

SURFACE SYMMETRIES AND $PSL_2(p)$

MURAD ÖZAYDIN, CHARLOTTE SIMMONS, AND JENNIFER TABACK

ABSTRACT. We classify, up to conjugacy, all orientation-preserving actions of $PSL_2(p)$ on closed connected orientable surfaces with spherical quotients. This classification is valid in the topological, PL, smooth, conformal, geometric and algebraic categories and is related to the Inverse Galois Problem.

1. INTRODUCTION

A classical fact, essentially due to Riemann, states that any finite group G can be realized as a subgroup of orientation-preserving homeomorphisms of some (closed, connected, orientable) surface X . In fact, one can also arrange it so that G is a subgroup of complex analytic automorphisms with respect to some complex structure on X , and the quotient $G \backslash X$ is the Riemann sphere. This is equivalent to a solution of the Inverse Galois Problem over the function field $\mathbb{C}(t)$. (The field of meromorphic functions on X is a field extension of $\mathbb{C}(t)$ = the field of meromorphic functions on the sphere $G \backslash X$ with Galois group G .) This realization can be accomplished by picking a set of generators for G , to be explained in detail in Section 2 below. Fixing the group G , we can then ask for $Gen(G) \subset \mathbb{Z}$, the set of all possible genera of closed, connected, orientable surfaces on which G can act faithfully, preserving the orientation, or the set of spherical genera when we also require that the quotient $G \backslash X$ is a sphere. The answer is best phrased in terms of G -signatures (defined below) and is given in our Corollaries 5.9 and 5.10 for $PSL_2(p)$, $p > 11$. These results, somewhat surprisingly, say that any signature satisfying some obviously necessary conditions is a $PSL_2(p)$ -signature.

Now let G be a nontrivial finite subgroup of orientation-preserving homeomorphisms of a closed connected orientable surface X . Then the *singular set* S of points with nontrivial stabilizer is discrete, hence finite. This is easy to show when the action is smooth (or piecewise-linear), but harder to prove in the topological category [T]. Denote the *branch set* $G \backslash S$ by $B = \{b_1, b_2, \dots, b_k\}$. We are primarily interested in the case when the quotient $G \backslash X$ is homeomorphic to a sphere, so B is nonempty (otherwise $X \rightarrow G \backslash X$ would be a nontrivial regular cover of the sphere).

Actions of G on a closed connected orientable surface X are usually classified by their *signatures* $(h; m_1, m_2, \dots, m_k)$, where h is the genus of the quotient $G \backslash X$ and $m_i \geq 2$ is the order of the (necessarily cyclic) stabilizer of any preimage of b_i in S . When $G \backslash X$ has genus $h = 0$, the signature will be denoted (m_1, m_2, \dots, m_k) . If we can find a G -action with signature (m_1, m_2, \dots, m_k) , then (m_1, m_2, \dots, m_k) is

Received by the editors February 1, 2003 and, in revised form, March 14, 2005.

2000 *Mathematics Subject Classification*. Primary 57M60; Secondary 12F12, 20H10, 30F10.

©2006 American Mathematical Society

called a G -signature. This is equivalent to finding a set of generators $\{g_1, g_2, \dots, g_k\}$ of G such that $g_1 g_2 \cdots g_k = 1$ with the order of g_i equaling m_i (see Proposition 2.1 below). We then say that (g_1, g_2, \dots, g_k) is a realization of the G -signature (m_1, m_2, \dots, m_k) . If we drop the requirement that $\{g_1, g_2, \dots, g_k\}$ generates G , then (m_1, m_2, \dots, m_k) is a partial G -signature. Clearly $k \geq 2$ when G is nontrivial, and if $k = 2$, then $m_1 = m_2$ and G is cyclic of order m_1 .

A finer classification of G -actions with spherical quotient is given by the ramification type $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k)$ where the \mathcal{C}_i 's are the conjugacy classes of the elements $\phi(c_i)$ in G . A ramification type $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k)$ corresponds to the signature $(m(\mathcal{C}_1), m(\mathcal{C}_2), \dots, m(\mathcal{C}_k))$, where $m(\mathcal{C})$ is the order of any element of \mathcal{C} . We realize a ramification type analogously (with $g_i \in \mathcal{C}_i$), and a ramification type yielding a G -signature is called a G -ramification type.

Any permutation of a ramification type yields another ramification type; if the elements (g_1, g_2, \dots, g_k) give a realization for the ramification type $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k)$, then the elements $(g_1, \dots, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, \dots, g_k)$ give a realization for the ramification type $(\mathcal{C}_1, \dots, \mathcal{C}_{i+1}, \mathcal{C}_i, \dots, \mathcal{C}_k)$.

In this paper, we determine all possible $PSL_2(p)$ -ramification types for primes $p > 11$. In particular we have the following result.

Corollary 5.9. *For p prime, $p > 11$, a signature (m_1, m_2, \dots, m_k) is a $PSL_2(p)$ -signature if and only if each m_i is either p or a divisor of $\frac{p \pm 1}{2}$ and $\sum_{i=1}^k \left(1 - \frac{1}{m_i}\right) > 2$.*

The first condition (on the m_i) is necessary because any element of $PSL_2(p)$ has order equal to p or dividing $\frac{p \pm 1}{2}$. The necessity of the second condition follows from the Riemann-Hurwitz formula below, and signatures satisfying this condition are called *hyperbolic*. Determining all $PSL_2(p)$ -signatures for $p \leq 11$ can be handled individually; for instance, $p = 7$ is done in detail in [MS]. Note that Corollary 5.9 is not valid for $p \leq 11$; for instance, one can easily check (using CAYLEY for example) that the signature $(2, 2, 2, 2, 2)$ satisfies the hypothesis but it is not a $PSL_2(p)$ -signature for $p \leq 11$.

While $X \rightarrow G \backslash X$ is a branched cover, its restriction to $X - S$ is a regular cover. Hence, $\chi(X - S) = |G| \chi(Y)$, where χ denotes the Euler characteristic and $Y = (G \backslash X) - B$. This is the *Riemann-Hurwitz formula*

$$2 - 2g = |G| \left(2 - 2h - \sum_{i=1}^k \left(1 - \frac{1}{m_i} \right) \right),$$

where g is the genus of X and h is the genus of $G \backslash X$. When the quotient $G \backslash X$ is a sphere, we have $h = 0$, so the genus g of X can be computed from the signature (m_1, m_2, \dots, m_k) .

The Riemann-Hurwitz formula imposes strong restrictions on the m_i , and consequently, on the group G when $g \leq 1$, as described in the table (next page).

In the spherical case, the standard actions of the cyclic and the dihedral groups (as rotations) and the rotational symmetries of the tetrahedron, the cube, and the dodecahedron give geometric realizations for G . If $\sigma := (m_1, m_2, \dots, m_k)$ is a Euclidean or hyperbolic signature, G is not determined by σ , in fact, we have infinitely many groups G for each signature. When σ is Euclidean, G is solvable (because G is a quotient of its lift to the universal cover, which is a subgroup of the orientation-preserving isometries of the Euclidean plane, a solvable group). When

σ is hyperbolic, it follows from our classification (Corollary 5.9 below) that σ can be realized as a $PSL_2(p)$ -signature for some $p > 11$ (so there is a nonsolvable G for each hyperbolic signature). In the next section, we will describe geometric realizations for all of these signatures.

Case	g	Possible signatures (m_1, \dots, m_k)	Group G
Spherical	0	(m,m)	cyclic
		(2,2,m)	Dihedral of order 2m
		(2,3,3)	A_4
		(2,3,4)	S_4
		(2,3,5)	A_5
Euclidean	1	(2,3,6)	See Section 2
		(2,4,4)	"
		(3,3,3)	"
		(2,2,2,2)	"
Hyperbolic	> 1	all remaining	"

We can eliminate certain signatures which cannot occur as $PSL_2(p)$ -signatures using the orbifold Euler characteristic $\chi(\sigma) := \left(2 - 2h - \sum_{i=1}^k \left(1 - \frac{1}{m_i}\right)\right)$ where $\sigma = (h, m_1, m_2, \dots, m_k)$. The following standard lemma follows from the discussion above.

Lemma 1.1. *Let G be a finite group.*

- (1) *If there exists a G -signature σ with $\chi(\sigma) > 0$, then G is isomorphic to one of the groups $\mathbb{Z}_n, \mathbb{D}_n, A_4, S_4$ or A_5 .*
- (2) *If there exists a G -signature σ with $\chi(\sigma) = 0$, then G is solvable. More specifically, G contains a normal abelian subgroup of index 1, 2, 3, 4 or 6 which is generated by 2 elements.*

Another consequence of the Riemann-Hurwitz formula is the Hurwitz $84(g - 1)$ Lemma which states that for $g > 1$, $84(g - 1)$ is an upper bound for the order of any group of orientation-preserving homeomorphisms of a surface of genus g (see e.g., [H], [St]). When the order of G equals $84(g - 1)$, the group G is called a *Hurwitz group*; this happens if and only if $G \backslash X$ is a sphere and the signature is $(2, 3, 7)$. If G is a Hurwitz group, then the smallest possible genus g for a surface admitting a G -action is $g = 1 + \frac{|G|}{84}$ (by the Riemann-Hurwitz formula). Macbeath [Ma1] proved that $PSL_2(q)$ is a Hurwitz group if and only if: $q = 7$ or q is a prime congruent to $\pm 1 \pmod{7}$ or $q = p^3$ where $p \neq 7$ is a prime not congruent to $\pm 1 \pmod{7}$ (see also [Ma2]).

As above, let $Gen(G)$ be the set of all possible genera of closed, connected, orientable surfaces on which G can act effectively, preserving the orientation. Glover and Sjerve [GS1, GS2] determined the smallest elements of $Gen(PSL_2(p))$ and $Gen(PSL_2(q))$ for q odd. It is easy to see that when the smallest genus arises, $G \backslash X$ is a sphere and the signature is a triple (m_1, m_2, m_3) . Hence, the smallest genus is obtained by plugging (m_1, m_2, m_3) satisfying the conditions of Corollary 5.9 above into the Riemann-Hurwitz formula and minimizing g .

We call $g \in Gen(G)$ a spherical genus for $PSL_2(p)$ if the quotient surface is a sphere. Corollary 5.9 lists all signatures corresponding to spherical genera for $PSL_2(p)$, where $p > 11$. However, a little more work yields all genera for $PSL_2(p)$.

The set $Gen(G)$ for a cyclic p -group G was computed in [KM]. The algebraic structure of $Gen(G)$ was studied in [K] and [McM]. The authors would like to thank Andy Miller for suggesting this problem for $PSL_2(p)$ to us.

2. BACKGROUND ON SURFACE SYMMETRIES

First, we want to give a short proof of a variant of the Riemann Existence Theorem (Proposition 2.1 below). Our strategy is to utilize equivariant *fatgraphs* to reduce the problem to a free action of the group G on a finite graph. This approach also explains the equivalence of the realization problem in the topological, piecewise linear, smooth, complex analytic, and Riemannian categories. Later we discuss some related topics.

Geometrically, a (finite) *fatgraph* (also called a *map* [JS], *dessins d'enfants* [SV], [Sc], or a *ribbon graph* [MP]) is a (finite) graph (i.e., a 1-dimensional CW-complex) embedded on an oriented closed surface so that its complement is a disjoint union of disks. The extra structure provided by the embedding is the (clockwise) circular ordering of the *darts*, i.e. directed edges, terminating at each vertex. The graph can be fattened to a bordered surface, or all the way to a punctured surface without changing its homotopy type. The punctures correspond to the 2-cells in the geometric cell decomposition of the surface where the 0-cells are the vertices of the graph and the 1-cells are the edges. The surface can be recovered by filling in the punctures, i.e., compactifying the ends. The data of a fatgraph Γ can be given combinatorially as a triple $(D_\Gamma, -, *)$, where $D = D_\Gamma$ is the (finite) set of darts, $d \rightarrow \bar{d}$ is a free involution on D corresponding to reversing the direction of d , and “ $*$ ” is a permutation defined on D , so that d^* is the next dart in the clockwise circular ordering of the darts terminating at a vertex. The edge set E_Γ of the underlying graph will be pairs $\{d, \bar{d}\}$, i.e., the orbits of $-$, and the vertex set V_Γ the $*$ -orbits of darts. The terminal vertex of a dart is its $*$ -orbit. Once the involution $-$ is specified, the fatgraph can also be defined using the permutation \prime of D given by $d \rightarrow d' = \overline{(d^*)}$ instead of $*$.

The orbits $\{d, d', \dots, d^{(n)}, \dots\}$ of the permutation \prime give the boundaries of the (oriented) faces, i.e., 2-cells, of the surface determined by the fatgraph. We obtain the surface $X(\Gamma)$ as the 2-complex whose 1-skeleton $X(\Gamma)^1$ is the underlying graph of Γ ; the 2-cells are obtained by gluing n -gons to the \prime -orbits along their (oriented) boundary, where n is the size of the orbit. It is easy to check that the 2-complex $X(\Gamma)$ is a (closed, oriented) surface. Then $X(\Gamma)$ will be connected if and only if $X(\Gamma)^1$ is connected; we say that Γ is connected when this happens. The fatgraph Γ will be connected if and only if $-$ and $*$ equivalently, $-$ and \prime generate a transitive permutation group.

The *dual fatgraph* Γ^\perp has dart set $\{d^\perp \mid d \in D_\Gamma\}$ and $\overline{d^\perp} = (\bar{d})^\perp$, $(d^\perp)^* = (d')^\perp$. We note that $d^{\perp\perp}$ is identified with d . Then Γ^\perp gives the dual cell structure on the surface X where the new vertices are the old faces (and vice-versa) and the new edges can be thought of as the old edges rotated ninety degrees counterclockwise. Thus, $X(\Gamma)$ and $X(\Gamma^\perp)$ are the “same” surface, but with opposite orientations.

