NON-ABELIAN SIMPLE GROUPS ACT WITH ALMOST ALL SIGNATURES

MARIELA CARVACHO, JENNIFER PAULHUS, TOM TUCKER, AND AARON WOOTTON

Abstract. The topological data of a finite group G acting conformally on a compact Riemann surface is often encoded using a tuple of non-negative integers $(h; m_1, \dots, m_s)$ called its signature, where the m_i are orders of non-trivial elements in the group. There are two easily verifiable arithmetic conditions on a tuple which are necessary for it to be a signature of some group action. We derive necessary and sufficient conditions on a group for the situation where all but finitely many tuples that satisfy these arithmetic conditions actually occur as the signature for an action of G on some Riemann surface. As a consequence, we show that all non-abelian finite simple groups exhibit this property.

1. Introduction

A finite group G is said to act conformally on a compact Riemann surface S of genus σ if there is an injection

$$i\colon G \hookrightarrow \mathrm{Aut}(S)$$

into the group of conformal automorphisms of S. The question of which finite groups can act conformally on a compact Riemann surface of genus σ (equivalently which groups exist as the monodromy group of a regular branched cover) is an old one; see for example [15], and specific knowledge of these groups and the corresponding monodromy has important applications in a number of different areas. For example, knowledge of these groups and their monodromies can help provide an explicit description of the equisymmetric strata of the branch locus in the moduli space of compact Riemann surfaces of genus σ; see for example [1], [5] and [13]. As another example, there is a natural correspondence between conjugacy classes of finite subgroups of the mapping class group in genus σ and equivalence classes of conformal group actions on a smooth oriented surface of genus σ (up to topological equivalence), so the study of conformal automorphisms provides insight into the general structure of the mapping class group; see for example [3], [7], [12], and [18]. Further examples of applications lie in the areas of inverse Galois theory [11], Shimura varieties [10], and Jacobian varieties [19] and [20].

We say that a tuple $(h; m_1, \dots, m_s)$ is the *signature* of a finite group G acting on a compact Riemann surface S of genus σ if the quotient surface S/G has genus h and the quotient map $\pi\colon S \to S/G$ is branched over s points with ramification indices $m_1, \dots, m_s$, called the *periods*. The integer h is called the *orbit genus* of the action, while the numbers $m_1, \dots, m_s$ form the *tail* of the tuple. When the tail has length zero, we write $(h; -)$. Since there is no natural order to the branch points in the quotient S/G, we will typically choose an ordering of the periods $m_1, \dots, m_s$ that is convenient depending on the context (see the remarks after Theorem 2.1).

Date: May 29, 2020.

[1] Partially supported by Anillo PIA ACT1415 and Proyecto Interno USM 116.12.2.

[2] Partially supported by a Frank and Roberta Furbush Scholarship from Grinnell College.

[3] Partially supported by Award 317689 from the Simons Foundation.

Riemann's Existence Theorem (see Theorem 2.1) provides arithmetic and group theoretic conditions which are necessary and sufficient for a tuple $(h; m_1, \dots, m_s)$ to be the signature of G acting on S. Outside of a few well known degenerate cases as outlined in Theorem 3.1, a tuple $(h; m_1, \dots, m_s)$ satisfies the necessary arithmetic conditions of Theorem 2.1 if and only if its tail consists only of non-trivial element orders from G. In particular, for any group G in which a complete list of orders of elements in the group are known, all tuples which satisfy just the arithmetic conditions are easy to compute. We call such tuples *potential signatures*, and each group has an infinite number of potential signatures.

In contrast however, outside of some small genus examples or special families of groups (see for example [5], [14] and the database provided in [4]) the potential signatures which satisfy the group theoretic conditions of Theorem 2.1 are far less well understood. The issue is that testing the group theoretic condition is much more difficult computationally than testing the arithmetic conditions (and grows progressively more difficult as the group order or the length of the tail of the signature grows), and so it is not currently possible to get the same complete information we have for potential signatures. Indeed, the problem of determining which groups act with which signatures and other related problems is part of a very active area of research, in no small part due to the tremendous advances in computational power over the last few decades; see for example [1], [8], [9], [17].

Since finding potential signatures is easy, but verifying when they are actually signatures is hard, these observations lead to the following natural line of inquiry: are there any groups for which the difference between potential signatures and actual signatures is finite? If G is a finite group which exhibits this property, we shall henceforth say that G *acts with almost all signatures*, or simply G is AAS.

The importance of AAS groups in the wider picture is the following. The *genus spectrum* of a group G is the (infinite) set of integers $\mathcal{S}(G) = \{\sigma_1, \sigma_2, \dots\}$ such that for each $\sigma_i \in \mathcal{S}(G)$, there exists a compact Riemann surface of genus σ_i on which G acts. In [16], Kulkarni showed that each $\sigma_i \in \mathcal{S}(G)$ satisfies a simple congruence dependent on the order of G and its exponent and moreover, there exists an integer Σ_G, called the *minimum stable genus of* G (see [22]), such that any $\sigma \geq \Sigma_G$ which satisfies this congruence lies in $\mathcal{S}(G)$. Our work expands on Kulkarni's work in the following sense. If G is an AAS group, then there exists a $\sigma_G \in \mathcal{S}(G)$ such that for any $\sigma \geq \sigma_G$ in the genus spectrum, G acts with *all* potential signatures on a surface of genus σ. That is, for any $\sigma \geq \sigma_G$, satisfaction of the arithmetic conditions for G to act on a surface of genus σ with signature $(h; m_1, \dots, m_s)$ is sufficient for the existence of a group action with that signature. Thus for AAS groups, finding the signatures with which they can act for the applications cited above becomes much more straightforward.

