$ and we let $z = a_1\tau + a_2$ and $q_z = e^{2\pi i z}$.

Theorem 2.7. [10, p. 29] *For each* $\mathbf{a} \in (\mathbb{Q}/\mathbb{Z})^2$, *the Siegel function* $g_{\mathbf{a}}(\tau)$ *can be given by the following* q*-expansion:*

$$g_{\mathbf{a}}(\tau) = -q_\tau^{(1/2)\mathbf{B}_2(a_1)} e^{2\pi i a_2(a_1-1)/2}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n/q_z)$$

where $\mathbf{B}_2(x) = x^2 - x + \frac{1}{6}$ *is the second Bernoulli polynomial.*

Theorem 2.8. *If* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ *as above and* $a \in (\mathbb{Q}/\mathbb{Z})^2$, *then*

$$g_{\mathbf{a}}(\alpha\tau) = \zeta(\alpha) \cdot g_{\mathbf{a}\alpha}(\tau)$$

where $\zeta(\alpha)$ *is a* 12*th root of unity that depends only on* α.

Proof: Using Propositions 2.3 and 2.5 we have,

$$\begin{aligned} g_{\mathbf{a}}(\alpha\tau) &= \mathfrak{f}_{\mathbf{a}}(\alpha\tau)(\eta(\alpha\tau))^2 \\ &= j(\alpha,\tau)^{-1}\mathfrak{f}_{\mathbf{a}\alpha}(\tau)\left(\xi(\alpha)\cdot\sqrt{j(\alpha,\tau)}\eta(\tau)\right)^2 \\ &= \xi(\alpha)^2\mathfrak{f}_{\mathbf{a}\alpha}(\tau)\eta(\tau)^2 = \zeta(\alpha)g_{\mathbf{a}\alpha}(\tau). \end{aligned}$$

Here $\zeta(\alpha) = \xi(\alpha)^2$ and since $\xi(\alpha)$ is a 24th root of unity, $\zeta(\alpha)$ is a 12th root of unity and since $\sqrt{j(\alpha,\tau)}$ appears inside the square, which square root we choose doesn't matter. ■

In [10], Kubert and Lang develop sufficient conditions for products of the $g_{\mathbf{a}}$'s to be modular of level N. These conditions are more difficult to state if N is not prime to 6, and also not of interest to us, so we will only state conditions for $(N, 6) = 1$.

Theorem 2.9. [10, Chapter 3, Theorem 5.2] *Let* $N \in \mathbb{N}$ *such that* $(N, 6) = 1$. *Let* A *be the set of all* $\mathbf{a} = \left(\frac{r_1}{N}, \frac{r_2}{N}\right) \in \left(\frac{1}{N}\mathbb{Z}\right)^2$ *and* $\mathbf{a} \notin \mathbb{Z}^2$. *Let*

$$g(\tau) = \prod_{\mathbf{a}\in A} g_{\mathbf{a}}^{m(\mathbf{a})}(\tau).$$

Then g is modular of level N if and only if the family $\{m(\mathbf{a})\}$ satisfies the following:

(1) $\displaystyle\sum_{\mathbf{a}\in A} m(\mathbf{a})r_1^2 \equiv \sum_{\mathbf{a}\in A} m(\mathbf{a})r_2^2 \equiv \sum_{\mathbf{a}\in A} m(\mathbf{a})r_1r_2 \equiv 0 \bmod N,$ *and*

(2) $\displaystyle\sum_{\mathbf{a}\in A} m(\mathbf{a}) \equiv 0 \bmod 12.$

In general, we will always assume that an element $\mathbf{a} = (a_1, a_2) \in (\mathbb{Q}/\mathbb{Z})^2$ is normalized so that $0 \leq a_1 < 1$ and $0 \leq a_2 < 1$. If we wish to remove this assumption then we will always use the notation $\langle a_1\rangle$ and $\langle a_2\rangle$ to mean the fractional part of a_1 and a_2.

Lemma 2.10. [10, p. 31] *For $\mathbf{a} = (a_1, a_2) \in (\mathbb{Q}/\mathbb{Z})^2$ we have*

$$\operatorname{ord}_{q_\tau} g_{\mathbf{a}}(\tau) = \operatorname{ord}_{i\infty} g_{\mathbf{a}}(\tau) = \frac{1}{2}\mathbb{B}_2\big(\langle a_1\rangle\big).$$

With this lemma we will be able to compute the divisor of any Siegel function we want. This will be important when we start to use these functions along with the Riemann-Roch theorem to compute models of curves.

2.2. **Modular Units for Congruence subgroups of Level p.** In this section we generalize the methods used in [6] to find a class of explicitly computable modular units for an arbitrary congruence subgroup of prime level $p \neq 2, 3$. For the rest of this section let Γ be a congruence subgroup of level $p \neq 2, 3$. Let $\Gamma^*(p) = \langle -I_2, \Gamma(p)\rangle$ if $-I_2 \in \Gamma$, otherwise let $\Gamma^*(p) = \Gamma(p)$. Next, let $\overline{\Omega} = \Gamma/\Gamma^*(p)$, and let Ω be a **fixed** set of representatives of $\overline{\Omega}$ in Γ.

Remark 2.11. Notice that Ω and $\overline{\Omega}$ are finite since Γ is a congruence subgroup of level p.

Now that we have defined these basic objects, we can define the basic functions that we are going to be interested in:

Definition 2.12. *For $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ with $\mathbf{a} \notin \mathbb{Z}^2$ let*

$$v_{\mathbf{a}}(\Gamma, \tau) = v_{\mathbf{a}}(\tau) = \Theta_{\mathbf{a}}(\Omega)\prod_{\gamma\in\Omega} g_{\mathbf{a}\gamma}(\tau)$$

where $\Theta_{\mathbf{a}}(\Omega) \in \mathbb{C}^\times$ is defined so that the leading term of the q-expansion of $v_{\mathbf{a}}(\tau)$ is 1. Also, let

$$u_{\mathbf{a}}(\Gamma, \tau) = u_{\mathbf{a}}(\tau) = v_{\mathbf{a}}(\Gamma, \tau)^c = \Theta_{\mathbf{a}}(\Omega)^c\prod_{\gamma\in\Omega} g_{\mathbf{a}\gamma}(\tau)^c$$

where c is the smallest positive integer such that $c \cdot \#\Omega \equiv 0 \bmod 12$. In each case, when the congruence subgroup is obvious, we will use the notation that omits Γ.

Lemma 2.13. *For $\delta \in \Gamma^*(p)$, $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$, $\mathbf{a} \notin \mathbb{Z}^2$, we have $g_{\mathbf{a}\delta}(\tau) = \varepsilon_{\mathbf{a}}(\delta)g_{\mathbf{a}}(\tau)$, where $\varepsilon_{\mathbf{a}}(\delta)$ is the $2p$-th root of unity in* **K3**.

Proof: Suppose $\delta \in \Gamma(p)$ and $\mathbf{a}$ is as above, then

$$g_{\mathbf{a}\delta}(\tau) = \mathfrak{f}_{\mathbf{a}\delta}(\tau)(\eta(\tau))^2 \overset{\mathbf{K3}}{=} \varepsilon_{\mathbf{a}}(\delta)\mathfrak{f}_{\mathbf{a}}(\tau)(\eta(\tau))^2 = \varepsilon_{\mathbf{a}}(\delta)g_{\mathbf{a}}(\tau).$$

Now, recall that

$$-I_2\tau = \frac{-1\cdot\tau + 0}{0\tau - 1} = \frac{-\tau}{-1} = \tau,$$

and $j(-I_1,\tau) = 0\tau - 1 = -1$. This means

$$g_{\mathbf{a}\cdot(-I_2)}(\tau) = j(-I_2,\tau)g_{\mathbf{a}}(-I_2\cdot\tau) = -g_{\mathbf{a}}(\tau).$$

Thus, for any element of the form $-\delta$ with $\delta \in \Gamma(P)$,

$$g_{\mathbf{a}(-\delta)}(\tau) = g_{\mathbf{a}(-I_2\cdot\delta)}(\tau) = g_{(\mathbf{a}(-I_2))\cdot\delta}(\tau) = \varepsilon_{\mathbf{a}}(\delta)g_{\mathbf{a}(-I_2)}(\tau) = -\varepsilon_{\mathbf{a}}(\delta)g_{\mathbf{a}}(\tau),$$

and since $\varepsilon_{\mathbf{a}}(\delta)$ is a $2p$-th root of unity, so is $-\varepsilon_{\mathbf{a}}(\delta)$ and the result follows. ■

Proposition 2.14. *Let $\Omega = \{\gamma_i\}_{i=1}^{\#\Omega}$ and $\Omega' = \{\gamma_i'\}_{i=1}^{\#\Omega}$ be two different choices of lifts for $\overline{\Omega}$ ordered so that there exists a $\delta_i \in \Gamma^*(p)$ such that $\gamma_i = \gamma_i'\delta_i$. Then*

$$\prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i}(\tau) = \kappa \cdot \prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'}(\tau)$$

where $\kappa = \prod_{i=1}^{\#\Omega} \varepsilon_{\mathbf{a}\gamma_i'}(\delta_i)$. Further,

$$\Theta_{\mathbf{a}}(\Omega') = \Theta_{\mathbf{a}}(\Omega)\cdot\kappa.$$

Proof: Suppose that Ω and Ω' are as above. For any $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ such that $\mathbf{a} \notin \mathbb{Z}^2$, we have

$$\prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i}(\tau) = \prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'\delta_i}(\tau) = \prod_{i=1}^{\#\Omega} \varepsilon_{\mathbf{a}\gamma_i'}(\delta_i)g_{\mathbf{a}\gamma_i'}(\tau) = \prod_{i=1}^{\#\Omega} \varepsilon_{\mathbf{a}\gamma_i'}(\delta_i)\cdot\prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'}(\tau) = \kappa\cdot\prod_{i=1}^{\#\Omega} g_{\mathbf{a}\gamma_i'}(\tau).$$

Therefore, we get that, if we choose a different set of lifts, we simply change our normalization constant by κ, more specifically, $\Theta_{\mathbf{a}}(\Omega') = \Theta_{\mathbf{a}}(\Omega)\cdot\kappa$. ■

Corollary 2.15. *The q-expansion $v_{\mathbf{a}}$ is independent of choice of the representatives of Ω and thus so it the q-expansions of $u_{\mathbf{a}}(\tau)$.*

Proof: Follows immediately from Proposition 2.14

■

Theorem 2.16. *Let $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$, with $\mathbf{a} \notin \mathbb{Z}^2$, then for any $\alpha \in \Gamma$,*

$$v_{\mathbf{a}}(\alpha\tau) = \zeta(\alpha)^{\#\Omega}\varepsilon_1(\mathbf{a},\alpha)v_{\mathbf{a}}(\tau),$$

where $\varepsilon_1(\mathbf{a},\alpha)$ is an explicitly computable $2p^{th}$-root of unity that depends on $\mathbf{a}$ and α and $\zeta(\alpha)$ is the 12^{th} root of unity in Theorem 2.8. Further, $\varepsilon_1(\mathbf{a},\alpha) = 1$ if and only if the product of Siegel functions defining $v_{\mathbf{a}}$ satisfies condition (1) of Theorem 2.9. Similarly, $\zeta(\alpha)^{\#\Omega}$ is 1 if and only if the product of Siegel functions defining $v_{\mathbf{a}}$ satisfies condition (2) of Theorem 2.9.

Proof: Recall that $\overline{\Omega} = \Gamma/\Gamma^*(p)$ and that Ω is a *fixed* set of lifts of $\overline{\Omega}$ to Γ. Fix $\alpha \in \Gamma$, $\overline{\alpha}$ its reduction to $\overline{\Omega}$. Let σ be the permutation of $\overline{\Omega}$ given by $\sigma(\overline{\beta}) = \overline{\beta}\cdot\overline{\alpha}$. For any $\gamma \in \Gamma$, we can write $\gamma\alpha = \gamma^\sigma\cdot\delta(\gamma,\alpha)$ where γ^σ is the unique lift of $\sigma(\overline{\gamma})$ into Ω and $\delta(\gamma,\alpha) \in \Gamma^*(p)$. By abuse of notation, we can let σ be a permutation of Ω by $\gamma \mapsto \gamma^\sigma$. Therefore,

$$g_{\mathbf{a}\gamma\alpha}(\tau) = g_{\mathbf{a}\gamma^\sigma\delta(\gamma,\alpha)}(\tau) = \varepsilon_{\mathbf{a}\gamma^\sigma}(\gamma,\alpha)g_{\mathbf{a}\gamma^\sigma}(\tau),$$

where $\varepsilon_{\mathbf{a}\gamma^\sigma}(\alpha,\gamma)$ is the $2p$-th root of unity from Lemma 2.13 that depends on $\mathbf{a}$ and $\delta(\gamma,\alpha)$. Let $\varepsilon_1(\mathbf{a},\alpha) = \prod_{\gamma\in\Omega} \varepsilon_{\mathbf{a}\gamma}(\gamma,\alpha)$. Then

$$v_{\mathbf{a}}(\alpha\tau) = \Theta_{\mathbf{a}}(\Omega)\prod_{\gamma\in\Omega} g_{\mathbf{a}\gamma}(\alpha\tau) = \Theta_{\mathbf{a}}(\Omega)\prod_{\gamma\in\Omega}\zeta(\alpha)\cdot g_{\mathbf{a}\gamma\alpha}(\tau) = \Theta_{\mathbf{a}}(\Omega)\cdot\zeta(\alpha)^{\#\Omega}\prod_{\gamma\in\Omega}\varepsilon_{\mathbf{a}\gamma}(\gamma,\alpha)g_{\mathbf{a}\gamma^\sigma}(\tau)$$

$$= \Theta_{\mathbf{a}}(\Omega)\cdot\zeta(\alpha)^{\#\Omega}\varepsilon_1(\mathbf{a},\alpha)\prod_{\gamma\in\Omega} g_{\mathbf{a}\gamma^\sigma}(\tau) = \zeta(\alpha)^{\#\Omega}\varepsilon_1(\mathbf{a},\alpha)v_{\mathbf{a}}(\tau),$$

where the last equality follows from the fact that σ is a permutation of Ω, so the terms are simply being reordered.

Finally, we note that the content of the proof of [10, Chapter 3, Theorem 5.2] is exactly showing that $\varepsilon_1(\mathbf{a},\alpha) = 1$ if and only if our product satisfies condition (1) of Theorem 2.9, while condition (2) ensures that $\zeta(\alpha)^{\#\Omega}$ would be 1. ■

Definition 2.17. *For* $\mathbf{a} = (a_1,a_2) = \left(\frac{r_1}{p},\frac{r_2}{p}\right) \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ *and* $\alpha \in \mathrm{SL}_2(\mathbb{Z})$*, let* $(\mathbf{a}\alpha)_1$ *and* $(\mathbf{a}\alpha)_2$ *be the integers such that* $\mathbf{a}\alpha = \left(\frac{(\mathbf{a}\alpha)_1}{p},\frac{(\mathbf{a}\alpha)_2}{p}\right)$.

Proposition 2.18. *For each* $\mathbf{a} = (a_1,a_2) = \left(\frac{r_1}{p},\frac{r_2}{p}\right) \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ *such that*

$$\sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_1^2 \equiv \sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_2^2 \equiv \sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_1(\mathbf{a}\gamma)_2 \equiv 0 \bmod p,$$

$u_{\mathbf{a}}(\tau)$ *is modular for* Γ*. Further, in this case* $\varepsilon_1(\mathbf{a},\alpha) = 1$ *for all* $\alpha\in\Gamma$*, where* $\varepsilon_1(\mathbf{a},\alpha)$ *is as defined in Theorem 2.16.*

Proof: Suppose that $\mathbf{a} \in \left(\frac{1}{p}\mathbb{Z}/\mathbb{Z}\right)^2$ such that

$$\sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_1^2 \equiv \sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_2^2 \equiv \sum_{\gamma\in\Omega} c(\mathbf{a}\gamma)_1(\mathbf{a}\gamma)_2 \equiv 0 \bmod p.$$

This means that the function $u_{\mathbf{a}}(\tau)$ is modular for $\Gamma^*(p)$ from Theorem 2.9. This implies $u_{\mathbf{a}}(\delta\tau) = u_{\mathbf{a}}(\tau)$ for all $\delta\in\Gamma^*(p)$, but by the definition $u_{\mathbf{a}}(\tau)$, this means that $\varepsilon_1(\mathbf{a},\gamma)$ is also 1 since the product that defines it only depends on the $\delta(\gamma,\alpha)$'s which are elements in $\Gamma^*(p)$. Therefore, for all $\alpha\in\Gamma$,

$$u_{\mathbf{a}}(\alpha\tau) = \left(\zeta(\alpha)^{\#\Omega}\varepsilon_1(\mathbf{a},\alpha)v_{\mathbf{a}}(\tau)\right)^c = \zeta(\alpha)^{\#\Omega\cdot c}\cdot 1^c\cdot v_{\mathbf{a}}(\tau)^c = v_{\mathbf{a}}(\tau)^c = u_{\mathbf{a}}(\tau),$$

and $u_{\mathbf{a}}(\tau)$ is modular for Γ. ■

3. The modular Curve $X_s^+(11)$

3.1. Modular curves associated to Normalizers of Split Cartan Subgroups.

We start this section by defining the basic groups that we will be interested in.

Definition 3.1. *A split Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ *is a conjugate of the group of diagonal matrices;*

$$C_s(p) = \left\{\begin{pmatrix} a & 0\\ 0 & b\end{pmatrix} : a,b\in(\mathbb{Z}/p\mathbb{Z})^\times\right\}.$$

The normalizer of $C_s(p)$ *is given by*

$$C_s^+(p) = \left\{\begin{pmatrix} a & 0\\ 0 & b\end{pmatrix}, \begin{pmatrix} 0 & c\\ d & 0\end{pmatrix} : a,b,c,d\in(\mathbb{Z}/p\mathbb{Z})^\times\right\}.$$

The congruence subgroup, $\Gamma_s^+(p)$, is the inverse image of $C_s^+(p)\cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ under the standard reduction map $\mathrm{SL}_2(\mathbb{Z})\to\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

With these definitions we are now ready to define the modular curve $X_s^+(p)$.

Definition 3.2. *Let $X_s^+(p)$ be the Riemann surface given by $\Gamma_s^+(p)\backslash\mathscr{H}^*$.*

Theorem 3.3. [7, p. 4] *For $p>3$, the genus of the curve $X_s^+(p)$ is given by*

$$g_s^+(p)=\frac{1}{24}\left(p^2-8p+11-4\left(\frac{-3}{p}\right)\right).$$

Example 3.4.

p	5	7	11	13	17	19	23	29	31	37	41	43	47
$g_s^+(p)$	0	0	2	3	7	9	15	26	30	45	57	63	77

3.2. **Curves of Genus Two.** Using Theorem 3.3, we can see that the genus of $X_s^+(11)$ is equal to 2. Before we start looking at this curve in particular it would be worth it to better understand general genus 2 curves.

Proposition 3.5. *Every smooth projective curve of genus two, C, is birationally equivalent to a curve of the form:*

$$y^2+yh(x)=f(x),$$

with $\deg(h)\le 3$ *and* $\deg(f)\le 5$.

Proposition 3.5 tells us that every genus two curve is hyperelliptic. In fact, if the base field of C is not of characteristic two, then C is birationally equivalent to a curve of the form $y^2=f(x)$ where $\deg(f)=5$ or 6. This model is obtained by completing the square on the left hand side and doing a change of variables.

Remark 3.6. Here we notice that it is impossible to embed a smooth genus two curve into $\mathbb{P}^2$. Indeed, if C is a smooth curve given as the vanishing set of a degree d homogeneous polynomial then its genus must be $g=\frac{(d-1)(d-2)}{2}$. A quick check shows that this formula never equals two since it is impossible for $(d-1)(d-2)$ to be 4. Therefore in regular projective space the models of these curves are always singular. To combat this, when we consider a genus two curve given by a hyperelliptic equation, we are really thinking about them in weighted projective space. More specifically, we give x and z weight 1 and y weight 3. Therefore, when the models are homogenized they become $Y^2+Yh(X,Z)=f(X,Z)$ where $\deg(h)=3$ and $\deg(f)=6$, or $Y^2=f(X,Z)$ with $\deg(f)=6$.

3.3. **Modular Units for $X_s^+(11)$.** Now, we aim to find a model for $X_s^+(11)$ using a technique similar to the proof of Proposition 3.5. We start noticing that in this case $\#\Omega=12$ and so $c=1$. Therefore in this case, have that $u_{\mathbf{a}}=v_{\mathbf{a}}$. To ease notation, we let

$$w_{\mathbf{a},\mathbf{b}}=\frac{v_{\mathbf{a}}}{v_{\mathbf{b}}}.$$

Using SAGE, we check that for every $\mathbf{a}\in\left(\frac{1}{11}\mathbb{Z}/\mathbb{Z}\right)^2$ the product defining $v_{\mathbf{a}}$ satisfies the condition in Proposition 2.18 and we compute the divisors of the modular units of the form $w_{\mathbf{a},\mathbf{b}}$. Doing so gives us the following table:

	$0/\infty$	1	2	3	4	5
$w_{(1/11,1/11),(0/11,1/11)}$	-5	1	3	1	0	0
$w_{(3/11,1/11),(0/11,1/11)}$	-5	1	0	3	1	0
$w_{(2/11,1/11),(0/11,1/11)}$	-5	3	0	0	1	1
$w_{(5/11,1/11),(0/11,1/11)}$	-5	0	1	0	3	1
$w_{(4/11,1/11),(0/11,1/11)}$	-5	0	1	1	0	3
$w_{(1/11,1/11),(3/11,1/11)}$	0	0	3	-2	-1	0
$w_{(3/11,1/11),(2/11,1/11)}$	0	-2	0	3	0	-1
$w_{(2/11,1/11),(5/11,1/11)}$	0	3	-1	0	-2	0
$w_{(5/11,1/11),(4/11,1/11)}$	0	0	0	-1	3	-2
$w_{(4/11,1/11),(1/11,1/11)}$	0	-1	-2	0	0	3
$w_{(4/11,1/11),(3/11,1/11)}$	0	-1	1	-2	-1	3
$w_{(1/11,1/11),(2/11,1/11)}$	0	-2	3	1	-1	-1
$w_{(3/11,1/11),(5/11,1/11)}$	0	1	-1	3	-2	-1
$w_{(2/11,1/11),(4/11,1/11)}$	0	3	-1	-1	1	-2
$w_{(5/11,1/11),(1/11,1/11)}$	0	-1	-2	-1	3	1

Remark 3.7. From Theorem 2.7 we know that the field of definition of the functions defined in Section 2.2 is the p-th cyclotomic field. In practice, the field of definition might actually be a subfield of the p-th cyclotomic field. In fact, using the Riemann-Roch Theorem, one can show that all of the functions above are actually defined over the maximal real subfield of $\mathbb{Q}(\zeta_{11})$, usually denoted $\mathbb{Q}(\zeta_{11})^+$.

Example 3.8. *Using SAGE, one can compute that the first few terms of the q-expansion of*
$w_{(2/11,1/11),(0/11,1/11)}(\tau)$ *are given by*

$$q^{-5} + (-\zeta_{11}^9 - \zeta_{11}^2 + 1)q^{-4} + (\zeta_{11}^8 + \zeta_{11}^7 + \zeta_{11}^6 + \zeta_{11}^5 + \zeta_{11}^4 + \zeta_{11}^3 + 4)q^{-3} +$$
$$(-2\zeta_{11}^9 - 2\zeta_{11}^2 + 4)q^{-2} + (-2\zeta_{11}^9 + \zeta_{11}^8 + \zeta_{11}^7 + \zeta_{11}^6 + \zeta_{11}^5 + \zeta_{11}^4 + \zeta_{11}^3 - 2\zeta_{11}^2 + 9)q^{-1} +$$
$$(-4\zeta_{11}^9 + \zeta_{11}^8 + 2\zeta_{11}^7 + \zeta_{11}^6 + \zeta_{11}^5 + 2\zeta_{11}^4 + \zeta_{11}^3 - 4\zeta_{11}^2 + 12) +$$
$$(-5\zeta_{11}^9 + 2\zeta_{11}^8 + 2\zeta_{11}^7 + 2\zeta_{11}^6 + 2\zeta_{11}^5 + 2\zeta_{11}^4 + 2\zeta_{11}^3 - 5\zeta_{11}^2 + 20)q +$$
$$(-8\zeta_{11}^9 + 2\zeta_{11}^8 + 2\zeta_{11}^7 + 2\zeta_{11}^6 + 2\zeta_{11}^5 + 2\zeta_{11}^4 + 2\zeta_{11}^3 - 8\zeta_{11}^2 + 27)q^2 +$$
$$(-9\zeta_{11}^9 + 5\zeta_{11}^8 + 5\zeta_{11}^7 + 5\zeta_{11}^6 + 5\zeta_{11}^5 + 5\zeta_{11}^4 + 5\zeta_{11}^3 - 9\zeta_{11}^2 + 43)q^3 +$$
$$(-16\zeta_{11}^9 + 5\zeta_{11}^8 + 5\zeta_{11}^7 + 5\zeta_{11}^6 + 5\zeta_{11}^5 + 5\zeta_{11}^4 + 5\zeta_{11}^3 - 16\zeta_{11}^2 + 57)q^4 +$$
$$(-19\zeta_{11}^9 + 7\zeta_{11}^8 + 7\zeta_{11}^7 + 7\zeta_{11}^6 + 7\zeta_{11}^5 + 7\zeta_{11}^4 + 7\zeta_{11}^3 - 19\zeta_{11}^2 + 84)q^5 + O(q^6)$$

If we have any hope to use these functions to compute a model for $X_s^+(11)$, we somehow have to use these functions to construct new functions that are defined over $\mathbb{Q}$ and apply the argument from Proposition 3.5 to them.

Proposition 3.9. *Let $K/\mathbb{Q}$ be a number field of degree n and let $\{e_1, e_2, \ldots, e_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Let $Gal(K/\mathbb{Q}) = \{\sigma_i\}_{i=1}^n$. Let Γ be a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *such that the cusp of $X(\Gamma)$ at infinity is rational. Further, let $f(\tau) =$*

$\sum_k a_k\, q^k$ *be the* q*-expansion of a modular function for* Γ *with coefficients in* K*. Let* $a_k = a_{k,1}e_1 + \cdots + a_{k,n}e_n$ *with* $a_{i,j} \in \mathbb{Q}$*. Then the function* $f_k(\tau) = \sum_i a_{k,j}\, q^k$ *is also modular for* Γ*. In particular, there are constants,* $b_j \in K$ *depending on* k*, such that* $f_k = \sum_{j=1}^{n} b_j\, \sigma_j(f(\tau))$*.*

Proof: Using the fact that every element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is a field automorphism that fixes $\mathbb{Q}$, for any $\alpha = \alpha_1\, e_1 + \cdots + \alpha_n\, e_n \in K$ we get

$$\begin{pmatrix} \sigma_1(e_1) & \sigma_1(e_2) & \dots & \sigma_1(e_n) \\ \sigma_2(e_1) & \sigma_2(e_2) & \dots & \sigma_2(e_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(e_1) & \sigma_n(e_2) & \dots & \sigma_n(e_n) \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}. \tag{3.1}$$

For convenience let A be the matrix on the left hand side of (3.1), and let A_i be the matrix obtained from replacing the i-th row of A with the column vector on the right hand side of (3.1). Applying Cramer's rule we get that $\alpha_i = \det A_i / \det A$. Now, if we let A_{ji} be the matrix obtained by deleting the j-th row and i-th column of A_i, we can compute the determinant of A_i by looking at the cofactor expansion of A_i along the i-th column. Doing this shows that:

$$\alpha_i = \frac{\det A_i}{\det A} = \frac{1}{\det A} \sum_{j=1}^{n} (-1)^{j+i} \sigma_j(\alpha) \det A_{ji}.$$

Letting $b_j = \dfrac{(-1)^{j+i} \det A_{ji}}{\det A}$ we have that $\alpha_i = \sum_{j=1}^{n} b_j\, \sigma_j(\alpha)$. Notice that the definition of b_j does not depend on α because both determinants are polynomials in the $\sigma_i(e_k)$'s.

Now, if we assume that $X(\Gamma)$ has a rational cusp at infinity, then $\mathrm{Gal}(K/\mathbb{Q})$ acts on the q-expansion of a modular form $f = \sum_k a_k\, q^k$ simply by acting on the coefficients. Since the b_j's don't depend on anything other than the choice of basis for $\mathcal{O}_K$, we get that

$$f_k(\tau) = \sum_{j=1}^{n} b_j\, \sigma_j(f(\tau)),$$

and the modularity of $f_j(\tau)$ follows from the modularity of $\sigma_j(f(\tau))$. ■

Looking at the first 5 functions on our table, we see that they all have poles of order 5 at infinity and no where else. Now, since ord_p is a non-archemedian valuation on the functions of $X_s^+(11)$, and ∞ is a rational point, we know that taking linear combinations of the Galois conjugates won't introduce any other poles. With this in mind we let $X = [w_{(2/11,1/11),(0/11,1/11)}(\tau)]_1$, $Y = [w_{(1/11,1/11),(0/11,1/11)}(\tau)]_2$, $Z = [w_{(3/11,1/11),(0/11,1/11)}(\tau)]_0$, where the subscript indicates which coefficients we are using to create the q-expansions. The important thing is that $\mathrm{ord}_\infty(X) = -3$, $\mathrm{ord}_\infty(Y) = -4$, and $\mathrm{ord}_\infty(Z) = -5$ and these functions don't have any other poles.

3.4. **Computing a Model for $X_s^+(11)$.** Now that we have computed some functions whose poles are concentrated at infinity, we need to find a polynomial relationship between them.

Proposition 3.10. *Let C be a smooth genus 2 curve. Let X, Y, and Z be in $K(C)$ the function field of C with poles of order 3, 4, and 5 respectively at ∞ and nowhere else. Then C can be mapped into $\mathbb{P}^2(K)$ as the vanishing set of a polynomials of degree at most 7.*

Proof: We start by noticing that all the monomials of degree $d > 0$ in X, Y, and Z are contained in $\mathscr{L}(5d\infty)$. Using the Riemann-Roch theorem, we know that the dimension of this space is

$$\ell(5d(\infty)) = \deg(5d(\infty)) - g + 1 = 5d - 1.$$

The number of three variable monomials of degree d is given by $\binom{d+2}{2}$.

So we build a table and see when the number of monomials of degree d becomes greater than the dimension of $\mathscr{L}(5d \cdot \infty)$.

d	1	2	3	4	5	6	7
$\ell(5d \cdot \infty)$	4	9	14	19	24	29	34
$\binom{d+2}{2}$	3	6	10	15	21	28	36

The table above shows that there must be a polynomial, p, of degree at most 7 such that $p(X, Y, Z) = 0$. ■

Lemma 3.11. *Let C be a genus g curve. The only function without any poles and a zero at infinity is the zero function.*

Proof: Let f be a function that has no poles and a zero at ∞. This means that f is in $\mathscr{L}(-\infty)$, but by the Riemann-Roch Theorem, we know that $\ell(-\infty) = 0$. Thus, f must be the zero function. ■

Now, we notice that since X, Y, and Z are functions whose only poles are at ∞, any polynomial in X, Y, and Z can also only have a pole at infinity. Thus, by Lemma 3.11, if we can find a polynomial in X, Y, and Z that has a zero at infinity, it must in fact be zero. Computing the q-expansions of X, Y, and Z to a reasonable precision, it is easy to show that

$$\begin{split}0 = p(X, Y, Z) = 3\,X^2Y^3 + X^2Y^2Z - X^2YZ^2 + 2\,XY^4 - 2\,XY^2Z^2 + 2\,XYZ^3 + \\ XZ^4 - Y^5 + 3\,Y^4Z - Y^3Z^2 - Y^2Z^3 + O(q^N).\end{split}$$

for some $N \geq 1$ depending on the initial precision that was used to calculate X, Y, and Z. Unfortunately, this is not in the best model for the modular curve. First of all it is singular, and secondly it isn't written in hyperelliptic form.

