# On Finite Groups of Symmetries of Surfaces

### Jürgen Müller and Siddhartha Sarkar

Abstract. The genus spectrum of a finite group G is the set of all  $g \ge 2$  such that G acts faithfully and orientation-preserving on a closed compact orientable surface of genus g. This article is an overview of some results relating the genus spectrum of G to its group theoretical properties. In particular, the arithmetical properties of genus spectra are discussed, and explicit results are given on the 2-groups of maximal class, certain sporadic simple groups and a some of the groups PSL(2, q), where q is a small prime power. These results are partially new, and obtained through both theoretical reasoning and application of computational techniques. Mathematics Subject Classification: 20D15, 20D08, 20H10, 30F35

### 1 Introduction

Let  $\Sigma_g$  denote an orientable closed compact surface of genus  $g \geq 0$ . Let G be a finite group acting on  $\Sigma_g$  preserving orientation. It is known that there is a complex structure  $(X, \Sigma_g)$  on the surface  $\Sigma_g$  such that the group action can be realized as a subgroup of  $\operatorname{Aut}(X, \Sigma_g)$ . Given such a surface  $\Sigma_g$ , there possibly are uncountably many such complex structures  $(X, \Sigma_g)$ . However, for a fixed  $g \geq 2$ , there are only finitely many groups of finite order which could possibly act faithfully on such surfaces. Indeed, it is well-known since the time of Hurwitz [16], that for any  $g \geq 2$  and finite subgroup G of  $\operatorname{Aut}(X, \Sigma_g)$  we have  $|G| \leq 84(g-1)$ .

It is however uninteresting to list the finite groups acting on surfaces without the knowledge of the topological action. The following result, also known as Hurwitz's Theorem, essentially translates the topological language into combinatorial group theory. From now on we will consider only faithful actions, unless otherwise stated.

**Theorem 1.1: (Riemann's Existence Theorem)** A finite group G acts on a surface  $\Sigma_g$  of genus  $g \ge 0$  if and only if

(1) there are integers  $h \ge 0$  and  $n_1, \ldots, n_r \ge 2$ , for some  $r \ge 0$ , such that the Riemann-Hurwitz relation

$$2(g-1) = |G| \left( 2(h-1) + \sum_{i=1}^{r} (1 - \frac{1}{n_i}) \right)$$

holds, and

(2) there are elements  $a_1, b_1, \ldots, a_h, b_h, c_1, \ldots, c_r \in G$  such that

$$G = \langle a_1, b_1, \dots, a_h, b_h, c_1, \dots c_r \rangle,$$

fulfilling the long relation

$$\prod_{i=1}^{h} [a_i, b_i] \cdot \prod_{j=1}^{r} c_j = 1$$

and such that

$$|c_j| = n_j, \quad 1 \le j \le r.$$

Applying this to the genera g = 0 and g = 1 leads to the well-known result, indicated in Table 1, on the finite groups which can act on such surfaces, see for example [3, Sect.I.3.4].

genus	finite groups
0	$C_n$ (cyclic), $D_n$ (dihedral), $A_4$ , $S_4$ , $A_5$
1	$(C_m \times C_n) : T$ , where $T = C_2, C_3, C_4$ or $C_6$
	TABLE 1

Thus we will henceforth only consider actions of finite groups on surfaces of genus  $g \ge 2$ . As was said earlier, for any fixed g there are only finitely many groups in question. But changing the point of view, and fixing a finite group, leads to the following notion:

**Definition 1.2:** Let G be a finite group. The set of all integers  $g \ge 2$  which satisfies the conditions in Theorem 1.1 is called the **genus** spectrum of G. We denote it by sp(G).

Let  $\delta = (h; n_1, n_2, \ldots, n_r)$  be a tuple of r+1 integers satisfying the conditions of Theorem 1.1. We see that if  $\delta' = (h; n'_1, n'_2, \ldots, n'_r)$  is another such tuple where  $(n'_1, n'_2, \ldots, n'_r)$  is a permutation of  $(n_1, n_2, \ldots, n_r)$ , then  $\delta'$  also satisfies the conditions of Theorem 1.1. Hence let  $\mathbb{D}_r(G)$ be the quotient of the collection of all tuples  $\delta = (h; n_1, n_2, \ldots, n_r)$ under the action of the symmetric group  $S_r$  on its last r coordinates. We call the set  $\mathbb{D}(G) := \bigcup_{r\geq 0} \mathbb{D}_r(G)$  the **data spectrum of** G, and its elements **data** or **signatures**. Then there is the **genus function**  $\mathbf{g}: \mathbb{D}(G) \longrightarrow \mathbb{N}_0$  defined by

$$\delta = (h; n_1, n_2, \dots, n_r) \mapsto g(\delta) := |G| \left( (h-1) + \frac{1}{2} \sum_{i=1}^r (1 - \frac{1}{n_i}) \right) + 1$$

sending a datum to its genus. Thus the image of  $\mathbf{g}$ , possibly after deleting a subset of  $\{0, 1\}$ , is precisely the genus spectrum of G. The basic arithmetic property of the genus spectrum  $\operatorname{sp}(G)$  is given as follows:

**Theorem 1.2** [17]: Let G be a finite group. Then there exists a natural number  $N_G$  such that:

(1) If  $g \in \operatorname{sp}(G)$  then  $g \equiv 1 \mod N_G$ , and

(2)  $\operatorname{sp}(G)$  is cofinite in the set  $1 + N_G \mathbb{N}$ , that is, up to finitely many exceptions for all g satisfying  $g \equiv 1 \mod N_G$  we have  $g \in \operatorname{sp}(G)$ .  $\Box$ 

The number  $N_G$  for a finite group G is called the **genus increment** for G, and is found easily as is outlined in Section 2.