In the following note, we produce necessary and sufficient conditions for when a finite group G is AAS. As a consequence of these conditions, we show in Theorem 4.6 that all finite non-abelian simple groups are AAS. We also provide deeper analysis of the structure of AAS groups including an array of explicit examples, and we lay the groundwork for further inquiry into such groups.

2. Preliminaries

We start by recalling some basic facts about surfaces and group actions on surfaces, and fixing some notation and terminology.

For a fixed finite group G, we let e_G denote its identity. We define the *order set* of G as

$$\mathrm{Ord}(G) = \{|g| : g \in G \setminus \langle e_G \rangle\}$$

where $|g|$ denotes the order of g, and the *set of generating orders* as

$$\mathrm{GenOrd}(G) = \{n \in \mathrm{Ord}(G) : G \text{ is generated by elements of order } n\}.$$

If $\mathrm{Ord}(G) = \{n_1, \ldots, n_r\}$ for positive integers $n_i > 1$, we shall assume $n_1 < n_2 < \cdots < n_r$. For a given $n_i \in \mathrm{Ord}(G)$ we define

$$X_{n_i} = \{g \in G : |g| = n_i\}.$$

We let $[G, G]$ denote the commutator (or derived) subgroup of G, namely the subgroup generated by all elements of the form $[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$ where $g_1,\ g_2 \in G$. Finally, we define

$$X_{[G,G]} = \{[g_1, g_2] : g_1, g_2 \in G\}.$$

Though many of the classical results we shall use hold for any genus, the primary focus of our work will be for genus greater than or equal to 2, since the finite group actions in genus 0 and 1 are well known; see for example [21] and [23]. Henceforth, unless otherwise stated, assume the genus $\sigma \geq 2$.

The following modern adaptation of Riemann's Existence Theorem, [5, Prop. 2.1], provides necessary and sufficient conditions for the existence of a finite group G acting with signature $(h; m_1, \ldots, m_s)$ on a compact Riemann surface S of genus σ.

Theorem 2.1. A finite group G acts on a compact Riemann surface S of genus σ with signature $(h; m_1, \ldots, m_s)$ if and only if:

(1) The Riemann–Hurwitz formula is satisfied:

$$\sigma = 1 + |G|(h-1) + \frac{|G|}{2} \sum_{j=1}^{s} \left(1 - \frac{1}{m_j}\right),$$

and

(2) there exists a word $w = \prod_{i=1}^{h} [a_i, b_i] \prod_{j=1}^{s} c_j$ of elements of G of length $2h + s$ called an $(h; m_1, \ldots, m_s)$-generating word for G which satisfies the following properties:
   (a) $G = \langle a_1, b_1, a_2, b_2, \ldots, a_h, b_h, c_1, \ldots, c_s \rangle$,
   (b) the order of c_j is m_j for $1 \leq j \leq s$, and
   (c) $w = e_G$.

Note that condition (2) of Theorem 2.1 allows for the possibility that there are several different actions for a given signature and group. Also, as observed in the introduction, there is no natural order to the periods in the tail of a signature, so we can permute them as needed. On the level of generating words, this is justified by the fact that if $w = \prod_{i=1}^{h} [a_i, b_i] \prod_{j=1}^{s} c_j$ is an $(h; m_1, \ldots, m_i, m_{i+1}, \ldots, m_s)$-generating word for G, then by letting $c'_{i+1} = c_i c_{i+1} c_i^{-1}$, the word

$$w_1 = \prod_{i=1}^{h} [a_i, b_i] \left(\prod_{j=1}^{i-1} c_j\right) \left(c'_{i+1} c_i\right) \left(\prod_{j=i+2}^{s} c_j\right)$$

is an $(h; m_1, \ldots, m_{i+1}, m_i, \ldots, m_s)$-generating word for G. With this in mind, when $\mathrm{Ord}(G) = \{n_1, \ldots, n_r\}$, we will often write a signature as $(h; [n_1, t_1], \ldots, [n_r, t_r])$ where the pair $[n_i, t_i]$ denotes t_i copies of n_i with $t_i \geq 1$ and excluding each term $[n_i, t_i]$ when there are no periods equal to n_i.

Remark 2.1. It is standard in the literature to use the existence of generating vectors rather than generating words in condition (2) of Theorem 2.1. We use generating words since they allow us to give a more concise and coherent presentation of our results.

3. The Space of Potential Signatures

From Theorem 2.1, we see there are two arithmetic conditions necessary for a tuple $(h; m_1, \dots, m_s)$ to be the signature of some finite group G acting on a compact Riemann surface S of genus $\sigma \geq 2$: (1) $m_i \in \mathrm{Ord}(G)$ for each i, and (2) the Riemann-Hurwitz formula is satisfied for $\sigma \geq 2$. This leads to the following definitions.

Definition 3.1. Let G be a finite group with order set $\mathrm{Ord}(G) = \{n_1, \dots, n_r\}$.