A *morphism* from a fatgraph Γ to a fatgraph Λ is a function $f : D_\Gamma \rightarrow D_\Lambda$ satisfying $f(\bar{d}) = \overline{f(d)}$ and $f(d^*) = f(d)^*$, hence $f(d') = f(d)'$, for every d in D_Γ . We say that a subgroup G of the automorphism group of Γ is acting *freely* on Γ when the induced actions on the vertex set V_Γ and the edge set E_Γ are both free. For such G , there is an induced fatgraph structure on $G \backslash \Gamma$ (the induced involution

– is free on $G \backslash D$ because G is acting freely on the edges), and the quotient map $\Gamma \rightarrow G \backslash \Gamma$ is a fatgraph morphism.

If G is acting freely on Γ , then the induced map $X(\Gamma)^1 \rightarrow X(G \backslash \Gamma)^1$ is a regular cover with G as the deck transformation group. Each dart d defines a path, every path is homotopic to a composition of darts, and we can talk about lifts of (compositions of) darts from $G \backslash \Gamma$ to Γ . There is an induced action on the surface $X := X(\Gamma)$ (because the action of G is compatible with ι), so G is a subgroup of $\text{Homeo}^+(X)$. This action is not necessarily free, but its singular set is a subset of the vertices of Γ^\perp (i.e., the punctures or the centers of the 2-cells of X). We can identify $G \backslash X$ with $X(G \backslash \Gamma)$. The restriction of the branched cover $X \rightarrow G \backslash X$ to a 2-cell is $z \mapsto z^m$ (where m is the order of the stabilizer of the 2-cell) when we use local coordinates identifying 2-cells (corresponding to faces of Γ and $G \backslash \Gamma$) with the unit disk in \mathbb{C} . If a face (equivalently, the corresponding puncture) is singular, then its stabilizer is a cyclic subgroup of G with a preferred generator given by the smallest nontrivial counterclockwise rotation fixing that face.

Example A. Consider the graph embedded on the sphere with two vertices, the north pole and the south pole, and k (≥ 2) edges given by meridians joining the two poles. The corresponding fatgraph Λ_k has $2k$ darts of the form i or \bar{i} , where i is an integer mod k . Each i is an oriented edge starting at the south pole and terminating at the north pole. Finally, let $i^* = i - 1$ and $(\bar{i} - 1)^* = \bar{i}$. The faces (= the orbits of ι) are the k bigons $\{\bar{i} - 1, i\}$. The dual fatgraph Λ_k^\perp has k vertices (corresponding to the faces of Λ_k), say b_1, b_2, \dots, b_k , ordered counterclockwise around the equator and k edges (hence $2k$ darts), which are arcs along the equator connecting adjacent vertices. The two faces of Λ_k^\perp are the northern and the southern hemispheres.

Example B. Let G be a (finite) group and let $g_1, g_2, \dots, g_k \in G$ with $g_1 g_2 \cdots g_k = 1$. We define $\Gamma = \Gamma(G; g_1, g_2, \dots, g_k)$ to be the fatgraph with $2k|G|$ darts (g, i) or (g, \bar{i}) where $g \in G$ and i is an integer mod k ; $(g, a) = (g, \bar{a})$; $(g, i)' = (g, \bar{i} - 1)$ and $(g, \bar{i} - 1)' = (gg_i, i)$ (equivalently, $(g, i)^* = (g, i - 1)$ and $(g, \bar{i} - 1)^* = (gg_i, \bar{i})$). The faces of Γ are the $2m_i$ -gons (where m_i is the order of g_i) with (oriented) boundary: $(g, i), (g, i)' = (g, \bar{i} - 1), (g, \bar{i} - 1)' = (gg_i, i), \dots, (gg_i^{m_i}, i) = (g, i)$. There are $|G| \sum_{i=1}^k \frac{1}{m_i}$ faces indexed by the (disjoint union of the) left cosets of the cyclic subgroups generated by g_i for $i = 1, \dots, k$. The connected components of the fatgraph Γ correspond to the left cosets of the subgroup $\langle g_1, g_2, \dots, g_k \rangle$, in particular, Γ is connected if and only if g_1, g_2, \dots, g_k generate G . We have a free action of G on Γ given by $g(h, a) := (gh, a)$, and $G \backslash \Gamma$ is the fatgraph Λ_k of Example A. Let x_i be the center of the face with boundary $(1, i), (1, i)' = (1, \bar{i} - 1), (1, \bar{i} - 1)' = (g_i, i), \dots, (g_i^{m_i}, i) = (1, i)$. The singular set of the G -action on $X(\Gamma) = X(\Gamma^\perp)$ consists of the G -orbits of those x_i for which g_i is nontrivial. The stabilizer subgroup G_{x_i} is $\langle g_i \rangle$. Two free G -orbits of k -gons, one with vertices x_1, x_2, \dots, x_k lying over the northern hemisphere, the other a mirror image of this lying over the southern hemisphere, make up the faces of Γ^\perp .

Conversely, assume that a finite group G is acting freely on a connected fatgraph Γ , with Λ_k as the quotient $G \backslash \Gamma$. The fundamental group π of the underlying graph of Λ_k (based at the north pole) is generated by $\beta_i := [\bar{i} - 1, i]$ satisfying the single relation $\beta_1 \cdots \beta_k = 1$ (where $[\bar{i} - 1, i]$ is the homotopy class of the loop given by the composition of the paths (darts) $\bar{i} - 1$ followed by i). We have an epimorphism $\phi : \pi \rightarrow G$, because G is the group of deck transformations of a

connected regular cover. Let $g_i := \phi(\beta_i)$, and let us fix a vertex v of Γ lying over the north pole. We will identify the dart set D_Γ with $G \times D$, where D is the dart set of the fatgraph Λ_k , as follows: Let $(1, i) \in D_\Gamma$ be the lift of $i \in D$ terminating at v , let $(1, \bar{i})$ be the lift of \bar{i} starting at v , and let $(g, d) := g(1, d)$ for $g \in G$ and $d \in D$. The action of G on $D_\Gamma = G \times D$ is the standard left action because $g(h, d) = g(h(1, d)) = (gh)(1, d) = (gh, d)$ for all $g, h \in G$ and $d \in D$. The projection $D_\Gamma \rightarrow D$ is given by the projection onto the second factor of $G \times D$, and we have $\overline{(g, d)} = (g, \bar{d})$. Now we want to determine the permutation $*$ on $D_\Gamma = G \times D$.

Let u denote the initial vertex of the dart $(1, 0)$ of Γ . The vertex set of Γ is the disjoint union of the G -orbits of u and v . From covering space theory, we have that the lift of the loop $\bar{0} 1$, starting at v , terminates at $\phi(\beta_1)v = g_1v$. But the lift of $\bar{0}$, starting at v , is $(1, 0)$ which terminates at u , hence the lift of 1 starting at u terminates at g_1v . Similarly, the lift of $\bar{0} i$ (which is homotopic to $\bar{0} 1 \bar{1} 2 \cdots \bar{i-1} i$), starting at v , terminates at $\phi(\beta_1 \cdots \beta_i)v = g_1g_2 \cdots g_iv$, and hence the lift of i starting at u terminates at $g_1g_2 \cdots g_iv$. Therefore, $(g_1 \cdots g_i, \bar{i})$, the unique dart lying over \bar{i} and starting at $g_1 \cdots g_iv$, has u as its terminal vertex. Considering the darts terminating at v , we see that $(1, i)^* = (1, i-1)$, because $*$ commutes with the projection $D_\Gamma \rightarrow D$; similarly, considering the darts terminating at u , we get that $(g_1 \cdots g_i, \bar{i})^* = (g_1 \cdots g_{i+1}, \overline{i+1})$. As the G -action also commutes with $*$, we have $(g, i)^* = (g, i-1)$ and $(g, \overline{i-1})^* = (gg_i, \bar{i})$ for all $g \in G$ and where i is an integer mod k . Thus, Γ is $\Gamma(G; g_1, g_2, \dots, g_k)$ defined above.

We can also put a geometric structure on $X(\Gamma)$, $\Gamma = \Gamma(G; g_1, g_2, \dots, g_k)$, i.e., a constant curvature (± 1 or 0) Riemannian metric such that G becomes a group of orientation preserving isometries. Let (m_1, m_2, \dots, m_k) denote the spherical signature associated with (g_1, g_2, \dots, g_k) as in Section 1 (where m_i is the order of g_i). In the cellular structure given by Γ^\perp , we have two free G -orbits of k -gons (one with vertices x_1, x_2, \dots, x_k , the other a mirror image). We can find a convex k -gon with interior angles (at x_i) being $\frac{\pi}{m_i}$ in the appropriate geometry (spherical, Euclidean, or hyperbolic depending on whether $\sum_{i=1}^k m_i$ is greater than, equal to, or less than $k-2$, respectively). This is elementary plane geometry when we have equality (Euclidean), easy to do case by case for the spherical signatures $(m, m), (2, 2, m), (2, 3, 3), (2, 3, 4), (2, 3, 5)$, and is standard hyperbolic geometry for the remaining cases (see, e.g., [B]). We use $|G|$ copies of such a k -gon and $|G|$ copies of its reflection as the faces of $X(\Gamma^\perp)$. The edge lengths match because we have k free G -orbits of edges, one orbit for each side of the k -gon with vertices x_1, x_2, \dots, x_k . At each vertex the geometry is defined because the $2m_i$ interior angles add up to 2π .

When G is a group of orientation-preserving isometries, then (forgetting the metric structure) it is also a group of conformal (equivalently complex analytic) automorphisms. Specifically, at the level of the universal cover of X , when $g = 0$, the orientation-preserving isometry group is $SO_2(\mathbb{R})$, a maximal compact subgroup of $PSL_2(\mathbb{C})$, the group of complex automorphisms of \mathbb{CP}^1 . When $g = 1$, the group of rigid motions of the Euclidean plane is a subgroup of $\{az + b \mid a \in \mathbb{C}^\times, b \in \mathbb{C}\}$, the automorphisms of the complex plane. Finally, when $g > 1$, $PSL_2(\mathbb{R})$ is both the orientation-preserving isometry group of the hyperbolic plane and the complex automorphism group of the upper half plane. Now we are ready to prove a variant of the Riemann Existence Theorem.

Proposition 2.1. *Let G be a finite group and let g_1, g_2, \dots, g_k be elements of G so that $G = \langle g_1, g_2, \dots, g_k \rangle$ and $g_1 g_2 \cdots g_k = 1$. Then there is a closed connected orientable surface X with constant curvature such that G is a subgroup of $Isom^+(X)$ and $G \backslash X$ is the sphere. Conversely, if G is a subgroup of $Homeo^+(X)$ for a closed connected orientable surface X with $G \backslash X$ homeomorphic to the sphere, then we can find x_1, x_2, \dots, x_k in X belonging to distinct G -orbits and a generating set $\{g_1, g_2, \dots, g_k\}$ of G with $G_{x_i} = \langle g_i \rangle$ and $g_1 g_2 \cdots g_k = 1$.*

Proof. The first implication follows from Example B. For the converse, let $B = \{b_1, b_2, \dots, b_k\}$ be the branch set in $G \backslash X = \mathbb{S}^2$. Let Λ_k (with vertices at the poles and $2k$ darts along meridians) be embedded in \mathbb{S}^2 as in Example A. Up to a homeomorphism, we may assume that b_i is placed on the equator, between the darts $i - 1$ and i . So $G \backslash X$ is $X(\Lambda_k)$. Let Z be the underlying graph of Λ_k and $Y = q^{-1}(Z)$, where $q : X - S \rightarrow \mathbb{S}^2 - B$. We can identify Y with the 1-skeleton of $X(\Gamma)$, $\Gamma = \Gamma(G; g_1, g_2, \dots, g_k)$, with g_i chosen as in Example B. Both q and the restriction of q to Y are regular covers (with deck transformation group G), and Z is a strong deformation retract of $\mathbb{S}^2 - B$, so Y is a G -equivariant strong deformation retract of $X - S$. Also, Y (as the 1-skeleton of $X(\Gamma)$) is a G -equivariant strong deformation retract of $X(\Gamma) - F$ where F is the vertices of Γ^\perp . From covering space theory, it follows that $q : X - S \rightarrow \mathbb{S}^2 - B$ and $X(\Gamma) - F \rightarrow \mathbb{S}^2 - B$ are the “same,” i.e., there is a G -equivariant homeomorphism from $X - S$ to $X(\Gamma) - F$. But the G -action on the punctures (= ends) is forced, and there is only one compactification of a punctured surface which is a closed surface, so X is homeomorphic to $X(\Gamma)$, the singular set S mapping to $F = \{x_1, x_2, \dots, x_k\}$ of Example B. \square

There are two more cases equivalent to realizing G as a group of conformal automorphisms of a Riemann surface X with spherical quotient. These are realizing G as a Galois group over the field $\mathbb{C}(t)$, and having G as a group of automorphisms of a complex projective curve. The Inverse Galois Problem over a field \mathbb{F} asks whether we can find a field extension \mathbb{E} of \mathbb{F} with G a subgroup of $Aut(\mathbb{E})$ so that the fixed field $\mathbb{E}^G = \{\alpha \in \mathbb{E} \mid \alpha g = \alpha\}$ is \mathbb{F} . When G is a group of complex analytic automorphisms of a Riemann surface X (with $G \backslash X = \mathbb{C}P^1$), then the field \mathbb{E} of meromorphic functions on X , i.e., $\mathbb{E} = \{f : X \rightarrow \mathbb{C}P^1 \mid f \text{ is holomorphic}\}$, has an induced right G -action via $(fg)(x) = f(gx)$. From our description above of the local structure of the G -action on X , it is rather transparent that \mathbb{E}^G can be identified with the meromorphic functions on $G \backslash X = \mathbb{C}P^1$. But the field of meromorphic functions on $\mathbb{C}P^1$ is isomorphic to $\mathbb{C}(t)$ [FK], so we have a solution for the Inverse Galois Problem.