A quick check show that if we use the change of variables

$$\begin{aligned}
X_1 &= Y^2Z^4 + \frac{1}{2}YZ^5,\\
Y_1 &= \frac{3}{2}XY^5Z^{12} - \frac{3}{2}Y^6Z^{12} + 2XY^4Z^{13} + \frac{1}{2}Y^5Z^{13} + \frac{3}{8}XY^3Z^{14} + \frac{5}{8}Y^4Z^{14}\\
&\quad - \frac{3}{8}XY^2Z^{15} - \frac{1}{2}Y^3Z^{15} - \frac{1}{8}XYZ^{16} + \frac{1}{4}Y^2Z^{16} + \frac{1}{2}YZ^{17} + \frac{1}{8}Z^{18},\\
Z_1 &= Y^2Z^4 - \frac{1}{2}YZ^5 - \frac{1}{2}Z^6.
\end{aligned}$$

and $x_1 = X_1/Z_1$ and $y_1 = Y_1/Z_1^3$, then we see that $X_s^+(11)$ is isomorphic to the hyperelliptic curve given by

$$y_1^2 + (x_1^3 + x_1^2 + x_1 + 1)y_1 = -2x_1^5 + 2x_1^4 - 3x_1^3 + 2x_1^2 - 2x_1.$$

Here we note that we are working in weighted projective space where x_1 and z_1 have weight one and y_1 has weight three. While this model is minimal, it will not be the most convenient for us to use. Instead we will use its simplified model:

$$\boxed{X_s^+(11) : y^2 = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1.}$$

Here the change of variables from the initial curve is given by

$$\begin{aligned}
X_2 &= Y^2Z^4 + 1/2YZ^5,\\
Y_2 &= -3XY^5Z^{12} - Y^6Z^{12} - 4XY^4Z^{13} - Y^5Z^{13} - \frac{3}{4}XY^3Z^{14} + \frac{3}{4}Y^4Z^{14}\\
&\quad + \frac{3}{4}XY^2Z^{15} + \frac{1}{4}XYZ^{16} - \frac{5}{4}Y^2Z^{16} - \frac{3}{4}YZ^{17} - \frac{1}{8}Z^{18},\\
Z_2 &= Y^2Z^4 - 1/2YZ^5 - 1/2Z^6,
\end{aligned}$$

and again $x = X_2/Z_2$ and $y = Y_2/Z_2^3$. This model has bad reduction at two and eleven, but the extra prime of bad reduction will not cause any problems.

Remark 3.12. The minimal and simplified models for $X_s^+(11)$, along with the changes of variables, were found using Magma and checked to work by hand.

3.5. **Computing the j-map for $X_s^+(11)$.** The last task for this section is to compute the map from $X_s^+(11)$ to $\overline{\mathbb{Q}}$ that takes a point on $X_s^+(11)$ and returns the j-invariant of the corresponding elliptic curve. Since we know that j must be a function in the function field of $X_s^+(11)$, it must be a rational function in x and y. Therefore, we know that there is a rational combination of the q-expansions of x and y that will give us the q-expansion of the j function. Recall, we are using the nonstandard notation $q = e^{\frac{2\pi i\tau}{11}}$, then

$$j(\tau) = q^{-11} + 744 + 196884q^{11} + 21493760q^{22} + 864299970q^{33} + O(q^{44}).$$

Since x and y satisfy a hyperelliptic relationship, $y^2 = f(x)$ we know that the highest powers of y that can occur in numerator and denominator of our rational function is one. Further, if the denominator of our rational function is $C'y + D'$ with C' and D' in $\mathbb{Q}[x]$, we can multiply both the numerator and denominator by

$C'y - D'$ to get the denominator to be completely in $\mathbb{Q}[x]$. Therefore we know that there must be A, B, and C in $\mathbb{Q}[x]$ such that

$$j = \frac{Ay + B}{C}.$$

This is equivalent to finding a solution to $Cj = Ay + B$. We do this by creating two vector spaces, one spanned by vectors made of the coefficients of the q-expansions of $V_1 = \{j, x \cdot j, x^2 \cdot j, \ldots, x^n \cdot j\}$, and the other spanned by $V_2 = \{1, x, xy, x^2, x^2y, \ldots, x^n, x^ny\}$ for various values of n. Then we look at the intersection of these two vector spaces, increasing n until there is a one dimensional intersection and we can use this to find j as a rational combination of x and y.

In the end, we find that A is a polynomial of degree 63, B is a polynomial of degree 66, and C is a polynomial of degree 66. Their explicit formulas can be found in the appendix to this section.

3.6. Appendix.

Throughout this section we will be using the nonstandard notation $q = e^{\frac{2\pi i\tau}{11}}$.

The functions that give the singular model of $X_s^+(11)$.

$$\begin{aligned}
X &= \frac{1}{q^3} + \frac{1}{q} + 1 + 2q + 2q^2 + 5q^3 + O(q^4) \\
Y &= \frac{1}{q^4} + \frac{1}{q^3} + \frac{2}{q^2} + \frac{3}{q} + 6 + 7q + 10q^2 + 14q^3 + O(q^4) \\
Z &= \frac{1}{q^5} + \frac{1}{q^4} + \frac{3}{q^3} + \frac{4}{q^2} + \frac{8}{q} + 11 + 18q + 25q^2 + 38q^3 + O(q^4)
\end{aligned}$$

4. The Mordell-Weil Group of the Jacobian of $X_s^+(11)$

4.1. Introduction.

Given a curve C, one can construct an associated abelian variety J called its *jacobian*. As an abelian group, the jacobian is isomorphic to the Picard group of C. The Mordell-Weil theorem says that for any number field K, the K-rational points of the jacobian, $J(K)$, form a finitely generated abelian group. Therefore, it is non-canonically isomorphic to the product of a finite abelian group, $J(K)_{\text{tors}}$, and a free abelian group; i.e.,

$$J(K) \cong J(K)_{\text{tors}} \times \mathbb{Z}^r.$$

for some $r \in \mathbb{Z}_{\geq 0}$. In this case we say that $J(K)$ has rank r.

It turns out that computing $J(\mathbb{Q})_{\text{tors}}$ is not very difficult using the following theorem.

Theorem 4.1. [9, Theorem C.1.4] *Let A be an abelian variety defined over a number field K, let v be a finite place of K at which A has good reduction, let $\widetilde{K}$ be the residue field of v, and let p be the characteristic of $\widetilde{K}$. Then for any $m \geq 1$ with $p \nmid m$, the reduction map*

$$A(K)[m] \to A(\widetilde{K})$$

is injective, where $A(K)[m]$ denotes the m-torsion of $A(K)$. In other words, the reduction modulo v map is injective on the prime-to-p torsion subgroup of $A(K)$.

The basic idea for computing the rank of J is to try and compute the $\mathbb{F}_2$-dimension of the so-called weak Mordel-Weil group, $J(\mathbb{Q})/2J(\mathbb{Q})$. This is something that is easily done if one already knows the structure of $J(\mathbb{Q})$, but since we don't know the structure of this group we have to find another way to do this. We describe a method below, the 2-descent method, to bound the $\mathbb{F}_2$-dimension of $J(\mathbb{Q})/2J(\mathbb{Q})$ and therefore calculate a bound on the rank of $J(K)$. The method of 2-descent relies on the fact that we have the following short exact sequence of Galois modules

$$\begin{tikzcd} 0 \arrow[r] & J[2] \arrow[r] & J \arrow[r, "{[2]}"] & J \arrow[r] & 0 \end{tikzcd}$$

where $J[2]$ is the 2-torsion of J. Let $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ be the *2-Selmer group* as defined in [9]. This gives us the following short exact sequence.

$$\begin{tikzcd} 0 \arrow[r] & J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[r] & \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \arrow[r] & Ш(\mathbb{Q}, J)[2] \arrow[r] & 0 \end{tikzcd}$$

Using this sequence we can get a formula that involves the rank of $J(\mathbb{Q})$ and the $\mathbb{F}_2$-dimensions of the other groups that we defined.

$$\operatorname{rank} J(\mathbb{Q}) + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] + \dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2] = \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J). \tag{4.1}$$

Using equation (4.1), we get the following computable upper bound on the rank

$$\operatorname{rank} J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]. \tag{4.2}$$

In order to calculate this upper bound we must compute the dimension of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$. If it turns out that this bound is not sharp, which frequently happens, one would need to compute $Ш(\mathbb{Q}, J)[2]$. This is a very subtle task that lies outside of the scope of this paper. The interested reader should consult either [17] or [16] to read about computing $Ш(\mathbb{Q}, J)[2]$ or $Ш(\mathbb{Q}, J)$ in the case that X is elliptic or hyperelliptic.

4.2. **The Two-Descent Procedure.** The notation that we use in this section will follow that set out in [17]. Throughout the rest of this section we will focus on computing the dimension of the 2-Selmer group of the jacobian of a smooth projective curve, C, given by an affine equation of the form

$$C : y^2 = f(x),$$

where f is squarefree and $\deg(f) = 6$. In this case, our curve is hyperelliptic of genus $g = 2$ with two points at infinity in the projective closure. Before we can compute the dimension of the 2-Selmer group, we must define a few objects of interest and examine some of their properties.

Remark 4.2. Almost all of what we do here will go through for $\deg(f) \geq 6$ with $\deg(f)$ even. We simply limit ourselves to this case for the sake of making this section cleaner. In fact, [14] considered the more general case of an equation of the form $y^p = f(x)$ with p a prime dividing $\deg(f)$. This is actually more difficult than the case when p does not divide $\deg(f)$.

Definition 4.3. *For any field extension K of $\mathbb{Q}$, let $L_K = K[T]/(f(T))$ denote the algebra defined by f and N_K denote the norm map from L_K down to K.*

Remark 4.4. We can denote $L_K = K[\theta]$, where θ is the image of T under the reduction map $K[T] \to K[T]/(f(T))$, and L_K is a product of finite extensions of K:

$$L_K = L_{K,1} \times \cdots \times L_{K,m_K},$$

where m_K is the number of irreducible factors of $f(x)$ in $K[x]$. Here, the fields $L_{K,j}$ correspond to the irreducible factors of $f(x)$ in $K[x]$. Here $N_K : L_K \to K$ is just the product of the norms on each component. That is if $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_{m_K})$, then $N_K(\alpha) = \prod_{i=1}^{m_K} N_{L_{K,i}/K}(\alpha_i)$ where $N_{L_{K,i}/K} : L_{K,i} \to K$ is the typical field norm.

When $K = \mathbb{Q}$ we will drop the subscripts altogether and if $K = \mathbb{Q}_p$, we will just use the subscript p. This convention will apply to anything that has a field as a subscript throughout the paper, e.g., $L_p = \mathbb{Q}_p[T]/(f(T))$ and $L = \mathbb{Q}[T]/(f(T))$.

We will let $\mathcal{O}_K$, $I(K)$, and $\mathrm{Cl}(K)$ denote the ring of integers of K, the group of fractional ideals, and the ideal class group of K, respectively. We would like to define analogous objects for the algebra L_K, and we do so in the most natural way:

$$\begin{aligned}\mathcal{O}_{L_K} &= \mathcal{O}_{L_{K,1}} \times \cdots \times \mathcal{O}_{L_{K,m_K}},\\ I(L_K) &= I(L_{K,1}) \times \cdots \times I(L_{K,m_K}),\\ \mathrm{Cl}(L_K) &= \mathrm{Cl}(L_{K,1}) \times \cdots \times \mathrm{Cl}(L_{K,m_K}).\end{aligned}$$

Definition 4.5. *Let $I_p(L)$ denote the subgroup of $I(L)$ consisting of prime ideals in L with support above p a prime in $\mathbb{Q}$. For a finite set S of finite places, let*

$$I_S(L) = \prod_{p \in S \setminus \infty} I_p(L).$$

Definition 4.6. *For any field extension K of $\mathbb{Q}$, let*

$$H_K = \ker\left(N_K : L_K^\times/(L_K^\times)^2 K^\times \to K^\times/(K^\times)^2\right).$$

For any place, v, of $\mathbb{Q}$, we let $\mathrm{res}_v : H \to H_v$ be the map induced by the natural inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$.

Remark 4.7. Notice that the norm map is well defined on $L_K^\times/(L_K^\times)^2K^\times$. Since the $\deg(f)$ is even, the dimension of L_K/K is even and $N(x) = x^{\deg(f)}$ is a square in K for all $x \in K$.

Definition 4.8. *Let $\mathrm{Div}^\times(C)$ denote the group of degree-zero divisors on C with support disjoint from the principal divisor* $\mathrm{div}(y)$.

Theorem 4.9. [4, Chapter 11] *For every K we get a homomorphism*

$$F_K : \mathrm{Div}^\times(C)(K) \to L_K^\times, \quad \sum_P n_P P \mapsto \prod_P (x(P) - \theta)^{n_P},$$

which induces a homomorphism

$$\delta_K : J(K) \to H_K.$$

Definition 4.10. *Let*

$$\mathrm{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J) = \{\xi \in H : \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \textit{ for all places } v\}.$$

We will call this group the fake 2-Selmer group.

The link between the fake 2-Selmer and the 2-Selmer group will be explained in Corollary 4.23.

Remark 4.11. If we use this definition for $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$, in order to check if $\xi \in H$ is in $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ we have to check that $\mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v))$ for ALL places v. In order to make this definition more tractable, we will need the following definition and proposition.

Definition 4.12. *Let K be a finitely ramified algebraic extension of $\mathbb{Q}_p$ with maximal ideal $\mathfrak{p}_K$. We let $I_{\mathfrak{p}_K}(L_K)$ be the group of ideals in L_K and*

$$I_K = \ker\left(N : I_{\mathfrak{p}_K}(L_K)^2 / I_{\mathfrak{p}_K}(L_K) I_{\mathfrak{p}_K}(K) \to I_{\mathfrak{p}_K}(K)/I_{\mathfrak{p}_K}(K)^2\right).$$

For all primes p in $\mathbb{Q}$, let

$$I_p = \ker\left(N : I_p(L)/(I_p(L))^2 I_p(\mathbb{Q}) \to I_p(\mathbb{Q})/(I_p(\mathbb{Q}))^2\right).$$

We also have maps $\mathrm{val}_p : H_p \to I_p$. These maps, taken together, give us a map $\mathrm{val} : H \subset L^\times/(L^\times)^2 \to I(L)/(I(L))^2 I(\mathbb{Q})$. We denote $\widetilde{\mathrm{val}}$ the canonical map $L^\times/(L^\times)^2 \to I(L)/(I(L))^2$.

Remark 4.13. The notation I_p is not breaking with the subscript convention that we established at the beginning of this section since I_p is naturally isomorphic to

$$I_{\mathbb{Q}_p} = \ker\left(N : I_p(L_p)/I_p(L_p)^2 I_p(\mathbb{Q}) \to I_p(\mathbb{Q}_p)/I_p(\mathbb{Q}_p)^2\right).$$

Proposition 4.14. [17, Proposition 5.10] *If $p \notin S = \{\infty, 2\} \cup \{p : p^2 | \operatorname{disc}(f)\}$, then*

$$\begin{tikzcd} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \arrow[r, "\delta_p"] & H_p \arrow[r, "\mathrm{val}_p"] & I_p \arrow[r] & 0 \end{tikzcd}$$

is exact.

Proposition 4.15. *If $S = \{\infty, 2\} \cup \{p : p^2 | \operatorname{disc}(f)\}$*

$$\begin{aligned} \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \{\xi \in H : & \mathrm{val}(\xi) \in I_S(L)/I_S(L)^2 I(\mathbb{Q}), \\ & \textit{and } \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \textit{ for } v \in S\}. \end{aligned}$$

Proof: Since

$$\begin{tikzcd} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \arrow[r, "\delta_p"] & H_p \arrow[r, "\mathrm{val}_p"] & I_p \arrow[r] & 0 \end{tikzcd}$$

is exact for $p \notin S$, we know that $\mathrm{res}_p(\xi) \in \delta_p(J(\mathbb{Q}_p))$ if and only if $\mathrm{val}_p(\mathrm{res}_p(\xi))$ is the trivial class for $p \notin S$. Each $\xi \in L^\times/(L^\times)^2\mathbb{Q}^\times$ has a squarefree representative β in $\mathcal{O}_L$. Fix $\xi = [\beta] \in H \subseteq L^\times/(L^\times)^2\mathbb{Q}^\times$ with β normalized to be a squarefree element of $\mathcal{O}_L$. Using the fact that for $\xi = [\beta] \in H$, $\mathrm{res}_p(\xi) \in \delta_p$ if and only if $[(\beta)] = [(1)] \in I_p$. Using this we can rewrite Definition 4.10 as

$$\begin{aligned} \mathrm{Sel}^{(2)}_{\mathrm{fake}} &= \{\xi \in H : \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all places } v\} \\ &= \{\xi \in H : \mathrm{val}_p(\mathrm{res}_v(\xi)) = [(1)] \text{ for } p \notin S, \text{ and } \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for } v \in S\} \\ &= \{\xi \in H : \mathrm{val}(\xi) \in I_S(L)/I_S(L)^2 I_S(\mathbb{Q}), \text{ and } \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for } v \in S\}. \end{aligned}$$

■

Before exploring the relationship between $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ and $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$, we need to figure out when the kernel of δ is exactly $2J(\mathbb{Q})$.

Definition 4.16. *We say that K satisfies condition (‡), if either of the following occurs:*

(‡.a) *$f(x)$ has a factor of odd degree in $K[x]$, or*
(‡.b) *f factors as $h\bar{h}$ over a quadratic extension K' of K, where $\bar{h}$ is the* $\mathrm{Gal}(K'/K)$*-conjugate of h.*

Remark 4.17. Condition (‡.b) is equivalent to L_K containing a quadratic extension of K.

Lemma 4.18. [14, Theorem 11.2] *The kernel of δ_K is $2J(K)$ if K satisfies condition (‡), or if there is no K-rational divisor class of degree 1 on C. Otherwise, $2J(K)$ has index two in* $\ker(\delta_K)$*.*

Lemma 4.19. [17, Lemma 5.2] *Condition (‡) is satisfied in each of the following situations.*

(1) *$K = \mathbb{R}$.*
(2) *K is a p-adic field, and the irreducible factors of f in $K[x]$ all define unramified extensions of K.*

Lemma 4.20. [17, Lemma 5.3] *Write $f(x) = \prod_{j=1}^{6}(x - \alpha_j)$, and let*

$$h(f) = \prod_{\sigma}(x - (\alpha_{\sigma(1)}\alpha_{\sigma(2)}\alpha_{\sigma(3)} + \alpha_{\sigma(4)}\alpha_{\sigma(5)}\alpha_{\sigma(6)})),$$

where the product is over left coset representative $\sigma \in S_6$ modulo the stabilizer of the partition $\{\{1,2,3\},\{4,5,6\}\}$. Then $h(f)$ has degree 10.

(1) *For $a \in K$, (‡.b) holds for f if and only if it holds for $f(x+a)$.*
(2) *If $h(f)$ has a simple root in K, then K satisfies (‡.b).*
(3) *If $h(f)$ has no root in K, then K does not satisfy (‡.b).*
(4) *There are at most 45 values of $a \in K$ such that $h(f(x+a))$ is not squarefree.*

Now, we answer the question about the relationship between $\mathrm{Sel}^{(2)}(K,J)$ and $\mathrm{Sel}^{(2)}_{\text{fake}}(K,J)$ with the following theorem.

Theorem 4.21. [14, Theorem 13.2] *There is an exact sequence*

$$\mu_2(K) \xrightarrow{\phi} \mathrm{Sel}^{(2)}(K,J) \xrightarrow{\epsilon} \mathrm{Sel}^{(2)}_{\text{fake}}(K,J) \longrightarrow 0.$$

Moreover, the image of ϕ is trivial in $\mathrm{Sel}^{(2)}(K,J)$ if and only if K satisfies (‡).

Remark 4.22. Here the map ϵ is a map that is closely related to a generalization of the Weil pairing defined on $J[2]\times J[2]$. The map ϕ is the connecting homomorphism on the Galois cohomology groups induced from the short exact sequence

$$0 \longrightarrow J[2] \xrightarrow{\epsilon} \mu_2(L_{\overline{K}})/\mu_2(\overline{K}) \xrightarrow{\text{Norm}} \mu_2(\overline{K}) \longrightarrow 0.$$

We use ϕ here only because δ has already been defined. We think of $\mu_2(\overline{K})$ living inside of $\mu_2(L_{\overline{K}})$ diagonally.

Corollary 4.23. *The relationship between the dimensions of $\mathrm{Sel}^{(2)}_{\text{fake}}(K,J)$ and $\mathrm{Sel}^{(2)}(K,J)$ is as follows:*

$$\dim_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(K,J) = \begin{cases} \dim_{\mathbb{F}_2}\mathrm{Sel}^{(2)}_{\text{fake}}(K,J) & \text{if } K \text{ satisfies (‡)},\\ \dim_{\mathbb{F}_2}\mathrm{Sel}^{(2)}_{\text{fake}}(K,J)+1 & \text{otherwise.}\end{cases}$$

Now that we have the relationship between $\dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ and $\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, we need to compute $\dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$. To make this possible we need to be able to compute the image of δ_K for various K. To do this, we will use a theorem that tells us what the images of some specific divisors are.

Theorem 4.24. [14] *Let K be a field extension of $\mathbb{Q}$.*

1. *Suppose that the points $\infty_\pm$ at infinity on C are K-rational. Then for a point $P \in C(K)$ not in the support of $\mathrm{div}(y)$, we have $\delta_K(P - \infty_\pm) = x(P) - \theta \bmod (L_K^\times)^2 K^\times$.*
2. *To every monic polynomial $h \in K[x]$ of even degree such that h divides f, we can associate an element $P_h \in J(K)[2]$ such that:*
   (a) *The P_h generate $J(K)[2]$ and satisfy $\sum_j P_j = 0$, if $\prod_j h_j = f$.*
   (b) *Let $\widetilde{h}$ be the polynomial such that $f = h\widetilde{h}$. Then $\delta_K(P_h) = h(\theta) - \widetilde{h}(\theta) \bmod (L_K^\times)^2 K^\times$.*
3. *$\dim J(K)[2] = m_K - 1$, if all irreducible factors of f over K have even degree, and $\dim J(K)[2] = m_K - 2$ otherwise.*

Now that we know what the images of these divisors are, we want to compute the dimensions of these $\mathbb{F}_2$-vector spaces. This way, we can compute the images of "enough" divisors until we have a basis. To make things a little easier we define the following quantities:

Definition 4.25. *For any field extension K of $\mathbb{Q}$, let:*

- *$t_K = 0$ if all the factors of f in $K[x]$ have even degree, and $t_K = 1$ otherwise,*
- *$u_K = 0$ if there is a quadratic extension of K contained in L_K, and $u_K = 1$ otherwise.*

For a p-adic field K, let:

- *Let $r_K = 0$ if all ramification indices of the field extensions $L_{K,j}/K$ are even, and $r_K = 1$ otherwise,*
- *Let $s_K = 0$ if all the residue class degrees of the field extensions $L_{K,j}/K$ are even and $s_k = 1$ otherwise,*
- *Let $d_K = [K : \mathbb{Q}_2]$ if $p = 2$ and $d_K = 0$ if p is odd.*

With these definitions we can now compute the dimensions of most of the local groups we are interested in.

Lemma 4.26. [17, Lemma 5.7] *Let K be a p-adic field. Then*

1. *$\dim J(K)/2J(K) = \dim J(K)[2] + d_K g = m_K - 1 - t_K + d_K \cdot g$.*
2. *$\dim I_K = m_K - r_K - s_K$.*
3. *$\dim H_K = 2 \dim I_K$ if p is odd.*
4. *If p is odd and $r_K = 1$, then $\mathrm{val}_p : H_p \to I_p$ is onto.*

The last thing we need is to compute the dimensions of some of these same spaces over $\mathbb{R}$.

Lemma 4.27. [17, Lemma 4.8]

1. *$\dim J(\mathbb{R})/2J(\mathbb{R}) = \dim \delta_\infty(J(\mathbb{R})) = \dim J(\mathbb{R})[2] - g$.*
2. *$\delta_\infty(J(\mathbb{R}))$ is generated by $\delta_\infty(P + Q - \infty_+ - \infty_-)$ with $P, Q \in C(\mathbb{R})$, and $\delta_\infty(P + Q - \infty_+ - \infty_-)$ only depends on the connected components of $C(\mathbb{R})$ contacting P and Q. Here $\infty_\pm$ are the two points at infinity on C.*

We have now translated the question of finding the dimension of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ to finding the dimension of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$, a finite subspace of $L^\times/(L^\times)^2\mathbb{Q}$. In order to compute $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ as a finite subspace of $L^\times/(L^\times)^2\mathbb{Q}^\times$, we consider the following diagram. We want to define Ker, Sel_1, and Sel_2 so that the top and bottom row of the diagram become exact.

(4.3)

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Ker} \arrow[r] \arrow[d, equal] & \mathrm{Sel}_2 \arrow[r] \arrow[d] & \mathrm{Sel}_1 \arrow[r] \arrow[d] & \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{Ker} \arrow[r] & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \arrow[r] & L^\times/(L^\times)^2 \arrow[r] & L^\times/(L^\times)^2\mathbb{Q}^\times \arrow[r] & 1
\end{tikzcd}$$

In order for the bottom row to be exact, clearly we need

$$\mathrm{Ker} = \{d \in \mathbb{Q} : \sqrt{d} \in L^\times\}.$$

So now we need to find finite subgroups, Sel_1 and Sel_2, of $L^\times/(L^\times)^2$ and $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, respectively, that makes the top row of the diagram exact.

To determine exactly what Sel_1 and Sel_2 are, we need the following proposition:

Proposition 4.28. [17, Lemma 4.9] *Let G_p be the image of $J(\mathbb{Q}_p)$ in I_p (i.e. $G_p = \mathrm{val}_p \circ \delta_p(J(\mathbb{Q}_p))$). Recall that $r_p = 0$ if and only if all the fields $L_{p,j}$ have even ramification index. Let Sel_2 be the span in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ of $\{-1\} \cup S'$, where*

$$S' = \{p : \ r_p = 0 \textit{ or } G_p \neq \{1\}\}.$$

Define

$$\begin{aligned}\widetilde{H} = \{\xi \in L^\times/(L^\times)^2 : \widetilde{\mathrm{val}}(\xi) \in I_{S'}(L)/I_{S'}(L)^2 \textit{ and} \\ \mathrm{val}_p(\xi) \in G_p \textit{ for all } p \in S'\}\end{aligned}$$

where $\widetilde{\mathrm{val}_v}$ is the canonical map from $L^\times/(L^\times)^2$ to $I(L)/I(L)^2$. Then $\widetilde{H}$ is finite. Let $S = S' \cup \{\infty, 2\}$ and set

$$\mathrm{Sel}_1 = \{\xi \in \widetilde{H} : \ \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \textit{ for all } v \in S\}.$$

Then with these definitions of Sel_1 and Sel_2, the top row of diagram (4.3) is exact.

With all of this, we finally have enough information to compute $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ and $\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ for a specific $f(x)$.

4.3. Explicit Computations.

Now that we have laid the foundation we are ready to perform a 2-descent. The curve we will be working with is given by the affine equation

$$C : y^2 = f(x) = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1.$$

In the projective closure, this curve has two points at infinity, call them $\infty_\pm$. Using SAGE, we compute $\mathrm{disc}(f) = -1 \cdot 2^{20} \cdot 11^3$ and that $f(x)$ is irreducible over $\mathbb{Q}$. We let $S = \{p : p^2 | \mathrm{disc}(f)\} \cup \{2, \infty\} = \{\infty, 2, 11\}$ and compute all of the basic information about the local groups associated to these places.

Using SAGE we can factor $f(x)$ over $\mathbb{Q}_p[x]$ to get the following table:

p	m_p	t_p	u_p	r_p	s_p	d_p
2	1	0	0	0	1	1
11	2	0	0	1	1	0
∞	3	–	–	–	–	–

From the information above and Lemmas 4.26 and 4.27 we have the following:

p	$\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$	$\dim \delta_p(J(\mathbb{Q}_p))$	$\dim H_p$	$\dim I_p$
2	2	2	?	0
11	1	0	0	0
∞	0	0	–	–

Remark 4.29. Lemma 4.26 doesn't give us a formula for $\dim H_2$. We could compute it directly, but we will postpone its computation for now as we will need to compute all of H_2 later in the paper.

Next we use SAGE to compute $h(f)$ as in Lemma 4.20 in our case and we get

$$h(f) = x^{10} - 7x^9 + 76x^8 - 696x^7 + 2800x^6 - 3328x^5 - 4464x^4 + 8256x^3 + 3712x^2 - 1280x - 512.$$

Reducing $h(f)$ mod 17 we get

$$x^{10} + 10x^9 + 8x^8 + x^7 + 12x^6 + 4x^5 + 7x^4 + 11x^3 + 6x^2 + 12x + 15,$$

which is irreducible in $\mathbb{F}_{17}$. Thus we know that $h(f)$ is irreducible in $\mathbb{Q}[x]$ and so Lemma 4.20 tells us that in our case $\mathbb{Q}$ does not satisfy (‡). So, by Corollary 4.23, we have that

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) + 1,$$

and we now turn our attention to determining the dimension of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$.

The first step to computing the dimension of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ is to find the subgroups Sel_1 and Sel_2 from Proposition 4.28. To do this we start by computing $\widetilde{H}$. Recall that

$$\widetilde{H} = \{\xi \in L^\times/(L^\times)^2 : \widetilde{\mathrm{val}}(\xi) \in I_{S'}(L)/I_{S'}(L)^2 \text{ and } \mathrm{val}_p(\xi) \in G_p \text{ for all } p \in S'\}$$

where $S' = \{p : r_p = 0 \text{ or } G_p \neq \{1\}\}$. In this case we can see that we have that $S' = \{2\}$. Using SAGE, we find that the class number of L is one and that the prime factorization of the ideal $2\mathcal{O}_L = \mathfrak{p}_2^6 = (\beta_2)^6$.

This means that $I_{S'}/I_{S'}(L)^2 = \{[(1)], [(\beta_2)]\}$, and so ξ is in $\widetilde{H}$ only if it is equivalent modulo $(L^\times)^2$ to either a unit, or a unit multiple of β_2. Since G_2 is a subset of I_2, we only need to check if $\mathrm{val}_2(\beta_2)$ is in G_2. The table above gives us that $G_2 = \{[(1)]\}$ since it is a subgroup of $I_2 = \{[(1)]\}$. Therefore, we know that $\mathrm{val}_2(\beta_2)$ is not in G_2, since $[(\beta_2)] \neq [(1)]$. Hence the only classes modulo squares in $\widetilde{H}$ correspond to ones that are represented by units.

To find representatives of these classes we simply compute the fundamental units of L. Using SAGE, we find that $r_1 = 0$ and $r_2 = 3$ and so by Dirchlet's unit theorem we know that there are $r_1 + r_2 - 1 = 2$ fundamental units. Again using SAGE, one can check that the only roots of unity in L are ± 1. Therefore,

$$\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 = \langle -1, u_1, u_2 \rangle$$

where

$$u_1 = \frac{53}{6455}\theta^5 - \frac{1334}{6455}\theta^4 + \frac{1729}{1291}\theta^3 + \frac{70491}{6455}\theta^2 + \frac{92264}{6455}\theta + \frac{4485}{1291},$$
$$u_2 = \frac{843}{71005}\theta^5 - \frac{21072}{71005}\theta^4 + \frac{132243}{71005}\theta^3 + \frac{238525}{14201}\theta^2 + \frac{1200429}{71005}\theta + \frac{235233}{71005}.$$

Recall that θ is the image of T under the map $K[T] \to K[T]/(f(T))$.