Let  $\mathcal{F}G$  denote the class of all finite groups, and  $\mathcal{A}$  denote all sets of positive integers which are cofinite subsets of some arithmetic set of the form  $1 + \lambda \mathbb{N}$ , for some  $\lambda \in \mathbb{N}$ . We consider the function **sp** :  $\mathcal{F}G \longrightarrow \mathcal{A}$ , which assigns to every finite group its genus spectrum, that is,  $\mathbf{sp}(G) := \mathbf{sp}(G)$ . We immediately see that the function **sp** is a decreasing function with respect to set-theoretic inclusion on both sides. It is natural to ask the following questions:

#### Question 1: Is sp surjective?

It is difficult to answer this question since it is not at all easy to compute the spectrum of finite groups. However the set  $\mathbb{N} \setminus \{1\}$  is the spectrum of the cyclic groups  $C_2$  and  $C_3$ , of order 2 and 3, respectively. Hence at least the full set  $\mathbb{N} \setminus \{1\}$  is in the image of **sp**.

The function  $\mathbf{sp}$  is clearly not injective, as seen in the previous paragraph. However for a specific subclass  $\mathcal{C}$  of  $\mathcal{F}G$ , we can restrict the function  $\mathbf{sp}$  to  $\mathcal{C}$ , and ask if the restricted function  $\mathbf{sp}|_{\mathcal{C}}$  is injective. For example, if  $\mathcal{C}_p$  is the class of all finite cyclic *p*-groups, with *p* fixed, the restricted function  $\mathbf{sp}|_{\mathcal{C}_p}$  is known to be injective [18]. The following question is still open:

**Question 2:** Let p be a fixed prime, and let  $\mathcal{AB}_p$  be the class of all finite abelian p-groups. Is  $\mathbf{sp}|_{\mathcal{AB}_p}$  injective?

A partial answer is given in [29], where it is shown that  $\mathbf{sp}|_{\mathcal{AB}_{(p,p^2)}}$  is injective, where  $\mathcal{AB}_{(p,p^2)}$  is the class of all finite abelian *p*-groups of exponent up to  $p^2$ .

Coming back to the question of surjectivity of **sp**, to get some idea we need a lot of information regarding the spectra of various types of finite groups. Towards this, we introduce more parameters:

**Definition 1.3** Let G be a finite group with genus increment  $N_G$ . The **minimum genus**  $\mu(G)$  and the **stable upper genus**  $\sigma(G)$  of G are defined as follows:

$$\mu(G) := \min \operatorname{sp}(G)$$
  
$$\sigma(G) := \min\{g \in \operatorname{sp}(G) : g + N_G \mathbb{N}_0 \subseteq \operatorname{sp}(G)\}$$

Moreover, the finite set

$$\mathcal{I}(G) := \{g \ge \mu(G) : g \in 1 + N_G \mathbb{N}\} \setminus \operatorname{sp}(G)$$

is called the **gap sequence** of G. Hence a complete spectrum sp(G) of G is determined by the quadruple  $(N_G, \mu(G), \sigma(G), \mathcal{I}(G))$ .

There is a long series of articles written by various authors describing the minimum genus  $\mu(G)$ , also referred to as the **(strong) symmetric genus**, for various finite groups G. These groups include cyclic groups [14], non-cyclic abelian groups [21], metacyclic groups [22], alternating and symmetric groups [5].

Moreover, the minimum genus is known for all 26 sporadic simple groups [6, 9, 20, 32, 33, 34], as indicated in Table 2. The corresponding actions are all given by some triangular datum of the form  $(0; n_1, n_2, n_3) \equiv (n_1, n_2, n_3)$ , where the adjacent letters represent the numerals of the conjugacy classes the corresponding group generators belong to, following the notation of [4]. For the groups Co<sub>1</sub> and Fi'<sub>24</sub> we have not been able to figure out all pieces of information, the uncertainties are indicated as question marks.