Conversely, if G is the Galois group of the field extension $\mathbb{E}/\mathbb{C}(t)$, we can construct a complex projective curve X which is obtained from a polynomial over $\mathbb{C}(t)$ whose splitting field is \mathbb{E} and a morphism $X \rightarrow \mathbb{C}P^1$ such that the meromorphic functions functor described above yields the inclusion $\mathbb{F} \rightarrow \mathbb{E}$ [Mi]. Now G can be recovered as the automorphisms of X covering the identity morphism on $\mathbb{C}P^1$. The points of X correspond to discrete valuations on \mathbb{E} , i.e., surjective maps $\nu : \mathbb{E}^\times \rightarrow \mathbb{Z}$ satisfying $\nu(ab) = \nu(a) + \nu(b)$ and $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$. The singular points correspond to valuations $\nu : \mathbb{E}^\times \rightarrow \mathbb{Z}$ such that the composition $\mathbb{F}^\times \rightarrow \mathbb{E}^\times \rightarrow \mathbb{Z}$ is not onto. The index of the image of this composition in \mathbb{Z} equals the order of the inertia group of ν , which corresponds to a stabilizer subgroup.

Realizing any finite group G as a Galois group over $\mathbb{C}(t)$ is essentially due to Riemann, and the discussion above contains a proof of the so-called Riemann Existence Theorem. The Inverse Galois Problem for G over \mathbb{Q} is a fundamental open problem and an active area of current research. The most common approach to this problem is to begin with a solution over $\mathbb{C}(t)$ and then to descend to a (regular) Galois extension of $\mathbb{Q}(t)$. This gives realizations over \mathbb{Q} via Hilbert's Irreducibility Theorem [MM], [Se], [FK]. Currently, the answer to the Inverse Galois Problem for $PSL_2(p)$ over \mathbb{Q} is still not known for infinitely many primes p . This was one of the motivations for our consideration of all ramification types for $PSL_2(p)$ over $\mathbb{C}(t)$.

A related question (in the topological version) comes from considering (closed, connected) branched covers $f : Z \rightarrow \mathbb{S}^2$ of the sphere, that is, there is a finite branch set $B := \{ p \in \mathbb{S}^2 \mid |f^{-1}(p)| < N \}$ such that the restriction $f : Z - f^{-1}(B) \rightarrow \mathbb{S}^2 - B$ is a finite (N -fold) cover. In our setup, this corresponds to looking at $M \backslash X \rightarrow \mathbb{S}^2$, where M is a subgroup of G which is a finite subgroup of orientation-preserving homeomorphisms of X . The group G and the (closed, connected, orientable) surface X can be recovered from the branched cover $f : Z \rightarrow \mathbb{S}^2$ as follows:

$$G \cong \pi_1(\mathbb{S}^2 - B) / \bigcap_{\alpha \in \pi_1(\mathbb{S}^2 - B)} (f_{\#} \pi_1(Z - f^{-1}(B)))^{\alpha},$$

or equivalently, $\pi_1(\mathbb{S}^2 - B, p)$ permutes the N points in a fiber $f^{-1}(p)$ for $p \in \mathbb{S}^2 - B$. This gives a transitive permutation representation $\rho : \pi_1(\mathbb{S}^2 - B, p) \rightarrow \text{Sym}(N)$. G is (isomorphic to) the image of ρ , and $M = \pi_1(Z - f^{-1}(B)) / \ker(\rho)$.

To recover X in the analytic/algebraic category, $f : Z \rightarrow \mathbb{S}^2$ corresponds to the field extension $\mathbb{K}(\mathbb{S}^2) = \mathbb{C}(t) \hookrightarrow \mathbb{K}(\mathbb{Z})$ (= meromorphic functions on \mathbb{Z}). Let \mathbb{E} be the splitting field of $\mathbb{K}(\mathbb{Z})$, that is, the smallest Galois extension containing $\mathbb{K}(\mathbb{Z})$. Now X is the Riemann surface which corresponds to \mathbb{E} , that is, $\mathbb{K}(X)$ is \mathbb{E} and $\mathbb{K}(X)^G = \mathbb{C}(t)$ and $\mathbb{K}(X)^M = \mathbb{K}(\mathbb{Z})$.

So a finite branched cover $f : Z \rightarrow \mathbb{S}^2$ corresponds to a pair (G, M) , where G is a finite subgroup of $\text{Homeo}^+(X)$ and $X \rightarrow G \backslash X = \mathbb{S}^2$ is a "regular" branched cover. The (transitive permutation) representation of G on $f^{-1}(p)$ (which is equivalent as a G -set to $M \backslash G$) is faithful by definition, hence M does not contain any nontrivial normal subgroup of G . Consequently, the branch set B of $f : Z \rightarrow \mathbb{S}^2$ coincides with the branch set $G \backslash S$, where $S = \{ x \in X \mid G_x \neq 1 \}$.

If X is also \mathbb{S}^2 , then $f : X \rightarrow \mathbb{S}^2$ is *indecomposable* if it cannot be factored as a composition of two nontrivial branched covers. Any branched cover $f : \mathbb{S}^2 \rightarrow \mathbb{S}^2$ is a product of indecomposable ones. An indecomposable branched cover $f : \mathbb{S}^2 \rightarrow \mathbb{S}^2$ corresponds to a pair (G, M) , where M is a maximal subgroup of G (i.e., the permutation action of G on $M \backslash G$ is primitive).

There is an ongoing program to classify all primitive nongeneric branched covers $f : \mathbb{S}^2 \rightarrow \mathbb{S}^2$ [GT, FGM]. (Nongeneric means that the image of ρ is not the full symmetric group or the alternating group.) The classification in [FGM] includes all Lie-type rank-one G , in particular, $PSL_2(q)$. However, these restrictions rule out many actions; specifically, in this case $|B| \leq 6$.

In this paper, we only consider "regular" branched covers $X \rightarrow G \backslash X$ with $G = PSL_2(p)$ (for $p > 11$), and show in particular that any branch data satisfying the two easy necessary conditions of Corollary 5.9 is realizable. The first condition

is that the genus of X is larger than one because the only finite simple G possible for genus 0 and 1 is $\text{Alt}(5) = PSL_2(5)$ as indicated in the table in Section 1. The second condition is the obvious one that there has to be an element g_i of order m_i for each i , $1 \leq i \leq k$. In particular, there is no bound on $k = |B|$, unlike the case of primitive nongeneric branched covers classified in [FGM].

3. THE STRUCTURE OF $PSL_2(q)$

In this section we discuss the structure of $PSL_2(q)$, the projective special linear group with entries in the finite field \mathbb{F}_q , where $q = p^n$ for p an odd prime.

Let $\mathbb{F} = \mathbb{F}_q$ and $\mathbb{E} = \mathbb{F}_{q^2}$. Let $f(x)$ be any monic irreducible quadratic of the form $x^2 + \beta$ in the ring of polynomials $\mathbb{F}[x]$, with $\pm\alpha \in \mathbb{E}$ as roots. Then

$$\mathbb{F}[x]/\langle f(x) \rangle \cong \mathbb{F} \oplus \mathbb{F}\alpha \cong \mathbb{E}.$$

Thus, any element of \mathbb{E} can be expressed uniquely as $a + b\alpha$ with a and b in \mathbb{F} . If $\lambda = a + b\alpha \in \mathbb{E}$, define $\bar{\lambda} = a - b\alpha$. For any field F , let $F^* = F - \{0\}$ and $F_+ = \{a^2 | a \in F\}$.

The *projective space of dimension 1 over \mathbb{F}* is defined to be

$$\mathbb{P}_{\mathbb{F}}^1 = \mathbb{F}^* I \setminus \mathbb{E}^*.$$

Any element $[u : v] \in \mathbb{P}_{\mathbb{F}}^1$ can be written uniquely as $[\frac{u}{v} : 1]$ if $v \neq 0$ or $[1 : 0]$ if $v = 0$. Thus we can identify $\mathbb{P}_{\mathbb{F}}^1$ with $\mathbb{F} \cup \{\infty\}$. Analogously, define $\mathbb{P}_{\mathbb{E}}^1 \cong \mathbb{E} \cup \{\infty\}$. The groups $PSL_2(F)$ and $PGL_2(F)$ for $F = \mathbb{F}$ or $F = \mathbb{E}$ act on \mathbb{P}_F^1 by matrix multiplication.

The lemmas in this section are easily verified. We refer the reader to [Su] or [Si] for more details on lemmas stated without proof.

Lemma 3.1. *Let $a, b \in \mathbb{F}$. Then $\frac{a}{b} \in \mathbb{F}^+$ iff $ab \in \mathbb{F}^+$.*

The *norm map* $N : \mathbb{E}^* \rightarrow \mathbb{F}^*$ is defined by $N(\lambda) = \lambda\bar{\lambda}$.

Lemma 3.2. *The norm map $N : (\mathbb{F}_{q^2})^* \rightarrow (\mathbb{F}_q)^*$ is surjective.*

Proof. We know that $\lambda \in \ker(N)$ iff $1 = \lambda\bar{\lambda} = \lambda\bar{\lambda}^q = \lambda^{q+1}$. So $|\ker(N)| = q + 1$. Thus,

$$|Im(N)| = \frac{|(\mathbb{F}_{q^2})^*|}{|\ker(N)|} = \frac{q^2 - 1}{q + 1} = q - 1 = |(\mathbb{F}_q)^*|.$$

□

Lemma 3.3. *The action of:*

- (1) $PGL_2(q^2)$ on $\mathbb{P}_{\mathbb{E}}^1$ is sharply triply transitive.
- (2) $PGL_2(q)$ on $\mathbb{E} - \mathbb{F}$ is transitive and on $\mathbb{P}_{\mathbb{F}}^1$ is sharply triply transitive.
- (3) $PSL_2(q^2)$ on $\mathbb{P}_{\mathbb{E}}^1$ is doubly transitive.
- (4) $PSL_2(q)$ on $\mathbb{P}_{\mathbb{F}}^1$ is doubly transitive.
- (5) $PSL_2(q)$ on $\mathbb{E} - \mathbb{F}$ is transitive.

The stabilizer of a point x in a group G will be denoted G_x . Any subgroup of $PSL_2(q)$ conjugate to $PSL_2(q)_\alpha$, for $\alpha \in \mathbb{P}_{\mathbb{F}}^1$ chosen above, is called a *Cartan*

subgroup. Any subgroup of $PSL_2(q)$ conjugate to $PSL_2(q)_\infty$ is called a *Borel* subgroup. A counting argument shows that $PGL_2(q)_\alpha \cong \mathbb{Z}_{q+1}$ and $PSL_2(q)_\alpha \cong \mathbb{Z}_{\frac{q+1}{2}}$.

Considering the fixed points of $g \in PGL_2(q)$ or $g \in PSL_2(q)$ yields the following classification of elements, according to type. This classification is invariant under conjugation.

Proposition 3.4 ([Su]). *Let $g \in PGL_2(q)$, and let $\epsilon : GL_2(q) \rightarrow PGL_2(q)$ be the projection map. Suppose $A \in GL_2(q)$ satisfies $\epsilon(A) = g$. Every $1 \neq g \in PGL_2(q)$ is one of the following types:*

1. *hyperbolic* iff $tr^2(A) - 4det(A) \in \mathbb{F}_+$,
 iff g is conjugate to ax for some $a \in \mathbb{F}_+$,
 iff $order(g) | \frac{q-1}{2}$ when $g \in PSL_2(q)$.
2. *parabolic* iff $tr^2(A) = 4$,
 iff g is conjugate to $x + b$ for some $b \in \mathbb{F}^*$,
 iff $order(g) = p$.
3. *elliptic* iff $tr^2(A) - 4det(A) \in \mathbb{F}^* - \mathbb{F}_+$,
 iff g is conjugate to $\frac{az-b\beta}{bz+a}$ for $a, b \in \mathbb{F}$, $\beta \in \mathbb{F}^* - \mathbb{F}_+$,
 iff $order(g) | \frac{q+1}{2}$ when $g \in PSL_2(q)$.

Thus, up to conjugation, we can assume that the fixed point set of an element g of $PGL_2(q)$ is either $\{0, \infty\}$, $\{\infty\}$, or $\{\alpha, \bar{\alpha}\}$, where $\bar{\alpha}$ denotes the conjugate of α .

We note that in $PSL_2(q)$ there are two conjugacy classes of parabolic elements which become conjugate in $PGL_2(q)$. There is an elementary way to distinguish the parabolic conjugacy classes.

Lemma 3.5. *The parabolic elements $x + a$ and $x + b$ are conjugate iff $\frac{b}{a} \in \mathbb{F}^+$.*

Conjugacy of hyperbolic and elliptic elements is the same in both groups. An elliptic element in $PSL_2(p)$ (resp. $PGL_2(q)$) is conjugate to a *hyperbolic* element in $PSL_2(q^2)$ (resp. $PGL_2(q^2)$) of the form az where $a \in (\mathbb{F}_{q^2})_+ - \mathbb{F}_+$ [Su].

Lemma 3.6. *Let $g \in PSL_2(q)$, and let $\epsilon : SL_2(q) \rightarrow PSL_2(q)$ be the projection map. Suppose $A \in SL_2(q)$ satisfies $\epsilon(A) = g$. Then $tr^2(A)$ determines both the type and the order of g in $PSL_2(q)$ and its conjugacy class in $PGL_2(q)$.*

Proof. According to Proposition 3.4, g is parabolic iff $|g| = p$ iff $tr^2(A) = 4$. Since all parabolic elements are conjugate in $PGL_2(q)$, the lemma is proved in this case.