Before moving on we notice that with u_1 and u_2 defined as above, $2 = -u_1u_2\beta_2^6$ and so $2 \equiv -u_1u_2 \bmod (L^\times)^2$. Thus, $\widetilde{H} = \langle -1, u_1, u_2\rangle = \langle -1, 2, u_1\rangle$. Here we are suppressing the equivalence class notation to make things cleaner. From the work we did in the last section and to compute the tables at the beginning of the section, we know that $\mathrm{Sel}_2 = \langle -1, 2\rangle$ and since L does not satisfy (‡) we know that $\mathrm{Ker} = \{1\}$. But using the fact that

$$\begin{tikzcd}
1 \arrow[r] & \langle -1, 2\rangle \arrow[r] \arrow[dd, hook] & \mathrm{Sel}_1 \arrow[r] \arrow[d, hook] & \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) \arrow[r] \arrow[dd, hook] & 1 \\
 & & \langle -1, 2, u_1\rangle \arrow[d, hook] & & \\
1 \arrow[r] & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \arrow[r] & L^\times/(L^\times)^2 \arrow[r] & L^\times/(L^\times)^2\mathbb{Q}^\times \arrow[r] & 1
\end{tikzcd}$$

has exact rows, we know that $\mathrm{Sel}_1 \supseteq \langle -1, 2\rangle$. So the question becomes, is u_1 in Sel_1? From Proposition 4.28, this question amounts to checking if $\mathrm{res}_v(u_1) \in \delta_v(J(\mathbb{Q}_v))$ for all $v \in S$, where $S = \{2, 11, \infty\}$. We start by checking if $\mathrm{res}_2(u_1)$ is in $\delta_2(J(\mathbb{Q}_2))$ and hope that, in fact, $\mathrm{res}_2(u_1) \notin \delta_2(J(\mathbb{Q}_2))$, and therefore we are done.

In order to do this, we need to find explicit generators for $\delta_2(J(\mathbb{Q}_2))$. From the table above we know that $\dim \delta_2(J(\mathbb{Q}_2)) = 2$, so we just start looking for points $P \in C(\mathbb{Q}_2)$ and using Theorem 4.24 to compute the images of $P - \infty_+$ under δ_2.

Lemma 4.30. *For $f(x) = x^5 - 6x^5 + 11x^4 - 8x^8 + 11x^2 - 6x + 1$, the field $\mathbb{Q}_2$ does not satisfy (‡).*

Proof: To prove this we just need to show that

$$h(f) = x^{10} + 10x^9 + 8x^8 + x^7 + 12x^6 + 4x^5 + 7x^4 + 11x^3 + 6x^2 + 12x + 15,$$

does not have a simple root in $\mathbb{Q}_2$. First, notice that since $h(f)$ is a monic polynomial, if it has a root in $\mathbb{Q}_2$, that root has to be in $\mathbb{Z}_2$. Next, if $h(f)$ has a root in $\mathbb{Z}_2$, then of course that root will reduce to a root in $\mathbb{F}_2$. So to show that $h(f)$ doesn't have a root in $\mathbb{Q}_2$ it is sufficient to show that the reduction of $h(f)$ modulo 2 doesn't have a root in $\mathbb{F}_2$. The reduction of $h(f)$ modulo 2 is

$$\overline{h(f)} = x^{10} + x^7 + x^4 + x^3 + 1.$$

Clearly zero isn't a root of $\overline{h(f)}$, and a quick check shows that one isn't a root of $\overline{h(f)}$ as well. Therefore since $\overline{h(f)}$ doesn't have a root in $\mathbb{F}_2$, we know that $h(f)$ doesn't have a root in $\mathbb{Q}_2$. ■

Lemma 4.31. *Two elements, a and b, in $L_2^\times$ are congruent modulo $(L_2^\times)^2\mathbb{Q}_2^\times$ if and only if there is an $r \in \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm1, \pm2, \pm5, \pm10\}$ such that $\frac{a}{br}$ is a square in $L_2^\times$.*

Proof: From Lemma 4.30 we know that L_2 does not contain a quadratic extension of $\mathbb{Q}_2$ and so we have the following exact sequence:

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \arrow[r, "\psi"] & L_2^\times/(L_2^\times)^2 \arrow[r, "\phi"] & L_2^\times/(L_2^\times)^2\mathbb{Q}_2^\times \arrow[r] & 1. \end{tikzcd}$$

Therefore, $a \equiv b \bmod (L_2^\times)^2\mathbb{Q}_2^\times \Leftrightarrow \frac{a}{b} \equiv 1 \bmod (L_2^\times)^2\mathbb{Q}_2^\times$ if and only if $\frac{a}{b}$ is in the kernel of ϕ. Since we know that the kernel of ϕ is $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm 1, \pm 2, \pm 5, \pm 10\}$, if we want to check if $a \equiv b \bmod (L_2^\times)^2\mathbb{Q}_2^\times$, it is sufficient to check if $\frac{a}{b} \equiv r \bmod (L^\times)^2$ for all representatives r of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{\pm 1, \pm 2, \pm 5, \pm 10\}$. Another way to say this is that $a \equiv b \ (L_2^\times)^2\mathbb{Q}_2^\times$ if and only if there is an $r \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ such that $\frac{a}{rb}$ is a square in $L_2^\times$. ■

Lemma 4.31 gives us an easy way to check if two elements are congruent modulo $(L_2^\times)^2\mathbb{Q}_2$ since Magma has a built in command that checks if an element of a field is a square or not, so we can check these equivalencies in Magma quite easily.

First, using Hensel's lemma, we can find that $P_1 = (2, 72512802334441 + O(2^{49}))$ is a point on $C(\mathbb{Q}_2)$ and from Theorem 4.24, we know that $\delta_2(P_1 - \infty_+) = 2 - \theta$. Using Lemma 4.31 we can check that $2 - \theta \not\equiv 1 \bmod (L_2^\times)^2\mathbb{Q}_2^\times$. Therefore, we only need to find one more non-trivial element in $\delta_2(J(\mathbb{Q}_2))$ that is not equivalent to $2 - \theta \bmod (L_2^\times)^2\mathbb{Q}_2$. Next, we search for points on $C(\mathbb{Q}_2)$ using Magma and find that $P_2 = (151123620125253 \cdot 2 + O(2^{50}), 1)$ is also a point on $C(\mathbb{Q}_2)$ and $\delta_2(P_2 - \infty_+) = \alpha - \theta$ where $\alpha = 151123620125253 \cdot 2 + O(2^{50})$. We just need to know if $2 - \theta \equiv \alpha - \theta \bmod (L_2^\times)^2\mathbb{Q}_2^\times$. Again using Lemma 4.31, we check this in Magma.

Remark 4.32. Here we note that $\text{div}(y) = \sum_{i=1}^{6}(0, \alpha_i)$ where the α_i's are the roots of $f(x)$. Therefore none of the points we found are in the support of $\text{div}(y)$.

Fortunately, it turns out that $2 - \theta \not\equiv \alpha - \theta \bmod (L_2^\times)^2\mathbb{Q}_2$. Thus we have two independent elements in a 2-dimensional $\mathbb{F}_2$-vector space and so we have generators for $\delta_2(J(\mathbb{Q}_2))$. One can directly check in Magma, using the same method as in Lemma 4.31, if $\text{res}_2(u_1)$ is in $\delta_2(J(\mathbb{Q}_2))$. A few calculations later we see that

$$\begin{aligned} \text{res}_2(u_1) &\not\equiv 2 - \theta \bmod L^\times/(L^\times)^2\mathbb{Q} \\ \text{res}_2(u_1) &\not\equiv \alpha - \theta \bmod L^\times/(L^\times)^2\mathbb{Q} \\ \text{res}_2(u_1) &\not\equiv (2 - \theta)(\alpha - \theta) \bmod L^\times/(L^\times)^2\mathbb{Q}. \end{aligned}$$

Again, the details of this computation can be found in the appendix to this section.

Thus we have that $u_1 \notin \text{Sel}_1$ and $\text{Sel}_1 = \langle -1, 2\rangle$. Using the top row in diagram 4.3 we know that $\text{Sel}_1 = \text{Sel}_2 = \langle -1, 2\rangle$ and $\text{Sel}^{(2)}_{\text{fake}}(\mathbb{Q}, J) = \{1\}$. Combining this with proposition 4.23 and equation (5.3) we get that the rank of $J(\mathbb{Q})$ is less than or equal to one.

In fact, using Magma, one can show that the divisor class of $\infty_+ - \infty_-$ is of infinity order. Further we can show that

$$J(X_s^+(11))(\mathbb{Q}) = \langle [(0, -1) - \infty_-], [\infty_+ - \infty_-]\rangle \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}.$$

5. Applying the Method of Chabauty and Coleman

5.1. **Introduction to the method.**

Theorem 5.1 (Faltings' Theorem)**.** *Let K be a number field and let C/K be a nonsingular curve defined over K of genus $g \geq 2$. Then the set of K-rational points on C is finite.*

Faltings' theorem tells us that there can only be finitely many rational points on a curve of genus greater than or equal to 2, but it does not give us any way to show that a set of points on a curve is complete. In 1941, Claude Chabauty proved the following weaker version of Faltings' theorem:

Theorem 5.2 (Chabauty's Theorem [5])**.** *Let X be a curve of genus $g \geq 2$ over $\mathbb{Q}$. Let J be the jacobian of X. Let p be a prime, and let $r' = \dim_{\mathbb{Q}_p} \overline{J(\mathbb{Q})}$ where $\overline{J(\mathbb{Q})}$ is the closure of $J(\mathbb{Q})$ with the p-adic topology. Suppose $r' < g$. Then $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite.*

Corollary 5.3. *If X is as in Chabauty's theorem, then $X(\mathbb{Q})$ is finite.*

The corollary follows because $X(\mathbb{Q})$ is inside of $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ and thus it must be finite as well.

Clearly, Chabauty's theorem is weaker than Faltings' as it requires the assumption that $r' < g$, which is not always true.

As they are stated, neither Faltings' theorem nor Chabauty's theorem is effective. In 1985 Robert Coleman was able to apply the theory of Newton polygons to Chabauty's theorem to come up with a method for finding an explicit bound on the size of $X(\mathbb{Q})$ in the case when r' is less then the genus of X.

Theorem 5.4 (Coleman's Theorem [8])**.** *Let X, J, p, r' be as in Theorem 5.2. Suppose that p is a prime of good reduction for X.*

a) *Let ω be a non-zero 1-form in $H^0(X_{\mathbb{Q}_p}, \Omega^1)$ satisfying conditions 1-3. We scale ω by an element of $\mathbb{Q}_p^\times$ so that it reduces to a nonzero 1-form $\widetilde{\omega} \in H^0(X_{\mathbb{F}_p}, \Omega^1)$. Let $m = \operatorname{ord}_{\widetilde{Q}} \widetilde{\omega}$. If $m < p-2$, then the number of points in $X(\mathbb{Q})$ reducing to $\widetilde{Q}$ is at most $m+1$.*

b) *If $p > 2g$, then*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g-2).$$

To apply Coleman's method and get an upper bound on the number of points on $X_s^+(\mathbb{Q})$, we will use the fact that the rank of the jacobian of $X_s^+(11)$ is one, which is less than its genus which is two in this case. It will turn out that the simplest bound obtained from Coleman's method is not sharp, but utilizing some extra structure of $X_s^+(11)$, we will be able to show that the only points on $X_s^+(11)$ are the ones found by a naive search. That is to say that

$$X_s^+(11)(\mathbb{Q}) = \{(0, \pm 1), (1, \pm 2), \infty_\pm\}. \tag{5.1}$$

5.2. **Applying Coleman's Theorem.** We now return to the question of computing all of the points on the genus 2 modular curve

$$X_s^+(11) : y^2 = f(x) = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1. \tag{5.2}$$

We know that this curve has two points at infinity, call them ∞_- and ∞_+, and a naive search yielded four other points, $(1, \pm 2)$, and $(0, \pm 1)$. Now, we have seen that the group of rational points on the jacobian of $X_s^+(11)$ has rank 1. Thus we can apply Theorem 5.4 to get that

$$\#X_s^+(11)(\mathbb{Q}) \leq \#X_s^+(11)(\mathbb{F}_5) + (2 \cdot 2 - 2) = 6 + 2 = 8. \tag{5.3}$$

Unfortunately this bound does not line up with the number of points that we found, there could still be two other points that we are missing. From the moduli interpretation, one expects that the six points in (5.1) are in fact, the *only* ones on $X_s^+(11)(\mathbb{Q})$, but how do we show that these are the only points?

One could try studying the η_J corresponding to the holomorphic 1-form we used in Theorem 5.4, but this turns out to be quite difficult in this case because all six of the points that we found are in unique residue classes for all odd p. Thus, computing the power series of ω in local coordinates is not a straightforward task since we cannot take our open set to be the kernel of the reduction map $J(\mathbb{Q}_p) \to J(\mathbb{F}_p)$.

Instead, we aim to exploit the symmetry of $f(x)$. Looking at the affine model of $X_s^+(11)$ given in (5.2), it becomes clear that there is a $\psi \in \operatorname{Aut}(X_s^+(11))$, given by $\psi((x,y)) = \left(\frac{1}{x}, \frac{y}{x^3}\right)$. Upon further inspection, the set

$$S = \{\infty_\pm, (0, \pm 1), (1, \pm 2)\}$$

is stable under ψ. In fact, S is also stable under the standard hyperelliptic "conjugation" automorphism that maps (x, y) to $(x, -y)$.

With this in mind, we can finally prove the following theorem:

Theorem 5.5. *The set of $\mathbb{Q}$-rational points on $X_s^+(11)$ is $S = \{\infty_\pm, (0, \pm 1), (1, \pm 2)\}$.*

Proof: The set S is stable under the automorphisms ψ and σ, so if P is a $\mathbb{Q}$-rational point not in S, the points P, $\sigma(P)$, $\psi(P)$, and $\sigma(\psi(P))$ are all not in S.

Next we notice that the only points that are fixed by either ψ or σ have either x-coordinate 0 or 1, or y-coordinate 0, but these points are already in S. Thus the points P, $\sigma(P)$, $\psi(P)$, and $\sigma(\psi(P))$ are actually distinct.

Therefore, if there is one $\mathbb{Q}$-rational point on $X_s^+(11)$ that is not in S then there must actually be four such points. But this would mean that there are at least ten points in $X_s^+(11)(\mathbb{Q})$, contradicting the upper bound of eight that we found in equation (5.3).

■

We know that $X_s^+(11)$ has one rational cusp and one can check using SAGE that there are 5 $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves with complex multiplication and split representation at 11.

Corollary 5.6. *The only elliptic curves whose Galois representation at 11 with image contained in the normalizer of a split Cartan subgroup have complex multiplication. Their j-invariants are* -3375, 16581375, 8000, -884736, -884736000.

Proof: Plugging the points in S into the j-map from Section 3.5 we get the following table.

P	$(0,1)$	$(0,-1)$	$(1,2)$	$(1,-2)$	∞_+	∞_-
$j(P)$	8000	cusp	-3375	16581375	-884736	-88473600

■

References

[1] Tom M. Apostol, *Modular functions and dirichlet series in number theory*, Second, Springer, 1990. ↑7

[2] Yuri Bilu and Pierre Parent, *Serre's uniformity problem in the split cartan case*, Annals of Mathematics **173** (2011), 569–584. ↑4

[3] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. MR3137477 ↑4

[4] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1996. ↑18

[5] Claude Chabauty, *Sur les points rationnels des courbes algebriques de genre superieur a lunite*, C. R. Acad. Sci. **212** (1941), no. 882-885. ↑26

[6] I. Chen and C. Cummins, *Elliptic curves with nonsplit mod 11 representations*, Mathematics of Computation **73** (2004), 869–880. ↑8

[7] Imin Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 1–38. MR1625491 (99m:11068) ↑11

[8] Robert Coleman, *Effective Chabauty*, Duke Math Journal **54** (1985), no. 3, 765–770. ↑26

[9] Marc Hindry and Joseph H. Silverman, *Diophantine geometry: An introduction*, Springer, 2000. ↑16, 17

[10] Daniel S Kubert and Serge Lang, *Modular units*, Springer-Verlag, New York Springer, 1981. ↑5, 6, 7, 8, 10

[11] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Inventiones Mathematicae **44** (1978), no. 2, 129–162. ↑4

[12] Fumiyuki Momose, *Rational points on the modular curves $X_{split}(p)$*, Compositio Mathematica **52** (1984), 115–137. ↑4

[13] Pierre Parent, *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$*, Compositio Mathematica **141** (2005), 561–572. ↑4

[14] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. (1997), 141–188. ↑17, 20, 21

[15] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae **15** (1972), 259–331. ↑4

[16] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed. Springer, 2009. ↑17

[17] Michael Stoll, *Implementing 2-descents for Jacobians of hyperelliptic curves.* Acta Arith. **98** (2001), 245–277. ↑17, 19, 20, 21, 22

ALBANIAN JOURNAL OF MATHEMATICS
Volume 9, Number 1, Pages 31–61
ISSN: 1930-1235; (**2015**)

QUASI-PLATONIC $PSL_2(q)$-ACTIONS ON CLOSED RIEMANN SURFACES

S. Allen Broughton
Department of Mathematics
Rose-Hulman Institute of Technology
5500 Wabash Ave.
Terre Haute, IN 47803 USA
Email: brought@rose-hulman.edu

Abstract. This paper is the first of two papers whose combined goal is to explore the dessins d'enfant and symmetries of quasi-platonic actions of $PSL_2(q)$. A quasi-platonic action of a group G on a closed Riemann S surface is a conformal action for which S/G is a sphere and $S \to S/G$ is branched over $\{0, 1, \infty\}$. The unit interval in S/G may be lifted to a dessin d'enfant $\mathcal{D}$, an embedded bipartite graph in S. The dessin forms the edges and vertices of a tiling on S by dihedrally symmetric polygons, generalizing the idea of a platonic solid. Each automorphism ψ in the absolute Galois group determines a transform S^ψ by transforming the coefficients of the defining equations of S. The transform defines a possibly new quasi-platonic action and a transformed dessin $\mathcal{D}^\psi$.

Here, in this paper, we describe the quasi-platonic actions of $PSL_2(q)$ and the action of the absolute Galois group on $PSL_2(q)$ actions. The second paper discusses the quasi-platonic actions constructed from symmetries (reflections) and the resulting triangular tiling that refines the dessin d'enfant. In particular, the number of ovals and the separation properties of the mirrors of a symmetry are determined.

1. Introduction

Let S be a closed Riemann surface, of genus $\sigma \geq 2$; we denote the group of conformal automorphisms by $\mathrm{Aut}(S)$. We say that a group G acts conformally on S, if there is a monomorphism

$$\epsilon : G \hookrightarrow \mathrm{Aut}(S). \tag{1}$$

A *symmetry* or *reflection* of S is an anti-conformal, involutary automorphism of the surface. The symmetries of S are contained in $\mathrm{Aut}^*(S)$, the group of isometries of S, both conformal and anti-conformal. A surface with a symmetry is called a *symmetric surface* and has a defining equation with real coefficients. A conformal G-action is *symmetric* if there is a symmetry ϕ of S normalizing $\epsilon(G)$. In this case

2010 *Mathematics Subject Classification.* Primary 17B20; Secondary 20H15, 51F15.
Key words and phrases. Riemann surface, quasi-platonic surface, automorphism group, symmetries.

the action extends to a reflection group $\epsilon : G^* \hookrightarrow \mathrm{Aut}^*(S)$. A subtlety is that G may not act symmetrically even though S is symmetric. This may happen if $\epsilon(G)$ is not normal in $\mathrm{Aut}(S)$; see [16] for a discussion.

Quasi-platonic surfaces, dessins, and symmetries. Quasi-platonic G-actions extend the notion of automorphism groups of platonic solids. A G-action is called *quasi-platonic* (or *triangular* see Section 2) if the quotient S/G is a sphere $\mathbb{S}^2 = \widehat{\mathbb{C}} = P^1(\mathbb{C})$ and the quotient map $\pi_G : S \to S/G$ is branched over three points. A surface is called quasi-platonic if the (natural) action of $\mathrm{Aut}(S)$ is quasi-platonic. It turns out that if the natural action of $G \leq \mathrm{Aut}(S)$ is quasi-platonic then all intermediate groups H, $G \leq H \leq \mathrm{Aut}(S)$ have natural quasi-platonic actions. There is a great interest in quasi-platonic actions for the following reasons:

(1) They are rigid, i.e., the conformal structure of the surfaces cannot be infinitesimally deformed without losing symmetry.
(2) The surface S has a defining equation with coefficients in a number field.
(3) Assume that $\pi_G : S \to S/G$ is branched over $\{0, 1, \infty\}$. Let $I = [0, 1] \subseteq \widehat{\mathbb{C}}$ be the standard unit interval. Then $\mathcal{D} = \pi_G^{-1}(I)$ is a bipartite graph in S, called a *(regular) dessin d'enfant.* The group G acts on $\mathcal{D}$, acting simply transitively on the edges. The complement $S - \mathcal{D}$ is a disjoint union of open, congruent convex hyperbolic polygons, permuted transitively by G. Each polygon is the lift to S of $\widehat{\mathbb{C}} - I$. This geometric structure on the surface and its invariance under G, generalizes the notion of a platonic solid and the tetrahedral, cubic, octahedral, dodecahedral and icosahedral tilings and automorphism groups of the sphere.
(4) There is a rich interplay between dessins and the action of the absolute Galois group on surfaces defined over number fields. We discuss this in detail in Section 5.

Most, though not all, quasi-platonic actions are symmetric. When the action is symmetric, the dessin is refined by a triangular tiling on S, generated by reflections in the sides of triangles on S. The mirror $\mathcal{M}_\phi$ of a symmetry ϕ is the fixed point subset of set ϕ and, if non-empty, consists of a finite number of circles called *ovals,* made up of edges of the tiling. The symmetry ϕ is called separating if $S - \mathcal{M}_\phi$ consists of two components, otherwise it is called *non-separating.* This paper and its sequel [7] discuss the dessins and the mirror structure of symmetric quasi-platonic actions of $PSL_2(q)$. The current paper classifies the quasi-platonic actions including the action of the absolute Galois group. The second paper discusses in detail the mirror structure of the symmetries of the actions.

Quasi-platonic actions, large actions, and genus actions. We conclude this section with a discussion of *large actions* on surfaces and the special place that quasi-platonic actions have among large actions. We say that G is a *large* group of automorphisms (G has a large action) if the ratio $|G|/(\sigma - 1)$ is fairly large, or alternatively a fundamental region for the G-action has small hyperbolic area $\frac{2\pi}{|G|/(\sigma-1)}$. For any given group G there are surfaces S, with an arbitrarily large genus, such that $G \simeq \mathrm{Aut}(S)$ and the values $|G|/(\sigma-1)$ is arbitrarily small. However there are only a finite number of large actions once a cutoff $|G|/(\sigma-1) \geq c$ has been decided. For large actions, the restriction on the size and geometry of a fundamental region forces some structure on the surface and simplifies the geometrical and group theoretic analysis of these surfaces and their symmetries.

According to the Riemann-Hurwitz theorem, we always have

$$|G|/(\sigma - 1) \leq 84. \tag{2}$$

For groups G which are efficiently generated, such as simple groups, there will always be a surface S with $G \subset \mathrm{Aut}(S)$ and for which $|G|/(\sigma - 1)$ is of reasonable size. For example, if G is generated by r elements, then a surface S with G-action may be constructed for which

$$\frac{2}{r-1} < |G|/(\sigma - 1) \leq 84. \tag{3}$$

If G is generated by 2 elements, then

$$2 < |G|/(\sigma - 1) \leq 84. \tag{4}$$

If G is generated by an involution and another element, then

$$4 < |G|/(\sigma - 1) \leq 84. \tag{5}$$

and, finally, if G is generated by two elements of order 2 and 3, then

$$12 < |G|/(\sigma - 1) \leq 84. \tag{6}$$

In all of the actions above S/G is a sphere $\pi_G : S \to S/G$ *is* branched over $r + 1$ points, The last three classes are all quasi-platonic $r = 3$, and the last two are of great interest to researchers on dessins d'enfant. The geometrical analyses are simplified in these four cases since there are associated tilings consisting of $(r + 1)$-gons (r-generator case), triangles (2-generator case), right-angled triangles (generation by an involution and another element), and triangles with a right angle and 60° angle (generation by elements of order 2 and 3). The r generator case for $PSL_2(p)$ is discussed in [20]. For simple groups the inequality 4 always holds and inequality 5 probably always holds. In the last case the groups are finite quotients of $PSL_2(\mathbb{Z})$. For $PSL_2(q)$ it follows from the works [13, 14] that we always be able get a surface for which the inequality 6 holds. The construction of actions of groups on surfaces from group generators is well known, see [3], [4], or [22] for example. The inequalities are derived from the Riemann-Hurwitz equation.

A *(hyperbolic) genus action* is an action of G on a surface S of genus $\sigma \geq 2$ such that G acts on no surface of lower genus ≥ 2. The surface S has the smallest hyperbolic area for a G action and, hence, the largest action of G. Genus actions are broadly studied; see [5, 10, 13, 14] for instance. We shall pay special attention to the genus actions of $G = PSL_2(q)$, since for genus actions the action is quasi-platonic, and $\epsilon(G)$ is a normal subgroup of $\mathrm{Aut}(S)$ of index 1 or 2 (see [5]).

Finally, why consider $PSL_2(q)$? They are simple groups; there are many low genus quasi-platonic actions among simple group actions; all the actions are symmetric, and the general calculations are fairly easy.

Overview of paper. Given the foregoing, we are going to focus on quasi-platonic actions in the rest of the paper and its sequel. The two papers are motivated by the prior work in [5], [6], [8], and [9], and, in particular, extend the earlier work in [8]. In the work [8] the symmetry structure of Hurwitz surfaces (surfaces for which $|G| = 84(\sigma-1)$) with $PSL_2(q)$ as automorphism group were completely determined. In that paper, all the symmetries are classified, an algorithm for computing the number of ovals is given; and it is proven that none of the symmetries on these surfaces are separating.

The remainder of this paper is organized as follows. In Section 2 we describe the construction of surfaces with quasi-platonic actions with symmetry for a given group G. In Section 3 we develop the tools to enumerate all quasi-platonic actions of $PSL_2(q)$. Our main results are Theorems 20 and 22. In Section 4 we sketch how a MAGMA [19] classification of the actions may be carried out and give complete lists for $q = 7, 8$. We then enumerate the actions for all $q < 50$ and $q = 64 = 2^6, q = 81 = 3^4$;consider a few other interesting examples; and describe four infinite families of large actions. Finally, in Section 5, we discuss the action of the absolute Galois group on the quasi-platonic actions. Our main results are Theorem 30 and 33.

One of the main tools we use is Macbeath's description of generators for $PSL_2(q)$ [18]. Indeed, a number of our results are implicit in his work. The bulk of our work consists in organizing a classification. For the work on dessins and the action of the absolute Galois group, we follow some ideas in [17].

2. Symmetric quasi-platonic group actions

2.1. **Symmetric G-actions and covering groups.** We briefly discuss the general case of a symmetric group action before getting down to the specifics of quasi-platonic actions. For more on the general case see [6]. The universal cover of S is the hyperbolic plane $\mathbb{H}$ with covering map $\pi_S : \mathbb{H} \to S$. We denote the group of covering transformations of π_S by $\Pi \backsimeq \pi_1(S)$. The conformal group action of G on S has a covering action by a Fuchsian group Γ defined by an exact sequence

$$\Pi \hookrightarrow \Gamma \overset{\eta}{\twoheadrightarrow} G. \tag{7}$$

The induced isomorphism $\overline{\eta} : \Gamma/\Pi \leftrightarrow G$ defines an action $\epsilon = \overline{\eta}^{-1}$ of G on S through the natural action of Γ/Π on $S = \mathbb{H}/\Pi$.

Now consider a symmetry ϕ on S. The symmetry ϕ lifts to a reflection or glide reflection Φ on $\mathbb{H}$ which normalizes the kernel Π. The lift Φ also normalizes the covering group Γ if ϕ normalizes the G-action and we get an NEC group $\Gamma^* = \langle \Phi, \Gamma \rangle$. So assume that ϕ normalizes the G-action, define $\theta = \epsilon^{-1}\phi\epsilon \in \mathrm{Aut}(G)$, and define $G^* = \langle\theta\rangle \ltimes G$. We get extended maps

$$\epsilon : G^* \hookrightarrow \langle \phi, \epsilon(G) \rangle \leq \mathrm{Aut}^*(S), \ \epsilon(\theta) = \phi \tag{8}$$

$$\Pi \hookrightarrow \Gamma^* \overset{\eta}{\twoheadrightarrow} G^*, \ \eta(\Phi) = \theta. \tag{9}$$

Remark 1. *Using the algebraic structure of G^* we may find all the symmetries in $\epsilon(G^*)$. Every symmetry comes form an element of the form θg where $1 = (\theta g)^2 = \theta g \theta g = \theta(g)g$, or $\theta(g) = g^{-1}$.*

Of crucial importance is the tiling of $\mathbb{H}$ induced by the mirrors of symmetries in G^*. The union

$$\mathcal{M}_{G^*} = \bigcup_{\phi} \mathcal{M}_{\phi}$$

of the non-empty mirrors of all the symmetries in G^* creates a pattern of geodesic edges and ovals on S. The complement of $S - \mathcal{M}_{G^*}$ is a disjoint union of regions upon which G^* acts transitively. The decomposition of $S - \mathcal{M}_{G^*}$ into disjoint regions induces a tiling $\mathcal{T}_S$ on S where the set of faces F_S, consists of the closures of the components of $S - \mathcal{M}_{G^*}$; the set of vertices V_S consists of points of transverse intersections of ovals; and, the set of edges E_S consists of the closures of the components of $\mathcal{M}_{G^*} - V_s$. If the action is small, the faces may not be simply connected and the edges may be ovals. With large actions, typically all faces are polygons and edges are arcs, not ovals, and in the case of quasi-platonic actions the faces are triangles. We may lift the tiling on S to a tiling $\mathcal{T}$ on $\mathbb{H}$ defined by $\pi_S^{-1}(\mathcal{M}_{G^*})$. An example is given in Figure 1. We will use the interplay between the tilings $\mathcal{T}_S$ and S and $\mathcal{T}$ on $\mathbb{H}$. We note without proof the following facts about the tiling $\mathcal{T}$ on $\mathbb{H}$:

(1) every edge in $\mathcal{T}$ belongs to a line made up of edges of $\mathcal{T}$;
(2) every vertex of $\mathcal{T}$ is the unique fixed point of some element of Γ; and
(3) the group Γ^* is generated by the reflections in the sides of a single triangle, and Γ^* permutes the tiles simply transitively.

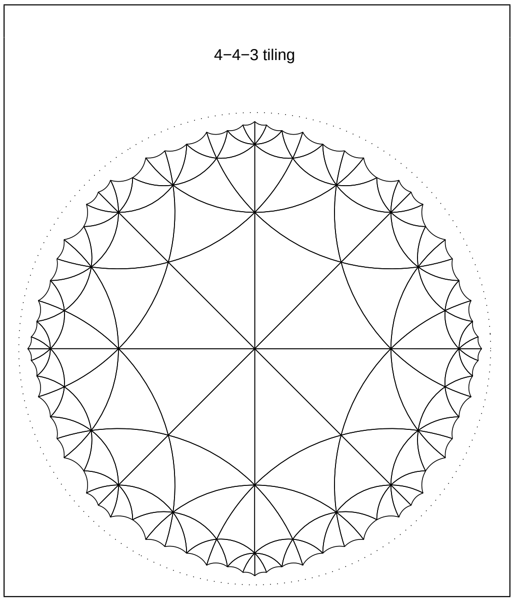

Figure 1.

2.2. **Quasi-platonic (triangular) group actions.** Throughout the remainder of this section we use the term triangular instead of quasi-platonic as it corresponds more directly to the construction. We can construct our surfaces, groups and symmetries through tilings of the hyperbolic plane by triangles. In Figure 2 we picture a (counter clockwise oriented) (l, m, n) triangle $\triangle DEF$ in the hyperbolic plane $\mathbb{H}$ (or Poincaré disc). The line segments $\overline{FD}$, $\overline{DE}$, and $\overline{EF}$ meet in the angles $\frac{\pi}{l}$, $\frac{\pi}{m}$, and $\frac{\pi}{n}$, respectively, where l, m, and n are integers ≥ 2. An (l, m, n)-triangle exists if and only if $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$. The triangles in Figure 1 are $(4, 4, 3)$ triangles.