The minimum genus of a finite group corresponding to the datum (0; 2, 3, 7) is of a special importance: From the Hurwitz upper bound we see that a possible genus  $g \ge 2$  for a finite group G would satisfy  $g \ge \frac{|G|}{84} + 1$ . Now, if g corresponds to the datum (0; 2, 3, 7) it follows from the Riemann-Hurwitz relation in Theorem 1.1, that  $g = \frac{|G|}{84} + 1$ , which is the lower bound for g. This gives rise to the question of determining finite groups G which have this property, known as **Hurwitz** 

group	minimum genus	action
M <sub>11</sub>	631	(2A, 4A, 11A)
M <sub>12</sub>	3,169	(2B, 3B, 10A)
J <sub>1</sub>	2,091	(2A, 3A, 7A)
M <sub>22</sub>	34,849	(2A, 5A, 7A)
J <sub>2</sub>	7,201	(2B, 3B, 7A)
M <sub>23</sub>	1,053,361	(2A, 4A, 23A)
HS	1,680,001	(2B, 3A, 11A)
J <sub>3</sub>	1,255,825	(2A, 4A, 5A)
M <sub>24</sub>	10,200,961	(3A, 3B, 4C)
McL	78, 586, 201	(2A, 5A, 8A)
Не	47,980,801	(2B, 3B, 7D)
Ru	1,737,216,001	(2B, 3A, 7A)
Suz	11,208,637,441	(2B, 4D, 5B)
O'N	9,600,323,041	(2A, 3A, 8A)
Co <sub>3</sub>	5,901,984,001	(2B, 3C, 7A)
Co <sub>2</sub>	1,602,478,080,001	(2C, 3A, 11A)
Fi <sub>22</sub>	768, 592, 281, 601	(2C, 3D, 7A)
HN	3,250,368,000,001	(2B, 3B, 7A)
Ly	616, 252, 131, 000, 001	(2A, 3B, 7A)
Th	1,080,308,855,808,001	(2A, 3C, 7A)
Fi <sub>23</sub>	85, 197, 301, 526, 937, 601	(2C, 3D, 8C)
Co <sub>1</sub>	86, 620, 350, 136, 320, 001	(2?, 3D, 8?)
$J_4$	1,033,042,512,453,304,321	(2B, 3A, 7A)
$\operatorname{Fi}_{24}'$	14, 942, 925, 109, 412, 639, 539, 201	(2B, 3E, 7?)
В	86, 557, 947, 525, 550, 545, 649, 532, 928,	(2D, 3B, 8x),
	000,001	$x \in \{K, M, N\}$
M	$9, 619, 25\overline{5}, 057, 077, 534, 236, 743, 570,$	(2B, 3B, 7B)
	297, 163, 223, 297, 687, 552, 000, 000, 001	

TABLE	2
-------	---

**groups**; for more details the reader is suggested to look into the survey articles [7, 8] and the references therein.

The stable upper genus  $\sigma(G)$  is rather harder to compute and only known for very few types of groups: for finite cyclic *p*-groups [18], metacyclic groups [31], as well as *p*-groups of cyclic deficiency  $\leq 2$  and elementary abelian *p*-groups for *p* odd [24]. The answer is also known partially for abelian *p*-groups [29], and cyclic groups of order *pq* for primes  $p \neq q$  [26]. A description of genus spectra of finite *p*-groups of exponent *p* is also given in [28].

Encouraged by the similarities of the genus spectra for p-groups (p odd) of exponent p whose lower central series have the same first two quotients, it was worth investigating the genus spectra for the finite non-abelian p-groups whose lower central series quotients would be relatively simple to study. The corresponding groups are known as p-groups of **maximal class** (or co-class 1, see [19]). It is shown in [28] that if p is an odd prime and  $n \leq p$  then all finite p-groups of maximal class and of order  $p^n$  would have the same genus spectrum. The following question is however open:

**Question 3:** Show that for n large there are only two genus spectra for the finite p-groups of maximal class of order  $p^n$  where p is odd.

The story for 2-groups of maximal class is relatively simpler. There are are only three isomorphism types of finite 2-groups of maximal class. The minimum and the stable upper genus for these groups, and hence the genus spectra, are all different. The proofs of this are outlined in Section 3.

There is rather a different and relatively complicated journey towards description of genus spectra for finite simple groups. The genus spectra of the first twelve sporadic simple groups (out of the total 26 of them) have been calculated using techniques of computational group theory and utilizing the computer algebra system GAP [10]. These result would encourage us to investigate the estimate of the number of solutions of the associated diophantine equations which are not realizable in G, also known as bad solutions. This is discussed in detail in Section 4.

Acknowledgement: The first author would like to thank partial funding credits to Lady Davis (2007-8) and Golda Meir (2008-9) post-doctoral scholarship funding (Hebrew University, Jerusalem), and the hospitality of RWTH Aachen.

## 2 Arithmetic of the spectrum and groups of GK-type

The genus increment  $N_G$  of a finite group G is connected to the 2-groups of GK-type which we will briefly describe now.

**Definition 2.1:** A finite *p*-group *G* of exponent  $p^e$  is said to be of **Gorenstein-Kulkarni type (GK-type)** if the set  $\kappa(G) := \{y \in G : |y| < p^e\}$  of elements of non-maximal order forms a subgroup of *G* of index *p*.