1. For arbitrary non-negative integers $t_1, \dots, t_r$, a tuple $(h; [n_1, t_1], \dots, [n_r, t_r])$ is called a *potential signature* for G if it satisfies the Riemann-Hurwitz formula for some $\sigma \geq 2$. We denote the space of all potential signatures by $\mathcal{P}_G$.
2. When an $(h; [n_1, t_1], \dots, [n_r, t_r])$-generating word for G exists, we call the signature an *actual signature* for G. We denote the space of all actual signatures by $\mathcal{A}_G$.
3. If $(h; [n_1, t_1], \dots, [n_r, t_r]) \in \mathcal{P}_G$, but $(h; [n_1, t_1], \dots, [n_r, t_r]) \notin \mathcal{A}_G$, we say it is a *non-signature* for G.

Clearly we have $\mathcal{A}_G \subseteq \mathcal{P}_G$. Our goal is to provide necessary and sufficient conditions for when the set of non-signatures, $\mathcal{P}_G - \mathcal{A}_G$, is finite. We start by describing explicitly the set $\mathcal{P}_G$.

Theorem 3.1. A tuple $(h; [n_1, t_1], \dots, [n_r, t_r])$ is in $\mathcal{P}_G$ for $n_i \in \mathrm{Ord}(G)$ if and only it is not one of the tuples in Table 1.

Proof. Simple application of the Riemann-Hurwitz formula shows that these are the only signatures which don't satisfy the arithmetic conditions given in Theorem 2.1 to be the signature of G acting on a surface of some genus $\sigma \geq 2$. □

Remark 3.1. We use standard notation in Table 1 with C_n denoting a cyclic group of order n, D_n a dihedral group of order $2n$, A_n the alternating group of degree n, S_n the symmetric group of degree n, and $G : H$ a semi-direct product of G and H.

As indicated in Table 1, many of the excluded tuples do occur as signatures of a group action, just in genus 0 or 1. For more details; see [21] for genus 1 and [23] for genus 0. The only exceptions are cases 2, 4 and 14. For the first two of these cases, the Riemann-Hurwitz formula produces a negative value for σ, and for the third, a non-integer value. However, in all three cases, it is impossible to construct a generating word for any group with such a signature since it would not satisfy condition (2c) of Theorem 2.1. For the first two cases, this is clear. For the signature $(h; [n_1, t_1], \dots, [n_r, t_r])$, since $|G| = 2^k m$ for m odd, any Sylow 2-subgroup will be cyclic which in turn implies that G has a unique normal subgroup H of order m. It follows that the quotient group G/H is cyclic of order 2^k, and any generating word for G reduces to a word of elements in G/H which satisfies condition (2c) of Theorem 2.1. By Harvey's Theorem, [14], this can only happen if the tuple contains an even number of elements whose order is divisible by the largest power of 2 dividing $|G|$.

4. Necessary and Sufficient Conditions for a Group to Act with Almost all Signatures

We are now ready to consider the problem of determining conditions for when a finite group is AAS. Before we prove the main result, we start with some initial observations about AAS groups.

Case	Tuple	Genus of S	G
1	$(0; -)$	0	Trivial (order 1)
2	$(0; [n_i, 1])$, $n_i \in \mathrm{Ord}(G)$	no actions	
3	$(0; [n_i, 2])$, $n_i \in \mathrm{Ord}(G)$	0	C_{n_i} (order n_i)
4	$(0; [n_i, 1], [n_j, 1])$, $n_i, n_j \in \mathrm{Ord}(G)$, $i \neq j$	no actions	
5	$(0; [2, 2], [n_i, 1])$, $n_i \in \mathrm{Ord} G$	0	D_{n_i} (order $2n_i$)
6	$(0; [2, 1], [3, 2])$	0	A_4
7	$(0; [2, 1], [3, 1], [4, 1])$	0	S_4
8	$(0; [2, 1], [3, 1], [5, 1])$	0	A_5
9	$(0; [2, 1], [3, 1], [6, 1])$	1	$(C_u \times C_v) : C_6$ $u, v \in \mathbb{Z}^+$ (order $6uv$)
10	$(0; [2, 1], [4, 2])$	1	$(C_u \times C_v) : C_4$, $u, v \in \mathbb{Z}^+$ $u, v \in \mathbb{Z}^+$ (order $4uv$)
11	$(0; [3, 3])$	1	$(C_u \times C_v) : C_3$, $u, v \in \mathbb{Z}^+$ (order $3uv$)
12	$(0; [2, 4])$	1	$(C_u \times C_v) : C_2$, $u, v \in \mathbb{Z}^+$ (order $2uv$)
13	$(1; -)$	1	$(C_u \times C_v)$, $u, v \in \mathbb{Z}^+$ (order uv)
14	$(h; [n_1, t_1], \ldots, [n_r, t_r])$, where the sum of the t_i over the i such that $2^k \mid n_i$ is odd	no actions	does not occur if $\lvert G \rvert = 2^k m$, where m is odd and $k > 0$

TABLE 1. Tuples Excluded from $\mathcal{P}_G$

Lemma 4.1. Suppose the group G is AAS. Then for every $n_i \in \mathrm{Ord}(G)$

(1) the commutator subgroup $[G, G]$ contains an element of order n_i, and
(2) G is generated by elements of order n_i.