Given g and A as above, with g hyperbolic or elliptic, we form the characteristic polynomial $x^2 - tr(A)x + 1$ which has roots λ and $\frac{1}{\lambda}$. Beginning with $-A$ we obtain the polynomial $x^2 + tr(A)x + 1$ which has roots $-\lambda$ and $\frac{-1}{\lambda}$. In either case, g is conjugate to the transformation $\lambda^2 z$, and thus its order is determined by $tr^2(A)$. For elliptic elements this conjugation occurs in $PGL_2(q^2)$, while hyperbolic elements can be conjugated in $PSL_2(q)$.

When g is elliptic, $\lambda \in \mathbb{E} - \mathbb{F}$, and when g is hyperbolic, $\lambda \in \mathbb{F}$. Thus conjugation by elements of $PSL_2(p)$ does not change the type of the element. It is already true that all elliptic or hyperbolic elements of a given order in $PSL_2(p)$ are conjugate, proving the lemma. □

The following elementary fact lists some specific instances of Lemma 3.6.

Lemma 3.7 ([GS2]. Order and trace of certain elements). *Let $g \in PSL_2(q)$, and let $\epsilon : SL_2(q) \rightarrow PSL_2(q)$ be the projection map. Suppose $A \in SL_2(q)$ satisfies $\epsilon(A) = g$. Then:*

- (1) $|g| = 2$ iff $tr(A) = 0$.
- (2) If $p > 3$, then $|g| = 3$ iff $tr(A) = \pm 1$.
- (3) $|g| = 4$ iff $tr(A)^2 = 2$.
- (4) If $p \neq 5$, then $|g| = 5$ iff $a^2 \pm a - 1 = 0$ where $a = tr(A)$.

4. A CHARACTERIZATION OF $PSL_2(p)$ -RAMIFICATION TRIPLES

We start with a special case in our characterization of all $PSL_2(p)$ -ramification types, namely the case of three conjugacy classes of elements. We call these *ramification triples*. In Section 5 we present the complete description of all $PSL_2(p)$ -ramification types and their corresponding $PSL_2(p)$ -signatures. We recall that for a signature (m_1, \dots, m_k) to be a $PSL_2(p)$ -signature, we must have m_i dividing the order of $PSL_2(p)$, for all i . In any ramification type $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k)$, each \mathcal{C}_i represents a conjugacy class of nontrivial elements of $PSL_2(p)$.

Since $PSL_2(p)$ for $p > 11$ is neither cyclic, dihedral, *polyhedral* (isomorphic to \mathbb{A}_4 , \mathbb{S}_4 or \mathbb{A}_5) nor solvable, by Lemma 1.1, all signatures with nonnegative Euler characteristic are not $PSL_2(p)$ -signatures. The following signatures comprise this list:

$$(n, n), (2, 2, n), (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 3, 6), (2, 4, 4), (3, 3, 3), (2, 2, 2, 2).$$

In the following two sections, we consider ramification triples $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ according to two cases. First we consider ramification-type triples whose corresponding signature has a realization which *might* generate a polyhedral subgroup of $PSL_2(p)$. If the signature does generate a polyhedral subgroup, we call $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ a *polyhedral ramification triple*. Second, we consider ramification triples without any restrictions on signature. In either case, we determine which ramification types are $PSL_2(p)$ -ramification types, i.e., represent a $PSL_2(p)$ action on a surface with spherical quotient. In §5 we give a complete characterization of all $PSL_2(p)$ -ramification types, using the fact that this set has the structure of a semigroup.

Each element $g \in PSL_2(p)$ corresponds to a pair of matrices $\pm A \in SL_2(p)$ whose traces have the same square. So given a k -tuple of elements (g_1, g_2, \dots, g_k) of $PSL_2(p)$, there is a corresponding k -tuple $(\pm t_1, \pm t_2, \dots, \pm t_k)$, where $\pm t_i$ is the trace of matrix $\pm A_i \in SL_2(q)$ corresponding to g_i . If $k = 3$ we call this vector a *trace triple*. When we choose a representative matrix from $\pm A_i$ to calculate with, we are making an initial choice of trace from each pair $\pm t_i$. We often change our choice from A to $-A$ (or t_i to $-t_i$) to simplify computations without changing conjugacy classes. In the proofs below, we often begin by considering traces of elements of $SL_2(p)$ rather than orders or conjugacy classes in $PSL_2(p)$, since Lemma 3.6 shows that $tr^2(A_i)$ determines the order and conjugacy class of g_i in $PSL_2(p)$, unless g_i is parabolic. When $t_i = \pm 2$, it will be necessary to consider different cases since there are two conjugacy classes of parabolic elements in $PSL_2(p)$. We often refer to Lemma 3.7 which lists some specific correlations between trace and order in $PSL_2(p)$.

We begin with an elementary lemma giving a specific example of matrices which realize a particular type of trace triple.

Lemma 4.1. *If the trace triple $(0, \pm t_2, \pm t_3)$ can be realized in a Cartan subgroup of $PSL_2(p)$, then the realization is given by matrices of the form*

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} a & -c \\ c & a \end{pmatrix}$$

for $a, c \in \mathbb{F}_p$.

4.1. Polyhedral ramification triples. We begin by showing that any ramification triple $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ corresponding to a polyhedral signature is a $PSL_2(p)$ -ramification triple. We begin with the following lemma about the subgroup structure of $PSL_2(q)$.

Lemma 4.2 ([D]). *Subgroup structure of $PSL_2(p)$. If H is a subgroup of $PSL_2(q)$, then H is either:*

- (1) *A projective subgroup, i.e., $PSL_2(p^m)$ if $m|n$ or $PSL_2(p^m)$ if $2m|n$.*
- (2) *A Borel subgroup.*
- (3) *A Cartan subgroup.*
- (4) *A polyhedral subgroup, i.e., dihedral, \mathbb{A}_4 , \mathbb{S}_4 , or \mathbb{A}_5 , when these exist within $PSL_2(q)$.*

The only dihedral signature is $(2, 2, n)$ and $\chi(2, 2, n) > 0$. Thus, we only need to consider ramification types corresponding to polyhedral signatures.

Let $\sigma = (m_1, m_2, m_3)$ be a polyhedral signature. If σ is an \mathbb{A}_4 signature, then $m_i \in \{2, 3\}$ for all i . Similarly, if σ is an \mathbb{S}_4 signature, then $m_i \in \{2, 3, 4\}$ for all i and $m_i \in \{2, 3, 5\}$ if σ is an \mathbb{A}_5 signature. Since we require that $\chi(\sigma) < 0$, there are no possible \mathbb{A}_4 signatures, and we have possible \mathbb{S}_4 signatures $(3, 3, 4)$, $(3, 4, 4)$, and $(4, 4, 4)$ and \mathbb{A}_5 signatures $(2, 5, 5)$, $(3, 3, 5)$, $(3, 5, 5)$, and $(5, 5, 5)$.

In \mathbb{S}_4 , every permutation of order 3 has sign 1, and every permutation of order 4 has sign -1 . Therefore neither $(3, 3, 4)$ nor $(4, 4, 4)$ can be realized in \mathbb{S}_4 . We are then left with a list of five potential polyhedral signatures corresponding to the ramification type $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$. We will need the following elementary lemma about the orders of certain elements in \mathbb{S}_4 and \mathbb{A}_5 .

Lemma 4.3 (Orders of products in $PSL_2(p)$). *Let C and D be elements of $PSL_2(p)$.*

- (1) *If $|C| = 3$, $|D| = 4$ and $|CD| = 4$ with $\langle C, D \rangle = \mathbb{S}_4$, then $|CD^{-1}| = 2$.*
- (2) *Assume $\langle C, D \rangle = \mathbb{A}_5$.*
 - (a) *If $|C| = |D| = 3$ and $|CD| = 5$, then $|D^{-1}C| = 5$.*
 - (b) *If $|C| = 3$, $|D| = 5$ and $|CD| = 3$, then $|D^{-1}C| = 5$.*
 - (c) *If $|C| = 3$, $|D| = 5$ and $|CD| = 5$, then $|D^{-1}C| = 2$ or $|D^{-1}C| = 3$.*
 - (d) *If $|C| = |D| = 5$ and $|CD| = 5$, then $|D^{-1}C| = 3$.*
 - (e) *If $|C| = 2$, $|D| = 5$ and $|CD| = 5$, then $|CDC^{-1}D^{-1}| = 3$.*

Lemma 4.4 (Subgroups of $PSL_2(q)$ containing elements of certain orders).

- (1) *If H is a subgroup of \mathbb{S}_4 , and $C, D \in H$ with $|C| = 3$ and $|D| = 4$, then $H \cong \mathbb{S}_4$.*
- (2) *Let H be a subgroup of \mathbb{S}_5 and $C, D \in H$.*
 - (a) *If $|C| = 3$ and $|D| = 5$, then $H \cong \mathbb{A}_5$.*
 - (b) *If $|C| = 2$, $|D| = 5$ and $|CD| = 5$, then $H \cong \mathbb{A}_5$.*
 - (c) *If $H = \langle C, D \rangle$ with $|C| = |D| = 5$, then $H \cong \mathbb{Z}_5$ or $H \cong \mathbb{A}_5$.*

We include the proofs of Lemmas 4.3 and 4.4 in the Appendix.

Let $\Sigma = (\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ be a ramification triple whose corresponding signature $\sigma = (m_1, m_2, m_3)$ is one of the five exceptional signatures listed above. In each case we will produce a realization of $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ which generates $PSL_2(p)$.

Let (g_1, g_2, g_3) be a realization of Σ . If $\sigma \neq (5, 5, 5)$, then $\langle g_1, g_2, g_3 \rangle$ is not abelian. (In a finite abelian group, $o(xy) = o(x)o(y)$ when $(o(x), o(y)) = 1$.) Since no g_i is parabolic ($p \geq 11$), the group $\langle g_1, g_2, g_3 \rangle$ is \mathbb{S}_4 or $PSL_2(p)$ if $\sigma = (3, 4, 4)$, and \mathbb{A}_5 or $PSL_2(p)$ otherwise. Thus, it suffices to show that the realization of Σ does not generate \mathbb{S}_4 or \mathbb{A}_5 , respectively. For $\sigma = (5, 5, 5)$ we must show that the realization of Σ does not generate \mathbb{A}_5 or a cyclic subgroup.

Lemma 4.3 shows that $|C^{-1}D|$ (resp. $|CDC^{-1}D^{-1}|$) is uniquely determined for any realization $(C, D, (CD)^{-1})$ of a polyhedral signature $(m_1, m_2, m_3) \neq (2, 5, 5)$ (resp. $(2, 5, 5)$). We will find a realization of the above triples in which the order of the element $C^{-1}D$ (resp. $CDC^{-1}D^{-1}$) contradicts Lemma 4.4. This will be checked via trace considerations using Lemma 3.7. It then follows that the realization generates $PSL_2(p)$ and not the polyhedral subgroup.

We will need the following elementary observations.

Lemma 4.5. *If r satisfies $x^2 \pm x - 1 = 0$, then neither $r + 1$ nor $r - 1$ satisfies the equation $(x^2 + x - 1)(x^2 - x - 1) = 0$.*

Lemma 4.6. *If $A, B \in SL_2(q)$, then*

$$\text{tr}(AB) + \text{tr}(AB^{-1}) = \text{tr}(A)\text{tr}(B)$$

and

$$\text{tr}(ABA^{-1}B^{-1}) = \text{tr}(A)^2 + \text{tr}(B)^2 + \text{tr}(AB)^2 - \text{tr}(A)\text{tr}(B)\text{tr}(AB) - 2.$$

We can now prove the following theorem.

Theorem 4.7 (All polyhedral ramification triples are $PSL_2(p)$ -ramification triples). *All ramification triples $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ whose corresponding signature σ is polyhedral with $\chi(\sigma) < 0$ are $PSL_2(p)$ -ramification triples.*

Proof. Let $\Sigma = (\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ have corresponding signature $\sigma = (m_1, m_2, m_3)$ with $\chi(\sigma) < 0$, and trace triple $(\pm t_1, \pm t_2, \pm t_3)$. Make an initial choice of traces (t_1, t_2, t_3) . If $m_i \nmid \frac{p-1}{2}$ for any i , then we may assume by permuting the m_i (and thus the \mathcal{C}_i) that $m_2 \mid \frac{p-1}{2}$.

We will produce a realization $(A, B, (AB)^{-1})$ of $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$. From the conjugacy classes \mathcal{C}_1 and \mathcal{C}_2 , choose representatives A and B as follows:

(1) If $m_2 \mid \frac{p-1}{2}$

$$A = \begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix} \text{ and } B = \begin{pmatrix} a & \frac{a\alpha-d}{\alpha} \\ 0 & \frac{1}{\alpha} \end{pmatrix}.$$

(2) If $m_2 \mid \frac{p+1}{2}$

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix} \text{ and } B = \begin{pmatrix} x & y \\ \bar{y} & \bar{x} \end{pmatrix} \text{ with } x\bar{x} - y\bar{y} = 1,$$

where in (1), we have $a, d \in \mathbb{F}_p$ and $\alpha \in (\mathbb{F}_p)^* - (\mathbb{F}_p)_+$, and in (2) we have $x, y \in \mathbb{F}_p$ and $\lambda \in (\mathbb{F}_p)^*$.

We will prove that any ramification triple Σ with corresponding signature $\sigma = (3, 3, 5)$ is a $PSL_2(p)$ -ramification type. For other polyhedral signatures, see the Appendix.

Suppose that σ is a permutation of $(3, 3, 5)$. If $m_2 = 3$, we may assume that $m_1 = 3$. Consider the realization $(A, B, (AB)^{-1})$ given above of the trace triple $(\pm 1, \pm 1, t_3)$, where t_3 satisfies one of the equations $x^2 \pm x - 1 = 0$. It follows that $-t_3$ satisfies the other equation, and $\text{tr}(BA^{-1})$ cannot be a root of either equation by Lemma 4.5. Consequently, $|BA^{-1}| \neq 5$, contradicting Lemma 4.4.