**Theorem 2.2** [17]: Given a finite group G, for every prime p let  $G_p$  denote a Sylow p-subgroup of G. Denote by  $p^{n_p}$  and  $p^{e_p}$  the order and exponent of  $G_p$ , respectively. Then the genus increment  $N_G$  of G is given as follows:

$$N_G := \epsilon \cdot \prod_{p \mid \mid G \mid} p^{n_p - e_p}$$

where

$$\epsilon := \begin{cases} 1 & \text{if } G_2 = \{1\} \text{ or } G_2 \text{ is of GK-type;} \\ 1/2 & \text{if } G_2 \neq \{1\} \text{ is not of GK-type.} \end{cases}$$

Although it is hard to find a finite group G, once a set  $S \in \mathcal{A}$  is given, which satisfies  $\operatorname{sp}(G) = S$ , it is relatively easy to find a group G which satisfies  $N_G = N$ , whenever  $N \in \mathbb{N}$  is given.

**Proposition 2.3:** Let  $N \in \mathbb{N}$ . Then there exists a non-trivial finite group G, such that  $N_G = N$ .

**Proof:** If N = 1, then let G be any non-trivial cyclic group. Next suppose  $N = p^{\alpha}$ , where  $\alpha \ge 1$  and p is a prime. If p is odd, then for  $G := C_{p^{\alpha}} \times C_{p^{\alpha}}$ , where  $C_{p^{\alpha}}$  denotes the cyclic group of order  $p^{\alpha}$ , we get  $N_G = p^{\alpha}$ ; if p = 2, then for  $G := C_{p^{\alpha+1}} \times C_{p^{\alpha+1}}$  we get  $N_G = 1/2 \cdot 2^{\alpha+1} = 2^{\alpha}$ . Finally, if  $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ , where the  $p_i$  are pairwise distinct primes and  $\alpha_i \ge 1$  for all i, let  $G_i$  be the finite abelian group with  $N_{G_i} = p_i^{\alpha_i}$ , as described in the last paragraph. Then define G to be the direct product  $G := \prod_{i=1}^k G_i$  and note that  $N_G = \prod_{i=1}^k N_{G_i}$ .  $\Box$ 

For p odd, the importance of finite p-groups of GK-type arrive from the results of [24], where groups having **maximal exponent property** (MEP) are considered. It follows easily that groups with GK-type have MEP, and hence the stable upper genus for 2-generated groups of GK-type is easily calculated, see [24, Thm.4.7].

**Question 4:** Find a closed formula for the stable upper genus for the finite *p*-groups of GK-type.

Looking at the structure of the finite p-groups of GK-type, it would be interesting to classify them through certain parameters. Towards this, we arrange them into trees as follows, see [23]:

If G is of GK-type, the subgroup  $\kappa(G)$  of index p might again turn out to be a p-group of GK-type. We inductively define  $\kappa^{i+1}(G) := \kappa(\kappa^i(G))$ , with  $\kappa^0(G) = G$ , if  $\kappa^i(G)$  is of GK-type. We call the subgroup  $\kappa^i(G)$  the *i*-th **GK-core** of G. We note that all subgroups  $\kappa^i(G)$  of G, if defined, are characteristic and normal. Conversely, G would be referred to as a **GK-extension** of  $\kappa^i(G)$  of degree  $|G/\kappa^i(G)|$ .

This leads to the levelled directed graphs  $\mathcal{T}(R) = (V_{\mathcal{T}}, E_{\mathcal{T}})$  which are defined as follows: The set  $V_{\mathcal{T}}$  of vertices consists of finite *p*-groups, amongst which there is a unique group R, also called the **root** of  $\mathcal{T}(R)$ , which is not of GK-type, and is designated as the group of level 0. Any other finite *p*-group G occurring is a vertex of level i > 0 if  $\kappa^i(G) = R$ . The set  $E_{\mathcal{T}}$  of directed edges consists of the edges e with initial vertex H and terminal vertex  $\kappa(H)$ , for some *p*-group  $H \in V_{\mathcal{T}}$  of GK-type.

Note that this implies that  $\mathcal{T}(R)$  is a directed tree, that is, a directed connected graph without circuits. Hence  $\mathcal{T}(R)$  is called the **GK-tree** associated with R. The question arises how these trees look like. A partial answer is given by the following statements:

**Theorem 2.4** [23]: Let R be a finite p-group of order  $p^n$  and exponent  $p^e$  which is not of GK-type. Then the tree  $\mathcal{T}(R)$  is infinite if and only if exponent of the center Z(R) of R is  $p^e$ .

**Definition 2.5:** A maximal infinite linear subgraph, that is, a subgraph topologically homeomorphic to the real line  $\mathbb{R}$ , of an infinite graph is called a **stem**.

**Theorem 2.6** [23]: Let R be a finite p-group of order  $p^n$  and exponent  $p^e$  which is not of GK-type, such that  $\mathcal{T}(R)$  is infinite. Then a finite p-group G of GK-type in  $\mathcal{T}(R)$  lies on a stem of  $\mathcal{T}(R)$  if and only if there exists  $t \in Z(G) \setminus \kappa^1(G)$  such that  $G = \langle t, R \rangle$ .

In this case, if G lies on level l > 0 of  $\mathcal{T}(R)$ , then G has order  $p^{n+l}$  and exponent  $p^{e+l}$ , and  $|t| = p^{e+l}$ .

We proceed a little further along these lines:

**Definition 2.7:** A finite *p*-group *G* is called **regular**, if for every  $x, y \in G$  we have  $x^p y^p = (xy)^p c^p$  for some  $c \in [H, H]$ , where  $H = \langle x, y \rangle \leq G$  and [H, H] denotes the derived subgroup of *K*.