Proof. In each case, it suffices to provide an infinite list of non-signatures for any G which doesn't satisfy the given condition.

In case 1, suppose that the commutator subgroup of G does not contain an element of order n_i. By Theorem 3.1, each tuple $(h; n_i)$ with $h \in \mathbb{Z}^+$ is a potential signature for G. However, no such tuple can be an actual signature for G since 2c from Theorem 2.1 cannot possibly hold.

In case 2, suppose that G is not generated by elements of order n_i. By Theorem 3.1, each tuple $(0; \underbrace{n_i, \ldots, n_i}_{t})$ for $t \geq 3$ when $n_i > 3$, $t \geq 4$ when $n_i = 3$ and $t \geq 5$ when $n = 2$ is a potential signature for G. No such tuple can be an actual signature for G since condition (2a) from Theorem 2.1 cannot possibly hold. □

Corollary 4.2. All AAS groups are non-abelian.

Proof. Since abelian groups have trivial commutator subgroups, condition (1) of Lemma 4.1 fails. □

We will see in Corollary 4.5 that the conditions in Lemma 4.1 are also sufficient for a group G to be AAS, but first we need some notation and terminology. For a given finite group G and elements $x_1, \dots, x_t \in X \subseteq G$, we call the product $x_1 \cdots x_t = g$ a *word in X of length t representing g*. Let $\ell(g, X)$ denote the length of the word of shortest length among all words in X representing g and let $M_G(X) = \max\{\ell(g, X) : g \in G\}$.

Lemma 4.3. For G a finite group and X an inverse closed generating set of G, if e_G can be represented as a word in X of odd length, then there exists an integer $\mathrm{MinWord}(G, X)$ so that for any $g \in G$ and any $t \geq \mathrm{MinWord}(G, X)$ there is a word of length t in X representing g.

Proof. Let k be the smallest odd integer such that w_{e_G} is a word in X of length k representing e_G (such a k exists by assumption) and let $\mathrm{MinWord}(G, X) = M_G(X) + k$. We shall show that any $g \in G$ can be represented by a word of length t in X for any $t \geq \mathrm{MinWord}(G, X)$.

Fix some $x \in X$. For a given $g \in G$ we can represent g by a word w_1 in X of length $\ell(g, X)$. When $t - \ell(g, X)$ is even, then $w_2 = (xx^{-1})^{(t-\ell(g,X))/2}$ is a word in X of even length $t - \ell(g, X) > 0$ representing e_G. When $t - \ell(g, X)$ is odd, then $w_2 = w_{e_G}(xx^{-1})^{(t-\ell(g,X)-k)/2}$ is a word in X of odd length $t - \ell(g, X) \geq k$ representing e_G. In both cases, the word $w_1 w_2 = g$ has length t. □

For an inverse closed generating set X of a finite group G, we let $\mathrm{MinGen}(X)$ denote the smallest subset of X that generates G. Before we restrict our attention to AAS groups, we consider the following more general statement about the realizability of signatures as the orbit genus or tail length exceeds certain bounds.

Theorem 4.4. A potential signature $(h; [n_1, t_1], \dots, [n_r, t_r])$ for the group G lies in $\mathcal{A}(G)$ if either of the following conditions hold:

(1) $h \geq \mathrm{MinWord}([G, G], X_{[G,G]}) + \lceil \mathrm{MinGen}(G)/2 \rceil$ and for $n_i \notin \mathrm{Ord}([G, G])$, either t_i is even, or both $t_i \geq 3$ is odd and n_i is odd, or
(2) $t_i \geq \mathrm{MinWord}(G, X_{n_i}) + \max(0, \mathrm{MinGen}(X_{n_i}) - 2h)$ for some $n_i \in \mathrm{GenOrd}(G) \cap \mathrm{Ord}([G, G])$.

Proof. We apply Lemma 4.3 to the sets X_{n_i} and $X_{[G,G]}$ given in the statement of the theorem as generating sets of G and $[G, G]$ respectively, so we first check the condition of the lemma, i.e. that e_G can be represented as a word of odd length.

Clearly $X_{[G,G]}$ generates $[G, G]$. Also, since each element of $X_{[G,G]}$ is of the form $[x_1, x_2]$ for $x_1, x_2 \in G$, for any $x \in G$, the commutator $[x, e_G]$ is a word in $X_{[G,G]}$ of length one representing e_G.

As for the particular n_i in condition (2), by assumption X_{n_i} generates G. To see that e_G can be represented by a word of odd length in X_{n_i} first observe that the words of even length in X_{n_i} are closed under multiplication and hence form a subgroup H of index at most two in G. If $H = G$, then any $x \in X_{n_i}$ can be represented as a word w in X_{n_i} of even length, and hence $wx^{-1} = e_G$ is a word of odd length in X_{n_i} representing e_G. If H has index two, then $[G, G] \subset H$. Since we are assuming $n_i \in \mathrm{GenOrd}(G) \cap \mathrm{Ord}([G, G])$, it follows that there is some $x \in H \cap X_{n_i}$. But then x can be represented by a word w of even length in X_{n_i}, giving a word wx^{-1} in X_{n_i} of odd length representing e_G.