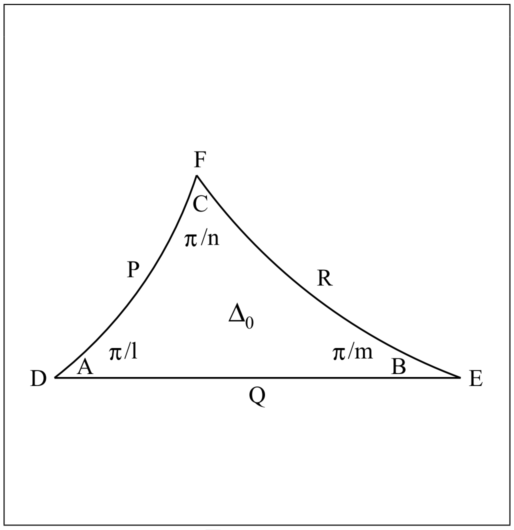

Figure 2.

Let $P, Q, R \in \mathrm{Aut}^*(\mathbb{H})$ be the hyperbolic reflections in the lines $\overline{FD}$, $\overline{DE}$, and $\overline{EF}$, respectively, and define the rotations:

$$A = PQ,\ B = QR,\ C = RP.$$

The mappings A, B, C are counter clockwise rotations, centered at D, E, F, respectively, through the angles $\frac{2\pi}{l}$, $\frac{2\pi}{m}$, $\frac{2\pi}{n}$, respectively. It is well known that $T_{l,m,n} = \langle A, B, C\rangle \subset PSL_2(\mathbb{R})$ is a discrete group of conformal isometries of the hyperbolic plane with the following presentation

$$T_{l,m,n} = \langle A, B, C | A^l = B^m = C^n = ABC = 1\rangle. \tag{10}$$

We call (l, m, n) the *signature* of $T_{l,m,n}$ and also call (l, m, n) the *signature* or *branching data* of the G-action on S. Now suppose that G is any group and (a, b, c) is a triple of elements generating G such that $a^l = b^m = c^n = abc = 1$. The triple (a, b, c) is a called a *generating* (l, m, n)*-triple* or *generating action triple.* If $\langle a, b, c\rangle$ is a proper subgroup of G, we just call (a, b, c) an (l, m, n)*-triple* or an *action triple.* The epimorphism of equation 7 is given by

$$\eta : T_{l,m,n} \to G,\ A \to a,\ B \to b,\ C \to c. \tag{11}$$

The kernel $\Pi = \ker(\eta)$ is torsion free and defines a closed Riemann surface $S = \mathbb{H}/\Pi$ whose genus σ satisfies the Riemann-Hurwitz equation

$$\frac{2\sigma - 2}{|G|} = 1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}. \tag{12}$$

One possibility for a symmetry on S is the involution q induced by the reflection Q in the side of $\triangle DEF$ if Q normalizes Π. The map 11 then extends to the following epimorphism

$$\eta : T^*_{l,m,n} \to G^*,\ P \to p,\ Q \to q,\ R \to r. \tag{13}$$

where

$$p = a\theta, q = \theta, r = \theta b$$

and $T^*_{l,m,n} = \langle P, Q, R\rangle$ is the group generated by the reflections in the sides of $\triangle DEF$. The automorphism θ satisfies

$$\theta(a) = a^{-1}, \theta(b) = b^{-1}. \tag{14}$$

The induced tiling on $\mathbb{H}$ is generated by reflection in the sides of the triangle. An example of the tiling on $\mathbb{H}$ for a $(4, 4, 3)$-action is given in Figure 1. Even if Q does not normalize Π, the tiling on $\mathbb{H}$ still projects to a tiling on the surface. For the rest of the paper we are going to assume that $\mathbb{H} \to \mathbb{H}/T_{l,m,n} = \widehat{\mathbb{C}}$ is adjusted so that $D \to 0, E \to 1, F \to \infty$ and correspondingly $S \to S/G$ maps $\overline{D} \to 0, \overline{E} \to 1, \overline{F} \to \infty$. Then the polygons of the dessin are the images of the polygons in $\mathcal{T}$ consisting of the dihedrally symmetric $2n$-gons surrounding the vertices of type F. If one of l, m equals 2 then we get regular n-gons. In Figure 1 the polygons are hexagons. The inverse image of $\mathcal{D}$ is the union of all edges of type $\overline{DE}$.

Remark 2. *There are additional possibilities for symmetries, which we explore in the sequel paper. They are irrelevant for the topic of dessins.*

Remark 3. *We get a Hurwitz surface when $\frac{2\sigma-2}{|G|}$ has the smallest possible value, if and only if $(l, m, n) = (2, 3, 7)$. If G is generated by the pair $\{a, b\}$ then upon setting $c = (ab)^{-1}$, we see that (a, b, c) is a generating (l, m, n)-triple for some l, m, n. Assuming that a and b have the appropriate orders, we get equations 3, 4, 5, 6. In the papers [13], [14], it is shown that all genus actions of $PSL_2(q)$ are the following types $(2, 3, n), n \geq 7$, $(2, 4, 5)$, $(2, 5, 5)$, $(3, 3, 4)$, and $(2, 5, 7)$.*

Remark 4. *The triangular tiling on S determines three different dessins on S. Let $I_1 = [0, 1]$, $I_2 = [1, \infty]$, $I_3 = [\infty, 0]$, be considered as oriented intervals of $\widehat{\mathbb{R}} = P^1(\mathbb{R})$ and set $\mathcal{D}_i{=}\pi_G^{-1}(I_i)$. The polygons of $\mathcal{D}_2$ and $\mathcal{D}_3$ in S are the images of the polygons in $\mathcal{T}$ consisting of the dihedrally symmetric $2l$-gons and $2m$-gons surrounding the vertices of type D and E, respectively. The inverse images of $\mathcal{D}_2$ and $\mathcal{D}_3$ in $\mathbb{H}$ are the unions of all edges of type $\overline{EF}$, and $\overline{FD}$ respectively. The tiling $\mathcal{T}$ encodes the information of all three dessins simultaneously. The triangles on S are the closures of connected components of inverse images, by π_G, of the upper half plane (counter clockwise oriented triangles) and the lower half of plane (clockwise oriented triangles).*

Epimorphisms and equivalence. We can use the tiling on S to construct an epimorphism for the G-action. Pick a clockwise oriented triangle $\overline{\Delta}$ on S. The point $\overline{D}$ on S corresponding to D in $\triangle DEF$ is $\pi_G^{-1}(0) \cap \overline{\Delta}$. The stabilizer $G_{\overline{D}}$ of $\overline{D}$ is cyclic of order l. The rotation number map rot:$G_{\overline{D}} \to \mathbb{C}$ given by the $g \to dg$ on the tangent plane $T_{\overline{D}}(S)$ is an isomorphism of g onto the lth roots of unity. Pick a in $G_{\overline{D}}$ so that $\text{rot}(a) = \text{rot}(A, \overline{D}) = \exp(\frac{2\pi i}{l})$. Do the same to get b and c such that $\text{rot}(b) = \exp(\frac{2\pi i}{m})$ and $\text{rot}(c) = \exp(\frac{2\pi i}{n})$. Using homotopy arguments with lifts of curves, it can be shown that $abc = 1$ and that $A \to a$, $B \to b$, $C \to c$ is a uniformizing epimorphism. The selection of a different counter clockwise oriented triangle gives the triple $\text{Ad}_g \cdot (a, b, c) = (gag^{-1}, gbg^{-1}, gcg^{-1})$, for some $g \in G$.

The enumeration of quasi-platonic actions is the same as the determination of $\text{Aut}(G)$ equivalence classes of generating (l, m, n)-triples of G. First we define our notions of equivalence of actions.

Definition 5. *We say that two conformal actions $\epsilon_1, \epsilon_2 : G \hookrightarrow \text{Aut}(S)$ are algebraically equivalent if $\epsilon_2 = \epsilon_1 \circ \omega$ for some $\omega \in \text{Aut}(G)$, or equivalently if $\epsilon_1(G)$*

and $\epsilon_2(G)$ *are the same subgroup of* $\mathrm{Aut}(S)$. *Two actions* $\epsilon_1 : G \hookrightarrow \mathrm{Aut}(S_1)$ *and* $\epsilon_2 : G \hookrightarrow \mathrm{Aut}(S_2)$ *on possibly different surfaces are conformally equivalent if there is a conformal equivalence* $h : S_1 \leftrightarrow S_2$ *such that*

$$\epsilon_2(g) = h \circ \epsilon_1(\omega(g)) \circ h^{-1}, g \in G.$$

Specifically, two actions of G *on the same surface are conformally equivalent if they determine conjugate subgroups of* $\mathrm{Aut}(S)$.

Remark 6. *Conformal equivalence is a mild refinement of algebraic equivalence, but we shall not go into it deeply in this paper. See* [4] *for more detail.*

Let (a, b, c) be a generating (l, m, n)-triple of G, $\Gamma = T_{l,m,n}$,and $\omega \in \mathrm{Aut}(G)$.Then the equation 7 can be expanded to a commutative diagram

$$\begin{tikzcd}
\Pi \arrow[r, hook] \arrow[d, "id"] & \Gamma \arrow[r, two heads, "\eta"] \arrow[d, "id"] & G \arrow[d, "\omega"] \\
\Pi \arrow[r, hook] & \Gamma \arrow[r, two heads, "\omega\circ\eta"] & G
\end{tikzcd} \tag{15}$$

Both epimorphisms determine the same group of automorphisms of $\Gamma/\Pi \subseteq \mathrm{Aut}(S)$ acting on $S = \mathbb{H}/\Pi$. The generating triple (a', b', c') determined by $\omega \circ \eta$ is

$$(\omega(a), \omega(a), \omega(a))\,.$$

Thus, each equivalence class determined by the action $\omega \cdot (a, b, c) = (\omega(a), \omega(a), \omega(a))$, $\omega \in \mathrm{Aut}(G)$, determines a unique surface $S = \mathbb{H}/\Pi$ and unique subgroup of $\mathrm{Aut}(S)$. Correspondingly, given two epimorphisms η_1, η_2 with the same kernel as in the left half of the diagram, we have $\eta_2 = \omega \circ \eta_1$ for an $\omega \in \mathrm{Aut}(G)$ and so η_1 and η_2 determine the equivalent triples. Equivalent epimorphisms determine equivalent conformal actions.

There is a braid action on triples generated by these transformations: $(a, b, c) \to (b, b^{-1}ab, c)$, $(a, b, c) \to (a, c, c^{-1}bc)$, $(a, b, c) \to (a^{-1}ca, b, a)$, and their inverses. The action commutes with the $\mathrm{Aut}(G)$-action on triples and defines $\mathrm{Aut}(G)$-invariant bijections of (l, m, n) triples to (m, l, n) and (n, m, l) triples. The other permutations of indices are obtained by composition. The permutation of signatures does not produce any new actions. Consider, for instance, the permutation $(l, m, n) \to (m, l, n)$. Reflect the triangle $\triangle DEF$ in the side $\overline{EF}$ to obtain the (clockwise oriented) $\triangle ED'F$ triangle, an (m, l, n)-triangle. The rotations, in order, at the corners are $B, B^{-1}AB, C$. The very same map $\eta : \Gamma \twoheadrightarrow G$ given in equation 11 takes the triple $(B, B^{-1}AB, C)$ to $(b, b^{-1}ab, c)$ and so the same surface $S = \mathbb{H}/\Pi$, $\ker(\eta) = \Pi$ is determined. As $\Gamma = \left\langle B, B^{-1}AB, C \right\rangle$ then the same subgroup of automorphisms of S is determined and the image of G in $\mathrm{Aut}(S)$ is the same. Therefore no new actions are determined. There is a similar argument for all other permutations. Therefore, we may assume the signature has standard lexicographic form $l \leq m \leq n$.

2.3. **Counting triple sets and the action of automorphism groups.** The discussion in this paragraph follows the discussion in [15]. To work with the action of $\mathrm{Aut}(G)$ on epimorphisms and conformal actions, and for later work on the Galois action on dessins, we define the following sets closely related to $\mathrm{Aut}(G)$-orbits on epimorphisms. First, an obvious one, which we call a *(generating) signature triple* *set.*

$$X_G(l,m,n) = \{(a,b,c) \in G^3 : o(a) = l, o(b) = m, o(c) = n, \\ abc = 1\}, \tag{16}$$

$$X_G^\circ(l,m,n) = \{(a,b,c) \in X_G(l,m,n) : \langle a,b,c\rangle = G\}. \tag{17}$$

For each element of $X_G(l,m,n)$, a map $\Pi \hookrightarrow \Gamma \overset{\eta}{\to} G$ with torsion free kernel Π is determined and thereby an action of $\eta(\Gamma)$ on $S = \mathbb{H}/\Pi$. Only those triples in $X_G^\circ(l,m,n)$ (generating signature triple set) determine actions of all of G. There are many cases where triples generate proper subgroups $\eta(\Gamma) \subset G$ so that $X_G^\circ(l,m,n)$ is strictly contained in $X_G(l,m,n)$. Indeed, $X_G^\circ(l,m,n)$ may even be empty. According to equation 12, the genus of the surface S is given by

$$\sigma = 1 + \frac{1}{2}\left|\eta(\Gamma)\right|\left(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}\right)$$

which is maximal when $\eta(\Gamma) = G$.

To understand the $\mathrm{Aut}(G)$ action on $X_G(l,m,n)$ we need to know the subgroups of G and the centralizers of subgroups. Let $H \subset G$ be a proper subgroup and (a,b,c) a triple such that $H = \langle a,b,c\rangle$. Then the size of the orbit $\mathrm{Aut}(G)\cdot(a,b,c)$ is given by

$$|\mathrm{Aut}(G)\cdot(a,b,c)| = \frac{|\mathrm{Aut}(G)|}{\left|\mathrm{Stab}_{\mathrm{Aut}(G)}((a,b,c))\right|} = \frac{|\mathrm{Aut}(G)|}{\left|\mathrm{Cent}_{\mathrm{Aut}(G)}(H)\right|}$$

After we remove all triples for all $\mathrm{Aut}(G)$-classes of proper subgroups H that have generating (l,m,n)-triples, we have only $X_G^\circ(l,m,n)$ left and so

$$|X_G^\circ(l,m,n)| = |X_G(l,m,n)| - \sum_{H=\langle a,b,c\rangle} \frac{|\mathrm{Aut}(G)|}{\mathrm{Cent}_{\mathrm{Aut}(G)}(H)} \tag{18}$$

where $H = \langle a,b,c\rangle$ denotes an $\mathrm{Aut}(G)$-class of triples generating H and its $\mathrm{Aut}(G)$-conjugates. Sometimes the right hand sum can be easily computed exactly as there may only be a small number of terms.

Closely related to the sets $X_G(l,m,n)$ are triples where the a,b,c are restricted to come from some class of elements somewhere between a conjugacy class and an automorphism class. These sets will be important when we study Galois actions on dessins in Section 5. The sets also allow more effective enumeration of actions. To this end, we define an "approximate automorphism group" to be a group of automorphisms of G satisfying $\mathrm{Inn}(G) \subseteq L \subseteq \mathrm{Aut}(G)$. The extreme cases $\mathrm{Inn}(G)$ and $\mathrm{Aut}(G)$ are denoted by K and A respectively. These notions are more appropriate when the index $|\mathrm{Aut}(G) : \mathrm{Inn}(G)| = |\mathrm{Out}(G)|$ is small, say, when the center of G is small. A specific intermediate case is $L = PGL_2(q)$ when q is a prime power. For $g \in G$ and L as above let and $g^L = \{\omega(g) : \omega \in L\}$, when $L = K$ we get conjugacy classes. For $(a,b,c) \in G^3$, we define *(generating) L-triple sets.*

$$L_G(a,b,c) = \{(x,y,z) : x \in a^L, y \in b^L, z \in c^L, xyz = 1\}, \tag{19}$$

$$L_G^\circ(a,b,c) = \{(x,y,z) : (x,y,z) \in L_G(a,b,c), \langle x,y,z\rangle = G\}\,. \tag{20}$$

If $L = \mathrm{Inn}(G)$ or $\mathrm{Aut}(G)$, we use the notation $K_G(a,b,c)$ and $K_G^\circ(a,b,c)$ or $A_G(a,b,c)$ and $A_G^\circ(a,b,c)$ respectively. Observe that $K_G(a,b,c) \subseteq L_G(a,b,c) \subseteq A_G(a,b,c) \subseteq X_G(l,m,n)$ and that both $A_G(a,b,c)$ and $X_G(l,m,n)$ are unions of

$\mathrm{Aut}(G)$ classes of triples. When $L = PGL_2(q)$ we call the sets *(generating) projective triple sets.* There are formulas similar to 18 for determining the number of generating triples in $K_G^\circ(a,b,c)$, $L_G^\circ(a,b,c)$, and $A_G^\circ(a,b,c)$. Moreover, if the character theory of G is tractable, then the following formula (see [2], [15]) may be used:

$$|K_G(a,b,c)| = \frac{|G|^2}{|\mathrm{Cent}(a)| \cdot |\mathrm{Cent}(b)| \cdot |\mathrm{Cent}(c)|} \sum_{\chi} \frac{\chi(a)\chi(b)\chi(c)}{\chi(1)}. \tag{21}$$

Remark 7. *The set $X_G^\circ(l,m,n)$ and their partitions into L and K classes are natural action spaces for the absolute Galois group. The sets $L_G^\circ(a,b,c)$ are useful in classifying the equivalence classes of actions. The sets $K_G^\circ(a,b,c)$ will be very useful in discussing the action of the absolute Galois group on group actions in Section 5.*

2.4. **Companion actions and a Schur cover.** For use in Section 5 we want make more precise the relation between $L_G^\circ(a,b,c)$ and $K_G^\circ(a,b,c)$ and to be able to separate the various automorphism classes of orbits in these sets. Both of these sets have orbit decompositions

$$L_G^\circ(a,b,c) = \bigcup_{(a',b',c')} (a',b',c')^L \tag{22}$$

$$K_G^\circ(a,b,c) = \bigcup_{(a'',b'',c'')} (a'',b'',c'')^G. \tag{23}$$

where the superscripts on the right hand side indicate orbits. Each orbit on the right hand side of these equations must be regular and so

$$\left|(a',b',c')^L\right| = |L|\,, \quad \left|(a'',b'',c'')^G\right| = |\mathrm{Inn}(G)| = |K|\,. \tag{24}$$

In our investigations in Section 5, it turns out the right hand sides will have more than one orbit which leads to some indeterminacy in the action of the absolute Galois group on $PSL_2(q)$ actions. To this end, we make the following definition:

Definition 8. *Suppose that $G = \langle a,b,c\rangle$ and $\mathrm{Inn}(G) \le L \le \mathrm{Aut}(G)$ and that $(a_1',b_1',c_1')^L$, $(a_2',b_2',c_2')^L$ are two distinct orbits in the right hand side of equation 22. Then we say that the two orbits are companion L-orbits and determine companion actions with respect to L. Similar definitions apply to the decomposition in equation 23. Companion orbits may determine equivalent actions upon lifting all the way up to $A_G^\circ(a,b,c)$.*

Let $\widetilde{G}$ be a Schur cover of G. Companion classes in $K_G^\circ(a,b,c)$ are a result of projecting multiple classes $(\widetilde{a},\widetilde{b},\widetilde{c})^{\widetilde{G}}$ in $\widetilde{G}$ to different classes $(a,b,c)^G$ in $K_G^\circ(a,b,c)$. Reversing the process, we many use a Schur cover to separate companion classes. In the case at hand $\widetilde{PSL_2}(q) = SL_2(q)$. We now discuss the general case of Schur covers.

Though we are primarily interested in a Schur covering group, let $\widetilde{G} \overset{\pi}{\twoheadrightarrow} G$ be any covering group of G satisfying:

(1) there is central subgroup $Z < \widetilde{G}$ such that

$$Z \overset{\iota}{\hookrightarrow} \widetilde{G} \overset{\pi}{\twoheadrightarrow} G$$

is exact;

(2) for every proper subgroup $\widetilde{H} < \widetilde{G}$, $\pi\left(\widetilde{H}\right) < G$.

We sketch how we may use a covering group to separate companion orbits. Each conjugacy class g^G in G may have several conjugacy classes in $\widetilde{G}$ lying over it. In fact, the totality of elements lying over g^G is $\bigcup_{z\in Z} (z\widetilde{g})^{\widetilde{G}} = \bigcup_{z\in Z} z\,(\widetilde{g})^{\widetilde{G}}$ for a fixed $\widetilde{g}$ lying over g. Thus, Z acts on the conjugacy classes lying over g^G, and they all have the same size. It is easily shown that

$$\frac{\left|(\widetilde{g})^{\widetilde{G}}\right|}{|g^G|} = \frac{|Z|\,|Z_G(g)|}{\left|Z_{\widetilde{G}}(\widetilde{g})\right|}$$

Hence the number of classes lying over is g^G is $|Z|$ divided by this number giving

$$\text{number of classes lying over } g^G = \frac{\left|Z_{\widetilde{G}}(\widetilde{g})\right|}{|Z_G(g)|}.$$

In the case of $PSL_2(q)$, for odd q, this number is 2 unless g is an involution.

Given a generating (l, m, n)-triple (a, b, c) we have numerous generating $(\widetilde{l}, \widetilde{m}, \widetilde{n})$-triples $(\widetilde{a}, \widetilde{b}, \widetilde{c})$ covering (a, b, c). For, if $(\widetilde{a}, \widetilde{b}, \widetilde{c}) \in \widetilde{G}^3$ is any triple with $\pi(\widetilde{a}, \widetilde{b}, \widetilde{c}) = (a, b, c)$, we may manufacture a covering generating $(\widetilde{l}, \widetilde{m}, \widetilde{n})$-triple. Noting that $\pi(\widetilde{a}\widetilde{b}\widetilde{c}) = abc = 1$, then $\widetilde{a}\widetilde{b}\widetilde{c} = z \in Z$, and so $(\widetilde{a}, \widetilde{b}, \widetilde{c}z^{-1})$ satisfies $\widetilde{a}\widetilde{b}\widetilde{c}z^{-1} = 1$. Also, $\pi\left(\widetilde{a}, \widetilde{b}, \widetilde{c}z^{-1}\right) = (a, b, c)$ and $\pi\left\langle \widetilde{a}, \widetilde{b}, \widetilde{c}z^{-1}\right\rangle = \langle a, b, c\rangle = G$, so $\left\langle \widetilde{a}, \widetilde{b}, \widetilde{c}z^{-1}\right\rangle = \widetilde{G}$. Thus it makes sense to assume that $\widetilde{a}\widetilde{b}\widetilde{c} = 1$ and that $\left\langle \widetilde{a}, \widetilde{b}, \widetilde{c}\right\rangle = \widetilde{G}$. We shall call such a triple a *lift* or *covering triple* of (a, b, c). The orders $\widetilde{l}, \widetilde{m}, \widetilde{n}$ of $\widetilde{a}, \widetilde{b}, \widetilde{c}$ are generally distinct from l, m, n, but l, m, n divide $\widetilde{l}, \widetilde{m}, \widetilde{n}$ respectively and the respective quotients divide the exponent of Z. If $(\widetilde{a}_0, \widetilde{b}_0, \widetilde{c}_0)$ is lift of (a, b, c), then all other lifts are of the form

$$(\widetilde{a}_0 z_1, \widetilde{b}_0 z_2, \widetilde{c}_0 z_3)$$

where

$$1 = \widetilde{a}_0 z_1 \widetilde{b}_0 z_2 \widetilde{c}_0 z_3 = \widetilde{a}_0 \widetilde{b}_0 \widetilde{c}_0 z_1 z_2 z_3 = z_1 z_2 z_3. \tag{25}$$

The collection of lifts defined above is called the *lift orbit* of (a, b, c). Indeed, let $J \le Z^3$ be the subgroup defined by equation 25. Then the lift orbit is the J orbit of the J action acting on covering triples. The signatures $(\widetilde{l}, \widetilde{m}, \widetilde{n})$ may be different for different lifts.

For conjugacy triple sets, we have

$$K_G^\circ(a, b, c) = \bigcup_{(\widetilde{a}, \widetilde{b}, \widetilde{c})} \pi\left(K_G^\circ(\widetilde{a}, \widetilde{b}, \widetilde{c})\right)$$

where $(\widetilde{a}, \widetilde{b}, \widetilde{c}) \in \pi^{-1}(a) \times \pi^{-1}(b) \times \pi^{-1}(c)$. With luck, each $K_G^\circ(\widetilde{a}, \widetilde{b}, \widetilde{c})$ will be a single $\widetilde{G}$ orbit and, hence, each G orbit in $K_G^\circ(a, b, c)$ will be the image of a single $K_G^\circ(\widetilde{a}, \widetilde{b}, \widetilde{c})$ triple set.

3. Classifying quasi-platonic actions of $PSL_2(q)$

Now we examine quasi-platonic actions of $PSL_2(q)$ on surfaces. To use the results of the previous section, we need to discuss the automorphisms and subgroups of $PSL_2(q)$, the covering of $PSL_2(q)$ by $SL_2(q)$, and trace triple sets of $SL_2(q)$. We set $q = p^e$ unless otherwise noted.

3.1. Properties of $PSL_2(q)$ and $SL_2(q)$.

The projective linear groups have coverings by matrix groups

$$\langle \pm 1 \rangle \hookrightarrow SL_2(q) \twoheadrightarrow PSL_2(q) \tag{26}$$

and its extension

$$\mathbb{F}_q^* \hookrightarrow GL_2(q) \twoheadrightarrow PGL_2(q). \tag{27}$$

For the prime $p = 2$, we observe that $SL_2(q) = PSL_2(q)$.

For effective computations in $PSL_2(q)$ we will need to work with elements of $SL_2(q)$ and their traces using the exact covering sequence 26. We recall some of the terminology and results of [18] and [13]. For any $U \in SL_2(q)$, U is called *parabolic, hyperbolic,* or *elliptic* if the characteristic polynomial $\lambda^2 - \mathrm{trace}(U)\lambda - 1$, has a double root, has two distinct roots over $\mathbb{F}_q$, or is irreducible over $\mathbb{F}_q$, respectively. The hyperbolic and elliptic elements are called semi-simple. The trace of an element U does not uniquely determine its $GL_2(q)$ conjugacy class, the exception being parabolic elements. Restricting our attention to the elements U of $SL_2(q) - \{1, -1\}$ we have the following proposition:

Proposition 9. *Let $U \in SL_2(q) - \{1, -1\}$. Then:*

(1) *the minimal polynomial is the characteristic polynomial $\lambda^2 - \upsilon\lambda - 1$, $\upsilon = \mathrm{trace}(U)$, and the order of U is determined by the value of the trace;*
(2) *two elements of $SL_2(q) - \{1, -1\}$ are $GL_2(q)$-conjugate if and only if they have the same trace υ. The elements are conjugate to $\begin{bmatrix} 0 & -1 \\ 1 & \upsilon \end{bmatrix}$.*

Automorphisms. The group $GL_2(q)$ acts on $SL_2(q)$ by conjugation and, hence, $PGL_2(q)$ acts as a group of automorphisms of both $SL_2(q)$ and $PSL_2(q)$. To find the full group of automorphisms we need to take the Galois group $\mathrm{Gal}(\mathbb{F}_q)$ of field automorphisms into account. A typical automorphism of $GL_2(q)$ has the form

$$\rho \circ Ad_U : X \to \rho\left(UXU^{-1}\right)$$

for $\rho \in \mathrm{Gal}(\mathbb{F}_q)$, $U \in GL_2(q)$, and, hence, $\mathrm{Aut}(PSL_2(q)) = \mathrm{Gal}(\mathbb{F}_q) \ltimes PGL_2(q)$. The order of the groups are as follows:

	$\lvert SL_2(q)\rvert$	$\lvert PSL_2(q)\rvert$	$\lvert GL_2(q)\rvert$	$\lvert PGL_2(q)\rvert$
$p = 2$	$(q-1)q(q+1)$	$(q-1)q(q+1)$	$(q-1)^2q(q+1)$	$(q-1)q(q+1)$
p odd	$(q-1)q(q+1)$	$\frac{(q-1)q(q+1)}{2}$	$(q-1)^2q(q+1)$	$(q-1)q(q+1)$

The Galois group $\mathrm{Gal}(\mathbb{F}_{p^e})$ is the cyclic group of order e generated by the Frobenius automorphism $x \to x^p$.

Cyclic subgroups of $PSL_2(q)$. Next we describe the cyclic and other subgroups of $PSL_2(q)$. For odd p there are three conjugacy classes of maximal cyclic subgroups of $PSL_2(q)$ of orders p, $\frac{q-1}{2}$, and $\frac{q+1}{2}$; and, for even q there are three conjugacy classes of orders $2, q-1$,and $q+1$. In Table 3.1 the third column describes the number of conjugacy classes of an element with the given trace. The fourth column describes the reducibility of the characteristic polynomial $\lambda^2 - \upsilon\lambda + 1$ with $\upsilon = \text{trace}(U)$.

Type	Order	# Classes	Reducibility over $\mathbb{F}_q$
parabolic, q odd	p	2	$\lambda^2 - \upsilon\lambda + 1$ is a square
hyperbolic, q odd	$\frac{q-1}{2}$	1	$\lambda^2 - \upsilon\lambda + 1$ distinct factors
elliptic, q odd	$\frac{q+1}{2}$	1	$\lambda^2 - \upsilon\lambda + 1$ irreducible
parabolic, q even		1	$\lambda^2 - \upsilon\lambda + 1$ is a square
hyperbolic, q even	$q-1$	1	$\lambda^2 - \upsilon\lambda + 1$ distinct factors
elliptic, q even	$q+1$	1	$\lambda^2 - \upsilon\lambda + 1$ irreducible

Table 3.1 Maximal cyclic subgroups of $PSL_2(q)$

Implicit in the table is that if s is relatively prime to the order of U, then the characteristic polynomial of U^s has the same irreducibility characteristics as that of U.

The observations about cyclic subgroups of $SL_2(q)$ and $PSL_2(q)$, recorded in the next proposition, will be useful later on. They are all easily proven by diagonalization of covering elements, possibly in an extension of $\mathbb{F}_q$.

Proposition 10. *Let $U, V \in SL_2(q)$ be elements covering $u, v \in PSL_2(q)$ respectively.*

1. *U is conjugate to an element with entries in $\mathbb{F}_p[\text{trace}(U)]$ (companion matrix).*
2. *If U and V are semi-simple and the order of V divides that of U, then $V = WU^sW^{-1}$ for some $W \in GL_2(q)$, and $\text{trace}(V)$ belongs to the subfield $\mathbb{F}_p[\text{trace}(U)]$ of $\mathbb{F}_q$.*
3. *If U and V are semi-simple and project to elements of the same order in $PSL_2(q)$, then the $\mathbb{F}_p[\text{trace}(U)] = \mathbb{F}_p[\text{trace}(V)]$,*
4. *If $u \in PSL_2(q)$ is semi-simple, then*
   - (a) *if u has odd order l, then the covering elements U and $-U$ can be chosen so that they have orders l and $2l$ in $SL_2(q)$, respectively;*
   - (b) *if u has even order then both of the covering elements have order $2l$;*
   - (c) *the number of traces of elements of $SL_2(q)$ that project to a semi-simple element of order l is the Euler number $\phi(l)$;*
   - (d) *the conjugacy classes $u^{PSL_2(q)}$ and $u^{PGL_2(q)}$ are equal.*
5. *If $u \in PSL_2(q)$ is parabolic, then*
   - (a) *if u has odd order p, then the covering elements U and $-U$ can be chosen so that they have orders p and $2p$ in $SL_2(q)$, respectively;*
   - (b) *if u has even order, then both of the covering elements have order 2;*
   - (c) *the traces of elements of $SL_2(q)$ that project to a parabolic element are ± 2; and,*
   - (d) *if q is odd, the conjugacy class $u^{PGL_2(q)}$ has twice as many elements as does $u^{PSL_2(q)}$. If q is even, then $u^{PSL_2(q)}$ and $u^{PGL_2(q)}$ are equal.*

Subgroups of $PSL_2(q)$. L.E. Dixon [12] classified the subgroups of $PSL_2(q)$ into three types: affine, projective, and exceptional. The types are summarized in Table 3.2 below where we show the maximal subgroups of each type.