Hence in particular abelian p-groups, as well as p-groups of exponent p are regular.

**Proposition 2.8:** Let G be a finite p-group of GK-type which lies on a stem of an infinite GK-tree  $\mathcal{T}(R)$ . Then G is regular if and only if all its GK-cores are regular, which holds if and only if R is regular.

In particular, if R is abelian or of exponent p, then all GK-extensions of R which lie on the stems of  $\mathcal{T}(R)$  are regular.

**Proof:** Since any subgroup of a finite regular *p*-group is regular again, it is enough to show that if *R* is regular and *G* is a GK-extension of *R* such that  $\exp(G) = \exp(Z(G))$ , then *G* is regular.

Now we have  $t \in Z(G)$  such that  $G = \langle t, R \rangle$ , and letting  $x, y \in G$ , we may write  $x = t^{\alpha}a$  and  $y = t^{\beta}b$  for some integers  $\alpha, \beta$  and  $a, b \in R$ . Hence we have  $x^p y^p = t^{p(\alpha+\beta)} a^p b^p$  and  $(xy)^p = t^{p(\alpha+\beta)} (ab)^p$ . Using the regularity of R, we have  $a^p b^p = (ab)^p c^p$  for some  $c \in [H, H]$  where  $H = \langle a, b \rangle$ . But t centralizes R, which means [H, H] = [K, K], where  $K = \langle x, y \rangle$ . Moreover, we get

$$x^p y^p = t^{p(\alpha+\beta)} a^p b^p = t^{p(\alpha+\beta)} (ab)^p c^p = (xy)^p c^p,$$

which implies that G is regular.

If we call these the **regular central groups of GK-type**, denoted by  $\mathcal{RCGK}_p$ , then we see that  $\mathcal{AB}_p \subseteq \mathcal{RCGK}_p$ . Then we can ask:

Question 5: Let p be a fixed prime. Is  $\mathbf{sp}|_{\mathcal{RCGK}_p}$  injective?

#### **3** Genus spectrum of 2-groups of maximal class

In this section we will show that the genus spectra of 2-groups of maximal class are all different. Quite contrary to what one would be expecting in case of p-groups of maximal class where p is odd.

For the terminologies specific to finite p-groups, we need to adopt the following specific notations.

Let p be a fixed odd prime and G be a finite p-group of order  $p^n$  and exponent  $p^e$ . Let  $\delta = (h; n_1, \ldots, n_r) \in \mathbb{D}(G)$ . Since  $n_i$  are powers of pwhich could be repeated, we denote them by  $\delta = (h; m_1, m_2, \ldots, m_e)$ instead of  $(h; p, \ldots, p, p^2, \ldots, p^2, \ldots, p^e, \ldots, p^e)$ , where  $p^i$  is repeated  $m_i$ times in  $\delta$ . A set  $\mathfrak{G} = \mathfrak{G}_{\delta} = H_{\mathfrak{G}} \cup \bigcup_{i=1}^e E_{\mathfrak{G},i}$  of generators corresponding to  $\delta$  would be labelled as follows:

- Hyperbolic generators:  $H_{\mathfrak{G}} = \{a_1, b_1, \dots, a_h, b_h\}.$
- Elliptic generators of order  $p^i$ :  $E_{\mathfrak{G},i} = \{x_{i1}, x_{i2}, \ldots, x_{im_i}\}$   $(1 \le i \le e)$ , where the repeated elements are considered as different in the union  $H_{\mathfrak{G}} \cup \bigcup_{i=1}^{e} E_{\mathfrak{G},i}$ .

The Riemann-Hurwitz equation takes the form:

$$2(g-1) = p^n \left( 2(h-1) + \sum_{i=1}^r m_i (1 - \frac{1}{p^i}) \right),$$

and the long relation looks like:

$$\prod H_{\mathfrak{G}} \cdot \prod_{i=1}^{e} \prod E_{\mathfrak{G},i} = 1,$$

where

$$\prod H_{\mathfrak{G}} := \prod_{i=1}^{h} [a_i, b_i] \text{ and } \prod E_{\mathfrak{G}, j} := \prod_{l=1}^{m_j} x_{jl}.$$

**Data extensions 3.1:** This is a method which will be applied in the main proof. Let  $\delta = (h; m_1, m_2, \ldots, m_e) \in \mathbb{D}(G)$ . Now every element x of order  $2^i$  in G can be expressed as  $x = x_1x_2$ , where  $|x_1| = 2^j < 2^i$  and  $|x_2| = 2^i$ . Replacing x by  $x_1x_2$  in the long relation and moving them to the right place using conjugates, we realize that  $\delta' = (h; m_1, m_2, \ldots, m_{j-1}, m_j + 1, m_{j+1}, \ldots, m_e) \in \mathbb{D}(G)$ . Inductively, this shows that the multiplicities  $m_i$  can be arbitrarily increased within  $\mathbb{D}(G)$ , if  $m_i$  is not the last non-zero term in  $\delta$  among the  $m_k$ 's. On the other hand arbitrarily many hyperbolic pairs of generators can be inserted on top of the existing ones. Hence if  $m_t$  is the last non-zero term,  $\delta' = (h'; m'_1, \ldots, m'_{t-1}, m_t, 0, \ldots, 0) \in \mathbb{D}(G)$  if  $h' \ge h, m'_k \ge m_k$ , where  $1 \le k \le t - 1$ .