We are now ready to prove the result. We shall show that there exists an $(h; [n_1, t_1], \dots, [n_r, t_r])$-generating word for a group G which satisfies either of the conditions by building subwords corresponding to each term in $(h; [n_1, t_1], \dots, [n_r, t_r])$ and concatenating them.

For condition (1), when $n_i \notin \mathrm{Ord}([G, G])$, let x be any element of order n_i. Then we can represent e_G with the word $w_{n_i} = (xx^{-1})^{t_i/2}$ when t_i is even and $w_{n_i} = (xxx^{-2})(xx^{-1})^{(t_i-3)/2}$ when n_i is odd and $t_i \geq 3$ is odd. Note that x^{-2} is in X_{n_i} since n_i is odd. When $n_i \in \mathrm{Ord}([G, G])$, then for any

$x \in [G,G]$ of order n_i we can build a word $w_{n_i} = x^{t_i}$ of length t_i whose product then lies in $[G,G]$. By construction, the word $w_{n_1} \cdots w_{n_r}$ is in $[G,G]$. Finally, we build a word $w_h = \prod_{i=1}^{h}[a_i,b_i]$ as follows. Let a_i, b_i for $i = 1,\ldots,\lceil \mathrm{MinGen}(G)/2\rceil$ be elements that generate G and let $w_{\mathrm{Min}} = \Pi_{i=1}^{\lceil \mathrm{MinGen}(G)/2\rceil}[a_i,b_i]$. Now, since $h - \lceil \mathrm{MinGen}(G)/2\rceil \geq \mathrm{MinWord}([G,G], X_{[G,G]})$, by Lemma 4.3, we can choose elements a_i, b_i for $i = \lceil \mathrm{MinGen}(G)/2\rceil + 1, \ldots, h$ so $\Pi_{i=\lceil \mathrm{MinGen}(G)/2\rceil+1}^{h}[a_i,b_i]$ is a word of length $h - \lceil \mathrm{MinGen}(G)/2\rceil$ representing $w_{\mathrm{Min}}^{-1}(w_{n_1}\cdots w_{n_r})^{-1}$. Then the word $w_h w_{n_1}\cdots w_{n_r}$ is an $(h;[n_1,t_1],\ldots,[n_r,t_r])$-generating word for G and so it follows that $(h;[n_1,t_1],\ldots,[n_r,t_r]) \in \mathcal{A}(G)$.

For condition (2), without loss of generality, we can assume that $n_r \in \mathrm{GenOrd}(G) \cap \mathrm{Ord}([G,G])$. Let $X \subseteq X_{n_r}$ be a generating set of G of size $\mathrm{MinGen}(X_{n_i})$. First, we build a word $w_h = \prod_{i=1}^{h}[a_i,b_i]$ as follows. If $2h \geq \mathrm{MinGen}(X_{n_i})$, we choose the a_i and b_i from the elements in X, ensuring that all elements of X are listed once, and allowing repeats. If $2h < \mathrm{MinGen}(X_{n_i})$, we choose a_i, b_i for $i = 1,\ldots,h$ to be distinct elements of X. For $i = 1,\ldots,r-1$ we choose words $w_{n_i} = x_{n_i}^{t_i}$ of length t_i where x_{n_i} has order n_i. For $i = r$, we construct the word $w_{n_r} = x_1 \cdots x_{t_r}$ as follows. If $2h > \mathrm{MinGen}(X_{n_i})$, then since $t_r \geq \mathrm{MinWord}(G, X_{n_r})$ by Lemma 4.3, there is a word w_{n_r} in X_{n_r} of length t_r with $w_{n_r} = (w_h w_{n_1} \cdots w_{n_{r-1}})^{-1}$. If $2h < \mathrm{MinGen}(X_{n_i})$, we choose $\{x_1,\ldots,x_{\mathrm{MinGen}(X_{n_i})-2h}\}$ from the remaining elements of X which were not chosen in the construction of w_h. This leaves $t_r - (\mathrm{MinGen}(X_{n_i}) - 2h) \geq \mathrm{MinWord}(G, X_{n_r})$ letters in the word w_{n_r}. It follows that there is a word w in X_{n_r} of length $t_r - (\mathrm{MinGen}(X_{n_i}) - 2h)$ with

$$w = (w_h w_{n_1} \cdots w_{n_{r-1}} x_1 \cdots x_{\mathrm{MinGen}(X_{n_i})-2h})^{-1}$$

by Lemma 4.3, so we let $w_{n_r} = x_1 \cdots x_{\mathrm{MinGen}(X_{n_i})-2h} w$. In both cases, $w_h w_{n_1} \cdots w_{n_r}$ is an $(h;[n_1,t_1],\ldots,[n_r,t_r])$-generating word for G and thus $(h;[n_1,t_1],\ldots,[n_r,t_r]) \in \mathcal{A}(G)$. □

We can now apply this result to determine necessary and sufficient conditions for when a finite group G is AAS.

Corollary 4.5. A finite group G is AAS if and only if for every $n_i \in \mathrm{Ord}(G)$

1. the commutator subgroup $[G,G]$ contains an element of order n_i, and
2. G is generated by elements of order n_i.

Proof. The necessity of the conditions are proved in Lemma 4.1.