Type	Maximal	Order	matrix type/condition
affine - parabolic	$\mathbb{F}_q^* \ltimes \mathbb{F}_q$	$\frac{q(q-1)}{2}$	$\begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix}$ $x \in \mathbb{F}_q^*,\ y \in \mathbb{F}_q$
affine - hyperbolic	$\mathbb{F}_q^*$	$\frac{q-1}{2}$	$\begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix}$, $x \in \mathbb{F}_q^*$
affine - elliptic		$\frac{q+1}{2}$	$\begin{bmatrix} y & z \\ -\lambda z & y \end{bmatrix}$, $y, z \in \mathbb{F}_q$, $\lambda \notin \mathbb{F}_q^2,\ y^2 + \lambda z^2 = 1$
projective	$PSL_2(r)$	$\frac{r(r^2-1)}{2}$	$\mathbb{F}_r \subset \mathbb{F}_q$
projective	$PGL_2(r)$	$r(r^2-1)$	$\mathbb{F}_{r^2} \subset \mathbb{F}_q$, q odd
exceptional dihedral	D_{q-1}	$q-1$	hyperbolic cyclic normalizer
exceptional dihedral	D_{q+1}	$q+1$	elliptic cyclic normalizer
exceptional	$A_4 = PSL_2(3)$	12	
exceptional	$\Sigma_4 = PGL_2(3)$	24	
exceptional	$A_5 = PSL_2(5)$	60	

Table 3.2 Subgroups of $PSL_2(q)$

3.2. **Lifting $PSL_2(q)$ triples to $SL_2(q)$.** This section recalls the work of MacBeath in [18] on generating triples, which was used extensively in [13] and [14]. First, we translate the discussion on Schur covers in Section 2.4 to the cover $\widetilde{PSL_2(q)} = SL_2(q) \twoheadrightarrow PSL_2(q)$. Let us consider a typical (l, m, n)-action of $G = PSL_2(q)$, with generating triple (a, b, c). Let (A, B, C) be a lift of (a, b, c) to $SL_2(q)$ – recall that $ABC = I$. For simplicity of notation in the remaining sections, we choose (A, B, C) to denote the lift of (a, b, c) to $SL_2(q)$, not the lift to Γ as in previous sections, no confusion should result.

Let

$$\alpha = \operatorname{trace}(A),\ \ \beta = \operatorname{trace}(B),\ \ \gamma = \operatorname{trace}(C),$$

and call (α, β, γ) a trace triple and (A, B, C) an (α, β, γ)-triple. For any other triple (A', B', C') projecting to (a, b, c) the corresponding traces satisfy $\alpha' = \pm\alpha$, $\beta' = \pm\beta$, $\gamma' = \pm\gamma$. We noted that the order of a non-identity element in $PSL_2(q)$ is determined by the trace of an element lying over it in $SL_2(q)$ and, hence, that any two $(\pm\alpha, \pm\beta, \pm\gamma)$-triples yield (l, m, n)-triples of the same type. We define the *trace triple set* $Tr(\alpha, \beta, \gamma)$ by

$$\begin{aligned} Tr(\alpha, \beta, \gamma) = \{&(A, B, C) \in (SL_2(q) - \{\pm 1\})^3 : ABC = I, \\ &\operatorname{trace}(A) = \alpha,\ \operatorname{trace}(B) = \beta,\ \operatorname{trace}(C) = \gamma\} \end{aligned}$$

This definition is a slight variation of the definitions in [18] and [13], where A, B, C are allowed to be ± 1.

In the following Remark, we record some properties of trace triple sets, which easily follow from Proposition 10.

Remark 11. *The following properties hold for trace triple sets:*

(1) *The four triple sets* $Tr(\alpha,\beta,\gamma)$, $Tr(\alpha,-\beta,-\gamma)$, $Tr(-\alpha,\beta,-\gamma)$, *and* $Tr(-\alpha,-\beta,\gamma)$ *form a lift orbit of* $(a,b,c)^{PGL_2(q)}$ *discussed in the Section 2.4 on Schur covers.*
(2) *The four sets in a lift orbit will be distinct if at least two of the three traces are non-zero. This will occur for hyperbolic signatures since at most one of* l,m,n *will equal* 2 *and trace zero elements of* $SL_2(q)$ *project to involutions.*
(3) *If all three of* α,β,γ *are non-zero, then* $Tr(\alpha,\beta,\gamma)$ *and* $Tr(-\alpha,\beta,\gamma)$ *will both correspond to the same* (l,m,n) *but must have disjoint projections to* $L_G(a,b,c)$*. For, if* $(A,B,C)\in Tr(\alpha,\beta,\gamma)$ *and* $(A',B',C')\in Tr(-\alpha,\beta,\gamma)$ *project to the same triple* (a,b,c)*, then* $A'=-A, B'=B, C'=C$ *and* $A'B'C'=-ABC=-I$*, a contradiction. Thus, the sets* $Tr(-\alpha,\beta,\gamma)$, $Tr(\alpha,-\beta,\gamma)$, $Tr(\alpha,\beta,-\gamma)$, $Tr(-\alpha,-\beta,-\gamma)$ *form a lift orbit for a companion action. Indeed, as we shall prove,* $L_G(a,b,c)$ *is the disjoint union of the two distinct of images of* $Tr(\alpha,\beta,\gamma)$ *and* $Tr(-\alpha,-\beta,-\gamma)$*.*

Macbeath originally proved in [18] that each $Tr(\alpha,\beta,\gamma)$ were non-empty except in a small number of special cases. A key concept introduced by Macbeath was the notion of singularity of a triple which we now describe. Select a triple $(A,B,C)\in Tr(\alpha,\beta,\gamma)$. Since A is not a scalar matrix it is conjugate to its companion matrix and, hence triple in $Tr(\alpha,\beta,\gamma)$ is conjugate to one in which

$$A=\begin{bmatrix}0 & -1\\ 1 & \alpha\end{bmatrix},\ B=\begin{bmatrix}\beta-x & y\\ z & x\end{bmatrix},\ C=(AB)^{-1}=\begin{bmatrix}\alpha x+y & x\\ x-\alpha z-\beta & -z\end{bmatrix}.$$

Now $\det(B)=1$ and $\mathrm{tr}(C)=\gamma$ so that we have

$$x\beta-x^2-zy=1,\ z=\alpha x+y-\gamma \tag{28}$$

or the following quadratic form equation:

$$x^2+\alpha xy+y^2-\beta x-\gamma y+1=0. \tag{29}$$

Note that solutions to this equation are solutions of the form $(x,y,1)$ of

$$x^2+y^2+z^2+\alpha xy-\beta xz-\gamma yz=0 \tag{30}$$

or in matrix form, for odd q,

$$X^tQX=\begin{bmatrix}x & y & z\end{bmatrix}\begin{bmatrix}1 & \frac{\alpha}{2} & \frac{-\beta}{2}\\ \frac{\alpha}{2} & 1 & \frac{-\gamma}{2}\\ \frac{-\beta}{2} & \frac{-\gamma}{2} & 1\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix}=0. \tag{31}$$

The form in equation 30 factors (possibly over an extension of $\mathbb{F}_q$) if and only if the determinant of Q is zero, which is equivalent to

$$DQ(\alpha,\beta,\gamma)=\alpha^2+\beta^2+\gamma^2-\alpha\beta\gamma-4=0. \tag{32}$$

Note that this holds for $p=2$ even though the derivation would no longer hold. Macbeath calls (α,β,γ) a singular triple in this case and non-singular otherwise. By extension we say that (A,B,C) and its projection (a,b,c) are singular or non-singular. In [18] Macbeath proves the following two propositions.

Proposition 12. *Let* $(A,B,C)\in Tr(\alpha,\beta,\gamma)$*, then* $\langle A,B,C\rangle$ *is an affine subgroup of* $SL_2(q)$ *if and only if* $x^2+y^2+z^2+\alpha xy-\beta xz-\gamma yz$ *factors, i.e., equation 32 holds.*

Proposition 13. *Let notation be as above and suppose that (α,β,γ) is a non-singular triple. Then*

$$|Tr(\alpha,\beta,\gamma)| = |PGL_2(q)|\,. \tag{33}$$

The two results above yield the following:

Corollary 14. *Let notation be as above and suppose that (α,β,γ) is a non-singular triple. For any $(A,B,C) \in Tr(\alpha,\beta,\gamma)$ the $PGL_2(q)$ orbit of (A,B,C) equals $Tr(\alpha,\beta,\gamma)$. Consequently, every non-singular trace triple class $Tr(\alpha,\beta,\gamma)$ has at most one $PGL_2(q)$ class of generating vectors.*

Proof: The centralizer of a subgroup of $PSL_2(q)$ is non-trivial if and only if the subgroup is cyclic. But, if $\langle A,B,C\rangle$ is cyclic, then it is affine, and (α,β,γ) is a singular. This contradiction shows that $\langle A,B,C\rangle$ has a trivial centralizer and

$$\left|\langle A,B,C\rangle^{PGL_2(q)}\right| = |PGL_2(q)| = |Tr(\alpha,\beta,\gamma)|$$

so that $\langle A,B,C\rangle^{PGL_2(q)} = Tr(\alpha,\beta,\gamma)$. If (A,B,C) is a generating vector, then $\langle A,B,C\rangle^{PGL_2(q)} = Tr(\alpha,\beta,\gamma)$, and there is no room for anything else. ■

It is instructive to give an alternate version of MacBeath's proof of Proposition 13 to see directly how the singularity condition 32 is used. We give a proof for odd q only.

Proof: (Proposition 13) Let $A_0 = \begin{bmatrix} 0 & -1 \\ 1 & \alpha \end{bmatrix}$. Each $(A,B,C) \in Tr(\alpha,\beta,\gamma)$ is conjugate to a triple of the form $(A_0,B',C') \in Tr(\alpha,\beta,\gamma)$. The number of triples of the form (A_0,B',C') in $Tr(\alpha,\beta,\gamma)$ is the number of solutions to equation 29. It follows then that

$$|Tr(\alpha,\beta,\gamma)| = \frac{|GL_2(q)|}{|\mathrm{Cent}(GL_2(q),A)|}\left|\{(x,y) : x^2+\alpha xy+y^2-\beta x-\gamma y+1=0\}\right|. \tag{34}$$

We show that this quantity is $q(q^2-1)$ by a case analysis in the following table, depending on the type of A. In the table, the $GL_2(q)$ conjugacy class $A^{GL_2(q)}$ has cardinality $\left|A^{GL_2(q)}\right| = \frac{|GL_2(q)|}{|\mathrm{Cent}(GL_2(q),A)|}$. The fourth column is the number of solutions to equation 29.

Type of A	$u^2+\alpha uv+v^2$	$\left\|A^{GL_2(q)}\right\|$	# of solutions	$\|Tr(\alpha,\beta,\gamma)\|$
elliptic	irreducible	$q(q-1)$	$q+1$	$q(q^2-1)$
hyperbolic	distinct factors	$q(q+1)$	$q-1$	$q(q^2-1)$
parabolic	square	q^2-1	q	$q(q^2-1)$

First let us calculate $|\mathrm{Cent}(GL_2(q),A)|$. The centralizer $\mathrm{Cent}(GL_2(q),A)$ is contained in the $\mathbb{F}_q$ linear span of A and the identity matrix I. The set of invertible matrices in this linear span is $\mathrm{Cent}(GL_2(q),A)$, with $Z^{-1} = \frac{1}{\det(Z)}(\mathrm{trace}(Z)I - Z)$ for a typical element $Z \in \mathrm{Cent}(GL_2(q),A)$, using the Cayley Hamilton theorem. Letting

$$Z = uI + vA = \begin{bmatrix} u & -v \\ v & u+\alpha v \end{bmatrix}$$

we see that $\det(Z) = u^2 + \alpha uv + v^2$. Thus

$$|\mathrm{Cent}(GL_2(q), A)| \;=\; q^2 - \left|\left\{(u,v) : u^2 - \alpha uv + v^2 = 0\right\}\right|.$$

Next we need the number of solutions to $u^2 + \alpha uv + v^2 = 0$. If the equation $u^2 - \alpha uv + v^2$ has a non-zero solution then it is reducible and, hence, there is only one solution $(0,0)$ in the irreducible case . If $u^2 + \alpha uv + v^2$ is reducible, but not a square, then the zero set is the union of two distinct intersecting lines and, hence, has $2q-1$ points. If $\alpha = \pm 2$, then $u^2 - \alpha uv + v^2 = (u \pm v)^2$ and there are q solutions. Thus

$$|\mathrm{Cent}(GL_2(q), A)| = q^2 - 1,\; (q-1)^2,\; q(q-1)$$

in the irreducible, distinct factors and the square cases respectively. This gives us column 3 of the table. To count the number of solutions of equation 33 in column 4 we consider three cases depending on the type of A.

Elliptic case. We eliminate the linear term in the equation as follows. Let $X = \begin{bmatrix} x \\ y \end{bmatrix}$, $Q = \begin{bmatrix} 1 & \frac{\alpha}{2} \\ \frac{\alpha}{2} & 1 \end{bmatrix}$, $E = \begin{bmatrix} -\beta \\ -\gamma \end{bmatrix}$ and then the matrix form of equation 29 is:

$$X^t Q X + E^t X + 1 = 0.$$

Replacing X by $Y + W$ with $Y = \begin{bmatrix} u \\ v \end{bmatrix}$ and $W = \frac{-1}{2} Q^{-1} E$ we get $Y^t Q Y = -1 + \frac{1}{4} E^t Q^{-1} E$ or

$$u^2 + \alpha uv + v^2 = \frac{\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma - 4}{\alpha^2 - 4}. \tag{35}$$

As (α, β, γ) is a non singular triple the right hand side of the equation is non-zero. The number of solutions to $u^2 + \alpha uv + v^2 = d \in \mathbb{F}_q^*$ is independent of d. To see this, observe that the map $\det : \mathrm{Cent}(GL_2(q), A) \to \mathbb{F}_q^*, Z \to \det(Z)$ is a group homomorphism and so

$$|\mathrm{Cent}(GL_2(q), A)| = |\mathrm{Im}(\det)| \times \left|\left\{(u,v) : u^2 + \alpha uv + v^2 = 1\right\}\right|.$$

Also as $\det(zZ) = z^2 \det(Z)$ then $\mathrm{Im}(\det)$ is either $\mathbb{F}_q^*$ or the set of squares in $\mathbb{F}_q^*$ with cardinalities $q-1$ and $(q-1)/2$ respectively. It follows that the number of solutions of $u^2 + \alpha uv + v^2 = 1$, is either $q+1$ or $2(q+1)$. But the fibres of the map $pr_2 : \{(u,v) : u^2 + \alpha uv + v^2 = 1\} \to \mathbb{F}_q$, $(u,v) \to v$ have at most two elements each, which implies that there are at most $2q$ points in $\{(u,v) : u^2 + \alpha uv + v^2 = 1\}$. We then must have $\left|\left\{(u,v) : u^2 + \alpha uv + v^2 = 1\right\}\right| = q+1$, It follows that $\mathrm{Im}(\det) = \mathbb{F}_q^*$ and that $\left|\left\{(u,v) : u^2 + \alpha uv + v^2 = d\right\}\right| = q+1$, for every $d \in \mathbb{F}_q^*$.

Hyperbolic Case: We eliminate the linear term as before. The equation $u^2 + \alpha uv + v^2 = d \in \mathbb{F}_q^*$ may be rewritten $(u + r_1 v)(u + r_2 v) = d$ for $r_1, r_2 \in \mathbb{F}_q^*$, where $r_1 r_2 = 1$, $r_1 + r_2 = \alpha$. Each possible solution satisfies $u + r_1 v = e$, $u + r_2 v = d/e$ for some $e \in \mathbb{F}_q^*$ and there are $q-1$ solutions.

Parabolic case. We may assume that $\alpha = 2$. If (α, β, γ) is non-singular then $0 \neq \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma - 4 = (\beta - \gamma)^2$. Our equation for counting is $x^2 + 2xy + y^2 + 2x - 2y + 1 = 0$. Setting $y = u - x$ in $x^2 + 2xy + y^2 - \beta x - \gamma y + 1 = 0$ we get $u^2 - \gamma u + 1 + (\gamma - \beta)x = 0$. There are q solutions to this equation, as there is a unique value of x for every value of u. ■

3.3. **Admissible trace triples.** We call a trace triple (α, β, γ) *admissible* if it is non-singular and the associated signature (l, m, n) is hyperbolic. Specifically, we must leave out the spherical signatures $(2, 2, n)$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$; and, the planar signatures $(2, 3, 6)$, $(2, 4, 4)$, $(3, 3, 3)$. Non-admissable (α, β, γ) cannot generate a hyperbolic action of $PSL_2(q)$ though admissible triples may generate a hyperbolic action of a proper subgroup. By Corollary 14 all action triples (a, b, c) corresponding to an admissible (α, β, γ) are generating action triples or generate a subgroup belonging to a single conjugacy class of proper subgroups. In the subgroup table below, we list all possible signatures for admissible trace triples that generate proper subgroups. The affine subgroups have no admissible trace triples. The dihedral groups can only have spherical signatures, and the subgroup A_4 has no hyperbolic signatures. Thus the projective subgroups $PSL_2(r)$, $PGL_2(r)$ and the exceptional subgroups Σ_4 and A_5 are the only proper groups that can be generated by an admissible trace triple.

Type	**Name**	**Order**	**Signatures**
affine - parabolic	$\mathbb{F}_q^* \ltimes \mathbb{F}_q$	$\frac{q(q-1)}{2}$	none
affine - hyperbolic	$\mathbb{F}_q^*$	$\frac{q-1}{2}$	none
affine - elliptic		$\frac{q+1}{2}$	none
projective	$PSL_2(r)$, $r \vert q$,	$r(r^2-1)/2$, $r(r^2-1)$	various
projective	$PGL_2(r)$, $r^2 \vert q$	$r(r^2-1)$	various
exceptional dihedral	D_{q-1}	$q-1$	none
exceptional dihedral	D_{q+1}	$q+1$	none
exceptional	$A_4 = PSL_2(3)$	12	none
exceptional	$\Sigma_4 = PGL_2(3)$	24	$(3, 4, 4)$
exceptional	$A_5 = PSL_2(5)$	60	$(2, 5, 5)$, $(3, 3, 5)$, $(3, 5, 5)$, $(5, 5, 5)$

Table 3.3 - Signatures for subgroups with admissible trace triples

Next we identify when trace triples generate projective subgroups.

Proposition 15. *Suppose that (α, β, γ) is a trace triple over $\mathbb{F}_q$ that determines determines a hyperbolic signature (l, m, n). Define e so that $\mathbb{F}_p[\alpha, \beta, \gamma] \backsimeq \mathbb{F}_{p^e}$ and $\mathbb{F}_{p^e} \subseteq F_q$. Then, for any other triple $(\alpha', \beta', \gamma')$ over any $\mathbb{F}_{p^s}$ that determines (l, m, n) we have*

$$\mathbb{F}_p[\alpha, \beta, \gamma] = \mathbb{F}_{p^e} = \mathbb{F}_p[\alpha', \beta', \gamma']$$

and e divides s. Moreover, there is at least one non-singular trace triple (α, β, γ) associated to (l, m, n).

Proof: First, consider an element a of order l. Then the order l divides p, $\frac{q-1}{2}$, or $\frac{q+1}{2}$ or in case $p = 2$, l divides one of 2, $q-1$, $q+1$. Let us deal with odd q first. If $PSL_2(q)$ has an element of order l then one of the following holds $l = p$, or $q = \pm 1 \bmod 2l$, i.e., $q^2 = 1 \bmod 2l$. If $l = p$, then $\alpha = \pm 2$ and set $e_l = 1$. Otherwise, the sequence of groups $PSL_2(p^s)$ with elements of order l is the set $\left\{PSL_2(p^s) : p^{2s} = 1 \bmod 2l\right\}$. Since p is invertible mod $2l$ the set of such integer exponents $\{s : p^{2s} = 1 \bmod 2l\}$ has the form $e_l\mathbb{Z}$ for some $e_l > 0$. So $PSL_2(q)$ can have an element of order l if and only if $\mathbb{F}_{p^{e_l}}$ is a subfield of $\mathbb{F}_q$. The subgroup $PSL_2(p^{e_l}) \subseteq PSL_2(q)$ has an element of U order l and hence $\mathrm{trace}(U) \in \mathbb{F}_{p^{e_l}}$.

By Proposition 10 the traces of covering elements of $PSL_2(q)$ of order l lie in $\mathbb{F}_{p^{e_l}}$; in fact, they individually generate $\mathbb{F}_{p^{e_l}}$. Define e_m and e_n similarly, and let $e = \operatorname{lcm}(e_l, e_m, e_n)$. Then the components of every trace triple $(\alpha', \beta', \gamma')$ with associated signature (l, m, n) of $PSL_2(q)$ lie in $\mathbb{F}_{p^e}$; in fact, $\mathbb{F}_{p^e} = \mathbb{F}_p[\alpha', \beta', \gamma']$. The proof for $p = 2$ is entirely similar.

Now we find a non-singular trace triple. Holding β, γ fixed, a singular trace triple must satisfy

$$p_{\beta,\gamma}(\alpha) = \alpha^2 - (\beta\gamma)\alpha + (\beta^2 + \gamma^2 - 4) = 0, \tag{36}$$

a quadratic equation in α. According to Proposition 10, unless the Euler function value $\phi(l) \le 2$ or $l = p$, there is an element A projecting to an element a of order l such that $p_{\beta,\gamma}(\mathrm{trace}(A)) \neq 0$. But $\phi(l) > 2$ unless $l = 2, 3, 4, 6$. Thus, assuming $p \neq 2, 3$, we must choose l from $\{2, 3, 4, 6, p\}$. By a similar argument, the same applies to m and n. The squares of the traces $\tau = \alpha, \beta, \gamma$ for $r = l, m, n$, respectively, would then have the values in the following table:

r	2	3	4	6	p
τ^2	0	1	2	3	4

Assuming that all the triples (α, β, γ) are singular, then

$$2\alpha\beta\gamma = p_{\beta,-\gamma}(\alpha) - p_{\beta,\gamma}(\alpha) = 0.$$

For the moment assume that p is odd. Since at most one of l, m, n can equal 2 by hyperbolicity, we may assume that $2\beta\gamma \neq 0$ and, hence, $\alpha = 0$ and $l = 2$. The possible hyperbolic triples are then $(2, 3, p)$, $(2, 4, 6)$, $(2, 4, p)$, $(2, 6, 6)$, $(2, 6, p)$, and $(2, p, p)$. The singular triple equation now becomes $\beta^2 + \gamma^2 = 4$, which cannot hold for any of these triples. If $p = 2$ then l, m, n must be chosen from $2, 3$ and there are no hyperbolic triples. For $p = 3$ they must be chosen from $2, 3, 4$ and there are no hyperbolic triples with $l = 2$. ■

Remark 16. *Using the above proof, we can immediately generalize the well known classification of Hurwitz surfaces with $PSL_2(p^e)$ as automorphism group (see [18]). There is a Hurwitz action of $PSL_2(p)$ if and only if $p = 7$, or $p = \pm 1 \bmod 7$. The only action of $PSL_2(p^e)$ for $e > 1$ is $PSL_2(p^3)$ where $p^3 = \pm 1 \bmod 7$, but $p \neq \pm 1 \bmod 7$.*

Corollary 17. *Let (l, m, n) be a hyperbolic triple. Then for every p there is an integer e, dependent on l, m, n and p, such that $PSL_2(p^e)$ has an (l, m, n) action on a surface. However, there is no (l, m, n) action for $PSL_2(p^{e'})$ where $e' \neq e$.*

Proof: As we saw previously, $PSL_2(p^e)$ has an action for $e = \operatorname{lcm}(e_l, e_m, e_n)$ defined in the preceding proof. For any other value of $q = p^{e'}$ divisible by p^e, all (l, m, n) triples (a, b, c) generate a proper subgroup of $PSL_2(q)$. ■

Finally, we give a complete description of all triples corresponding to lifts of a hyperbolic triple (a, b, c) in $PSL_2(q)$. It is convenient to split the even and odd cases into two separate propositions.

Proposition 18. *Suppose that q is odd. Let (a, b, c) in $PSL_2(q)$ be an (l, m, n)-triple and let $(A, B, C) \in Tr(\alpha, \beta, \gamma)$ be a covering triple. Let $G = PSL_2(q)$ and $L = PGL_2(q)$, considered as automorphism groups of $PSL_2(q)$. Let $Tr(\alpha', \beta', \gamma')$*

be one of the disjoint sets $Tr(\pm\alpha, \pm\beta, \pm\gamma)$ (1, 2, 4, or 8 in number). Then we have the following.

(1) *The set $L_G(a, b, c)$ is the image of $\bigcup_{\alpha',\beta',\gamma'} Tr(\alpha', \beta', \gamma')$ under the map $(A', B', C') \to (a', b', c')$, $(A', B', C') \in Tr(\alpha', \beta', \gamma')$.*

(2) *Suppose that (a, b, c) has a hyperbolic signature. Then, at most, one of α, β, γ is zero and the projection $(A', B', C') \to (a', b', c')$ is 1-1 when restricted to $Tr(\alpha', \beta', \gamma')$.*

(3) *Suppose that (A, B, C) is hyperbolic and non-singular. Then the image of $Tr(\alpha, \beta, \gamma)$ is a single $PGL_2(q)$ class of triples. If $\langle a, b, c\rangle$ is a proper subgroup of $PSL_2(q)$, then the signature must occur in Table 3.3.*

(4) *Suppose that (A, B, C) is hyperbolic, non-singular and $\alpha\beta\gamma \neq 0$, so that there are eight disjoint sets among the $Tr(\pm\alpha, \pm\beta, \pm\gamma)$. Then we have these two cases:*
   (a) *Both lift orbits in $Tr(\pm\alpha, \pm\beta, \pm\gamma)$ correspond to non-singular triples, and there are two disjoint $PGL_2(q)$ classes in $L_G(a, b, c)$.*
   (b) *One lift orbit $Tr(\pm\alpha, \pm\beta, \pm\gamma)$ consists of non-singular triples and the other does not. The set $L_G(a, b, c)$ contains a single $PGL_2(q)$ class of non-singular triples. All the other triples generate proper affine subgroups.*

(5) *Suppose that (A, B, C) is hyperbolic, non-singular and $\alpha\beta\gamma = 0$ so that there are only four disjoint sets among the $Tr(\pm\alpha, \pm\beta, \pm\gamma)$. Then, assuming that $l \leq m \leq n$, we have $l = 2$, $\alpha = 0$, and $DQ(\alpha, \beta, \gamma) = \beta^2 + \gamma^2 - 4 \neq 0$. All four triple sets $Tr(\pm\alpha, \pm\beta, \pm\gamma)$ comprise a lift orbit, and $L_G(a, b, c)$ is a single $PGL_2(q)$ class of non-singular triples.*

Proposition 19. *Suppose that q is even. Let $G = PSL_2(q) = SL_2(q)$ and $L = PGL_2(q)$, considered as automorphism groups of $PSL_2(q)$. Let (A, B, C) in $SL_2(q)$ be an (l, m, n)-triple.*

(1) *Suppose that (A, B, C) has a hyperbolic signature. Then, at most one of α, β, γ is zero.*

(2) *Suppose that (A, B, C) is hyperbolic and non-singular. $Tr(\alpha, \beta, \gamma)$ is a single $PGL_2(q)$ class of triples. If $\langle A, B, C\rangle$ is a proper subgroup of $SL_2(q)$, then the signature must occur in Table 3.3.*

Proof: For Proposition 18 we argue as follows.

Statement 1. This follows from the discussion on Schur covers in Section 2.4.

Statement 2. As noted in Remark 11, at most one of α, β, γ can be zero for a hyperbolic signature. Next let us show that the projection $(A, B, C) \to (a, b, c)$ is 1-1 when restricted to $Tr(\alpha, \beta, \gamma)$. Any cover (A', B', C') of (a, b, c) must satisfy $A' = \pm A, B' = \pm B$, $C' = \pm C$. If, for instance, $A' = -A$, then $\alpha = \text{trace}(A') = -\text{trace}(A) = -\alpha$, and so $\alpha = 0$. Since $\beta, \gamma \neq 0$ then $B' = B$ and $C' = C$. But $I = A'B'C' = -ABC = -I$, a contradiction.

Statement 3. This is Corollary 14.

Statements 4 and 5. As noted in Remark 11, the transformation

$$(A, B, C) \to (-A, -B, C)$$

carries $Tr(\alpha, \beta, \gamma)$ to $Tr(-\alpha, -\beta, \gamma)$ and preserves the form $DQ(\alpha, \beta, \gamma) = \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma - 4$. With similar arguments, we see that the entire lift orbit consists of non-singular triples if (α, β, γ) is non-singular. The entire lift orbit determines the same $PGL_2(q)$ class $L_G(a, b, c)$. If the other lift orbit is non-singular, we get a second $PGL_2(q)$ in $L_G(a, b, c)$ disjoint from the first, according to Remark 11. If $\alpha\beta\gamma \neq 0$ then we cannot have both $DQ(\alpha, \beta, \gamma)$ and $DQ(-\alpha, \beta, \gamma)$ equal to 0. For then $2\alpha\beta\gamma = DQ(\alpha, \beta, \gamma) -$ $DQ(-\alpha, \beta, \gamma) = 0$. The rest of the statements follow easily.

For Proposition 19 the arguments are similar. ■

Theorem 20. *Every quasi-platonic action of $PSL_2(p)$ on a surface of genus $\sigma \geq 2$ is determined by a unique lift orbit representative of a trace triple (α, β, γ) satisfying the following conditions:*

1. *the corresponding signature (l, m, n) is hyperbolic, non-singular, and $l \leq m \leq n$;*
2. *there is an (A, B, C) in $Tr(\alpha, \beta, \gamma)$ such that $|\langle A, B, C\rangle| = |PSL_2(q)|$; and,*
3. *the generating triple for the action is (a, b, c), the projection of (A, B, C) into $PSL_2(p)$.*

To formulate the theorem for composite q, we need the following proposition.

Proposition 21. *The action of $Gal(\mathbb{F}_q)$ on the generating non-singular hyperbolic trace triples has no fixed points.*

Proof: The action of $\mathrm{Gal}(\mathbb{F}_q)$ on trace triple sets is

$$Tr(\alpha, \beta, \gamma) \to Tr(\rho(\alpha), \rho(\beta), \rho(\gamma))$$

for $\rho \in \mathrm{Gal}(\mathbb{F}_q)$. Thus, $\mathrm{Gal}(\mathbb{F}_q)$ permutes the trace triple sets. Also

$$DQ(\rho(\alpha), \rho(\beta), \rho(\gamma)) = \rho\left(DQ(\alpha, \beta, \gamma)\right)$$

so that $Tr(\alpha, \beta, \gamma)$ permutes the non-singular trace triple sets. Additionally, $\mathrm{Gal}(\mathbb{F}_q)$ normalizes the $PGL_2(q)$ conjugation action so that $\mathrm{Gal}(\mathbb{F}_q)$ permutes the $PGL_2(q)$ orbits of triples (A, B, C). Now suppose that $(\rho(\alpha), \rho(\beta), \rho(\gamma)) = (\alpha, \beta, \gamma)$ for a non-singular triple. Then $\rho \cdot (A, B, C) = (\rho(A), \rho(B), \rho(C)) \in Tr(\alpha, \beta, \gamma)$ and so there is a $U \in GL_2(q)$ such that $\rho \cdot (A, B, C) = Ad_U \cdot (A, B, C)$. Then $\rho \circ Ad_{U^{-1}}$ fixes (A, B, C), so $\rho = Ad_U$ and thus $\rho = Ad_U = 1$. ■

Let $J \leq \langle \pm I\rangle^3$ be the subgroup defining the lift orbits. Then $\mathrm{Gal}(\mathbb{F}_q) \times J$ acts without fixed points on non-singular hyperbolic trace triples.