If $m_2 = 5$, then $m_1 = 3$. Interchanging the roles of t_2 and t_3 in the argument above again yields $|BA^{-1}| \neq 5$. Thus $\langle A, B \rangle \not\cong \mathbb{A}_5$, and we conclude that Σ is a $PSL_2(p)$ -ramification triple. \square

4.2. Nonpolyhedral ramification triples. We now prove the following theorem.

Theorem 4.8 (Complete characterization of $PSL_2(p)$ -ramification triples). *All ramification triples (C_1, C_2, C_3) corresponding to the trace triple $(\pm t_1, \pm t_2, \pm t_3)$ are $PSL_2(p)$ -ramification triples except:*

- (1) *All ramification triples corresponding to one of two signatures: $(\pm 2, \pm 3, \pm 6)$ and $(\pm 2, \pm 2, \pm 4)$.*
- (2) *All ramification triples (C_1, C_2, C_3) having all C_i conjugacy classes of parabolic elements, with one of the following conditions:*
 - (a) *When -1 is a square in \mathbb{F}_q , any permutation of (C_1, C_1, C_2) .*
 - (b) *When -1 is not a square in \mathbb{F}_q , the triple (C_1, C_1, C_1) .*
- (3) *All ramification triples (C_1, C_2, C_3) with C_1 and C_2 distinct conjugacy classes of parabolic elements and C_3 not a conjugacy class of parabolic elements, with one of the following conditions:*
 - (a) *When $2 - t_3$ is a square in \mathbb{F}_q , the triple (C_1, C_2, C_3) .*
 - (b) *When $2 - t_3$ is not a square in \mathbb{F}_q , one of two ramification types (C_1, C_1, C_3) and (C_2, C_2, C_3) .*

If -1 is a square in \mathbb{F}_q , then C_3 is a conjugacy class of hyperbolic elements.

If -1 is not a square in \mathbb{F}_q , then C_3 is a conjugacy class of elliptic elements.

Proof. Let $(\pm t_1, \pm t_2, \pm t_3)$ be a trace triple and choose initial traces (t_1, t_2, t_3) . Let (C_1, C_2, C_3) be a ramification triple corresponding to the trace triple, i.e., each C_i is the conjugacy class of an element of $PSL_2(p)$ whose trace is t_i . We present one case of the proof and leave the rest to the Appendix. All the cases are similar in nature.

Case 1. Suppose $t_1 = 2$ and $t_2, t_3 \neq 2$. By Proposition 3.4, C_1 is a conjugacy class of parabolic elements. We may assume that $\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ is a representative of C_1 . If this matrix was not in C_1 , but in the other conjugacy class of parabolic elements, then we conjugate it by an appropriate element of $PGL_2(p)$ so that it lies in C_1 .

We want to find elements $g_i \in C_i$ with $g_3 = (g_1 g_2)^{-1}$. Let $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in SL_2(p)$, so $xw - yz = 1$. Choose traces $(2, t_2, t_3)$. Multiplying these matrices, we see that $(2, t_2, t_3)$ can only be realized if we can solve the equations

- (1) $x + w = t_2, x + w + z = t_3,$
- (2) $x^2 - t_2 x + (t_3 - t_2)y + 1 = 0,$ and
- (3) $xw - yz = 1.$

(i) Suppose $t_2 = 0 = t_3$. In this case, the signature corresponding to the trace triple is $(2, 2, p)$ by Lemma 3.7. Moreover, the equation $x^2 - t_2 x + (t_3 - t_2)y + 1 = 0$

becomes $x^2 + 1 = 0$, which has a solution if and only if -1 is a square in \mathbb{F}_p . If -1 is a square in \mathbb{F}_p , then the signature $(2, 2, p)$ can be realized, but it is not a $PSL_2(p)$ -signature since it has nonnegative Euler characteristic. When -1 is not a square, the dihedral group \mathbb{D}_p is not a subgroup of $PSL_2(p)$ and thus the signature $(2, 2, p)$ does not arise.

(ii) Suppose t_2 and t_3 are not both zero. Substituting $-t_2$ for t_2 if necessary, we can assume that $t_2 - t_3 \neq 0$. We solve the equation $x^2 - t_2x + (t_3 - t_2)y + 1 = 0$, where x is any element of \mathbb{F}_p , for y , to get $y = \frac{-x^2+t_2x-1}{t_3-t_2}$. Thus, the matrix $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ becomes $\begin{pmatrix} x & \frac{-x^2+t_2x-1}{t_3-t_2} \\ t_3-t_2 & t_2-x \end{pmatrix}$, and the ramification type (C_1, C_2, C_3) is realizable.

We must now determine whether (C_1, C_2, C_3) is a $PSL_2(p)$ -ramification type. Let $g_1 = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} x & \frac{-x^2+t_2x-1}{t_3-t_2} \\ t_3-t_2 & t_2-x \end{pmatrix}$. Since g_1 fixes infinity but g_2 does not (since $t_3 - t_2 \neq 0$), these two elements are not contained in the same Borel subgroup. Since g_1 is parabolic, the subgroup generated by these two elements is not contained in a Cartan subgroup. Moreover, g_1 has order p and therefore $\langle g_1, g_2 \rangle$ cannot be an exceptional subgroup since $p > 11$. Hence, $\langle g_1, g_2 \rangle \cong PSL_2(p)$ by Lemma 3.2 and (C_1, C_2, C_3) is a $PSL_2(p)$ -ramification triple. \square

5. A COMPLETE DESCRIPTION OF $PSL_2(p)$ -RAMIFICATION TYPES

Recall that a *semigroup* \mathcal{S} is a nonempty set S together with a binary operation on S which is associative. An *atom* a for a semigroup \mathcal{S} satisfies $a + s \in \mathcal{S}$ for all $s \in \mathcal{S}$. Consider the following addition operation defined on G -signatures. Suppose $(g; m_1, m_2, \dots, m_l)$ and $(h; n_1, n_2, \dots, n_k)$ are G -signatures. Then their sum is the G -signature

$$(g + h; m_1, m_2, \dots, m_l, n_1, n_2, \dots, n_k).$$

It is proved in [MS] that G -signatures corresponding to a finite group G form a commutative semigroup with identity $(0;)$ under this addition. In fact, the following stronger statement is true.

Proposition 5.1. *Let G be a finite group with subgroups H and K , and $k, l \geq 1$. If $(g; C_1, C_2, \dots, C_k)$ is an H -ramification type and $(h; D_1, D_2, \dots, D_l)$ is a K -ramification type with $(C_k)^{-1} = D_l$, then there is an $\langle H, K \rangle$ -ramification type*

$$(g + h; C_1, C_2, \dots, C_{k-1}, D_1, \dots, D_{l-1}).$$

Proof. First choose a realization of each ramification type:

$$(a_1, b_1, \dots, a_g, b_g, y_1, \dots, y_k) \text{ and } (a'_1, b'_1, \dots, a'_h, b'_h, z_1, \dots, z_l),$$

with all entries elements of G . We have the relations

$$\prod_{i=1}^g [a_i, b_i] \prod_{s=1}^k y_s = 1 = \prod_{j=1}^h [a'_j, b'_j] \prod_{t=1}^l z_t$$

and

$$\langle \{a_i, b_i\}, \{y_s\} \rangle \cong H \text{ and } \langle \{a'_j, b'_j\}, \{z_t\} \rangle \cong K.$$

This yields a realization of the ramification type

$$(g + g'; C_1, C_2, \dots, C_{k-1}, D_1, D_2, \dots, D_{l-1})$$

using the elements

$$\{a_1, b_1, \dots, a_k, b_k, a'_1, b'_1, \dots, a'_l, b'_l, y_1, \dots, y_{s-1}, z_1, \dots, z_{t-1}\}.$$

For this to be an $\langle H, K \rangle$ -ramification type, we must show that

$$\prod_{i=1}^g [a_i, b_i] \prod_{j=1}^h [a'_j, b'_j] \prod_{s=1}^{k-1} y_s \prod_{t=1}^{l-1} z_t = 1$$

and

$$\langle \{a_i, b_i\}, \{a'_j, b'_j\}, \{y_s\}, \{z_t\} \rangle = \langle H, K \rangle,$$

where $s = 1, 2, \dots, k-1$ and $t = 1, 2, \dots, l-1$. If the highest indices in the product relation above were k and l , then the product would be the identity by construction. Since we chose $y_k = z_l^{-1}$, the above product relation also holds.

Let $\mathcal{G} = \{a_i, b_i\} \cup \{a'_i, b'_i\} \cup \{y_s\} \cup \{z_t\}$, where $s = 1, 2, \dots, k-1$ and $t = 1, 2, \dots, l-1$. To show that \mathcal{G} generates $\langle H, K \rangle$, note that both y_k and z_l can be expressed in terms of elements of \mathcal{G} . Thus both H and K are subgroups of $\langle \mathcal{G} \rangle$, and $\langle \mathcal{G} \rangle$ is clearly a subgroup of $\langle H, K \rangle$. \square

So far we have completely described all $PSL_2(p)$ -ramification types with exactly three conjugacy classes of elements of $PSL_2(p)$. We now describe all $PSL_2(p)$ -ramification types consisting of more than three conjugacy classes of elements, using the semigroup structure of the set of ramification types.

We note that \mathcal{C} and \mathcal{C}^{-1} represent the same conjugacy class of elements of $PSL_2(p)$.

Lemma 5.2. *Suppose that $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ is a $PSL_2(p)$ -ramification triple, and that \mathcal{C} is a conjugacy class of nontrivial elements of $PSL_2(p)$. Then $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C})$ is also a $PSL_2(p)$ -ramification type.*

Proof. Using Theorem 4.8, we can determine if $(\mathcal{C}_i, \mathcal{C}, \mathcal{C}_i)$ is a $PSL_2(p)$ -ramification triple for any $i = 1, 2, 3$. If it is, we may assume that $i = 3$, and using the semigroup structure of the set of ramification types outlined in Proposition 5.1, it follows that $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3) + (\mathcal{C}_3, \mathcal{C}, \mathcal{C}_3) = (\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C})$ is a $PSL_2(p)$ -ramification type.

Suppose that $(\mathcal{C}_i, \mathcal{C}, \mathcal{C}_i)$ is not a $PSL_2(p)$ -ramification triple for any $i = 1, 2, 3$. This could happen in two ways.

Case 1. If the ramification triple is not realizable, then from Theorem 4.8 we know that \mathcal{C}_i is a conjugacy class of parabolic elements for all i .

- (1) Suppose that \mathcal{C} is a conjugacy class of parabolic elements. Two of the conjugacy classes $\mathcal{C}_1, \mathcal{C}_2$ and \mathcal{C}_3 are identical; without loss of generality assume they are \mathcal{C}_1 and \mathcal{C}_2 .
 - (a) If \mathcal{C}_3 and \mathcal{C} are conjugate, let \mathcal{D} be any conjugacy class of hyperbolic elements. Then both ramification types $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{D})$ and $(\mathcal{C}_3, \mathcal{C}, \mathcal{D})$ are $PSL_2(p)$ -ramification triples by Theorem 4.8, and it follows from Proposition 5.1 that $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C})$ is a $PSL_2(p)$ -ramification type.
 - (b) If \mathcal{C}_3 and \mathcal{C} do not represent the same conjugacy class of elements, then according to Theorem 4.8 there is a unique choice of nonparabolic conjugacy class \mathcal{D} so that $(\mathcal{C}_3, \mathcal{C}, \mathcal{D})$ is a $PSL_2(p)$ -ramification triple. It also follows from Theorem 4.8 that $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{D})$ is a $PSL_2(p)$ -ramification triple. Then by Proposition 5.1, $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C})$ is a $PSL_2(p)$ -ramification type.
- (2) If \mathcal{C} is not a conjugacy class of parabolic elements, then $(\mathcal{C}_3, \mathcal{C}, \mathcal{C}_3)$ is a $PSL_2(p)$ -ramification triple and it follows from Proposition 5.1 that $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C})$ is a $PSL_2(p)$ -ramification type.

Case 2. If the ramification triple corresponds to a signature σ with two identical entries, which is not a $PSL_2(p)$ -signature, then σ must be one of $(2, 2, n)$, $(2, 3, 3)$, or $(2, 4, 4)$. In any of these cases, the ramification triple does not contain a conjugacy class of parabolic elements, which are all of order p . (Note that $(2, 2, p)$ is not a $PSL_2(p)$ -signature.) Let \mathcal{D} be a conjugacy class of parabolic elements of $PSL_2(p)$, chosen in accordance with Theorem 4.8 so that $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{D})$ is a $PSL_2(p)$ -ramification triple. Since neither \mathcal{C}_3 nor \mathcal{C} is a conjugacy class of parabolic elements, it follows that $(\mathcal{C}_3, \mathcal{C}, \mathcal{D})$ is also a $PSL_2(p)$ -ramification triple. Then by Proposition 5.1 their sum, $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C})$, is a $PSL_2(p)$ -ramification type. \square

Lemma 5.3. *All ramification types $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4)$ are $PSL_2(p)$ -ramification types except for any corresponding to the signature $(2, 2, 2, 2)$.*

Proof. Suppose there is a permutation of the \mathcal{C}_i so that the triple $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ is a $PSL_2(p)$ -ramification triple. Then by Lemma 5.2 so is $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4)$.

Suppose that no permutation of the \mathcal{C}_i yields a triple which is a $PSL_2(p)$ -ramification type. If the signature corresponding to this ramification type is $(2, 2, 2, 2)$, which is not a $PSL_2(p)$ -signature since it has nonnegative Euler characteristic, then the ramification type is not a $PSL_2(p)$ -ramification type.

Otherwise, any permutation $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ contains at least two conjugacy classes of parabolic elements. Since there are only two such conjugacy classes in $PSL_2(p)$, we may assume that \mathcal{C}_2 and \mathcal{C}_3 represent the same conjugacy class of parabolic elements.