To understand the stable upper genus of 2-groups of exponent  $2^e$ , where  $e \ge 5$ , we need to look at the following diophantine equation:

$$M = 2^{e} \cdot h + \sum_{i=1}^{e-1} m_i (2^{e-1} - 2^{e-1-i})$$

Let  $\Omega_e(2)$  denote the set of solutions M of the above equation for which  $h, m_i \geq 0$ . For a fixed e, consider the 2-adic expansion

$$M = a_0 + a_1 2 + \ldots + a_{e-1} 2^{e-1}$$

where  $a_i = 0, 1$  for  $0 \le i \le e - 2$  and  $a_{e-1} \ge 0$ . Let  $S_e(M)$  denote the sum  $a_0 + a_1 + ... + a_{e-1}$ .

**Theorem 3.2** [18]: We have

$$\Omega_e(2) = \{ M \in \mathbb{N} : S_e(M) \ge e - 1 - i, a_i \text{ is the first non zero coefficient} \}.$$

Let  $\delta_e(2)$  denote the smallest positive integer such that all  $M \geq \delta_e(2)$ are realized as a solution of the above diophantine equation, for some  $h, m_i \geq 0$ . It is known from the properties of diophantine equations that such an integer  $\delta_e(2)$  exists.

**Theorem 3.3** [18]: The least stable solution  $\delta_e(2)$  is given by:

$$\delta_e(2) = (e-3)2^{e-1} + 2$$

There are three isomorphism types of 2-groups of maximal class in each order  $2^{e+1}$ ; namely, dihedral, quaternion and semi-dihedral 2-groups, being given in terms of presentations as follows, see [19]:

- (1) Dihedral Group :  $\langle y, x : x^2 = 1 = y^{2^e}, x^{-1}yx = y^{-1} \rangle$
- (2) Quaternion Group :  $\langle y, x : x^2 = y^{2^{e-1}}, x^4 = 1, x^{-1}yx = y^{-1} \rangle$
- (3) Semi-Dihedral Group :  $\langle y, x : x^2 = 1 = y^{2^e}, x^{-1}yx = y^{2^{e-1}-1} \rangle$

**Theorem 3.4:** Let G be a finite 2-group of order  $2^{e+1}$ , where  $e \ge 5$ , and of maximal class. Then the minimum and stable upper genus of G are as given in Table 3.

Туре	Minimum Genus $\mu_0$	Stable Upper Genus $\delta_0$
Dihedral	$2^{e-1}$	$(e-3)2^e+4$
Quaternion	$2^{e-1}$	$(e-3)2^e + 2^{e-1} + 3$
Semi-Dihedral	$2^{e-2}$	$(e-3)2^e + 2^{e-2} + 3$
	TADLD 2	

TABLE 3	3
---------	---

All these three groups of order  $2^{e+1}$  contain a (maximal) cyclic subgroup of index 2. Since none of these are of GK-type, the genus increment  $N_G$ for all of them equals 1. We will only show the details of the remaining calculations for dihedral groups. The calculations for other two groups are similar. The proof for the dihedral group relies on the following lemmas: **Lemma 3.5:** Let G be a dihedral group of order  $2^{e+1}$  with generators x, y satisfying the relations given above. If  $G = \langle xy^a, xy^b \rangle$ , then a - b is odd. If  $G = \langle y^a, xy^b \rangle$ , then a is odd.

**Proof of Lemma 3.5:** The Frattini subgroup is  $\Phi(G) = \langle y^2 \rangle$ , and hence the quotient equals  $G/\Phi(G) = C_2 \times C_2 = \langle \overline{x}, \overline{y} \rangle$ . Now if a - b is even, we have  $\overline{xy^a} = \overline{xy^b}$ , which implies  $G/\Phi(G)$  is cyclic, a contradiction. In the second case if a is even, it again implies  $G/\Phi(G)$  is cyclic, a contradiction.

The elements of order 2 in the dihedral group G which are of the form  $xy^a$ , for  $a \in \mathbb{Z}$ , are often referred to as reflections in geometry. Next we note that:

**Lemma 3.6:** The number of reflections among the elliptic generators  $E_{\mathfrak{G},1}$  (with repetitions allowed) is even.

**Proof of Lemma 3.6:** Assume that  $E_{\mathfrak{G},1}$  contains k reflections, say  $xy^{i_1}, xy^{i_2}, \ldots, xy^{i_k}$ . Since the reflections in G form a union of conjugacy classes, we note that  $\prod E_{\mathfrak{G},1} = xy^{i_1}xy^{i_2}\ldots xy^{i_k}\xi$  for some  $\xi \in \{1, y^{2^{e-1}}\}$ . Since  $xy^axy^b = y^{b-a}$ , for k odd we get  $\prod E_{\mathfrak{G},1} = xy^j$  for some  $j \in \mathbb{Z}$ . Now since  $\prod H_{\mathfrak{G}}, \prod E_{\mathfrak{G},i} \in \langle y \rangle$ , where  $i \geq 2$ , using the long relation we get  $xy^j \in \langle y \rangle$ , a contradiction.