In order to prove the sufficiency of the conditions, we apply Theorem 4.4. First observe that the restriction in case 1 of Theorem 4.4 is irrelevant since $\mathrm{Ord}([G,G]) = \mathrm{Ord}(G)$. For case 2 of Theorem 4.4, since any group which is AAS will have $\mathrm{GenOrd}(G) = \mathrm{Ord}(G)$, we only need to check that there is one n_i with a corresponding t_i satisfying the bound in Theorem 4.4 in order to apply the theorem. Then, any signature $(h;m_1,\ldots,m_s) = (h;[n_1,t_1],\ldots,[n_r,t_r])$ where

$$\begin{aligned} h + s \geq{} & \mathrm{MinWord}([G,G], X_{[G,G]}) + \lceil \mathrm{MinGen}(G)/2\rceil \\ & + \sum_{i=1}^{r} (\mathrm{MinWord}(G, X_{n_i}) + \max(0, \mathrm{MinGen}(X_{n_i}) - 2h)) \end{aligned}$$

satisfies either condition (1) or (2) of Theorem 4.4 since either $h \geq \mathrm{MinWord}([G,G], X_{[G,G]}) + \lceil \mathrm{MinGen}(G)/2\rceil$, or $s \geq \sum_{i=1}^{r} (\mathrm{MinWord}(G, X_{n_i}) + \max(0, \mathrm{MinGen}(X_{n_i}) - 2h))$ and so by the Pigeon-Hole principle, one particular t_i must be large enough to apply Theorem 4.4. Thus $\mathcal{P}(G) - \mathcal{A}(G)$ is finite. □

Our main result now follows from Corollary 4.5.

Theorem 4.6. A non-abelian finite simple group is AAS.

Proof. Since G is simple, its commutator subgroup is all of G, hence condition (1) of Corollary 4.5 is satisfied. For condition (2), observe that for a given n_i, if we let H be the subgroup generated by a conjugacy class of elements of order n_i, then H is normal, and hence equal to G. □

5. Families of AAS Groups

Non-abelian simple groups are just one family which satisfy the two conditions given in Corollary 4.5. In this section, we look at AAS groups more generally. We start with the following, which shows that AAS groups fall into two very different categories.

Proposition 5.1. If a group G is AAS, then it is either a non-abelian p-group or a perfect group (a group whose commutator subgroup is the whole group).

Proof. Suppose that G is AAS. Corollary 4.2 ensures that G is not abelian.

Now suppose that G is not a p-group, and let p and q be distinct primes dividing $|G|$. Since G is AAS, by condition (2) of Corollary 4.5, G must be generated by elements of order p. It follows that $G/[G,G]$ must also be generated by elements of order p and so must be elementary abelian of order p^k for some k. By identical reasoning, since G is also generated by elements of order q, we know $G/[G,G]$ is elementary abelian of order q^s for some s. It follows that $G/[G,G]$ must be trivial, and in particular, G is perfect. □

Proposition 5.1 leads to the obvious question of whether it is sufficient for an AAS group to be either perfect or a non-abelian p-group. Unfortunately this is not the case. Though we shall see in the following that it is quite easy to generate families which are AAS, or are not AAS, determining a unified statement about such groups seems to be a very difficult problem. With this in mind, our goal here is to provide evidence, both computationally and through explicit examples of families, to motivate further study toward such a unified statement.

5.1. p-groups.

We now show there are infinite families of finite p-groups that are AAS, and infinite families of finite p-groups that are not AAS.

Proposition 5.2. A non-abelian finite p-group of order p^n and exponent p^{n-1} is never AAS.

Proof. Suppose G is a p-group of order p^n. Since p-groups have a normal subgroup of every possible order, let H be a normal subgroup of G of order p^{n-2}. Then the quotient G/H has order p^2 and hence is abelian, so the commutator subgroup $[G,G]$ is a subgroup of H. Since H has order p^{n-2}, it cannot contain an element of order p^{n-1}, so neither does the commutator subgroup $[G,G]$. Hence G fails condition (1) of Corollary 4.5. □

We can, in fact, exhibit a larger family (containing the family in Proposition 5.2) of non-abelian p-groups which are not AAS.

Corollary 5.3. No metacyclic groups are AAS.

Proof. First, a metacyclic group which is not a p-group is not perfect, so cannot be AAS. Now, suppose that G is an AAS metacyclic p-group of order p^n with normal cyclic subgroup C and cyclic quotient G/C. Now, by assumption, G is generated by elements of order p, so it follows that G/C is also generated by elements of order p. Therefore, G/C is cyclic of order p, and C has index p in G. It follows that C is cyclic of order p^{n-1} and so G has exponent p^n or p^{n-1}. In the first case, G is abelian so cannot be AAS by Corollary 4.2, and in the second case Proposition 5.2 shows G cannot be AAS. □

Proposition 5.2 and Corollary 5.3 illustrate specific examples of p-groups which are not AAS. It is also fairly straightforward to construct explicit examples of AAS p-groups. Since any non-abelian p-group of exponent p must, by definition, be generated by elements of order p, and has a non-trivial commutator containing at least one element of order p, we can conclude that

Proposition 5.4. A non-abelian finite p-group of exponent p is AAS.

Once we find p-groups that are AAS, it is easy to generate more.