Let \mathcal{C}'_3 denote the conjugacy class of parabolic elements which is distinct from \mathcal{C}_3 . It follows from Theorem 4.8 that both $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}'_3)$ and $(\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}'_3)$ are $PSL_2(p)$ -ramification triples, and from Proposition 5.1 that $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4)$ is a $PSL_2(p)$ -ramification type. \square

Lemma 5.4. *$(2, 2, 2, 2, 2)$ is a $PSL_2(p)$ -signature.*

Proof. We know that $(2, \frac{p\pm 1}{2}, \frac{p\pm 1}{2})$ is a $PSL_2(p)$ -signature when $p > 11$. Let (g_1, g_2, g_3) be a realization of this signature with $(g_1, g_2, g_3) = PSL_2(p)$. Now g_2 and g_3 are rotations in the dihedral group $\mathbb{D}_{\frac{p\pm 1}{2}}$. Consequently, each can be written as the product of two reflections, say $g_2 = h_1h_2$ and $g_3 = h_3h_4$. Then $(g_1, h_1, h_2, h_3, h_4)$ is also a realization of a $PSL_2(p)$ -signature. Since the order of any reflection is two, it follows that $(2, 2, 2, 2, 2)$ is a $PSL_2(p)$ -signature. \square

Corollary 5.5. *All ramification types corresponding to the signature $(2, 2, 2, 2, 2)$ are $PSL_2(p)$ -ramification types.*

Proof. Since all subgroups of $PSL_2(p)$ of order 2 are conjugate [D], the only possible ramification type corresponding to this signature is $(\mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C})$ where \mathcal{C} is the conjugacy class of elements of $PSL_2(p)$ of order 2. \square

Proposition 5.6. *For $k \geq 4$, all ramification types are $PSL_2(p)$ -ramification types except for any corresponding to the signature $(2, 2, 2, 2)$.*

Proof. We prove the lemma by induction on the following statement. For $k \geq 4$, suppose that $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k)$ is a $PSL_2(p)$ -ramification type, and \mathcal{C} is a conjugacy class of nontrivial elements of $PSL_2(p)$. Then $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k, \mathcal{C})$ is also a $PSL_2(p)$ -ramification type, and all $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{k+1})$ are $PSL_2(p)$ -ramification types except for any corresponding to the signature $(2, 2, 2, 2)$.

When $k = 4$ the above statement is proved in Lemmas 5.2 and 5.3. We use this as the base case for our proof by induction.

Assume that the statement of the proposition is true for $n = 4, 5, \dots, k$ and consider the ramification type $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k, \mathcal{C}_{k+1})$. Suppose that for some permutation of the \mathcal{C}_i , the triple $(\mathcal{C}_k, \mathcal{C}_{k+1}, \mathcal{C}_k)$ is a $PSL_2(p)$ -ramification triple. By the induction hypothesis, $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k)$ is a $PSL_2(p)$ -ramification type. It follows from Proposition 5.1 that $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k, \mathcal{C}_{k+1})$ is a $PSL_2(p)$ -ramification type.

If $(\mathcal{C}_j, \mathcal{C}_{k+1}, \mathcal{C}_j)$ is not a $PSL_2(p)$ -ramification triple for any $j \in \{1, 2, \dots, k\}$, then \mathcal{C}_k must be parabolic for all j . There must be a pair of equivalent conjugacy classes; without loss of generality we assume that \mathcal{C}_{k-1} and \mathcal{C}_k are identical. Let \mathcal{C}'_k be the conjugacy class of parabolic elements which is distinct from \mathcal{C}_k . We know that $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}'_k)$ is a $PSL_2(p)$ -ramification type by the induction hypothesis, and that $(\mathcal{C}_k, \mathcal{C}_{k+1}, \mathcal{C}'_k)$ is a $PSL_2(p)$ -ramification triple by Theorem 4.8. It follows from Proposition 5.1 that $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k, \mathcal{C}_{k+1})$ is a $PSL_2(p)$ -ramification type.

We can now show that all $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k, \mathcal{C}_{k+1})$ are $PSL_2(p)$ -ramification types, except for any ramification types corresponding to the signature $(2, 2, 2, 2)$.

Suppose that $k = 5$ and consider the ramification type $\Sigma = (\mathcal{C}_1, \dots, \mathcal{C}_5)$. If no permutation of Σ yields a $PSL_2(p)$ -ramification type $(\mathcal{C}_1, \dots, \mathcal{C}_4)$, then Σ corresponds to the signature $(2, 2, 2, 2, 2)$. In this case, Σ is a $PSL_2(p)$ -ramification type according to Corollary 5.5.

If some permutation of Σ yields a $PSL_2(p)$ -ramification type $(\mathcal{C}_1, \dots, \mathcal{C}_4)$, then by the above argument, $(\mathcal{C}_1, \dots, \mathcal{C}_5)$ is a $PSL_2(p)$ ramification type. If $k > 5$ then the above argument also shows that all ramification types $(\mathcal{C}_1, \dots, \mathcal{C}_{k+1})$ are $PSL_2(p)$ -ramification types. □

Corollary 5.7. *Let \mathcal{C} be a conjugacy class of nontrivial elements of $PSL_2(p)$. Then (\mathcal{C}) is an atom for the semigroup of $PSL_2(p)$ -ramification types.*

We summarize these results in the following theorem.

Theorem 5.8. *All ramification types $(\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_k)$ are $PSL_2(p)$ -ramification types except when the corresponding signature is $(2, d, d)$, $(2, d, 2d)$ or $(2, 2, 2, 2)$.*

Corollary 5.9. *For $p > 11$, a signature (m_1, m_2, \dots, m_k) is a $PSL_2(p)$ -signature if and only if each m_i is either p or a divisor of $\frac{p \pm 1}{2}$ and $\sum_{i=1}^k \left(1 - \frac{1}{m_i}\right) > 2$, i.e., the Euler characteristic is negative.*

We would now like to determine the set of spherical genera g so that the surface S_g of genus g admits a $PSL_2(p)$ -action with spherical quotient. It is easier to describe a translate of this set. For a finite group G , the set $Genera(G)$ is the set of all genera g so that G acts on S_g . The set $\mathcal{H}(G) = Genera(G) + |G| - 1$ is called the *Hurwitz semigroup* for G and was first defined in [MS]. The Hurwitz semigroup is a subset of the positive integers which is closed under addition. It follows from the Riemann-Hurwitz formula that an element h is in the Hurwitz semigroup if and only if there exists a G -signature σ with $h = |G|(1 - \frac{1}{2}\chi(\sigma))$. We will denote the *Spherical Hurwitz semigroup*, which is a translate of the set of spherical genera, by

$$\mathcal{H}_s G = \{ |G|(1 - \frac{1}{2}\chi(\sigma)) \mid \sigma = (m_1, m_2, \dots, m_l) \text{ is a } G\text{-signature} \}.$$

We define

$$\mathcal{H}_o(G) = \{ |G|(1 - \frac{1}{2}\chi(\sigma)) \mid \sigma = (m_1, m_2, \dots, m_l), 1 \neq m_i, \text{ divides } |G| \text{ for all } i \}.$$

We are now able to give a concise description of $\mathcal{H}_s(PSL_2(p))$.

Corollary 5.10. $\mathcal{H}_s(PSL_2(p)) = \mathcal{H}_o(PSL_2(p)) \cap [|PSL_2(p)| + 1, \infty)$ when $p > 11$.

Proof. First observe that the Hurwitz semigroup is always contained in the interval $[|PSL_2(p)| - 1, \infty)$. The only signatures which are not $PSL_2(p)$ -signatures are those with nonnegative Euler characteristic, which occur in $\mathcal{H}_o(PSL_2(p))$ as:

- $|PSL_2(p)| - 1$, corresponding to actions of $PSL_2(p)$ on the sphere, and
- $|PSL_2(p)|$, corresponding to actions of $PSL_2(p)$ on the torus.

Therefore $\mathcal{H}_s(PSL_2(p)) = \mathcal{H}_o(PSL_2(p)) \cap [|PSL_2(p)| + 1, \infty)$. □

The description of the sets $\mathcal{H}(PSL_2(7))$ and $\mathcal{H}_s(PSL_2(7))$ are given in [MS]. The analog of Lemma 5.4 fails in this case since $(2, 2, 2, 2, 2)$ is not a $PSL_2(7)$ -signature. Moreover, a careful analysis of our proofs shows that every possible signature for $PSL_2(11)$ with negative Euler characteristic is a $PSL_2(11)$ signature with the possible exception of $(2, 2, 2, 3)$. A computer check shows that $(2, 2, 2, 3)$ cannot possibly be a $PSL_2(11)$ -signature. These are the only exceptions to Corollary 5.9 for $p = 7$ or $p = 11$. As $PSL_2(2) = \mathbb{D}_3$, $PSL_2(3) = \mathbb{A}_4$, and $PSL_2(5) = \mathbb{A}_5$, we see that there is no loss of generality in restricting to the case $p > 11$.

APPENDIX

We now present proofs of several results stated in Section 4.

Proof of Lemma 4.3. Orders of products in $PSL_2(p)$.

- (1) Since $\langle C, D \rangle = \mathbb{S}_4$, we know that the signature

$$(|C^{-1}|, |D|, |D^{-1}C|) = (3, 4, |D^{-1}C|)$$

is an \mathbb{S}_4 -signature. Therefore the order $|CD^{-1}| \neq 3$, since $(3, 3, 4)$ is not a possible \mathbb{S}_4 -signature. Relabelling if necessary, we may assume that as an element of \mathbb{S}_4 , we have $C = (123)$. Since $|CD| = 4$, the element CD has no fixed points. Consequently, we know that as a permutation on 3 letters, $D(2) \neq 1$, $D(3) \neq 2$ and $D(1) \neq 3$. If $|D^{-1}C| = |C^{-1}D| = 4$ then $C^{-1}D$ has no fixed points. Since $C^{-1} = (132)$, we know that $D(3) \neq 1$, $D(2) \neq 3$ and $D(1) \neq 2$. But D has no fixed points since $|D| = 4$. Thus D satisfies the following conditions: $D(1) = 4$, $D(2) = 4$ and $D(3) = 4$ and so $|D^{-1}C| = 2$.

- (2) Assume $\langle C, D \rangle = \mathbb{A}_5$.

- (a) Since $\langle C, D \rangle = \mathbb{A}_5$, the signature

$$(|C^{-1}|, |D|, |D^{-1}C|) = (3, 3, |D^{-1}C|)$$

is an \mathbb{A}_5 -signature. Since $\chi(3, 3, 3) = 0$ and \mathbb{A}_5 is not solvable, $|D^{-1}C| \neq 3$. If $|D^{-1}C| = 2$, then we may assume that $D = (123)$ and 1 is the fixed point of $D^{-1}C$. Since $|C| = 3$ and $C \neq D$, we must have $C = (124)$ or $C = (125)$, contradicting the order of CD . Thus $|D^{-1}C| \neq 2$, and we must have $|D^{-1}C| = 5$.

- (b) Since $|C^{-1}| = 3$, $|CD| = 3$ and $|c^{-1}CD| = |D| = 5$, it follows from (a) above that $|D^{-1}C| = 5$.
- (c) The argument given above in (1) shows that $|D^{-1}C| \neq 5$. If $|D^{-1}C| = 2$, then we have found a realization of the triple $(2, 3, 5)$, a contradiction. Thus $|D^{-1}C| = 3$.

- (d) Relabelling if necessary, we may assume that $D = (12345)$. Since $|C| = |CD| = 5$, neither C nor D has fixed points. We then deduce that $C(n)$ cannot be n or $n - 1$, for $1 \leq n \leq 5$, and we reduce modulo 5. If in addition $|D^{-1}C| = 5$, we add the restriction that $C(n) \neq n + 1$. Choosing $C(1)$, we see that either $C = (13524)$ or $C = (14253)$. It follows in the first case that $D^{-1}C = D$ and in the second that $CD = D^{-1}$. In either case we contradict the fact that $\langle C, D \rangle = \mathbb{A}_5$. Thus $|D^{-1}C| \neq 5$.
 If $|D^{-1}C| = 2$, without loss of generality assume that $D^{-1} = (1a)(bc)$ where $a, b, c \in \{2, 3, 4\}$, making 5 the fixed point of D . The assumptions $a = 2, 3, 4$ respectively give the contradictions $C(2) = 2$, $C(2) = 1$ and $C(5) = 4$. Thus $|D^{-1}C| \neq 2$, and we must have $|D^{-1}C| = 3$.
- (e) We may assume that $D = (12345)$ and 3 is the fixed point of C . Since CD has no fixed points, we know that $C(1) \neq 5$, $C(2) \neq 1$, $C(3) \neq 2$, $C(4) \neq 3$ and $C(5) \neq 4$. Since $C = (1b)(cd)$ with $b, c, d \in \{2, 4, 5\}$, we must have $C = (14)(25)$. Consequently, $CDC^{-1}D^{-1} = (134)$, which has order 3. \square

Proof of Lemma 4.4. Subgroups of $PSL_2(q)$ containing elements of certain orders.

- (1) Since $|C| = 3$ and $|D| = 4$, we know that $12 \mid |H|$. Since $D \in H$ and $H \neq \mathbb{A}_4$, we know that $|H| \neq 12$. Thus $|H| = 24$ and $H = \mathbb{S}_4$.
- (2) Since \mathbb{A}_5 is simple, it has no subgroups of order 15, 20 or 30.
 - (a) Since $15 \mid |H|$ and $|H| \mid 60$, we must have $|H| = 60$ and $H = \mathbb{A}_5$.
 - (b) Since $10 \mid |H|$ and $|H| \mid 60$, we must have $|H| = 10$ or $H = \mathbb{A}_5$. If $|H| = 10$, then H has a unique Sylow 5-subgroup S . Since D and CD are in S , we must have $C \in S$. But $|C| = 2$. Thus $H = \mathbb{A}_5$.
 - (c) Since $5 \mid |H|$ and $|H| \mid 60$, we must have $|H| \in \{5, 10, 60\}$. If $|H| = 10$, then H has a unique Sylow 5-subgroup S . Since C and D^{-1} are in S , we must have $D^{-1}C \in S$. This contradicts Lemma 4.3, which says that $|D^{-1}C| = 3$. This $H \cong \mathbb{Z}_5$ or $H = \mathbb{A}_5$. \square

Proof of Theorem 4.7. All polyhedral ramification triples are $PSL_2(p)$ -ramification triples.