**Lemma 3.7:** If  $\delta = (h; m_1, \ldots, m_e) \in \mathbb{D}(G)$  with  $h \leq 1$  and  $m_{e-1} = m_e = 0$ , then  $E_{\mathfrak{G},1}$  contains at least two reflections.

**Proof of Lemma 3.7:** Assume the contrary, then we have  $E_{\mathfrak{G},i} \subseteq \Phi(G) = \langle y^4 \rangle$  for all *i*. Hence  $H_{\mathfrak{G},i}$  generates *G*, thus h = 1 and this contradicts the long relation using Lemma 3.6.

**Proof of Theorem 3.1** for the dihedral group G of order  $2^{e+1}$ : We will first show that the minimum genus  $\mu(G)$  corresponds to the datum  $\delta_0 = (0; 3, 0, \ldots, 0, 1)$  given by  $\mathbf{g}(\delta_0) = 2^{e-1}$ .

Let  $\delta = (h; m_1, \ldots, m_e) \in \mathbb{D}(G)$  correspond  $\mu$ . If  $h \ge 2$ , then  $\mathbf{g}(\delta) \ge 2^{e+1} + 1$ . Hence h = 0 or 1.

We consider the case h = 1. If  $m_e \neq 0$ , since  $\gamma_2(G) = \langle y^2 \rangle$  we have from the long relation that  $m_e \geq 2$ . Then  $\mathbf{g}(\delta) \geq 2^{e+1}(1 - \frac{1}{2^e}) + 1 > 2^{e-1}$ , hence  $m_e = 0$ . Next, if  $m_{e-1} \geq 1$ , then  $\mathbf{g}(\delta) \geq 2^e(1 - \frac{1}{2^{e-1}}) + 1 > 2^{e-1}$ , hence  $m_{e-1} = 0$ .

By lemma 3.4 we have that  $E_{\mathfrak{G},1}$  contains at least two reflections, that is,  $m_2 \geq 2$ . Hence  $\mathbf{g}(\delta) \geq 2^e + 1 > 2^{e-1}$ . This proves that  $h \neq 1$ .

Now we consider the case h = 0. Since the group cannot be generated without at least one reflection, we have  $m_2 \ge 2$ . If  $m_2 = 2$  and  $m_e \ge 2$ , then  $g(\delta) \ge 2^e$ . But with  $m_2 = 2$  and  $m_e = 1$ , we need some more elliptic generators to make the right side of the Riemann-Hurwitz formula positive, say  $m_i \ge 1$ . Then  $g(\delta) \ge 2^{e+1}(\frac{3}{2} - \frac{1}{2^i} - \frac{1}{2^e}) + 1 > 2^e$ . Hence with  $m_2 = 2$  we have  $m_e = 0$ . But the product of two reflections generating G is  $2^e$ . Hence if  $m_2 \ge 2$  and  $m_e = 0$  we would need at least four reflections in  $E_{\mathfrak{G},1}$ . Hence  $m_2 \ge 4$ . Now with  $m_2 \ge 5$  we have  $g(\delta) \ge 2^{e-1} + 1$ . Hence we consider  $m_2 = 4$ . We would then need more elliptic generators to make the genus > 1, say  $m_i \ge 1$  for some i. Then  $g(\delta) \ge 1 + 2^e - 2^{e-i} \ge 2^{e-1} + 1$ .

This shows that the minimum genus of G is  $\mu(G) = 2^{e-1}$ . We will next show that the stable upper genus  $\sigma(G)$  equals  $(e-3)2^e + 4$ . For this we show, recalling hat  $N_G = 1$ :

(1) If  $g \ge (e-3)2^e + 4$ , then  $g \in \operatorname{sp}(G)$ . (2)  $(e-3)2^e + 3$  is not realized by any datum of G.

**Proof of (1):** For such an integer g, consider  $V_g := g + 2^{e+1} - 1$ . Equivalently we will show that if  $V_g \ge (e-1)2^e + 3$ , then there exists a datum  $\delta = (h; m_1, m_2, \ldots, m_e) \in \mathbb{D}(G)$  such that  $\mathbf{g}(\delta) = g$ .

Case I :  $V_g$  is odd.

This ensures that  $m_e$  is odd. We first consider  $m_e = 1$ , and then any  $\delta' = (h; m_1, m_2, \dots, m_{e-1}, 1)$  is a datum if  $m_1 \ge 2$ , since it is a proper extension of  $(0; 2, 0, \dots, 0, 1)$ , where  $(0; 2, 0, \dots, 0, 1)$  is realized by  $\mathfrak{G} = \{x, xy, y^{-1}\}$  and does not associate to a genus  $\ge 2$ . Now

$$\frac{V_g - 2^e + 1}{2} = 2^e \cdot h + \sum_{i=1}^{e-1} (2^{e-1} - 2^{e-1-i})m_i.$$

From Theorem 3.3 it follows that all odd integers  $V_g$  with  $\frac{V_g - 2^e + 1}{2} \ge (e-3)2^{e-1} + 2 + 2 \cdot (2^{e-1} - 2^{e-2})$  can be realized. This means that all odd integers  $V_g \ge (e-1)2^e + 3$  with  $m_e = 1$  can be realized. For an arbitrary odd  $m_e$ , insert a slot  $uu^{-1}$  in the elliptic part of the long relation, where the order of u is  $2^e$ . Finally, this means that all even integers  $g \ge (e-3)2^e + 4$  are genera.