Theorem 22. *Let notation be as in Theorem 22 except that we consider $PSL_2(q)$ actions. Then the conclusion of Theorem 22 holds except that we consider $Gal(\mathbb{F}_q) \times$ J orbit representatives on non-singular hyperbolic trace triples.*

4. Sample quasi-platonic actions of $PSL_2(q)$

In this section, we determine all actions for $q = 7, 8$; give interesting partial results for some other small primes; and give a table of the number of actions for values of $q \leq 50$ and $q = 2^6, q = 3^4$. Finally, we determine all $(2, 3, n)$, $(2, 4, n)$, $(2, 6, n)$, and $(3, 3, n)$ actions as these capture almost all genus actions and correspond to families with the small tiling polygons and large actions.

All calculations, except the families, can be completed using MAGMA [19], following these steps.

(1) Find all orders of elements of $PSL_2(q)$ and then all possible hyperbolic signatures, (l, m, n) with $l \leq m \leq n$.
(2) Determine the trace order map $\mathbb{F}_q \to \{PSL_2(q)$ orders$\}$.
(3) For each (l, m, n) in Step 1, construct the set of associated trace triples, using the map constructed in Step 2.
(4) For odd q, select one trace triple from each lift orbit.
(5) Eliminate all singular trace triples.
(6) For each trace triple remaining, construct a triple (A, B, C) and compute the size of $\langle A, B, C\rangle$. Reject those triples for which $|\langle A, B, C\rangle| \neq |SL_2(q)|$.

Example 23. *Let $G = PSL_2(7)$ The orders of elements and the corresponding traces of covering elements are given in the order-trace table following.*

order	2	3	4	7
traces	0	± 1	± 3	± 2

The table of actions follows. Each line gives the signature, a representative trace triple, and the genus for each action class. The notes column describes situations when the number of actions is less than expected for a given signature.

(l, m, n)	(α, β, γ)	*genus*	*notes*
$(2, 3, 7)$	$(0, 1, 2)$	3	
$(2, 4, 7)$	$(0, 3, 2)$	10	
$(2, 7, 7)$	$(0, 2, 2)$	19	
$(3, 3, 4)$	$(1, 1, 3), (1, 1, 4)$	8	
$(3, 3, 7)$	$(1, 1, -2)$	17	$(1, 1, 2)$ *is singular*
$(3, 4, 4)$	$(-1, 3, 3)$	15	$(1, 3, 3)$ *yields* Σ_4
$(3, 4, 7)$	$(1, 3, 2), (1, 3, -2)$	24	
$(3, 7, 7)$	$(1, 2, 2), (-1, 2, 2)$	33	
$(4, 4, 4)$	$(3, 3, 3), (3, 3, 4)$	22	
$(4, 4, 7)$	$(3, 3, -2)$	31	$(3, 3, 2)$ *is singular*
$(4, 7, 7)$	$(3, 2, 2), (-3, 2, 2)$	40	
$(7, 7, 7)$	$(2, 2, -2)$	49	$(2, 2, 2)$ *is singular*

Table 4.1 $PSL_2(7)$ actions

Remark 24. *We observe from the preceding example that the signature $(3, 3, 7)$ has half of its trace triples singular and the other half non-singular. This holds for all $PSL_2(p)$. For, the two trace triples are $(1, 1, 2)$ and $(1, 1, -2)$. The first is singular and the second is non-singular. For the non-singular triple the only possible proper subgroups with an element of order p are the parabolic affine subgroups and the full $PSL_2(p)$. So the group must be $PSL_2(p)$. Similar remarks apply to the (p, p, p) signature and the trace triples $(2, 2, 2)$ and $(2, 2, -2)$.*

Example 25. *Let $G = PSL_2(8)$ The orders of elements and the corresponding traces of covering elements are given. We write $\mathbb{F}_8 = \mathbb{F}_2[w]$ where w is a generator of the cyclic group $\mathbb{F}_8^*$, and construct the order-trace table.*

order	2	3	7	9
traces	0	1	w^3, w^5, w^6	w, w^2, w^4

The table of actions follows. We do not have to worry about the sign action on triples, though $\mathrm{Out}(G)$ *is now generated by the Frobenius action $z \to z^2$ on $\mathbb{F}_8$.*

The table organization is as in Table 4.1. There are no projective or exceptional subgroups with hyperbolic signatures.

(l,m,n)	(α,β,γ)	*genus*	*notes*
$(2,3,7)$	$(0,1,w^3)$	7	
$(2,3,9)$	$(0,1,w^2)$	15	
$(2,7,7)$	$(0,w^3,w^5),(0,w^3,w^6)$	55	$(0,w^3,w^3)$ *is singular*
$(2,7,9)$	$(0,w^3,w),(0,w^3,w^2),(0,w^3,w^4)$	63	$(0,w,w)$ *is singular*
$(2,9,9)$	$(0,w,w^2),(0,w,w^4)$	71	$(0,w,w)$ *is singular*
$(3,3,7)$	$(1,1,w^3)$	41	
$(3,3,9)$	$(1,1,w)$	57	
$(3,7,7)$	$(1,w^3,w^3),(1,w^3,w^5),(1,w^3,w^6)$	97	
$(3,7,9)$	$(1,w^3,w),(1,w^3,w^2),(1,w^3,w^4)$	105	
$(3,9,9)$	$(1,w,w)$	113	*6 singular classes*
$(7,7,7)$	$(w^3,w^3,w^5),(w^3,w^3,w^6),$ $(w^3,w^5,w^3),(w^3,w^6,w^3)$	145	*5 singular classes*
$(7,7,9)$	$(w^a,w^b,w),a,b=3,5,6$	153	
$(7,9,9)$	$(w^3,w^a,w^b),a,b=1,2,4$	161	
$(9,9,9)$	$(w,w,w),(w,w,w^4),\ (w,w^2,w^2)$ $(w,w^2,w^4),(w,w^4,w),\ (w,w^4,w^2)$	169	*3 singular classes*

Table 4.2 $PSL_2(8)$ *actions*

Example 26. *Let* G *be one of* $PSL_2(11)$, $PSL_2(13)$, $PSL_2(32)$, $PSL_2(47)$. *The orders of elements and the corresponding traces of covering elements are given below.*

$q=11,$

order	2	3	5	6	11
traces	0	±1	$\pm3,\pm4$	±5	±2

$q=13,$

order	2	3	6	7	13
traces	0	±1	±4	$\pm3,\pm5,\pm6$	±2

$q=32,$

order	2	3	11	31	33
traces	0	1	5 vals	15 vals	10 vals

$q=47,$

order	2	3	4	6	8	12	23	24	47
traces	0	±1	±7	±14	4 vals	4 vals	22 vals	8 vals	±2

$q=49,$

order	2	3	4	5	6	7	8	12	24	25
traces	0	±1	±3	4 vals	2 vals	±2	4 vals	4 vals	8 vals	20 vals

There are too many hyperbolic, non-singular trace triples to list, but we write down a few of interest. Of special interest are the signatures with proper subgroup actions *and equilateral signatures ($l = m = n$) with many actions.*

q	$\|PSL_2(q)\|$	$(\mathbf{l}, \mathbf{m}, \mathbf{n})$	*# admissible trace triples*	*number of actions*	*proper subgroup*	*genus*
11	660	$(2, 5, 5)$	16	2	2 (A_5)	34
11	660	$(3, 3, 5)$	16	2	2 (A_5)	45
11	660	$(3, 5, 5)$	32	4	4 (A_5)	89
11	660	$(5, 5, 5)$	40	8	2 (A_5)	133
13	1092	$(7, 7, 7)$	156	39	0	313
32	32736	$(31, 31, 31)$	2940	518	0	14785
47	51888	$(3, 3, 4)$	8	1	1 (Σ_4)	4325
47	51888	$(23, 23, 23)$	9724	2431	0	22561
49	58800	$(2, 3, 7)$	4	0	1 ($PSL_2(7)$)	701
49	58800	$(2, 3, 8)$	8	0	2 ($PGL_2(7)$)	701

Table 4.3 Other Sample Actions

Example 27. *Next, we give a summary table for all q in the range $5 \leq q \leq 49$ and the prime powers $64 = 2^6$ and $81 = 3^4$.*

q	$\|PSL_2(q)\|$	orders	signatures	actions	min genus	max genus
5	60	3	4	5	4	13
7	168	4	12	17	3	49
$8 = 2^3$	504	4	14	46	7	169
$9 = 3^2$	360	4	10	18	10	73
11	660	5	26	72	26	241
13	1092	5	27	162	14	421
$16 = 2^4$	4080	5	27	341	205	1681
17	2448	6	46	329	52	1009
19	3420	6	47	441	96	1441
23	6072	7	72	901	231	2641
$25 = 5^2$	7800	7	71	618	326	3001
$27 = 3^3$	9828	5	28	542	118	3862
29	12180	7	74	1578	146	5461
31	14880	8	107	1897	311	6721
$32 = 2^5$	32736	5	28	2370	1241	14881
37	25308	7	74	4302	704	11629
41	34440	9	151	4385	411	15961
43	39732	7	75	5517	474	18481
47	51888	9	151	8443	1082	24289
$49 = 7^2$	58880	10	175	4247	1471	25873
$64 = 2^6$	262080	9	135	13332	11761	124993
$81 = 3^4$	265680	9	122	11672	15499	123121

Table 4.3 Enumeration of actions for selected $PSL_2(q)$

Example 28. *Let us determine $(2, 3, n)$, $(2, 4, n)$, $(2, 6, n)$, and $(3, 3, n)$ actions. The discussion that follows may need small adjustments for even q. Using the table* *in the proof of Proposition 15, the trace triples (α, β, γ) may be assumed to have the following form by selecting an appropriate lift orbit representative. In the last row we assume that $n \neq p$.*

(l, m, n)	$(2, 3, n)$	$(2, 4, n)$	$(2, 6, n)$	$(3, 3, n)$
condition on n	$n \geq 7$	$n \geq 5$	$n \geq 4$	$n \geq 4$
(α, β, γ)	$(0, 1, \gamma)$	$(0, \sqrt{2}, \gamma)$	$(0, \sqrt{3}, \gamma)$	$(1, 1, \gamma)$
$QD(\alpha, \beta, \gamma)$	$\gamma^2 - 3$	$\gamma^2 - 2$	$\gamma^2 - 1$	$(\gamma - 2)(\gamma + 1)$
#projective action classes	$\frac{\phi(n)}{2e}$	$\frac{\phi(n)}{2e}$	$\frac{\phi(n)}{2e}$	$\frac{\phi(n)}{e}$

There are no singular triples that yield hyperbolic signatures. If $n = p$, then $QD(\alpha, \beta, \gamma) \neq 0$ except in the case $(3, 3, p)$. There is exactly one automorphism class in each case. The split nature of the $(3, 3, p)$ actions was noted in the $PSL_2(7)$ discussion.

Now suppose that $n \neq p$, so that c is semi-simple. Recall that $PSL_2(q)$ has a semi-simple element of order n iff $q^2 = 1 \mod 2n$. There are $\phi(n)$ possible traces for elements of that project to elements of order n. However, the trace triple sets $Tr(0, \beta, \gamma)$ and $Tr(0, \beta, -\gamma)$ project to the same projective class, whereas $Tr(1, 1, \gamma)$ and $Tr(1, 1, -\gamma)$ project to different projective classes. Thus we get $\phi(n)/2$ projectively inequivalent actions in the first three cases and $\phi(n)$ projectively inequivalent $(3, 3, n)$ actions. Furthermore, all of these traces belong to the same minimal field $\mathbb{F}_{p^e}$. So all the actions occur only for $PSL_2(p^e)$. After accounting for the Galois action we obtain the number of actions listed in the table. This example extends the well known result that $PSL_2(p)$ has three inequivalent Hurwitz actions when $p = \pm 1 \bmod 7$ and exactly $PSL_2(p^3)$ action when $p \neq \pm 1 \bmod 7$.

5. Galois action on $PSL_2(q)$ dessins

5.1. **The Galois action in the general case.** Given a quasi-platonic G action on a surface S there is a projection $\pi_G : S \to S/G = \widehat{\mathbb{C}}$ which we may assume is branched over $\{0, 1, \infty\}$. Any such map $\beta : S \to \widehat{\mathbb{C}}$ branched over $\{0, 1, \infty\}$ is called a Belyi function; it is called regular if $\beta = \pi_G$ is induced by a group action of some group G. According to Belyi's theorem, [1], S can be defined over a number field as long as there is a Belyi function of any type. The intersection of all such defining fields is called the *moduli field* of S. It can be shown that S has a defining equation over its moduli field (see [11]), and we shall assume that S is defined over its moduli field for the remainder of the paper.

If $\psi \in \mathrm{Gal}(\mathbb{C})$, then we define S^ψ to be the Riemann surface obtained by applying ψ to the coefficients of the defining equation(s) of S. There is an induced map, still denoted ψ, $\psi : S \to S^\psi$ by applying ψ coordinatewise. The map is a bijection, but definitely not a morphism. Since S is defined over a number field, the surface S^ψ only depends on the action of ψ on the algebraic closure of $\mathbb{Q}$. For any two affine or projective varieties X, Y and map $f : X \to Y$, we define X^ψ, Y^ψ, $\psi : X \to X^\psi$, and $\psi : Y \to Y^\psi$ in a similar fashion. The map $f^\psi : X^\psi \to Y^\psi$ is defined by $f^\psi(\psi(x)) = \psi(f(x)), x \in X$ or $f^\psi = \psi f \psi^{-1}$. Consequently, for every automorphism g of S, g^ψ is an automorphism of S^ψ, and $g \to \psi g \psi^{-1}$ is an isomorphism of $\mathrm{Aut}(S)$ to $\mathrm{Aut}(S^\psi)$. If $\epsilon : G \to \mathrm{Aut}(S)$ defines the G-action, then $\epsilon^\psi : g \to \epsilon(g)^\psi$ is a G-action on S^ψ, the quotient map $\pi_G^\psi : S^\psi \to S^\psi/G$, is branched over $\{0, 1, \infty\}$ and the following diagram commutes.

$$\begin{tikzcd} S \arrow[r, "\psi"] \arrow[d, "\pi_G"'] & S^\psi \arrow[d, "\pi_G^\psi"] \\ \widehat{\mathbb{C}} \arrow[r, "\psi"] & \widehat{\mathbb{C}} \end{tikzcd} \tag{37}$$

Observe that ψ fixes $0, 1, \infty \in \widehat{\mathbb{C}}$ so that ψ maps the G ramification points on S to those on S^ψ. Specifically,

$$\begin{aligned} \pi_G^{-1}(0) &\overset{\psi}{\to} \left(\pi_G^\psi\right)^{-1}(0) \\ \pi_G^{-1}(1) &\overset{\psi}{\to} \left(\pi_G^\psi\right)^{-1}(1) \\ \pi_G^{-1}(\infty) &\overset{\psi}{\to} \left(\pi_G^\psi\right)^{-1}(\infty) \end{aligned} \tag{38}$$

are bijections. We will call ϵ^ψ the ψ Galois transform of ϵ.

Remark 29. *The diagram 37 and the equations 38 hold with π_G replaced by any Belyi function β. A new dessin or bipartite graph is created between the isomorphic images $\psi(\beta^{-1}(0))$ and $\psi(\beta^{-1}(1))$ by removing and reconnecting the arcs of the dessin according to the new Belyi function β^ψ. The new dessin captures the geometry of S^ψ. This approach is needed when there is no group action. We shall phrase everything in terms of the group actions and tilings on S and S^ψ. There is always a cover $S' \to S$ which carries a regular dessin.*

Without actually knowing the equations of S and S^ψ, we can determine the action of ψ on rotation numbers, information we shall use shortly. Let a non-trivial automorphism $g \in \operatorname{Aut}(S)$ fix the point $x_0 \in S$ and let f be any function that vanishes at x_0 to order 1. Then, $f \circ g = \operatorname{rot}(g, x_0) f + k$ where k vanishes at x_0 with order 2 or greater. Now apply ψ to get

$$g^\psi(\psi(x_0)) = \psi g \psi^{-1}(\psi(x_0)) = \psi(x_0),$$

and

$$f^\psi \circ g^\psi = \psi\left(\operatorname{rot}(g, x_0)\right) f^\psi + k^\psi,$$

and k^ψ vanishes at $\psi(x_0)$ with order 2 or greater. We see that g^ψ fixes $\psi(x_0)$ and

$$\operatorname{rot}(g^\psi, \psi(x_0)) = \psi(\operatorname{rot}(g, x_0)). \tag{39}$$

Now let $N > 1$ be any integer and $\zeta = \exp(2\pi i/N)$. The cyclotomic field $\mathbb{Q}[\zeta]$ is a normal subfield of $\mathbb{C}$, and the action of ψ on $\mathbb{Q}[\zeta]$ is given by $\zeta \to \zeta^s$ for some number s relatively prime to N. Applying equation 39 to $h = \epsilon(g)$ we get

$$\operatorname{rot}(\epsilon^\psi(g), \psi(x_0)) = (\operatorname{rot}(\epsilon(g), x_0))^s. \tag{40}$$

Now we work out the Galois action on epimorphisms. There are epimorphisms

$$\begin{aligned} \eta_1 &: T_{l,m,n} \to G,\ A \to a_1,\ B \to b_1,\ C \to c_1 \\ \eta_2 &: T_{l,m,n} \to G,\ A \to a_2,\ B \to b_2,\ C \to c_2, \end{aligned}$$

such that η_1 uniformizes the ϵ action on S, with generating vector (a_1, b_1, c_1); and η_2 uniformizes the ϵ^ψ action on S^ψ with generating vector (a_2, b_2, c_2). Following the discussion in Section 2; let $\triangle\overline{DEF}$ be a triangle in S determining the triple (a_1, b_1, c_1) and let $\triangle\overline{D'E'F'}$ be a triangle in S^ψ determining (a_2, b_2, c_2). Since

$G \cdot \overline{D} = \pi_G^{-1}(0)$ and $G \cdot \overline{D}' = \left(\pi_G^{\psi}\right)^{-1}(0)$, (equation 38) then there is a $u \in G$, so that $\psi(u\overline{D}) = \overline{D'}$, and the stabilizer of $\overline{D}'$ is $u\langle a_1\rangle u^{-1}$. To determine the element $a_2 \in u\langle a_1\rangle u^{-1}$ we work with rotation numbers. To this end, let $N = \mathrm{lcm}(l,m,n)$ and $\zeta = \exp(2\pi i/N)$ as above. Then the cyclotomic field $\mathbb{Q}[\zeta]$ contains the rotation numbers of a_1, b_1, c_1. Let t be an integer such that $st = 1 \bmod N$. Then

$$\begin{aligned}\mathrm{rot}(\epsilon^{\psi}(ua_1^t u^{-1}), \overline{D'}) &= (\mathrm{rot}(\epsilon(ua_1^t u^{-1}), u\overline{D}))^s\\ &= (\mathrm{rot}(\epsilon(a_1), \overline{D}))^{st}\\ &= \exp\left(\frac{2\pi i}{l}\right);\end{aligned}$$

and similarly $\mathrm{rot}(\epsilon^{\psi}(vb_1^t v^{-1}), \overline{E'}) = \exp\left(\frac{2\pi i}{m}\right)$, $\mathrm{rot}(\epsilon^{\psi}(wc_1^t w^{-1}), \overline{E'}) = \exp\left(\frac{2\pi i}{m}\right)$. It follows that $(a_2, b_2, c_2) = (ua_1^t u^{-1}, vb_1^t v^{-1}, wc_1^t w^{-1})$. We summarize the preceding discussion by the following theorem. It is known as the branch cycle argument and a proof is given as Lemma 2.8 in [21].

Theorem 30. *Let $\eta_1 : T_{l,m,n} \to G,\ A \to a_1,\ B \to b_1,\ C \to c_1$ be an epimorphism defining an (l,m,n) G-action on the Riemann surface S. Let $\psi \in \mathrm{Gal}(\mathbb{C})$, $N = \mathrm{lcm}(l,m,n)$, $\zeta = \exp(2\pi i/N)$, and suppose that $\psi(\zeta) = \zeta^s$. Select t so that $st = 1 \bmod N$. Then the ϵ^{ψ}, the ψ Galois transform action on S^{ψ}, is induced by $\eta_2 : T_{l,m,n} \to G,\ A \to a_2,\ B \to b_2,\ C \to c_2$, such that*

$$(a_2, b_2, c_2) = (ua_1^t u^{-1}, vb_1^t v^{-1}, wc_1^t w^{-1}) \tag{41}$$

for some $u, v, w \in G$. Moreover, $a_2b_2c_2 = 1$ and $G = \langle a_2, b_2, c_2\rangle$.

Remark 31. *As discussed in Section 2,we have $(a_1, b_1, c_1) \in K_G^{\circ}(a_1, b_1, c_1)$ and $(a_2, b_2, c_2) \in K_G^{\circ}(a_1^t, b_1^t, c_1^t)$. We shall see below that both $K_G^{\circ}(a_1, b_1, c_1)$ and also $K_G^{\circ}(a_1^t, b_1^t, c_1^t)$ have exactly the same number of elements. However, because of the possible presence of companion orbits in $K_G^{\circ}(a_1^t, b_1^t, c_1^t)$ the action determined by equation 41 may not be uniquely identifiable in $K_G^{\circ}(a_1^t, b_1^t, c_1^t)$. So we shall call $K_G^{\circ}(a_1^t, b_1^t, c_1^t)$ a* Galois $t-$target. *We can use covers of $SL_2(q)$ to resolve the indeterminacy.*

There is no simple formula for (a_2, b_2, c_2) known to the author and the triple needs to be found computationally. Indeed, it is not immediately apparent that the Galois t-target $K_G^{\circ}(a_1^t, b_1^t, c_1^t)$ is non-empty from simple group theoretic considerations. We demonstrate that $K_G^{\circ}(a_1^t, b_1^t, c_1^t)$ is non-empty in a non-constructive way using character theory. The field automorphism $\psi^{-1} \in \mathrm{Gal}(\mathbb{C})$ act by $\zeta \to \zeta^t$ on the primitive Nth roots of unity. For any representation $\rho : G \to GL_k(\mathbb{C})$ the eigenvalues of the matrices $\rho(a), \rho(b), \rho(c)$ are Nth roots of unity, and, so if χ is the character of ρ then.

$$\chi(a^t) = \psi^{-1}(\chi(a)), \chi(b^t) = \psi^{-1}(\chi(b)), \chi(c^t) = \psi^{-1}(\chi(c)).$$

Applying this to equation 21 it follows then that

$$\begin{aligned}
\left|K_G(a^t,b^t,c^t)\right| &= \frac{|G|^2}{|\mathrm{Cent}(a^t)|\cdot|\mathrm{Cent}(b^t)|\cdot|\mathrm{Cent}(c^t)|}\sum_{\chi}\frac{\chi(a^t)\chi(b^t)\chi(c^t)}{\chi(1)}\\
&= \frac{|G|^2}{|\mathrm{Cent}(a)|\cdot|\mathrm{Cent}(b)|\cdot|\mathrm{Cent}(c)|}\sum_{\chi}\frac{\psi^{-1}\left(\chi(a)\chi(b)\chi(c)\right)}{\chi(1)}\\
&= \psi^{-1}\left(\frac{|G|^2}{|\mathrm{Cent}(a)|\cdot|\mathrm{Cent}(b)|\cdot|\mathrm{Cent}(c)|}\sum_{\chi}\frac{\chi(a)\chi(b)\chi(c)}{\chi(1)}\right)\\
&= \psi^{-1}\left(|K_G(a,b,c)|\right) = |K_G(a,b,c)|\,.
\end{aligned}$$

Using formulas similar to equation 18 we deduce

$$\left|K_G^\circ(a^t,b^t,c^t)\right| = |K_G^\circ(a,b,c)|\,. \tag{42}$$

Separating companion actions with a Schur cover. Now we use lifts to a Schur cover discussed in Section 2.4 to resolve Galois t-target indeterminacy. Let $\widetilde{S}$ be a surface upon which $\widetilde{G}$ acts with signature $(\widetilde{l},\widetilde{m},\widetilde{n})$, and generating vector $(\widetilde{a},\widetilde{b},\widetilde{c})$. Then $G=\widetilde{G}/Z$ has a natural (l,m,n) action on $S=\widetilde{S}/Z$ with generating vector (a,b,c). We have the following diagram

$$\begin{tikzcd}
\widetilde{S} \arrow[r, "\psi"] \arrow[d, "\pi_Z"] & \widetilde{S}^{\psi} \arrow[d, "\pi_Z^{\psi}"] \\
S \arrow[r, "\psi"] \arrow[d, "\pi_G"] & S^{\psi} \arrow[d, "\pi_G^{\psi}"] \\
\widehat{\mathbb{C}} \arrow[r, "\psi"] & \widehat{\mathbb{C}}
\end{tikzcd} \tag{43}$$

where the composite maps on the left and right columns are $\pi_{\widetilde{G}}$ and $\pi^{\psi}_{\widetilde{G}}$.

Remark 32. *The map π_Z is a $|Z|$-fold branched cover of the $\widetilde{G}$ dessin to the G dessin. The cover is 1-1 on arcs and has ramification degrees $\widetilde{l}/l$, $\widetilde{m}/m$ and $\widetilde{n}/n$ over $\pi_G^{-1}(0)$, $\pi_G^{-1}(1), \pi_G^{-1}(\infty)$ respectively. Once this is understood combinatorially, the two dessins can be completed to surfaces by gluing in the appropriate polygons.*

Now suppose we are lucky enough to have $K_G^\circ(\widetilde{a},\widetilde{b},\widetilde{c})$ be a single $\widetilde{G}$ orbit. Define $\widetilde{N}$, $\widetilde{s},\widetilde{t}$ as in Theorem 30. Then the Galois transform of $(\widetilde{a},\widetilde{b},\widetilde{c})$ is

$$\left(\widetilde{u}\widetilde{a}^{\widetilde{t}}\widetilde{u}^{-1},\widetilde{v}\widetilde{b}^{\widetilde{t}}\widetilde{v}^{-1},\widetilde{w}\widetilde{c}^{\widetilde{t}}\widetilde{w}^{-1}\right)$$

for suitable elements. By equation 42, the Galois t target has a unique $\widetilde{G}$ orbit. We now just apply π to $\left(\widetilde{u}\widetilde{a}^{\widetilde{t}}\widetilde{u}^{-1},\widetilde{v}\widetilde{b}^{\widetilde{t}}\widetilde{v}^{-1},\widetilde{w}\widetilde{c}^{\widetilde{t}}\widetilde{w}^{-1}\right)$ to find the action of a unique class for $(ua^tu^{-1},vb^tv^{-1},wc^tw^{-1})$. We can now state a theorem for computing the Galois action on $PSL_2(q)$ quasi-platonic actions.

Theorem 33. *Let ϵ be a quasi-platonic action of $PSL_2(q)$ determined by a generating (l,m,n) triple $(a_1,b_1,c_1)$and $\psi\in\mathrm{Gal}(\mathbb{C})$. Then the Galois transform ϵ^{ψ} with generating vector (a_2,b_2,c_2) may be determined as follows.*

1. *Select a covering triple $(\widetilde{a}_1,\widetilde{b}_1,\widetilde{c}_1)$ in $SL_2(q)$ and the corresponding action $\widetilde{\epsilon}$.*
2. *Determine the ψ transform $(\widetilde{a}_2,\widetilde{b}_2,\widetilde{c}_2)$ of $(\widetilde{a}_1,\widetilde{b}_1,\widetilde{c}_1)$ by Theorem 30.*

(3) *Project the ψ transform $(\widetilde{a}_2, \widetilde{b}_2, \widetilde{c}_2)$ by π*

$$(a_2, b_2, c_2) = \pi(\widetilde{a}_2, \widetilde{b}_2, \widetilde{c}_2).$$

5.2. **Galois action examples for $PSL_2(q)$.** As in the classification of actions we will just give examples instead of a comprehensive theorem. For the $PSL_2(7)$, $PSL_2(8)$ we the use the same table format as Tables 4.1 and 4.2 except the last column now contains the list of Galois orbit sizes. Every orbit of size one corresponds to a surface with rational coefficients.

(l, m, n)	(α, β, γ)	genus	Orbit Sizes
$(2, 3, 7)$	$(0, 1, 2)$	3	$\{1\}$
$(2, 4, 7)$	$(0, 3, 2)$	10	$\{1\}$
$(2, 7, 7)$	$(0, 2, 2)$	19	$\{1\}$
$(3, 3, 4)$	$(1, 1, 3), (1, 1, 4)$	8	$\{2\}$
$(3, 3, 7)$	$(1, 1, -2)$	17	$\{1\}$
$(3, 4, 4)$	$(-1, 3, 3)$	15	$\{1\}$
$(3, 4, 7)$	$(1, 3, 2), (1, 3, -2)$	24	$\{1\}$
$(3, 7, 7)$	$(1, 2, 2), (-1, 2, 2)$	33	$\{1, 1\}$
$(4, 4, 4)$	$(3, 3, 3), (3, 3, 4)$	22	$\{2\}$
$(4, 4, 7)$	$(3, 3, -2)$	31	$\{1\}$
$(4, 7, 7)$	$(3, 2, 2), (-3, 2, 2)$	40	$\{2\}$
$(7, 7, 7)$	$(2, 2, -2)$	49	$\{1\}$

Table 5.1 Galois action on $PSL_2(7)$ actions

(l, m, n)	(α, β, γ)	genus	Orbit Sizes
$(2, 3, 7)$	$(0, 1, w^3)$	7	$\{1\}$
$(2, 3, 9)$	$(0, 1, w^2)$	15	$\{1\}$
$(2, 7, 7)$	$(0, w^3, w^5), (0, w^3, w^6)$	55	$\{1, 1\}$
$(2, 7, 9)$	$(0, w^3, w), (0, w^3, w^2), (0, w^3, w^4)$	63	$\{3\}$
$(2, 9, 9)$	$(0, w, w^2), (0, w, w^4)$	71	$\{1, 1\}$
$(3, 3, 7)$	$(1, 1, w^3)$	41	$\{1\}$
$(3, 3, 9)$	$(1, 1, w)$	57	$\{1\}$
$(3, 7, 7)$	$(1, w^3, w^3), (1, w^3, w^5), (1, w^3, w^6)$	97	$\{3\}$
$(3, 7, 9)$	$(1, w^3, w), (1, w^3, w^2), (1, w^3, w^4)$	105	$\{3\}$
$(3, 9, 9)$	$(1, w, w), (1, w^2, w^2), (1, w^4, w^4)$	113	$\{1\}$
$(7, 7, 7)$	$(w^3, w^3, w^5), (w^3, w^3, w^6),$ $(w^3, w^5, w^3), (w^3, w^6, w^3)$	145	$\{1, 1, 1, 1\}$
$(7, 7, 9)$	$(w^a, w^b, w), a, b = 3, 5, 6$	153	$\{3, 3, 3\}$
$(7, 9, 9)$	$(w^3, w^a, w^b), a, b = 1, 2, 4$	161	$\{3, 3, 3\}$
$(9, 9, 9)$	$(w, w, w), (w, w, w^4),\ (w, w^2, w^2)$ $(w, w^2, w^4), (w, w^4, w),\ (w, w^4, w^2)$	169	$\{1, 1, 1, 1, 1, 1\}$

Table 5.2 Galois action on $PSL_2(8)$ actions

Before proceeding with the remaining examples, we characterize the size of the orbits of the Galois action.