- (1) Let σ be a permutation of $(3, 3, 4)$. Suppose $m_1 = 3$ and $m_2 = 4$. Choose a realization $(A, B, (AB)^{-1})$ as in Section 4.1, of the trace triple $(1, t, -t)$. Then $\text{tr}(B^{-1}A) = 2t \neq 0$, and it follows from lemma 4.3 that $|BA^{-1}| \neq 2$. Any permutation of the trace triple yields $|BA^{-1}| \neq 2$. Thus $\langle A, B, (AB)^{-1} \rangle \neq \mathbb{S}_4$ by Lemma 4.4.
- (2) Let σ be a permutation of $(3, 5, 5)$. Suppose that $m_1 = 3$ and $m_2 = 5$. Choose a realization $(A, B, (AB)^{-1})$ as above, of the trace triple $(1, t, \alpha)$, where t is a root of $z^2 + z - 1$ and α is a root of $z^2 - z - 1$. Then $\text{tr}(B^{-1}A) = dt - \alpha = -\alpha - 1 \neq 0$ since $t \neq -\alpha$. If $\text{tr}(B^{-1}A) = \pm 1$, then either $-\alpha = t - 1$ or $t = \alpha - 1$. In either case it follows from Lemma 4.5 that $|B^{-1}A| \neq 1$.
 Interchanging t and d yields the same contradiction when $m_2 = 3$. Thus $|B^{-1}A| \neq 2$ and $|B^{-1}A| \neq 3$ by Lemma 3.7 and $\langle A, B \rangle \neq \mathbb{A}_5$ by Lemma 4.3.
- (3) Let σ be a permutation of $(2, 5, 5)$. If $m_2 = 5$ we may assume that $m_1 = 2$. Choose a realization as above of the trace triple $(0, t, \alpha)$, where t is a root of

$z^2 - z - 1$ and α is a root of $z^2 + z - 1$. Then $tr(ABA^{-1}B^{-1}) = t + \alpha^2 - 2 = t - \alpha \neq \pm 1$. Consequently, $|ABA^{-1}B^{-1}| \neq 3$.

We obtain the same contradiction when $m_2 = 2$, and it follows from Lemma 4.3 that $\langle A, B, (AB^{-1}) \rangle \neq \mathbb{A}_5$.

- (4) Let σ be a permutation of $(5, 5, 5)$. Let $(\alpha, -\alpha, \alpha)$ be a trace triple corresponding to this signature, where α satisfies $z^2 - z - 1$, and choose a realization $(A, B, (AB)^{-1})$ as above. Compute that $tr(B^{-1}A) = -\alpha^2 - \alpha$. If $tr(B^{-1}A) = \pm 1$, then α satisfies the equations $-\alpha^2 - \alpha \pm 1 = 0$ and $\alpha^2 - \alpha - 1 = 0$ simultaneously, leading to the contradiction $\alpha = 0$ or $\alpha = 1$. Thus $|B^{-1}A| \neq \pm 1$ and $|B^{-1}A| \neq 3$.

Choose a realization of the trace triple $(\alpha, \frac{-1}{\alpha}, \alpha)$ as above, where α satisfies $z^2 - z - 1 = 0$. Then $tr(B^{-1}A) = 1 - \alpha \neq \pm 1$ and $|B^{-1}A| \neq 3$. Thus $\langle A, B, (AB)^{-1} \rangle \neq \mathbb{A}_5$.

We now check that $\langle A, B, (AB)^{-1} \rangle$ is not cyclic. If $m_2 | \frac{p-1}{2}$, then the matrix B in our realization fixes ∞ , while the matrix A does not. Thus $\langle A, B, (AB)^{-1} \rangle$ is not abelian.

If $m_2 | \frac{p+1}{2}$, then the realization given in §4.1 yields the matrices $A = \begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}$ with trace α and $B = \begin{pmatrix} x & y \\ \bar{y} & \bar{x} \end{pmatrix}$ with trace $-\alpha$ or trace $\frac{-1}{\alpha}$. We will show that $x\bar{x} \neq 1$, which implies that $\bar{y} \neq 0$ since ∞ will not be a fixed point of B . It then follows that $\langle A, B, (AB)^{-1} \rangle$ is not abelian, hence not cyclic.

Solving the equation $tr(AB)^{-1} = \alpha$ we see that $x = \frac{\bar{\lambda}t - \alpha}{\bar{\lambda} - \lambda}$, where $t = -\alpha$ or $t = \frac{-1}{\alpha}$. Setting $x\bar{x} = 1$ yields the equation $\alpha^3 - 3\alpha^2 - 4 = 0$ when $t = -\alpha$ and $\alpha^4 - \alpha^3 + \alpha^2 - 3 = 0$ when $t = \frac{-1}{\alpha}$. Solving either equation simultaneously with $\alpha^2 - \alpha - 1 = 0$ yields a contradiction. Consequently, $\langle A, B, (AB)^{-1} \rangle$ is not cyclic and must be $PSL_2(p)$. □

Proof of Theorem 4.8. Characterization of $PSL_2(p)$ -ramification triples. Consider a trace triple $(\pm t_1, \pm t_2, \pm t_3)$ and choose initial traces (t_1, t_2, t_3) . Let $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ be a ramification triple corresponding to the trace triple, i.e., each \mathcal{C}_i is the conjugacy class of an element of $PSL_2(p)$ whose trace is t_i .

Case 2. Suppose \mathcal{C}_1 is a conjugacy class of hyperbolic elements, and neither \mathcal{C}_2 nor \mathcal{C}_3 is a conjugacy class of parabolic elements. Without conjugacy classes of parabolic elements, $PGL_2(q)$ -ramification types are exactly the same as $PSL_2(q)$ -ramification types. We conjugate \mathcal{C}_1 in $PSL_2(p)$ so that $\begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}$ is a representative of \mathcal{C}_1 , where $\lambda \in \mathbb{F}_q - \{\pm 1\}$ and $t_1 = \lambda + \frac{1}{\lambda}$. Let $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ be a representative of \mathcal{C}_2 , with $x + w = t_2$. If $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ can be realized, then we can solve the equations $x + w = t_2$ and $\lambda x + \frac{w}{\lambda} = t_3$ subject to the constraint $xw - yz = 1$.

This set of equations has the following solution:

$$w = \frac{\lambda t_2 - t_3}{\lambda - \frac{1}{\lambda}}, \quad x = \frac{\lambda t_3 - t_2}{\lambda^2 - 1}, \quad yz = \frac{(\lambda t_2 - t_3)(\lambda t_3 - t_2)}{(\lambda - \frac{1}{\lambda})(\lambda^2 - 1)} - 1.$$

Taking $y = 1$ we see that all ramification types containing at least one conjugacy class of hyperbolic elements can be realized.

Now we must see which of these ramification types are $PSL_2(p)$ -ramification types, i.e., when elements from the three conjugacy classes generate $PSL_2(p)$. We will denote the subgroup of $PSL_2(p)$ generated by representatives of the conjugacy

classes by $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$. The matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix} \in \mathcal{C}_1$ has fixed points 0 and ∞ . We now consider whether or not $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ is contained in a Borel subgroup.

- (1) Suppose that $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ is contained in a Borel subgroup B . Then B fixes 0 or ∞ which implies that $y = 0$ or $z = 0$. In either case, $yz = 0$.

If $yz = 0$, then $(\lambda^2 t_2 - \lambda t_3)(\lambda t_3 - t_2) = (\lambda^2 - 1)(\lambda^2 - 1)$. If we change t_2 to $-t_2$ with the result that this equation changes, then $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ will no longer be contained in a Borel subgroup. If this does not occur, then after negating, the trace $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ is still contained in a Borel subgroup, and both t_2 and $-t_2$ satisfy the quadratic equation $\lambda x^2 - (\lambda^2 + 1)t_3 x + \lambda t_3^2 + (\lambda - \frac{1}{\lambda})^2 = 0$. But $\pm t_2$ are also roots of the quadratic $x^2 - t_2^2 = 0$, and scaling by λ to equate leading terms, we obtain

$$\lambda t^2 - (\lambda^2 + 1)t_3 x + \lambda t_3^2 + (\lambda - \frac{1}{\lambda})^2 = \lambda(x^2 - t_2^2).$$

It follows that $(\lambda^2 + 1)t_3 = 0$, so either $t_3 = 0$ or $\lambda^2 + 1 = 0$, which occurs iff $t_1 = 0$. The above equation then reduces to $\lambda t_3 + (\lambda - \frac{1}{\lambda})^2 = -t_2^2 \lambda$. Rearranging terms yields $t_2^2 + t_3^2 + (t_1 - \frac{2}{\lambda})^2$ which simplifies to $t_1^2 + t_2^2 + t_3^2 = 4$.

- (a) Suppose $t_3 = 0$. Then $t_1^2 + t_2^2 - 4 = 0$, and making the substitution $\delta = \lambda - \frac{1}{\lambda}$ yields $t_2^2 + \delta^2 = 0$ which has a solution iff -1 is a square in \mathbb{F}_q . In this case, $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ will always generate a Borel subgroup, and the ramification type will not be a $PSL_2(p)$ -ramification type. This ramification type is represented by the trace triple $(0, \pm(\lambda + \frac{1}{\lambda}), \pm\sqrt{-1}(\lambda + \frac{1}{\lambda}))$, and \mathcal{C}_3 is a conjugacy class of hyperbolic elements.

When -1 is not a square in \mathbb{F}_q the equation $t_2^2 + \delta^2 = 0$ has no solutions and thus $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ is a $PSL_2(p)$ -ramification type.

- (b) Suppose $t_1 = 0$. Then $t_1^2 + t_2^2 + t_3^2 = 0$ simplifies to $t_2^2 + t_3^2 - 4 = 0$, which again has a solution iff -1 is a square in \mathbb{F}_q . In this case, \mathcal{C}_3 is a conjugacy class of hyperbolic elements, and switching t_1 and t_3 brings us back to case (a).

- (2) Now suppose that $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ is not contained in a Borel subgroup, so $yz \neq 0$. Since \mathcal{C}_1 is a conjugacy class of hyperbolic elements, $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ cannot be contained in a Cartan subgroup of $PSL_2(p)$. If it generates a polyhedral subgroup, then the ramification type is a $PSL_2(p)$ -ramification type. If not, then it must generate $PSL_2(p)$.

Thus, when \mathcal{C}_1 is a conjugacy class of hyperbolic elements and \mathcal{C}_2 and \mathcal{C}_3 are not conjugacy classes of parabolic elements, the only triple that is not a $PSL_2(p)$ -ramification type corresponds to the trace triple $(0, \pm(\lambda + \frac{1}{\lambda}), \pm\sqrt{-1}(\lambda - \frac{1}{\lambda}))$.

We now compute the signatures corresponding to this ramification type which is not a $PSL_2(p)$ -ramification type. These traces correspond to the transformations $T_1(z) = \lambda^2 z$ and $T_2(z) = -\lambda^2 z$ in $PSL_2(p)$. Suppose that d is the multiplicative order of T_1 . If d is odd, then the order of T_2 is $2d$, where $2d \mid \frac{q-1}{2}$ since T_2 is also hyperbolic. Then the signature corresponding to this trace triple is $(2, d, 2d)$. If d is even, then $4 \mid d$ and the order of T_2 is also d , so the corresponding signature is $(2, d, d)$.

In the signature $(2, d, d)$, all three conjugacy classes are of hyperbolic elements, since $2d$ and hence d divide $\frac{q-1}{2}$. Although the quadratic $\lambda(t^2 - t_2^2)$ has only the roots $\pm t_2$, we can find other traces $\pm t_2$ giving rise to elements of order d . A counting

argument shows that there are $\frac{\phi(d)}{2}$ traces (up to sign) giving elements of order d , and $\frac{\phi(d)}{2} > 1$ unless $d = 3, 4, 6$. The signature $(2, 6, 6)$ does not correspond to non- $PSL_2(p)$ -ramification type because 6 is not divisible by 4. Thus, all σ except $(2, 3, 6)$ and $(2, 4, 4)$ can be moved out of a Borel subgroup.

Case 3. All \mathcal{C}_i are conjugacy classes of elliptic elements. We can conjugate $PSL_2(p)$ inside $PGL_2(q)$ so that a representative element of \mathcal{C}_1 is of the form $\begin{pmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{pmatrix}$ where $\lambda \in \mathbb{E} - \mathbb{F}$, and a representative element of \mathcal{C}_2 is of the form $\begin{pmatrix} x & -y \\ y & \bar{x} \end{pmatrix}$ where $x, y \in \mathbb{E}$. We know that $\lambda + \bar{\lambda} = t_1$ and $x + \bar{x} = t_2$ by trace considerations, and $x\bar{x} + y\bar{y} = 1$. Multiplying yields the additional restriction $\lambda x + \bar{\lambda}\bar{x} = t_3$.

Solving the above equations, we obtain expressions for x and \bar{x} :

$$x = \frac{\bar{\lambda}t_2 - t_3}{\lambda - \bar{\lambda}} \text{ and } \bar{x} = \frac{\lambda t_2 - t_3}{\lambda - \bar{\lambda}}.$$

Rewriting $x\bar{x} + y\bar{y} = 1$ as $y\bar{y} = 1 - x\bar{x}$, we see that unless $x\bar{x} = 1$ we apply Lemma 3.2 to find a value of y realizing the above equation since $y\bar{y} = ||y||$ and the norm map is surjective onto \mathbb{F}^* . Thus all ramification types can be realized when $x\bar{x} \neq 1$.