Theorem 5.5. Let G be a finite p-group of exponent p^e that is AAS. Let H be any other finite p-group of exponent p^d where $d \leq e$, such that H is generated by elements of order p. Then $G \times H$ is AAS. In particular, the direct product of two AAS p-groups is an AAS p-group.

Proof. First note that the commutator subgroup of $G \times H$ is the direct product of $[G, G]$ and $[H, H]$. In particular, since $[G, G]$ contains elements of all possible orders and $\mathrm{Ord}(H) \subseteq \mathrm{Ord}(G)$, it follows that the commutator subgroup of $G \times H$ must contain elements of all possible orders. Hence condition (1) of Corollary 4.5 is satisfied.

Now suppose that $p^i \in \mathrm{Ord}(G)$. By assumption, G is generated by elements of order p^i, so let $g_1, \ldots, g_k$ be such a set of generators. Also, by assumption, H is generated by elements of order p, so let $h_1, \ldots, h_\ell$ be such a set of generators. Then it follows that the elements (g_i, e_H) and (g_1, h_j) for $1 \leq i \leq k$ and $1 \leq j \leq \ell$, all of which have order p^i, generate $G \times H$. Hence condition (2) of Corollary 4.5 is satisfied. □

The importance of Theorem 5.5 is that once we have found a single AAS p-group of any exponent, we can generate infinitely many other AAS p-groups of that same exponent simply by forming direct products. This suggests that AAS p-groups should appear quite regularly as the order of the group increases. Indeed, for $p \neq 2$, there exists at least one AAS p-group of order p^n for $n \geq 3$ which may be constructed by taking a direct product of the non-abelian p-group of order p^3 (AAS by Proposition 5.4) with an appropriate elementary abelian p-group.

Although the frequency with which AAS p-groups appear should increase as the group order increases, how the number of them increases relative to the growth rate of p-groups is not clear from our current work. The available computational data on p-groups is limited, as the orders of the groups quickly get beyond the capabilities of computer algebra systems, so it is difficult to determine reasonable conjectures from computational data. Therefore, we venture that an interesting line of study would be of the asymptotic limit

$$\lim_{n \to \infty} (\#\text{ AAS } p - \text{groups of order } p^n)/(\#\text{non-abelian } p - \text{groups of order } p^n).$$

In Magma [2], we checked all p groups for $p \in \{2, 3, 5, 7\}$ up to exponent 9 for $p = 2$, and up to exponent 7 for the odd primes, and found only a small handful of AAS examples not covered by Proposition 5.4.

5.2. **Perfect Groups.** As with p-groups, we illustrate specific examples of perfect groups which are AAS, and others which are not AAS. We already know from Theorem 4.6 that non-abelian finite simple groups form a family of perfect groups which are AAS. We now show that not all perfect groups are AAS.

Proposition 5.6. If q is odd, then $SL(2, q)$ is not AAS.

Proof. For each such group, there is a unique subgroup of order 2, hence $SL(2, q)$ cannot be generated by elements of order 2. □

Conversely, it is not necessary for a perfect AAS group to be simple.

Example 1. Using Magma, [2], we can verify that, up to order 2000, there are 10 different perfect AAS groups that are not simple – two of order 960, one of order 1080, four of order 1344, and three of the eight perfect groups of order 1920. We note that one of the AAS perfect groups of order 960 is the group of inner automorphisms of the wreath product of C_2 and A_5.

Moreover, as with p-groups, once we have found a perfect AAS group, it is easy to construct more.

Theorem 5.7. If G, H are AAS groups and $|G|$ and $|H|$ have the same primes in their factorization, then $G \times H$ is AAS.

Proof. Theorem 5.5 shows the result for p-groups, so we only need prove the result assuming that G and H are perfect AAS groups. Assuming G and H are perfect, it follows that $G \times H$ is also perfect and thus we need only check condition (2) of Corollary 4.5.

We need to show that for any $n \in \mathrm{Ord}(G \times H)$, the elements of order n generate $G \times H$. Now if $n \in \mathrm{Ord}(G \times H)$, then $n = \mathrm{lcm}(k, m)$ where k is the order of an element of G and m is the order of an element in H. Let (g, h) be an arbitrary element in $G \times H$. We shall show that (g, h) can be written as a product of elements of order n.

First assume both $k, m > 1$. Since both G and H are AAS, Lemma 4.3 applies to the sets $X_k \subset G$ and $X_m \subset H$, so let $t = \max(\mathrm{MinWord}(G, X_k), \mathrm{MinWord}(H, X_m))$. Then g can be represented as a word $g_1 \cdots g_t$ of length t in X_k and h can be represented as a word $h_1 \cdots h_t$ of length t in X_m. It follows that $(g, h) = \prod_{i=1}^{t}(g_i, h_i)$ where each (g_i, h_i) has order n, hence (g, h) can be written as a product of elements of order n.