Proposition 34. *For the Galois action of $Gal(\mathbb{C})$, on the hyperbolic (l, m, n) actions of $PSL_2(q)$ all orbits have the same size.*

Proof: Let (A, B, C) be any lift to $\widetilde{G} = SL_2(q)$ of a generating (l, m, n) triple (a, b, c). Let $(\widetilde{l}, \widetilde{m}, \widetilde{n})$ be the signature of (A, B, C) and set $N = \operatorname{lcm}(l, m, n)$ and $\widetilde{N} = \operatorname{lcm}(\widetilde{l}, \widetilde{m}, \widetilde{n})$. Consider the set $X^{\circ}_{\widetilde{G}}(\widetilde{l}, \widetilde{m}, \widetilde{n})$. It can be partitioned into disjoint projective classes

$$X^{\circ}_{\widetilde{G}}(\widetilde{l}, \widetilde{m}, \widetilde{n}) = \bigcup_{(A', B', C')} L^{\circ}_{\widetilde{G}}(A', B', C')$$

where $\left| L^{\circ}_{\widetilde{G}}(A', B', C') \right| = |PGL_2(q)|$ for various $(\widetilde{l}, \widetilde{m}, \widetilde{n})$ triples (A', B', C'). Two elements $U, V \in SL_2(q)$ have the same order if an only if they are power conjugate, $V = WU^tW^{-1}$ for some $W \in GL_2(q)$. Thus

$$(A', B', C') = (W_1A^{t_1}W_2^{-1}, W_2B^{t_2}W_2^{-1}, W_3C^{t_3}W_3^{-1}),$$

for some selection of t_i and W_i. By definition

$$L^{\circ}_{\widetilde{G}}(A', B', C') = L^{\circ}_{\widetilde{G}}(W_1A^{t_1}W_2^{-1}, W_2B^{t_2}W_2^{-1}, W_3C^{t_3}W_3^{-1}) = L^{\circ}_{\widetilde{G}}(A^{t_1}, B^{t_2}, C^{t_3}).$$

Then we see that the abelian group $\left(\mathbb{Z}^*_{\widetilde{N}}\right)^3$ acts on the $PGL_2(q)$ classes in $X^{\circ}_{\widetilde{G}}(\widetilde{l}, \widetilde{m}, \widetilde{n})$ by $L^{\circ}_{\widetilde{G}}(A, B, C) \to L^{\circ}_{\widetilde{G}}(A^{t_1}, B^{t_2}, C^{t_3})$. The action has a kernel containing $\langle \pm 1 \rangle^3$. The action of the absolute Galois group is simply the diagonal action of $\mathbb{Z}^*_{\widetilde{N}}$ on $X^{\circ}_{\widetilde{G}}(\widetilde{l}, \widetilde{m}, \widetilde{n})/PGL_2(q)$, namely $L^{\circ}_{\widetilde{G}}(A, B, C) \to L^{\circ}_{\widetilde{G}}(A^t, B^t, C^t)$. Since $\left(\mathbb{Z}^*_{\widetilde{N}}\right)^3$ acts transitively, then the Galois orbit space of $X^{\circ}_{\widetilde{G}}(\widetilde{l}, \widetilde{m}, \widetilde{n})/PGL_2(q)$ is the coset space of an appropriate homomorphic image of the pair $\left(\left(\mathbb{Z}^*_{\widetilde{N}}\right)^3, \mathbb{Z}^*_{\widetilde{N}}\right)$. The structure is independent of the type of lift chosen. The Galois orbit space structure maps $1-1$ onto a subset of the corresponding orbit space structure of $X^{\circ}_{G}(l, m, n)/PGL_2(q)$. ■

Example 35. *We consider again $(2, 3, n)$, $(2, 4, n)$, $(2, 6, n)$, and $(3, 3, n)$ actions, with $q \geq 7$.*

1. *Any q, $n = p$. There is only one action as previously discussed.*
2. *Odd q, $l = 2$, $n \neq p$. There are $\phi(n)/2$ projective classes of triples - note that $L^{\circ}_{\widetilde{G}}(A, B, C)$ and $L^{\circ}_{\widetilde{G}}(A^{-1}, B^{-1}, C^{-1})$ are projectively equivalent. The Galois action consists of a single orbit of size $\phi(n)/2$. If $q = p^e$ is composite, we must further divide by the faithful action of $Gal(\mathbb{F}_q)$.*
3. *Odd q, $n \neq p$. For the $(3, 3, n)$ signature we get two Galois orbits of size $\phi(n)/2$. The same remarks as above apply for composite q.*
4. *Even q, $n \neq p$. There is a single Galois orbit with $\phi(n)/2$ projectively inequivalent actions.*

Example 36. *For $PSL_2(47)$ there are 2431 $(23, 23, 23)$ actions consisting of 121 Galois orbits each of size 11. For $PSL_2(32)$ there are 2940 projective classes of actions in 196 Galois orbits of size 15 each. Each Galois orbit provides $3 = 15/5$ inequivalent actions.*

References

[1] G.V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. 43915 (1979) 267–276, 479.

[2] T. Breuer, *Characters and Automorphism Groups of Compact Riemann Surfaces*, Cambridge University Press (2001).

[3] S.A. Broughton, *The Equisymmetric Stratification of the Moduli Space and the Krull dimension of Mapping Class Groups*, Topology and its Applications, Vol. 37 (1990) pp. 101–113.

[4] S.A. Broughton, *Classifying Finite Group Actions on Surfaces of Low Genus*, J. Pure and Appl. Alg., Vol. 69 (1990) pp. 233–270.

[5] S.A. Broughton, *Simple group actions on hyperbolic surfaces of least area*, Pacific J. of Math. Vol. 158 (1) (1993), 23-48.

[6] S.A. Broughton, *Counting Ovals on a Symmetric Riemann Surface,* (1997). Mathematical Sciences Technical Reports (MSTR). Paper 68. http://scholar.rose-hulman.edu/math_mstr/68

[7] S.A. Broughton**,** *The mirrors on a symmetric Riemann surface with quasi-platonic PSL2(q)-action*, under preparation.

[8] S.A. Broughton, E. Bujalance, A.F. Costa, J.M. Gamboa, G. Gromadski, *Symmetries of Riemann surfaces on which $PSL(2,q)$ acts as a Hurwitz automorphism group*, J. of Pure and Appl. Algebra. Vol. 106 (1996) 113.

[9] S.A. Broughton, E. Bujalance, A.F. Costa, J.M. Gamboa, G. Gromadski, *Symmetries of Accola-Machlaclan and Kulkarni surfaces*, Proc. AMS, Vol. 127 (3), (1999), 637-646.

[10] M.E. Conder *The symmetric genus of alternating and symmetric groups.* J. Combin. Theory Ser. B, Vol 39 (1985), pp. 179–186.

[11] K. Coombes and D. Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. Vol. 52 (1985) pp. 821–839.

[12] L.E. Dixon, Linear Groups with an Exposition of Galois Field Theory, Linear groups (1901), Dover Phoenix editions, New York.

[13] H. Glover & D. Sjerve, Representing $PSL_2(p)$ on a Surface of Least Genus, L'Enseignement Mathématique, Vol. 31 (1985), pp. 305–325.

[14] H. Glover & D. Sjerve, The Genus of $PSL_2(q)$, J. reine angew. Math, Vol. 380 (1987), pp. 59–86.

[15] G.A. Jones, Enumerating Regular maps and Hypermaps, Disertaciones del Semiario de Matematics Fundematales num. 3, UNED, (1989).

[16] G.A. Jones, D. Singerman, P.A. Watson, *Symmetries of quasi-platonic Riemann surfaces,* http://arxiv.org/abs/1401.2575v1

[17] Gareth Jones, Manfred Streit and Jurgen Wolfart,*Wilson's Map Operations on Regular Dessins and Cyclotomic Fields of Definition*, Proc. London Math. Soc., Vol 100 (2) (2010), pp. 510-532ry 201.

[18] A.M. MacBeath, *Generators of the Linear Fractional Groups*, Proc. Symp. Pure Math. Vol. XII, Amer. Math. Soc. (1969), pp. 14–32.

[19] MAGMA. Magma Computational Algebra System, Computational Algebra Group, University of Sydney.

[20] M. Ozaydin, C.Simmons, J. Tabak, *Surface Symmetries and $PSL_2(p)$*, Trans. Amer. Math. Soc. 359 (2007), 2243-2268.

[21] H. Volklein, *Groups as Galois groups: an introduction,* Cambridge University Press, New York, 1996.

[22] H. Zieschang, Finite Groups of Mapping Classes of Surfaces, Lecture Notes in Math., No. 875, Springer-Verlag, Berlin, New York (1981).

ALBANIAN JOURNAL OF MATHEMATICS
Volume 9, Number 1, Pages 63–75
ISSN: 1930-1235; (**2015**)

MATRIX MULTIVARIATE PEARSON II-RIESZ DISTRIBUTION

José A. Díaz-García
Universidad Autónoma Agraria Antonio Narro,
Calzada Antonio Narro 1923, Col. Buenavista,
25315 Saltillo, Coahuila, México
Email: jadiaz@uaaan.mx

Ramón Gutiérrez-Sánchez
Department of Statistics and O.R,
University of Granada,
Granada 18071, Spain
Email: ramongs@ugr.es

Abstract. Matrix multivariate Pearson type II-Riesz distribution is defined and some of its properties are studied. In particular, the associated matrix multivariate beta distribution type I is derived. Also the singular values and eigenvalues distributions are obtained.

1. Introduction

When a new statistic theory is proposed, the statistician known well about the rigorously mathematical foundations of their discipline, however in order to reach a wider interdisciplinary public, some of the classical statistical techniques have been usually published without explaining the supporting abstract mathematical tools which governs the approach. For example, in the context of the distribution theory of random matrices, in the last 20 years, a number of more abstract and mathematical approaches have emerged for studying and generalizing the usual matrix variate distributions. In particular, this needing have appeared recently in the generalization, by using abstract algebra, of some results of real random matrices to another supporting fields, such as complex, quaternion and octonion, see [26], [27], [12], [15], among many others authors. Studying distribution theory by another algebras, beyond real, have led several generalizations of substantial understanding in the theoretical context, and we expect that it is more extensively applied when a an improvement of its unified potential can be explored in other

2010 *Mathematics Subject Classification.* Primary 60E05; 15A52; 15B33; Secondary 15A09; 15B52; 62E15;

Key words and phrases. Matrix multivariate; Pearson Type II distribution; Riesz distribution; Kotz-Riesz distribution; real, complex,quaternion and octonion random matrices; real normed division algebras.

contexts. Two main tendencies have been considered in literature, Jordan algebras and real normed division algebras. Some works dealing the first approach are due to [14], [24], [3], [19], [20, 21], [23], and the references therein, meanwhile, the second technique has been studied by [16], [7], [4, 5, 6], among many others.

In the same manner, different generalizations of the multivariate statistical analysis have been proposed recently. This generalized technique studies the effect of changing the usual matrix multivariate normal support by a general matrix multivariate family of distributions, such as the elliptical contoured distributions (or simply, matrix multivariate elliptical distributions), see [13] and [18]. This family of distributions involves a number of known matrix multivariate distributions such as normal, Kotz type, Bessel, Pearson type II and VII, contaminated normal and power exponential, among many others. Two important properties of these distributions must be emphasized:

i) Matrix multivariate elliptical distributions provide more flexibility in the statistical modeling by including distributions with heavier or lighter tails and/or greater or lower degree of kurtosis than matrix multivariate normal distribution;

ii) Most of the statistical tests based on matrix multivariate normal distribution are invariant under the complete family of matrix multivariate elliptical distributions.

Recently, a slight combination of these two theoretical generalizations have appeared in literature; namely, Jordan algebras has been led to the matrix multivariate Riesz distribution and its associated beta distribution. [6] proved that the above mentioned distributions can be derived from a particular matrix multivariate elliptical distribution, termed matrix multivariate Kotz-Riesz distribution. Similarly, matrix multivariate Riesz distribution is also of interest from the mathematical point of view; in fact most of their basic properties under *the structure theory of normal j-algebras* and *the theory of Vinberg algebras* in place of Jordan algebras have been studied by [22] and [2], respectively.

In this scenario, we can now propose a generalization of the matrix multivariate beta, T and Pearson type II distributions based on a matrix multivariate Kotz-Riesz distribution. As usual in the normal case, extensions of beta, T and Pearson type II distributions involves two alternatives, the matrix variate and the matrix multivariate versions[1], see [4, 5, 6], [7, 8, 9] and [10].

This article derives the matrix multivariate beta and Pearson type II distributions obtained from a matrix multivariate Kotz-Riesz distribution and some of their basic properties are studied. Section 2 gives some basic concepts and the notation of abstract algebra, Jacobians and distribution theory. The nonsingular central matrix multivariate Pearson type II-Riesz distribution and the corresponding generalized matrix multivariate beta type I distribution are studied in Section 3. Finally, the joint densities of the singular values are derived in Section 4.

[1] The term matricvariate distribution was first introduced [11], but the expression matrix-variate distribution or matrix variate distribution or matrix multivariate distribution was later used to describe any distribution of a random matrix, see [17] and [18], and the references therein. When the density function of a random matrix is written including the trace operator then the matrix multivariate designation shall be used.

2. Preliminary results

A detailed discussion of real normed division algebras can be found in [1] and [25]. For your convenience, we shall introduce some notation, although in general, we adhere to standard notation forms.

For our purposes: Let $\mathbb{F}$ be a field. An *algebra* $\mathfrak{A}$ over $\mathbb{F}$ is a pair $(\mathfrak{A}; m)$, where $\mathfrak{A}$ is a *finite-dimensional vector space* over $\mathbb{F}$ and *multiplication* $m : \mathfrak{A} \times \mathfrak{A} \to A$ is an $\mathbb{F}$-bilinear map; that is, for all $\lambda \in \mathbb{F}$, $x, y, z \in \mathfrak{A}$,

$$\begin{aligned} m(x, \lambda y + z) &= \lambda m(x; y) + m(x; z) \\ m(\lambda x + y; z) &= \lambda m(x; z) + m(y; z). \end{aligned}$$

Two algebras $(\mathfrak{A}; m)$ and $(\mathfrak{E}; n)$ over $\mathbb{F}$ are said to be *isomorphic* if there is an invertible map $\phi : \mathfrak{A} \to \mathfrak{E}$ such that for all $x, y \in \mathfrak{A}$,

$$\phi(m(x, y)) = n(\phi(x), \phi(y)).$$

By simplicity, we write $m(x; y) = xy$ for all $x, y \in \mathfrak{A}$.

Let $\mathfrak{A}$ be an algebra over $\mathbb{F}$. Then $\mathfrak{A}$ is said to be

1. *alternative* if $x(xy) = (xx)y$ and $x(yy) = (xy)y$ for all $x, y \in \mathfrak{A}$,
2. *associative* if $x(yz) = (xy)z$ for all $x, y, z \in \mathfrak{A}$,
3. *commutative* if $xy = yx$ for all $x, y \in \mathfrak{A}$, and
4. *unital* if there is a $1 \in \mathfrak{A}$ such that $x1 = x = 1x$ for all $x \in \mathfrak{A}$.

If $\mathfrak{A}$ is unital, then the identity 1 is uniquely determined.

An algebra $\mathfrak{A}$ over $\mathbb{F}$ is said to be a *division algebra* if $\mathfrak{A}$ is nonzero and $xy = 0_{\mathfrak{A}} \Rightarrow x = 0_{\mathfrak{A}}$ or $y = 0_{\mathfrak{A}}$ for all $x, y \in \mathfrak{A}$.

The term “division algebra", comes from the following proposition, which shows that, in such an algebra, left and right division can be unambiguously performed.

Let $\mathfrak{A}$ be an algebra over $\mathbb{F}$. Then $\mathfrak{A}$ is a division algebra if, and only if, $\mathfrak{A}$ is nonzero and for all $a, b \in \mathfrak{A}$, with $b \neq 0_{\mathfrak{A}}$, the equations $bx = a$ and $yb = a$ have unique solutions $x, y \in \mathfrak{A}$.

In the sequel we assume $\mathbb{F} = \mathfrak{R}$ and consider classes of division algebras over $\mathfrak{R}$ or “*real division algebras*" for short.

We introduce the algebras of *real numbers* $\mathfrak{R}$, *complex numbers* $\mathfrak{C}$, *quaternions* $\mathfrak{H}$ and *octonions* $\mathfrak{O}$. Then, if $\mathfrak{A}$ is an alternative real division algebra, then $\mathfrak{A}$ is isomorphic to $\mathfrak{R}$, $\mathfrak{C}$, $\mathfrak{H}$ or $\mathfrak{O}$.

Let $\mathfrak{A}$ be a real division algebra with identity 1. Then $\mathfrak{A}$ is said to be *normed* if there is an inner product $(\cdot, \cdot)$ on $\mathfrak{A}$ such that

$$(xy, xy) = (x, x)(y, y) \qquad \text{for all } x, y \in \mathfrak{A}.$$

If $\mathfrak{A}$ is a *real normed division algebra*, then $\mathfrak{A}$ is isomorphic $\mathfrak{R}$, $\mathfrak{C}$, $\mathfrak{H}$ or $\mathfrak{O}$.

There are exactly four normed division algebras: real numbers ($\mathfrak{R}$), complex numbers ($\mathfrak{C}$), quaternions ($\mathfrak{H}$) and octonions ($\mathfrak{O}$), see [1]. We take into account that should be taken into account, $\mathfrak{R}$, $\mathfrak{C}$, $\mathfrak{H}$ and $\mathfrak{O}$ are the only normed division algebras; furthermore, they are the only alternative division algebras.

Let $\mathfrak{A}$ be a division algebra over the real numbers. Then $\mathfrak{A}$ has dimension either 1, 2, 4 or 8. Finally, observe that

$\mathfrak{R}$ is a real commutative associative normed division algebra,
$\mathfrak{C}$ is a commutative associative normed division algebra,
$\mathfrak{H}$ is an associative normed division algebra,
$\mathfrak{O}$ is an alternative normed division algebra.

Let $\mathfrak{L}_{n,m}^{\beta}$ be the set of all $n \times m$ matrices of rank $m \leq n$ over $\mathfrak{A}$ with m distinct positive singular values, where $\mathfrak{A}$ denotes a *real finite-dimensional normed division algebra*. Let $\mathfrak{A}^{n \times m}$ be the set of all $n \times m$ matrices over $\mathfrak{A}$. The dimension of $\mathfrak{A}^{n \times m}$ over $\Re$ is βmn. Let $\mathbf{A} \in \mathfrak{A}^{n \times m}$, then $\mathbf{A}^* = \bar{\mathbf{A}}^T$ denotes the usual conjugate transpose.

Table 1 sets out the equivalence between the same concepts in the four normed division algebras.

TABLE 1. Notation

Real	Complex	Quaternion	Octonion	Generic notation
Semi-orthogonal	Semi-unitary	Semi-symplectic	Semi-exceptional type	$\mathcal{V}_{m,n}^{\beta}$
Orthogonal	Unitary	Symplectic	Exceptional type	$\mathfrak{U}^{\beta}(m)$
Symmetric	Hermitian	Quaternion hermitian	Octonion hermitian	$\mathfrak{S}_m^{\beta}$

We denote by $\mathfrak{S}_m^{\beta}$ the real vector space of all $\mathbf{S} \in \mathfrak{A}^{m \times m}$ such that $\mathbf{S} = \mathbf{S}^*$. In addition, let $\mathfrak{P}_m^{\beta}$ be the *cone of positive definite matrices* $\mathbf{S} \in \mathfrak{A}^{m \times m}$. Thus, $\mathfrak{P}_m^{\beta}$ consist of all matrices $\mathbf{S} = \mathbf{X}^*\mathbf{X}$, with $\mathbf{X} \in \mathfrak{L}_{n,m}^{\beta}$; then $\mathfrak{P}_m^{\beta}$ is an open subset of $\mathfrak{S}_m^{\beta}$.

Let $\mathfrak{D}_m^{\beta}$ consisting of all $\mathbf{D} \in \mathfrak{A}^{m \times m}$, $\mathbf{D} = \operatorname{diag}(d_1, \dots, d_m)$. Let $\mathfrak{T}_U^{\beta}(m)$ be the subgroup of all *upper triangular* matrices $\mathbf{T} \in \mathfrak{A}^{m \times m}$ such that $t_{ij} = 0$ for $1 < i < j \leq m$. Let $\mathbf{Z} \in \mathfrak{L}_{n,m}^{\beta}$, define the norm of $\mathbf{Z}$ as $||\mathbf{Z}|| = \sqrt{\operatorname{tr} \mathbf{Z}^*\mathbf{Z}}$.

For any matrix $\mathbf{X} \in \mathfrak{A}^{n \times m}$, $d\mathbf{X}$ denotes the *matrix of differentials* (dx_{ij}). Finally, we define the *measure* or volume element $(d\mathbf{X})$ when $\mathbf{X} \in \mathfrak{A}^{n \times m}, \mathfrak{S}_m^{\beta}$, $\mathfrak{D}_m^{\beta}$ or $\mathcal{V}_{m,n}^{\beta}$, see [7] and [9].

If $\mathbf{X} \in \mathfrak{A}^{n \times m}$ then $(d\mathbf{X})$ (the Lebesgue measure in $\mathfrak{A}^{n \times m}$) denotes the exterior product of the βmn functionally independent variables

$$(d\mathbf{X}) = \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{m} dx_{ij} \quad \text{where} \quad dx_{ij} = \bigwedge_{k=1}^{\beta} dx_{ij}^{(k)}.$$

If $\mathbf{S} \in \mathfrak{S}_m^{\beta}$ (or $\mathbf{S} \in \mathfrak{T}_U^{\beta}(m)$ with $t_{ii} > 0$, $i = 1, \dots, m$) then $(d\mathbf{S})$ (the Lebesgue measure in $\mathfrak{S}_m^{\beta}$ or in $\mathfrak{T}_U^{\beta}(m)$) denotes the exterior product of the exterior product of the $m(m-1)\beta/2 + m$ functionally independent variables,

$$(d\mathbf{S}) = \bigwedge_{i=1}^{m} ds_{ii} \bigwedge_{i>j}^{m} \bigwedge_{k=1}^{\beta} ds_{ij}^{(k)}.$$

Observe, that for the Lebesgue measure $(d\mathbf{S})$ defined thus, it is required that $\mathbf{S} \in \mathfrak{P}_m^{\beta}$, that is, $\mathbf{S}$ must be a non singular Hermitian matrix (Hermitian definite positive matrix).

If $\mathbf{\Lambda} \in \mathfrak{D}_m^{\beta}$ then $(d\mathbf{\Lambda})$ (the Legesgue measure in $\mathfrak{D}_m^{\beta}$) denotes the exterior product of the βm functionally independent variables

$$(d\mathbf{\Lambda}) = \bigwedge_{i=1}^{n} \bigwedge_{k=1}^{\beta} d\lambda_i^{(k)}.$$

If $\mathbf{H}_1 \in \mathcal{V}_{m,n}^{\beta}$ then

$$(\mathbf{H}_1^* d\mathbf{H}_1) = \bigwedge_{i=1}^{m} \bigwedge_{j=i+1}^{n} \mathbf{h}_j^* d\mathbf{h}_i.$$

where $\mathbf{H} = (\mathbf{H}_1^*|\mathbf{H}_2^*)^* = (\mathbf{h}_1, \dots, \mathbf{h}_m|\mathbf{h}_{m+1}, \dots, \mathbf{h}_n)^* \in \mathfrak{U}^{\beta}(n)$. It can be proved that this differential form does not depend on the choice of the $\mathbf{H}_2$ matrix. When $n = 1$; $\mathcal{V}_{m,1}^{\beta}$ defines the unit sphere in $\mathfrak{A}^m$. This is, of course, an $(m-1)\beta$-dimensional surface in $\mathfrak{A}^m$. When $n = m$ and denoting $\mathbf{H}_1$ by $\mathbf{H}$, $(\mathbf{H}d\mathbf{H}^*)$ is termed the *Haar measure* on $\mathfrak{U}^{\beta}(m)$.

The surface area or volume of the Stiefel manifold $\mathcal{V}_{m,n}^{\beta}$ is

$$\text{(1)} \qquad \operatorname{Vol}(\mathcal{V}_{m,n}^{\beta}) = \int_{\mathbf{H}_1 \in \mathcal{V}_{m,n}^{\beta}} (\mathbf{H}_1 d\mathbf{H}_1^*) = \frac{2^m \pi^{mn\beta/2}}{\Gamma_m^{\beta}[n\beta/2]},$$

where $\Gamma_m^{\beta}[a]$ denotes the multivariate *Gamma function* for the space $\mathfrak{S}_m^{\beta}$ and is defined as

$$\begin{aligned} \Gamma_m^{\beta}[a] &= \int_{\mathbf{A} \in \mathfrak{P}_m^{\beta}} \operatorname{etr}\{-\mathbf{A}\}|\mathbf{A}|^{a-(m-1)\beta/2-1}(d\mathbf{A}) \\ &= \pi^{m(m-1)\beta/4} \prod_{i=1}^{m} \Gamma[a-(i-1)\beta/2], \end{aligned}$$

and $\operatorname{Re}(a) > (m-1)\beta/2$. This can be obtained as a particular case of the *generalized gamma function of weight* κ for the space $\mathfrak{S}_m^{\beta}$ with $\kappa = (k_1, k_2, \dots, k_m) \in \Re^m$, taking $\kappa = (0, 0, \dots, 0) \in \Re^m$ and which for $\operatorname{Re}(a) \geq (m-1)\beta/2 - k_m$ is defined by, see [16] and [14],

$$\begin{aligned} \text{(2)} \qquad \Gamma_m^{\beta}[a, \kappa] &= \int_{\mathbf{A} \in \mathfrak{P}_m^{\beta}} \operatorname{etr}\{-\mathbf{A}\}|\mathbf{A}|^{a-(m-1)\beta/2-1} q_{\kappa}(\mathbf{A})(d\mathbf{A}) \\ &= \pi^{m(m-1)\beta/4} \prod_{i=1}^{m} \Gamma[a + k_i - (i-1)\beta/2] \\ \text{(3)} \qquad &= [a]_{\kappa}^{\beta} \Gamma_m^{\beta}[a], \end{aligned}$$

where $\operatorname{etr}(\cdot) = \exp(\operatorname{tr}(\cdot))$, $|\cdot|$ denotes the determinant, and for $\mathbf{A} \in \mathfrak{S}_m^{\beta}$

$$\text{(4)} \qquad q_{\kappa}(\mathbf{A}) = |\mathbf{A}_m|^{k_m} \prod_{i=1}^{m-1} |\mathbf{A}_i|^{k_i - k_{i+1}}$$

with $\mathbf{A}_p = (a_{rs})$, $r, s = 1, 2, \dots, p$, $p = 1, 2, \dots, m$ is termed the *highest weight vector*, see [16], [14] and [19]; And, $[a]_{\kappa}^{\beta}$ denotes the generalized Pochhammer symbol of weight κ, defined as

$$\begin{aligned} [a]_{\kappa}^{\beta} &= \prod_{i=1}^{m} (a-(i-1)\beta/2)_{k_i} \\ &= \frac{\pi^{m(m-1)\beta/4} \displaystyle\prod_{i=1}^{m} \Gamma[a + k_i - (i-1)\beta/2]}{\Gamma_m^{\beta}[a]} \\ &= \frac{\Gamma_m^{\beta}[a, \kappa]}{\Gamma_m^{\beta}[a]}, \end{aligned}$$

where $\mathrm{Re}(a) > (m-1)\beta/2 - k_m$ and

$$(a)_i = a(a+1)\cdots(a+i-1),$$

is the standard Pochhammer symbol.

Additional, note that, if $\kappa = (p,\dots,p)$, then $q_\kappa(\mathbf{A}) = |\mathbf{A}|^p$. In particular if $p = 0$, then $q_\kappa(\mathbf{A}) = 1$. If $\tau = (t_1, t_2, \dots, t_m)$, $t_1 \geq t_2 \geq \cdots \geq t_m \geq 0$, then $q_{\kappa+\tau}(\mathbf{A}) = q_\kappa(\mathbf{A})q_\tau(\mathbf{A})$, and in particular if $\tau = (p,p,\dots,p)$, then $q_{\kappa+\tau}(\mathbf{A}) \equiv q_{\kappa+p}(\mathbf{A}) = |\mathbf{A}|^p q_\kappa(\mathbf{A})$. Finally, for $\mathbf{B} \in \mathfrak{T}_U^\beta(m)$ in such a manner that $\mathbf{C} = \mathbf{B}^*\mathbf{B} \in \mathfrak{S}_m^\beta$, $q_\kappa(\mathbf{B}^*\mathbf{A}\mathbf{B}) = q_\kappa(\mathbf{C})q_\kappa(\mathbf{A})$, and $q_\kappa(\mathbf{B}^{*-1}\mathbf{A}\mathbf{B}^{-1}) = (q_\kappa(\mathbf{C}))^{-1}q_\kappa(\mathbf{A}) = q_{-\kappa}(\mathbf{C})q_\kappa(\mathbf{A})$, see [21].

Finally, the following Jacobians involving the β parameter, reflects the generalized power of the algebraic technique; the can be seen as extensions of the full derived and unconnected results in the real, complex or quaternion cases, see [14] and [7]. These results are the base for several matrix and matrix variate generalized analysis.

Proposition 2.1. *Let $\mathbf{X}$ and $\mathbf{Y} \in \mathfrak{L}_{n,m}^\beta$ be matrices of functionally independent variables, and let $\mathbf{Y} = \mathbf{A}\mathbf{X}\mathbf{B} + \mathbf{C}$, where $\mathbf{A} \in \mathfrak{L}_{n,n}^\beta$, $\mathbf{B} \in \mathfrak{L}_{m,m}^\beta$ and $\mathbf{C} \in \mathfrak{L}_{n,m}^\beta$ are constant matrices. Then*

$$(d\mathbf{Y}) = |\mathbf{A}^*\mathbf{A}|^{m\beta/2}|\mathbf{B}^*\mathbf{B}|^{mn\beta/2}(d\mathbf{X}). \tag{5}$$

Proposition 2.2 (Singular Value Decomposition, SVD)**.** *Let $\mathbf{X} \in \mathcal{L}_{n,m}^\beta$ be matrix of functionally independent variables, such that $\mathbf{X} = \mathbf{W}_1\mathbf{D}\mathbf{V}^*$ with $\mathbf{W}_1 \in \mathcal{V}_{m,n}^\beta$, $\mathbf{V} \in \mathfrak{U}^\beta(m)$ and $\mathbf{D} = \mathrm{diag}(d_1,\cdots,d_m) \in \mathfrak{D}_m^1$, $d_1 > \cdots > d_m > 0$. Then*

$$(d\mathbf{X}) = 2^{-m}\pi^\varrho \prod_{i=1}^m d_i^{\beta(n-m+1)-1} \prod_{i<j}^m (d_i^2 - d_j^2)^\beta (d\mathbf{D})(\mathbf{V}^* d\mathbf{V})(\mathbf{W}_1^* d\mathbf{W}_1), \tag{6}$$

where

$$\varrho = \begin{cases} 0, & \beta = 1; \\ -m, & \beta = 2; \\ -2m, & \beta = 4; \\ -4m, & \beta = 8. \end{cases}$$

Proposition 2.3. *Let $\mathbf{X} \in \mathfrak{L}_{n,m}^\beta$ be matrix of functionally independent variables, and write $\mathbf{X} = \mathbf{V}_1\mathbf{T}$, where $\mathbf{V}_1 \in \mathcal{V}_{m,n}^\beta$ and $\mathbf{T} \in \mathfrak{T}_U^\beta(m)$ with positive diagonal elements. Define $\mathbf{S} = \mathbf{X}^*\mathbf{X} \in \mathfrak{P}_m^\beta$. Then*

$$(d\mathbf{X}) = 2^{-m}|\mathbf{S}|^{\beta(n-m+1)/2-1}(d\mathbf{S})(\mathbf{V}_1^* d\mathbf{V}_1). \tag{7}$$

Finally, to define the matrix multivariate Pearson type II-Riesz distribution we need to recall the following two definitions of Kotz-Riesz and Riesz distributions.