- (1) Suppose $x\bar{x} = 1$ and $t_2t_3 \neq 0$. Then by negating a nonzero trace (either t_2 or t_3) we obtain new expressions for x' and \bar{x}' for x and \bar{x} . It is easy to see that the equations $x\bar{x} = 1$ and $x'\bar{x}' = 1$ cannot be satisfied simultaneously, allowing us to use the above argument to realize the ramification type.

Since the representative matrices of \mathcal{C}_1 and \mathcal{C}_2 given above have different fixed points, $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ cannot be contained in a Cartan subgroup. It is easily checked that $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$ is not contained in a dihedral or polyhedral subgroup and thus must generate $PSL_2(p)$.

- (2) Suppose $x\bar{x} = 1$ and $t_2t_3 = 0$, so that either \mathcal{C}_2 or \mathcal{C}_3 is a conjugacy class of elements of order 2. If $t_2 = 0$ or $t_3 = 0$, then the corresponding signature would be dihedral, since trace 0 corresponds to an element of order 2. However, we showed in Section 4 that a dihedral signature will not be a $PSL_2(p)$ signature.

Rewriting $t_2^2 + t_3^2 = 4$ as $t_2^2 - 4 = -t_3^2$ we see that $t_2^2 - 4 \in \mathbb{F}^+$, and thus t_2 corresponds to a conjugacy class of hyperbolic elements. Similarly t_3 corresponds to a conjugacy class of hyperbolic elements. We know that \mathcal{C}_1 is not a conjugacy class of parabolic elements, since parabolic elements have trace 2, and this case reduces to case 2.

Thus all ramification types with three conjugacy classes of elliptic elements can be realized. We now show that they must be $PSL_2(p)$ -ramification types.

Case 4. Suppose \mathcal{C}_1 and \mathcal{C}_2 represent conjugacy classes of parabolic elements, with corresponding trace triple $(\pm 2, \pm 2, \pm t_3)$, including the case $t_3 = \pm 2$. Choose initial traces $(2, 2, \pm t_3)$.

Up to conjugacy in $PGL_2(p)$ let $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ be a representative of \mathcal{C}_1 and let $\begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix}$ be a representative of \mathcal{C}_2 . Multiplying, we get the matrix $\begin{pmatrix} 1+w & 1 \\ w & 1 \end{pmatrix}$ with $t_3 = w + 2$. Solving for w , we get a realization of the trace triple. We first show that any ramification type corresponding to this trace triple must be a $PSL_2(p)$ -ramification type.

Suppose this ramification type $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ can be realized. Since \mathcal{C}_1 and \mathcal{C}_2 are conjugacy classes of parabolic elements with different fixed points, $\langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$

cannot be contained in a Borel or a Cartan subgroup of $PSL_2(p)$. It is easily checked that it does not generate a polyhedral subgroup. It cannot generate a dihedral subgroup since its corresponding signature is of the form $(p, p, *)$, which cannot be a dihedral signature. We then conclude that it must generate $PSL_2(p)$.

We now decide which ramification types corresponding to the trace triple $(2, 2, t_3)$ can be realized. The above argument shows that if it can be realized, then it is a $PSL_2(p)$ -ramification type.

- (1) Suppose $t_3 = \pm 2$, so \mathcal{C}_3 is also a conjugacy class of parabolic elements. We choose $t_3 = -2$ and check that $\begin{pmatrix} -3 & 1 \\ -4 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix}$ both belong to \mathcal{C}_3 . From Lemma 3.5 it follows that \mathcal{C}_1 and \mathcal{C}_3 represent the same conjugacy class iff -4 and thus $-1 \in \mathbb{F}^+$. So if $-1 \in \mathbb{F}^+$, any realizable ramification type is of the form $(\mathcal{C}_1, \mathcal{C}_1, \mathcal{C}_1)$. If $-1 \notin \mathbb{F}^+$, then the only realizable ramification type has exactly two identical conjugacy classes of parabolic elements.
- (2) Choose an initial trace $t_3 \neq \pm 2$ and $t_3 \neq 0$, so \mathcal{C}_3 is not a conjugacy class of parabolic elements. Solving for w , we see that $w = t_3 - 2$. The matrices $\begin{pmatrix} 1 & 0 \\ t_3 - 2 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & -t_3 + 2 \\ 0 & 1 \end{pmatrix}$ are conjugate, thus both in \mathcal{C}_2 . If we had chosen $-t_2$ as the initial trace, we would have $\begin{pmatrix} 1 & t_3 + 2 \\ 0 & 1 \end{pmatrix}$ as the representative of \mathcal{C}_2 . Since both of these matrices belong to the conjugacy class \mathcal{C}_2 , we apply Lemma 3.5 to say that they are conjugate iff $\frac{-(t_3 - 2)}{-(-t_3 - 2)} = \frac{-t_3 + 2}{t_3 - 2} \in \mathbb{F}^+$.

We now determine the type of \mathcal{C}_3 . Multiply $\frac{-t_3 + 2}{t_3 - 2}$ by $(t_3 - 2)^2$ to see that $4 - t_3^2 = (-1)(t_3^2 - 4) \in \mathbb{F}^+$. It then follows that

- if $-1 \in \mathbb{F}_q$, then $t_3^2 - 4 \in \mathbb{F}^+$, which means that \mathcal{C}_3 is a conjugacy class of hyperbolic elements, or
- if $-1 \notin \mathbb{F}_q$, then $t_3^2 - 4 \notin \mathbb{F}^+$, which means that \mathcal{C}_3 is a conjugacy class of elliptic elements.

We now consider whether or not \mathcal{C}_1 and \mathcal{C}_2 represent the same conjugacy class of parabolic elements of $PSL_2(p)$. Conjugate $\begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix}$ to the matrix $\begin{pmatrix} 1 & -w \\ 0 & 1 \end{pmatrix}$ to see that it is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ iff $-w = -t_3 + 2 \in \mathbb{F}^+$, by Lemma 3.5. If we had chosen $-t_3$ as an initial trace for \mathcal{C}_3 , we would have the condition $t_3 + 2 \in \mathbb{F}^+$.

- (a) Suppose that \mathcal{C}_1 and \mathcal{C}_2 represent the same conjugacy class of elements of $PSL_2(p)$. We know that $\frac{-t_3 + 2}{t_3 - 2} \in \mathbb{F}^+$ by trace considerations in \mathcal{C}_2 . Since $\mathcal{C}_1 = \mathcal{C}_2$ we know that the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & \pm t_3 + 2 \\ 0 & 1 \end{pmatrix}$ are conjugate. By Lemma 3.5 we must have $\pm t_3 + 2 \in \mathbb{F}^+$.
 - If $-t_3 + 2 \in \mathbb{F}^+$ it follows from Lemma 3.1 that $t_3 + 2 \in \mathbb{F}^+$ and we can only realize ramification types of the form $(\mathcal{C}_1, \mathcal{C}_1, \mathcal{C}_3)$.
 - If $-t_3 + 2 \notin \mathbb{F}^+$, then it follows from Lemma 3.1 that $t_3 + 2 \notin \mathbb{F}^+$ and we can only realize ramification types of the form $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$.

In these cases we cannot realize both ramification types corresponding to the trace triple $(\pm 2, \pm 2, \pm t_3)$ as $PSL_2(p)$ -ramification types. In the remaining cases all ramification types are $PSL_2(p)$ -ramification types.

- (b) If \mathcal{C}_1 and \mathcal{C}_2 are distinct conjugacy classes, then we have given a realization of the ramification type, which is a $PSL_2(p)$ -ramification type by the argument above.
- (3) Suppose that $t_3 = 0$ and consider the matrix $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, which is conjugate to $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. This matrix is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ iff $2 \in \mathbb{F}^+$. In this case, \mathcal{C}_1 and \mathcal{C}_2 represent the same conjugacy class of parabolic elements, and the

ramification type $(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ is not realizable. If $2 \notin \mathbb{F}^+$, then the ramification type $(\mathcal{C}_1, \mathcal{C}_1, \mathcal{C}_3)$ is not realizable. Note that this does not rule out any $PSL_2(p)$ -signatures, only certain ramification types. \square

REFERENCES

- [B] A. F. Beardon, *The geometry of discrete groups*, Springer-Verlag, New York (1983). MR0698777 (85d:22026)
- [D] L.E. Dickson, *Linear groups with an exposition of the Galois field theory*, Leipzig (1901) reprinted by Dover, New York (1960). MR104735 (21:3488)
- [EKS] A.L. Edmonds, R.S. Kulkarni and R. Stong, *Realizability of branched coverings of surfaces*, Transactions of the Amer. Math. Soc., **282**, no. 2 (1984), pp. 773-790. MR0732119 (85k:57005)
- [FK] H.M. Farkas and I. Kra, *Riemann Surfaces*, Springer-Verlag, New York (1980). MR0583745 (82c:30067)
- [FGM] D. Frohardt, R. Guralnick, and K. Magaard, *Genus 0 Actions of Groups of Lie Rank 1*, Proceedings of Symposia in Pure Mathematics, Fried and Ihara, eds., **70** (2002), pp. 449-483. MR1935417 (2003j:20019)
- [GS1] H. Glover and D. Sjerve, *Representing $PSL_2(p)$ on a Riemann surface of least genus*, L'enseignement Mathématique **31** (1985), pp. 305-325. MR0819357 (87a:20051)
- [GS2] H. Glover and D. Sjerve, *The genus of $PSL_2(q)$* , Journal für die reine und angewandte Mathematik **380** (1987), pp. 59-86. MR0916200 (89e:20087)
- [GT] R.M. Guralnick and J.G. Thompson, *Finite Groups of Genus Zero*, J. Algebra **131** (1990), pp. 303-341. MR1055011 (91e:20006)
- [H] A. Hurwitz, *Ueber algebraische gebilde mit eindeutigen transformationen in sich*, Math. Ann. **41** (1897) pp. 428-471. MR1510753
- [JS] G.A. Jones and D. Singerman, *Maps, Hypermaps, and Triangle Groups*, in The Grothendieck Theory of Dessins d'Enfants (ed. L. Schneps), London Math. Soc. Lecture Note Ser. 200 (1994), pp. 115-145. MR1305395 (95m:20055)
- [K] R. Kulkarni, *Symmetries of Surfaces*, Topology **26**, no. 2 (1987), pp. 195-203. MR0895571 (88m:57051)
- [KM] R. Kulkarni and C. Maclachlan, *Cyclic p -groups of symmetries of surfaces*, Glasgow Math. J. **33** (1991) no. 2, pp. 213-221. MR1108745 (92e:57052)
- [Ma1] A.M. MacBeath, *Generators of the linear fractional groups*, Proc. Symp. Pure Math. **12** (1969), pp. 14-32. MR0262379 (41:6987)
- [Ma2] A.M. Macbeath, *Hurwitz Groups and Surfaces*, in The Eightfold Way, MSRI Publications, Volume 35 (1998), pp. 103-113. MR1722414 (2001c:14002)
- [Mi] R. Miranda, *Algebraic Curves and Riemann Surfaces*, Graduate Studies in Mathematics, Vol. 5, American Mathematical Society (1995). MR1326604 (96f:14029)
- [MM] B. Malle and B.H. Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin (1999). MR1711577 (2000k:12004)
- [McM] D. McCullough and A. Miller, *The stable genus increment for group actions on closed 2-manifolds*, Topology **31** (1992), pp. 367-397. MR1167177 (93d:57024)
- [MP] M. Mulase and M. Penkava, *Ribbon Graphs, Quadratic Differentials on Riemann Surfaces, and Algebraic Curves Defined Over $\overline{\mathbb{Q}}$* , Asian J. Math. **2** (1998), pp. 875-919. MR1734132 (2001g:30028)
- [MS] A. Miller and J.A. Smith, *Klein's group and the Hurwitz semigroup*, preprint (1991).
- [Sc] L. Schneps (editor), *The Grothendieck Theory of Dessins d'Enfants*, London Mathematical Society Lecture Note Series 200, Cambridge University Press, Cambridge (1994). MR1305390 (95f:11001)
- [Se] J.P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Vol. 1, Jones and Bartlett Publishers, Boston (1992). MR1162313 (94d:12006)
- [SV] G.B. Shabat and V.A. Voevodsky, *Drawing Curves Over Number Fields* in The Grothendieck Festschrift III, Progress in Math. 88, Birkhäuser, Basel (1990), pp. 199-227. MR1106916 (92f:11083)
- [Si] C. Simmons, *Euclidean, conformal and hyperbolic geometry over classical, finite and other fields*, Ph.D. thesis (1998).

- [St] R.E. Stong, *Pseudofree actions and the Greedy algorithm*, Math. Ann. **265** (1983), pp. 501-512. MR0721884 (85i:57012)
- [Su] M. Suzuki, *Group Theory*, Springer-Verlag, Berlin, New York (1982). MR0648772 (82k:20001c)
- [T] T. Tucker, *Finite groups acting on surfaces and the genus of a group*, J. Comb. Theory Ser. B **34**, no. 1 (1983), pp. 82-98. MR0701174 (85b:20055)
- [Y] K. Yang, *Compact Riemann surfaces and algebraic curves*, World Scientific, Singapore (1988). MR0986072 (90e:14023)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OKLAHOMA, NORMAN, OKLAHOMA 73019
E-mail address: mozaydin@math.ou.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CENTRAL OKLAHOMA, EDMOND, OKLAHOMA 73034
E-mail address: cksimmons@ucok.edu

DEPARTMENT OF MATHEMATICS, BOWDOIN COLLEGE, BRUNSWICK, MAINE 04011
E-mail address: jtaback@bowdoin.edu