Next assume without loss of generality that $m = 1$. It immediately follows that $k = n$. Now if p is any prime dividing k, then by assumption $p||H|$. Since both G and H are AAS, Lemma 4.3 applies to the sets $X_k \subset G$ and $X_p \subset H$. Therefore, we let $t = \max(\mathrm{MinWord}(G, X_k), \mathrm{MinWord}(H, X_p))$. Then g can be represented as a word $g_1 \cdots g_t$ of length t in X_k and h can be represented as a word $h_1 \cdots h_t$ of length t in X_p. It follows that $(g, h) = \prod_{i=1}^{t}(g_i, h_i)$, where each (g_i, h_i) has order n, and so (g, h) can be written as a product of elements of order n. □

As with Theorem 5.5 for p-groups, the importance of Theorem 5.7 is that once we have found a single AAS perfect group, we can generate infinitely many other AAS perfect groups by forming direct products with itself, or with other AAS perfect groups with the same primes in its factorization. In particular, this immediately shows that there are many perfect groups which are not simple but are AAS, as we can take as many direct products of a simple group with itself as we please. As with p-groups, this suggests that AAS groups should appear quite regularly as the order of the group increases. How this number increases relative to the growth rate of perfect groups is not clear from our current work. Therefore, as with p-groups, we venture that an interesting line of study would be a study of the asymptotic growth rate of AAS perfect groups.

Magma [2] contains a database of all perfect groups up to order 50,000. We tested each of these for AAS and found that there are 229 perfect groups up to order 50,000, of which 26 are simple, and 86 are non-simple and AAS, and 117 are not AAS.

References

1. G. Bartolini, M. Izquierdo, 'On the connectedness of the branch locus of the moduli space of Riemann surfaces of low genus', *Proc. Amer. Math. Soc. 140* (2012), no. 1, 35–45.

2. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) 235–265. `http://magma.maths.usyd.edu.au`
3. T. Brendle, B. Farb, 'Every mapping class group is generated by 6 involutions', *Journal of Algebra* Vol. 278 (2004), 187–198.
4. T. Breuer, 'Characters and automorphism groups of compact Riemann surfaces'. Cambridge University Press (2001).
5. S. A. Broughton, 'Classifying finite group actions on surfaces of low genus', *J. Pure Appl. Algebra* **69** (1990), 233–270.
6. S. A. Broughton, 'The equisymmetric stratification of the moduli space and the Krull dimension of the mapping class group', *Topology Appl.* 37 (1990), 101-113.
7. S. A. Broughton, A. Wootton, 'Finite abelian subgroups of the mapping class group', *Algebr. Geom. Topol.* 7 (2007), 1651–1697.
8. E. Bujalance, F. J. Cirre, M. D. E. Conder, 'On automorphism groups of Riemann double covers of Klein surfaces', *J. Algebra* 472 (2017), 146–171.
9. M. Conder, 'An update on Hurwitz groups', *Groups Complex. Cryptol.* 2 (2010), no. 1, 35–49.
10. P. Frediani, A . Ghigi, M. Penegini, 'Shimura varieties in the Torelli locus via Galois coverings' *Int. Math. Res. Not.* IMRN 2015, no. 20, 10595–10623.
11. M. D. Fried, H. Völklein, 'The inverse Galois problem and rational points on moduli spaces', *Math. Ann.* 290 (1991), no. 4, 771–800.
12. T. Ghaswala, R. Winarski, 'Lifting homeomorphisms and cyclic branched covers of spheres', *Michigan Math. J.* 66 (2017), no. 4, 885–890.
13. G. Gromadzki, A. Weaver, A. Wootton, 'Connectivity and Dimension of the p-locus in moduli space', Riemann and Klein Surfaces, Automorphisms, Symmetries and Moduli Spaces, *Contemp. Math* 629, AMS (2014) 189–202.
14. W. J. Harvey, 'Cyclic groups of automorphisms of a compact Riemann surface', *Quart. J. Math.* 17 (1966) 86–97.
15. A. Hurwitz, 'Uber algebraische Gebilde mit eindeutigen Transformationen in sich', *Math. Ann.* 41 (1892), no. 3, 408–442.
16. R.S. Kulkarni, 'Symmetries of surfaces', *Topology* **26** (2), (1987) 195–203.
17. J. Müller, S. Siddhartha, 'A structured description of the genus spectrum of abelian p-groups', *Glasg. Math. J.* 61 (2019), no. 2, 381–423.
18. G. Nakamura, T. Nakanishi, 'Generation of finite subgroups of the mapping class group of genus 2 surface by Dehn twists', *J. Pure Appl. Algebra* 222 (2018), no. 11, 3585–3594.
19. J. Paulhus, 'Decomposing Jacobians of curves with extra automorphisms', Acta Arith. 132 (2008), no. 3, 231–244.
20. A. M. Rojas, 'Group actions on Jacobian varieties', *Rev. Mat. Iberoam.* 23 (2007), no. 2, 397–420.
21. E. Tyszkowska, A. Weaver, 'Exceptional points in the elliptic-hyperelliptic locus', *J. Pure Appl. Algebra* 212 (2008), no 6, 1415–1426.
22. A. Weaver, 'Genus spectra for split metacyclic groups', *Glasg. Math. J.* 43 (2001), no. 2, 209–218.
23. A. Wootton, 'Non-Normal Belyĭ p-gonal Surfaces.' Lecture Notes Ser. Comput., 13, World Sci. Publ., (2005) 95–108.

Universidad Metropolitana de Ciencias de la Educación
E-mail address: `mariela.carvacho@umce.cl`

Grinnell College
E-mail address: `paulhus@math.grinnell.edu`

Colgate University (emeritus)
E-mail address: `ttucker@colgate.edu`

The University of Portland
E-mail address: `wootton@up.edu`