From [6].

Definition 2.1. Let $\mathbf{\Sigma} \in \mathbf{\Phi}_m^\beta$, $\mathbf{\Theta} \in \mathbf{\Phi}_n^\beta$, $\boldsymbol{\mu} \in \mathfrak{L}_{n,m}^\beta$ and $\kappa = (k_1, k_2, \dots, k_m) \in \Re^m$. And let $\mathbf{Y} \in \mathfrak{L}_{n,m}^\beta$ and $\mathcal{U}(\mathbf{B}) \in \mathfrak{T}_U^\beta(n)$, such that $\mathbf{B} = \mathcal{U}(\mathbf{B})^*\mathcal{U}(\mathbf{B})$ is the Cholesky decomposition of $\mathbf{B} \in \mathfrak{S}_m^\beta$. Then it is said that $\mathbf{Y}$ has a *Kotz-Riesz distribution of* *type I* and its density function is

(8)
$$\frac{\beta^{mn\beta/2+\sum_{i=1}^{m}k_i}\Gamma_m^\beta[n\beta/2]}{\pi^{mn\beta/2}\Gamma_m^\beta[n\beta/2,\kappa]|\boldsymbol{\Sigma}|^{n\beta/2}|\boldsymbol{\Theta}|^{m\beta/2}}\times\operatorname{etr}\left\{-\beta\operatorname{tr}\left[\boldsymbol{\Sigma}^{-1}(\mathbf{Y}-\boldsymbol{\mu})^*\boldsymbol{\Theta}^{-1}(\mathbf{Y}-\boldsymbol{\mu})\right]\right\}$$
$$\times\, q_\kappa\left[\mathcal{U}(\boldsymbol{\Sigma})^{*-1}(\mathbf{Y}-\boldsymbol{\mu})^*\boldsymbol{\Theta}^{-1}(\mathbf{Y}-\boldsymbol{\mu})\mathcal{U}(\boldsymbol{\Sigma})^{-1}\right](d\mathbf{Y})$$

with $\operatorname{Re}(n\beta/2)>(m-1)\beta/2-k_m$; denoting this fact as

$$\mathbf{Y}\sim\mathcal{KR}_{n\times m}^{\beta,I}(\kappa,\boldsymbol{\mu},\boldsymbol{\Theta},\boldsymbol{\Sigma}).$$

From [19] and [4] we have

Definition 2.2. Let $\boldsymbol{\Xi}\in\boldsymbol{\Phi}_m^\beta$ and $\kappa=(k_1,k_2,\dots,k_m)\in\Re^m$. Then it is said that $\mathbf{V}$ has a *Riesz distribution of type I* if its density function is

$$\frac{\beta^{am+\sum_{i=1}^{m}k_i}}{\Gamma_m^\beta[a,\kappa]|\boldsymbol{\Xi}|^a q_\kappa(\boldsymbol{\Xi})}\operatorname{etr}\{-\beta\boldsymbol{\Xi}^{-1}\mathbf{V}\}|\mathbf{V}|^{a-(m-1)\beta/2-1}q_\kappa(\mathbf{V})(d\mathbf{V}),\tag{9}$$

for $\mathbf{V}\in\mathfrak{P}_m^\beta$ and $\operatorname{Re}(a)\geq(m-1)\beta/2-k_m$; denoting this fact as $\mathbf{V}\sim\mathcal{R}_m^{\beta,I}(a,\kappa,\boldsymbol{\Xi})$.

3. Matrix multivariate Pearson type II-Riesz distribution

A detailed discussion of Riesz distribution may be found in [19] and [4]. In addition the Kotz-Riesz distribution is studied in detail in [6]. For convenience, we adhere to standard notation stated in [4, 6].

Theorem 3.1. *Let* $\left(S_1^{1/2}\right)^2=S_1\sim\mathcal{R}_1^{\beta,I}(\nu\beta/2,k,1)$, $k\in\Re$ *and* $\operatorname{Re}(\nu\beta/2)>-k$*; independent of* $\mathbf{Y}\sim\mathcal{KR}_{n\times m}^{\beta,I}(\tau,\mathbf{0},\mathbf{I}_n,\mathbf{I}_m)$, $\operatorname{Re}(n\beta/2)>(m-1)\beta/2-t_m$. *In addition, define* $\mathbf{R}=S^{-1/2}\mathbf{Y}$ *where* $S=S_1+||\mathbf{Y}||^2$. *Then*

$$S\sim\mathcal{R}_1^{\beta,I}((\nu+mn)\beta/2+\sum_{i=1}^{m}t_i,k,1)$$

is independent of $\mathbf{R}$. *Furthermore, the density of* $\mathbf{R}$ *is*

(10)
$$\frac{\Gamma_m^\beta[n\beta/2]\Gamma_1^\beta\left[(\nu+mn)\beta/2+k+\sum_{i=1}^{m}t_i\right]}{\pi^{\beta mn/2}\Gamma_m^\beta[n\beta/2,\tau]\Gamma_1^\beta[\nu\beta/2+k]}\left(1-||\mathbf{R}||^2\right)^{\nu\beta/2+k-1}q_\tau\left(\mathbf{R}^*\mathbf{R}\right)(d\mathbf{R}),$$

where $\left(1-||\mathbf{R}||^2\right)>0$*; which is termed the* standardized matrix multivariate Pearson type II-Riesz type distribution *and is denoted as*

$$\mathbf{R}\sim\mathcal{P}_{\mathcal{II}}\mathcal{R}_{m\times n}^{\beta,I}(\nu,k,\tau,1,\mathbf{0},\mathbf{I}_n,\mathbf{I}m).$$

Proof. From definition 2.1 and 2.2, the joint density of S_1 and $\mathbf{Y}$ is

$$\propto s_1^{\beta\nu/2+k-1}\operatorname{etr}\left\{-\beta\left(s_1+||\mathbf{Y}||^2\right)\right\}q_\tau\left(\mathbf{Y}^*\mathbf{Y}\right)(ds_1)(d\mathbf{Y})$$

where the constant of proportionality is

$$c=\frac{\beta^{\nu\beta/2+k}}{\Gamma_1^\beta[\nu\beta/2+k]}\cdot\frac{\beta^{mn\beta/2+\sum_{i=1}^{m}t_i}\Gamma_m^\beta[n\beta/2]}{\pi^{mn\beta/2}\Gamma_m^\beta[n\beta/2,\tau]}.$$

Making the change of variable $S=S_1-||\mathbf{Y}||^2$ and $\mathbf{Y}=S_1^{1/2}\mathbf{R}$, by (5)

$$(ds_1)\wedge(d\mathbf{Y})=s^{\beta mn/2}(ds)\wedge(d\mathbf{R}).$$

Now, observing that $S = S_1 - ||\mathbf{Y}||^2 = S\left(1 - ||\mathbf{R}||^2\right)$, the joint density of S and $\mathbf{R}$ is

$$\propto \left(1 - ||\mathbf{R}||^2\right)^{\beta\nu/2+k-1} s^{\beta\nu/2+k-1} \operatorname{etr}\{-\beta s\}\, q_\tau\left(s\mathbf{R}^*\mathbf{R}\right)(ds)(d\mathbf{R}).$$

Also, note that

$$q_\tau\left(s\mathbf{R}^*\mathbf{R}\right) = q_\tau\left((s^{1/2}\mathbf{I}_m)\mathbf{R}^*\mathbf{R}(s^{1/2}\mathbf{I}_m)\right) = q_\tau\left(s\mathbf{I}_m\right) q_\tau\left(\mathbf{R}^*\mathbf{R}\right) = s^{\sum_{i=1}^m t_i} q_\tau\left(\mathbf{R}^*\mathbf{R}\right).$$

From where, the joint density of S and $\mathbf{R}$ is given by

$$\frac{\beta^{(\nu+mn)\beta/2+k+\sum_{i=1}^m t_i}}{\Gamma_1^\beta\left[(\nu+mn)\beta/2+k+\sum_{i=1}^m t_i\right]} \operatorname{etr}\{-\beta s\}\, s^{(\nu+mn)\beta/2+k+\sum_{i=1}^m t_i - 1}(ds)$$
$$\times \frac{\Gamma_m^\beta[n\beta/2]\Gamma_1^\beta\left[(\nu+mn)\beta/2+k+\sum_{i=1}^m t_i\right]}{\pi^{\beta mn/2}\Gamma_m^\beta[n\beta/2,\tau]\Gamma_1^\beta[\nu\beta/2+k]} \left(1 - ||\mathbf{R}||^2\right)^{\nu\beta/2+k-1} q_\tau\left(\mathbf{R}^*\mathbf{R}\right)(d\mathbf{R}),$$

which shows that

$$S \sim \mathcal{R}_1^{\beta,I}((\nu+mn)\beta/2 + \sum_{i=1}^m t_i, k, 1),$$

and is independent of $\mathbf{R}$, where $\mathbf{R}$ has the density (10).

□

The following is an immediate consequence of the previous result.

Corollary 3.1. *Let* $\mathbf{R} \sim \mathcal{P}_{\mathcal{II}}\mathcal{R}_{m\times n}^{\beta,I}(\nu, k, \tau, 1, \mathbf{0}, \mathbf{I}_n, \mathbf{I}m)$ *and define*

$$\mathbf{C} = \rho^{-1/2}\,\mathcal{U}(\boldsymbol{\Theta})^*\mathbf{R}\,\mathcal{U}(\boldsymbol{\Sigma}) + \boldsymbol{\mu}$$

where $\mathcal{U}(\mathbf{B}) \in \mathfrak{T}_U^\beta(n)$, *such that* $\mathbf{B} = \mathcal{U}(\mathbf{B})^*\mathcal{U}(\mathbf{B})$ *is the Cholesky decomposition of* $\mathbf{B} \in \mathfrak{S}_m^\beta$, $\boldsymbol{\Theta} \in \mathfrak{P}_n^\beta$, $\boldsymbol{\Sigma} \in \mathfrak{P}_m^\beta$, $\rho > 0$ *constant and* $\boldsymbol{\mu} \in \mathfrak{L}_{n,m}^\beta$ *is a matrix of constants. Then the density of* $\mathbf{S}$ *is*

$$\propto \left(1 - \rho \operatorname{tr} \boldsymbol{\Sigma}^{-1}(\mathbf{C}-\boldsymbol{\mu})^*\boldsymbol{\Theta}^{-1}(\mathbf{C}-\boldsymbol{\mu})\right)^{\nu\beta/2+k-1}$$

$$\times\ q_\tau\left[\mathcal{U}(\boldsymbol{\Sigma})^{*-1}(\mathbf{C}-\boldsymbol{\mu})^*\boldsymbol{\Theta}^{-1}(\mathbf{C}-\boldsymbol{\mu})\,\mathcal{U}(\boldsymbol{\Sigma})^{-1}\right](d\mathbf{S}) \tag{11}$$

where $\left(1 - \rho \operatorname{tr} \boldsymbol{\Sigma}^{-1}(\mathbf{C}-\boldsymbol{\mu})^*\boldsymbol{\Theta}^{-1}(\mathbf{C}-\boldsymbol{\mu})\right) > 0$*; with constant of proportionality*

$$\frac{\Gamma_m^\beta[n\beta/2]\Gamma_1^\beta\left[(\nu+mn)\beta/2 - k - \sum_{i=1}^m t_i\right]\rho^{mn\beta/2-\sum_{i=1}^m t_i}}{\pi^{\beta mn/2}\Gamma_m^\beta[n\beta/2,-\tau]\Gamma_1^\beta[\nu\beta/2-k]|\boldsymbol{\Sigma}|^{\beta n/2}|\boldsymbol{\Theta}|^{\beta m/2}},$$

which is termed the matrix multivariate Pearson type II-Riesz distribution *and is denoted as* $\mathbf{C} \sim \mathcal{P}_{\mathcal{II}}\mathcal{R}_{m\times n}^{\beta,I}(\nu, k, \tau, \rho, \boldsymbol{\mu}, \boldsymbol{\Theta}, \boldsymbol{\Sigma})$.

Proof. Observe that $\mathbf{R} = \rho^{1/2}\,\mathcal{U}(\boldsymbol{\Theta})^{*-1}(\mathbf{C}-\boldsymbol{\mu})\,\mathcal{U}(\boldsymbol{\Sigma})^{-1}$ and

$$(d\mathbf{R}) = \rho^{mn\beta/2}|\boldsymbol{\Sigma}|^{-\beta n/2}|\boldsymbol{\Theta}|^{-\beta m/2}(d\mathbf{C}).$$

The desired result is obtained making this change of variable in (10).

□

Next we derive the corresponding *matrix multivariate beta type I distribution.*

Theorem 3.2. *Let*

$$\mathbf{R} \sim \mathcal{P}_{\mathcal{II}}\mathcal{R}_{n\times m}^{\beta,I}(\nu, k, \tau, \rho, \mathbf{0}, \mathbf{I}_n, \boldsymbol{\Sigma}),$$

and define $\mathbf{B} = \mathbf{R}^*\mathbf{R} \in \mathfrak{P}_m^\beta$, *with* $n \geq m$. *Then the density of* $\mathbf{B}$ *is,*

$$\propto |\mathbf{B}|^{(n-m+1)\beta/2-1}(1 - \rho \operatorname{tr} \boldsymbol{\Sigma}^{-1}\mathbf{B})^{\nu\beta/2+k-1} q_\tau(\mathbf{B})(d\mathbf{B}), \tag{12}$$

where $1-\rho\,\mathrm{tr}\,\mathbf{\Sigma}^{-1}\mathbf{B}>0$*; and with constant of proportionality*

$$\frac{\Gamma_1^{\beta}\left[(\nu+mn)\beta/2+k+\sum_{i=1}^{m}t_i\right]\rho^{\beta mn/2+\sum_{i=1}^{m}t_i}}{\Gamma_m^{\beta}[n\beta/2,\tau]\Gamma_1^{\beta}[\nu\beta/2+k]|\mathbf{\Sigma}|^{n\beta/1}q_{\tau}(\mathbf{\Sigma})}.$$

$\mathbf{B}$ *is said to have a* non standardized matrix multivariate beta-Riesz type I distribution.

Proof. The desired result follows from (10), by applying (7) and then (1); and observing that

$$q_{\tau}(\mathcal{U}(\mathbf{\Sigma})^{*-1}\mathbf{B}\,\mathcal{U}(\mathbf{\Sigma})^{-1})=q_{-\tau}(\mathbf{\Sigma})q_{\tau}(\mathbf{B}).$$

□

In particular if $\mathbf{\Sigma}=\mathbf{I}_m$ in Theorem 3.2, we obtain:

Corollary 3.2. *Let*

$$\mathbf{R}\sim\mathcal{P}_{\mathcal{II}}\mathcal{R}_{n\times m}^{\beta,I}(\nu,k,\tau,1,\mathbf{0},\mathbf{I}_n,\mathbf{I}_m),$$

and define $\mathbf{B}=\mathbf{R}^{*}\mathbf{R}\in\mathfrak{P}_m^{\beta}$*, with* $n\geq m$*. Then the density of* $\mathbf{B}$ *is,*

(13)
$$\frac{\Gamma_1^{\beta}\left[(\nu+mn)\beta/2+k+\sum_{i=1}^{m}t_i\right]}{\Gamma_m^{\beta}[n\beta/2,\tau]\Gamma_1^{\beta}[\nu\beta/2+k]}|\mathbf{B}|^{(n-m+1)\beta/2-1}(1-\rho\,\mathrm{tr}\,\mathbf{B})^{\nu\beta/2+k-1}q_{\tau}(\mathbf{B})(d\mathbf{B}),$$

where $1-\rho\,\mathrm{tr}\,\mathbf{B}>0$*.* $\mathbf{B}$ *is said to have a* matrix multivariate beta-Riesz type I distribution.

Remark 3.1. Observe that alternatively to classical definitions of generalized *matricvariate* beta function (for symmetric cones), see [5], [14] and [20], defined as

$$\begin{aligned}\mathcal{B}_m^{\beta}[a,\kappa;b,\tau]&=\int_{\mathbf{0}<\mathbf{S}<\mathbf{I}_m}|\mathbf{B}|^{b-(m-1)\beta/2-1}q_{\tau}(\mathbf{B})|\mathbf{I}_m-\mathbf{B}|^{a-(m-1)\beta/2-1}q_{\kappa}(\mathbf{I}_m-\mathbf{B})(d\mathbf{B})\\&=\int_{\mathbf{F}\in\mathfrak{P}_m^{\beta}}|\mathbf{F}|^{b-(m-1)\beta/2-1}q_{\tau}(\mathbf{F})|\mathbf{I}_m+\mathbf{F}|^{-(a+b)}q_{-(\kappa+\tau)}(\mathbf{I}_m+\mathbf{F})(d\mathbf{F})\\&=\frac{\Gamma_m^{\beta}[a,\kappa]\Gamma_m^{\beta}[b,\tau]}{\Gamma_m^{\beta}[a+b,\kappa+\tau]},\end{aligned}$$

where $\kappa=(k_1,k_2,\dots,k_m)\in\Re^m$, $\tau=(t_1,t_2,\dots,t_m)\in\Re^m$, $\mathrm{Re}(a)>(m-1)\beta/2-k_m$ and $\mathrm{Re}(b)>(m-1)\beta/2-t_m$. From Corollary 3.2 and Díaz-García and Gutiérrez-Sánchez [10, Theorem 3.3.1], we have the following alternative definition:

Definition 3.1. The *matrix multivariate* beta function is defined an denoted as:

$$\begin{aligned}\mathcal{B}_m^{*\ \beta}[a,k;b,\tau]&=\int_{1-\mathrm{tr}\,\mathbf{B}>0}|\mathbf{B}|^{b-(m-1)\beta/2-1}(1-\mathrm{tr}\,\mathbf{B})^{a+k-1}q_{\tau}(\mathbf{B})(d\mathbf{B})\\&=\int_{\mathbf{R}\in\mathfrak{P}_m^{\beta}}|\mathbf{F}|^{b-(m-1)\beta/2-1}(1+\mathrm{tr}\,\mathbf{F})^{-(a+mb+k+\sum_{i=1}^{m}t_i)}q_{\tau}(\mathbf{F})(d\mathbf{F})\\&=\frac{\Gamma_1^{\beta}[a+k]\Gamma_m^{\beta}[b,\tau]}{\Gamma_1^{\beta}\left[a+mb+k+\sum_{i=1}^{m}t_i\right]}.\end{aligned}$$

Also, observe that, when $m=1$, then $\tau=t$ and $\kappa=k$ and

$$\mathcal{B}_1^{\beta}[a,k;b,t]=\frac{\Gamma_1^{\beta}[a+k]\Gamma_1^{\beta}[b+t]}{\Gamma_1^{\beta}\left[a+b+k+t\right]}=\mathcal{B}_1^{*\ \beta}[a,k;b,t]$$

Finally observe that if in results in this section are defined $k=0$ and $\tau=(0,\dots,0)$, the results in [8] are obtained as particular cases.

4. Singular value densities

In this section, the joint densities of the singular values of random matrix $\mathbf{R} \sim \mathcal{P}_{\mathcal{II}}\mathcal{R}^{\beta,I}_{n\times m}(\nu, k, \tau, 1, \mathbf{0}, \mathbf{I}_n, \mathbf{I}_m)$ are derived. In addition, and as a direct consequence, the joint density of the eigenvalues of matrix multivariate beta-Riesz type I distribution is obtained for real normed division algebras.

Theorem 4.1. *Let $\delta_1, \dots, \delta_m$, $1 > \delta_1 > \cdots > \delta_m > 0$, be the singular values of the random matrix $\mathbf{R} \sim \mathcal{P}_{\mathcal{II}}\mathcal{R}^{\beta,I}_{n\times m}(\nu, k, \tau, 1, \mathbf{0}, \mathbf{I}_n, \mathbf{I}_m)$. Then its joint density is*

$$\frac{2^m \pi^{\beta m^2/2+\varrho}}{\Gamma^\beta_m[\beta m/2]\mathcal{B}^{*\,\beta}_m[\nu\beta/2, k; n\beta/2, \tau]} \prod_{i=1}^m \left(\delta_i^2\right)^{(n-m+1)\beta/2-1/2} \left(1 - \rho\sum_{i=1}^m \delta_i^2\right)^{\nu\beta/2+k-1}$$

$$\times \prod_{i<j}^m \left(\delta_i^2 - \delta_j^2\right)^\beta \frac{C^\beta_\tau(\mathbf{D}^2)}{C^\beta_\tau(\mathbf{I}_m)} \left(\bigwedge_{i=1}^m d\delta_i\right) \tag{14}$$

for $1 - \rho\sum_{i=1}^m \delta_i^2 > 0$. Where ϱ is defined in Lemma 2.2, $\mathbf{D} = \operatorname{diag}(\delta_1, \dots, \delta_m)$, *and $C^\beta_\kappa(\cdot)$ denotes the zonal spherical functions or spherical polynomials, see [16] and Faraut and Korányi [14, Chapter XI, Section 3].*

Proof. This follows immediately from (10). First using (6), then applying (1) and observing that, from [16, Equation 4.8(2) and Definition 5.3] and Faraut and Korányi [14, Chapter XI, Section 3], we have that for $\mathbf{L} \in \mathfrak{P}^\beta_m$,

$$C^\beta_\tau(\mathbf{Z}) = C^\beta_\tau(\mathbf{I}_m) \int_{\mathbf{H}\in\mathfrak{U}^\beta(m)} q_\kappa(\mathbf{HZH}^*)(d\mathbf{H}),$$

□

Finally, observe that $\delta_i = \sqrt{\operatorname{eig}_i(\mathbf{R}^*\mathbf{R})}$, where $\operatorname{eig}_i(\mathbf{A})$, $i = 1, \dots, m$, denotes the i-th eigenvalue of $\mathbf{A}$. Let $\lambda_i = \operatorname{eig}_i(\mathbf{R}^*\mathbf{R}) = \operatorname{eig}_i(\mathbf{B})$, observing that, for example, $\delta_i = \sqrt{\lambda_i}$. Then

$$\bigwedge_{i=1}^m d\delta_i = 2^{-m} \prod_{i=1}^m \lambda_i^{-1/2} \bigwedge_{i=1}^m d\lambda_i,$$

the corresponding joint densities of $\lambda_1, \dots, \lambda_m$, $1 > \lambda_1 > \cdots > \lambda_m > 0$ is obtained from (14) as

$$\frac{\pi^{\beta m^2/2+\varrho}}{\Gamma^\beta_m[\beta m/2]\mathcal{B}^{*\,\beta}_m[\nu\beta/2, k; n\beta/2, \tau]} \prod_{i=1}^m \lambda_i^{(n-m+1)\beta/2-1} \left(1 - \sum_{i=1}^m \lambda_i\right)^{\nu\beta/2+k-1}$$

$$\times \prod_{i<j}^m (\lambda_i - \lambda_j)^\beta \frac{C^\beta_\tau(\mathbf{G})}{C^\beta_\tau(\mathbf{I}_m)} \left(\bigwedge_{i=1}^m d\lambda_i\right)$$

for $1 - \sum_{i=1}^m \lambda_i > 0$, where $\mathbf{G} = \operatorname{diag}(\lambda_1, \dots, \lambda_m)$.

5. Conclusions

As visual examples, different Pearson type II-Riesz densities for $m = 1$ are showed in figures 1 and 2,

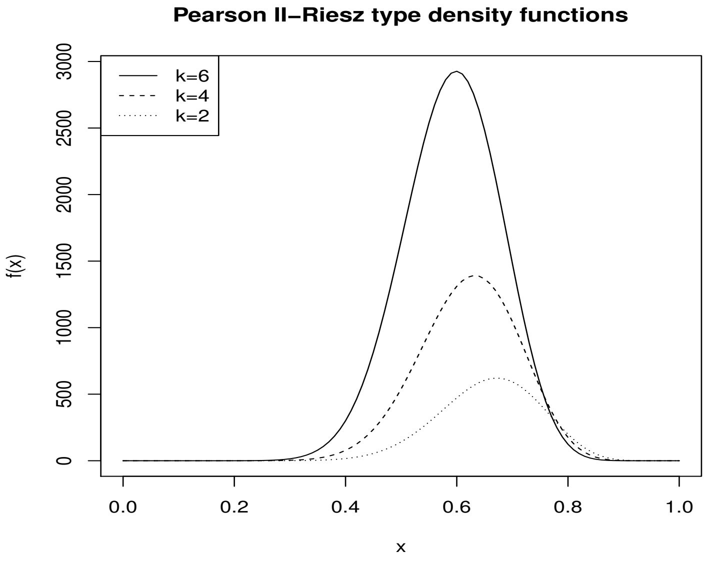

Figure 1. With $\nu = 15$, $n = 18$ and $t = 7$

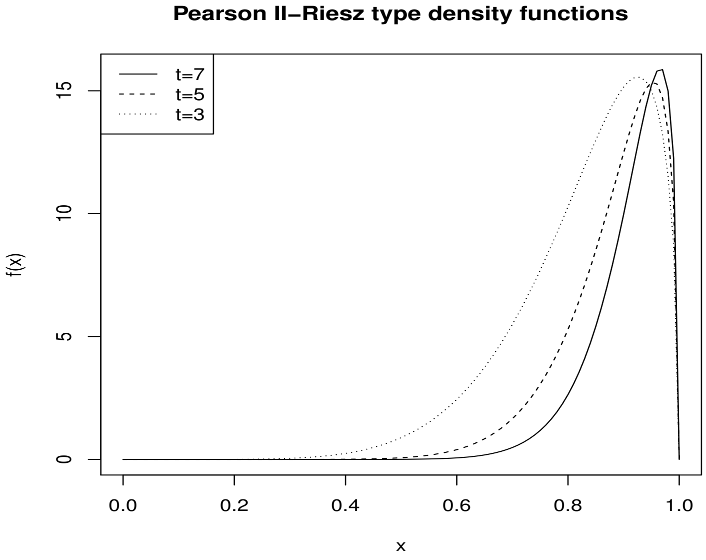

Figure 2. With $\nu = 3$, $n = 18$ and $k = 0$

Recall that in octonionic case, from the practical point of view, we most keep in mind the fact from [1], *there is still no proof that the octonions are useful for understanding the real world.* We can only hope that eventually this question will be settled on one way or another. In addition, as is established in [14] and [28] the result obtained in this article are valid for the *algebra of Albert*, that is when hermitian matrices ($\mathbf{S}$) or hermitian product of matrices ($\mathbf{X}^*\mathbf{X}$) are 3×3 octonionic matrices.

Acknowledgements

The authors wish to thank the Editor and the anonymous reviewers for their constructive comments on the preliminary version of this paper.

This paper was written during J. A. Díaz-García's stay as a visiting professor at the Department of Statistics and O. R. of the University of Granada, Spain; it stay was partially supported by IDI-Spain, Grants No. MTM2011-28962 and under the existing research agreement between the first author and the Universidad Autónoma Agraria Antonio Narro, Saltillo, México.

References

[1] J. C. Baez, The octonions. Bull. Amer. Math. Soc. **39** (2002), 145–205.

[2] I. Boutouria and A. Hassiri, Riesz exponential families on homogeneous cones. (2009). `http://arxiv.org/abs/0906.1892`. Also submitted.

[3] M. Casalis and G. Letac, The Lukascs-Olkin-Rubin characterization of Wishart distributions on symmetric cones, Ann. Statist. **24** (1996), 768–786.

[4] J. A. Díaz-García, Distributions on symmetric cones I: Riesz distribution. (2015a). `http://arxiv.org/abs/1211.1746v2`.

[5] J. A. Díaz-García, Distributions on symmetric cones II: Beta-Riesz distributions. (2015b). Cornell University Library, `http://arxiv.org/abs/1301.4525v2`.

[6] J. A. Díaz-García, A generalised Kotz type distribution and Riesz distribution. (2015c). Cornell University Library, `http://arxiv.org/abs/1304.5292v2`.

[7] J. A. Díaz-García and R. Gutiérrez-Jáimez, On Wishart distribution: Some extensions. Linear Algebra Appl. **435**(2011), 1296-1310.

[8] J. A. Díaz-García and R. Gutiérrez-Jáimez, Matricvariate and matrix multivariate Pearson type II distributions and related distributions. South African Statist. J. **46** (2012), 31-52.

[9] J. A. Díaz-García and R. Gutiérrez-Jáimez, Spherical ensembles. Linear Algebra Appl. **438**(2013), 3174 – 3201.

[10] J. A. Díaz-García and R. Gutiérrez-Sánchez. Generalised matrix multivariate T-distribution. (2015). Cornell University Library, `http://arxiv.org/abs/1402.4520v2`.

[11] J. M. Dickey, Matricvariate generalizations of the multivariate t- distribution and the inverted multivariate t-distribution. Ann. Mathemat. Statist. **38** (1967), 511-518.

[12] A. Edelman and R. R. Rao, Random matrix theory, Acta Numerica **14** (2005), 233–297.

[13] K. T. Fang and Y. T. Zhang, Generalized Multivariate Analysis. Science Press, Beijing, Springer-Verlang, 1990.

[14] J. Faraut and A. Korányi, Analysis on symmetric cones. Oxford Mathematical Monographs, Clarendon Press, Oxford, 1994.

[15] P. J. Forrester, Log-gases and random matrices. `http://www.ms.unimelb.edu.au/~matpjf/matpjf.html`, to appear.

[16] K. I. Gross and D. St. P. Richards, Special functions of matrix argument I: Algebraic induction zonal polynomials and hypergeometric functions. Trans. Amer. Math. Soc. **301** (1987) no. 2, 475–501.

[17] A. K. Gupta and D. K. Nagar, Matrix variate distributions. Chapman & Hall/CR, New York, 2000.

[18] A. K. Gupta and T. Varga, Elliptically Contoured Models in Statistics. Kluwer Academic Publishers, Dordrecht, 1993.

[19] A. Hassairi and S. Lajmi, Riesz exponential families on symmetric cones. J. Theoret. Probab. **14** (2001), 927–948.

[20] A. Hassairi, S. Lajmi and R. Zine, Beta-Riesz distributions on symmetric cones. J. Satatist. Plan. Inference, 1**33** (2005), 387 – 404.

[21] A. Hassairi, S. Lajmi and R. Zine, A chacterization of the Riesz probability distribution. J. Theoret. Probab. **21** (2008), 773-Ű790.

[22] H. Ishi, Positive Riesz distributions on homogeneous cones. J. Math. Soc. Japan, **52** (2000) no. 1, 161 – 186.

[23] B. Kołodziejek, The Lukacs-Olkin-Rubin theorem on symmetric cones without invariance of the "Quotient". J. Theoret. Probab. (2014). DOI 10.1007/s10959-014-0587-3.

[24] H. Massam, An exact decomposition theorem and unified view of some related distributions for a class of exponential transformation models on symmetric cones. Ann. Statist. **22** (1994) no. 1, 369–394.

[25] J. Neukirch, A. Prestel and R. Remmert, Numbers. GTM/RIM 123, H.L.S. Orde, tr. NWUuser, 1990.

[26] T. Ratnarajah, R. Villancourt and A. Alvo, Complex random matrices and Rician channel capacity. Probl. Inf. Transm. **41** (2005a), 1–22.

[27] Ratnarajah, T., Villancourt, R. and Alvo, A. (2005b), Eigenvalues and condition numbers of complex random matrices. SIAM J. Matrix Anal. Appl. **26** (2005b), 441–456.

[28] P. Sawyer, Spherical Functions on Symmetric Cones. Trans. Amer. Math. Soc. **349** (1997), 3569 – 3584.

Albanian Journal of Mathematics (ISSN: 1930-1235) was founded by T. Shaska in 2007 with the idea to support Albanian mathematicians in Albania and abroad.

The journal is not associated with any government institutions in Albania or any public or private universities in Albania or abroad. The journal does not charge any fees to the authors and has always been an open access journal. The journal supports itself with private donations and voluntary work from its staff. Its main office is in Vlora, Albania.

www.albanian-j-math.com