Case II :  $V_q$  is even.

Here  $m_e$  is even. Consider  $m_e = 0$ , and then any tuple  $\delta' = (h; m_1, m_2, \ldots, m_{e-1}, 0)$  is a datum if  $m_1 \ge 4$ , since it is a proper extension of  $(0; 4, 0, \ldots, 0)$ , where  $(0; 4, 0, \ldots, 0)$  is realized by  $\mathfrak{G} = \{x, xy, x, xy^{-1}\}$  and does not associate to a genus  $\ge 2$ . Now

$$\frac{V_g}{2} = 2^e \cdot h + \sum_{i=1}^{e-1} (2^{e-1} - 2^{e-1-i})m_i.$$

From Theorem 3.3 it follows that all odd integers  $V_g$  with  $\frac{V_g}{2} \ge (e - 3)2^{e-1} + 2 + 4 \cdot (2^{e-1} - 2^{e-2})$  associate a realized data. This mean all even integers  $V_g \ge (e - 1)2^e + 4$  realize a data, and therefore all odd integers  $g \ge (e - 3)2^e + 5$  are genus.

**Proof of (2):** In this part we will examine all possible solutions of the equation:

$$V_g = (e-1) \cdot 2^e + 2 = 2^{e+1} \cdot h + \sum_{i=1}^{e} (2^e - 2^{e-i})m_i$$

**Lemma 3.8:**  $m_e$  is even and  $\geq 4$ .

**Proof of Lemma 3.8:** It is clear that  $m_e$  is even. Now from the above equation we get

(A)  $2^{e} \cdot (2h + m_1 + \ldots + m_e) - M(m_1, \ldots, m_e) = (e - 1)2^{e} + 2$ where  $M(m_1, \ldots, m_e) = 2^{e-1}m_1 + 2^{e-2}m_2 + \ldots + 2m_{e-1} + m_e$ . This implies that  $M(m_1, \ldots, m_e) \equiv -2 \mod 2^e$ .

Sub-case I :  $m_e \equiv 2 \mod 2^2$ . It is possible to define the following equations, with integers  $r_i \geq 0$ :

$$m_{e} = 2 + 2^{2}r_{e}$$

$$m_{e-1} + 2 + 2r_{e} = 2r_{e-1}$$

$$m_{e-2} + r_{e-1} = 2r_{e-2}$$

$$m_{e-3} + r_{e-2} = 2r_{e-3}$$

$$m_{e-4} + r_{e-3} = 2r_{e-4}$$

$$\dots$$

$$m_{2} + r_{3} = 2r_{2}$$

$$m_{1} + r_{2} = 2r_{1}$$

From equation (A) we get

$$2^{e} \cdot 2h = 2^{e}(e - 1 + r_1 - (m_1 + \ldots + m_e)).$$

Since  $h \ge 0$  we have that  $m_1 + \ldots + m_e - r_1 \le e - 1$ , which implies

(B) 
$$r_1 + r_2 + \ldots + r_{e-1} + 2r_e \le e - 1$$

Now suppose  $m_e \ge 6$ , which implies  $r_e \ge 1$ . From the list of relations we get that  $m_{e-1} \ge 2$ , and  $r_i \ge 1$  if  $1 \le i \le e-2$ . This contradicts (B). Hence  $r_e = 0$  and consequently  $m_e = 2$ .

Sub-case II :  $m_e \equiv 0 \mod 2^2$ . It is possible to define the following equations, with integers  $r'_i \geq 0$ :

$$m_{e} = 2^{2}r'_{e}$$

$$m_{e-1} + 1 + 2r'_{e} = 2r'_{e-1}$$

$$m_{e-2} + r'_{e-1} = 2r'_{e-2}$$

$$m_{e-3} + r'_{e-2} = 2r'_{e-3}$$

$$m_{e-4} + r'_{e-3} = 2r'_{e-4}$$

$$\dots$$

$$m_{2} + r'_{3} = 2r'_{2}$$

$$m_{1} + r'_{2} = 2r'_{1}$$

From equation (A) we get

$$2^{e} \cdot 2h = 2^{e}(e - (r'_{1} + r'_{2} + \ldots + r'_{e-1} + 2r'_{e})).$$

Since  $h \ge 0$  we get

(C) 
$$r'_1 + r'_2 + r'_{e-1} + 2r'_e \le e$$

Now if  $m_e \ge 4$  we have  $r'_e \ge 1$ . Also inductively we obtain  $r'_{e-2} \ge 2$ , and  $r'_i \ge 1$  if  $1 \le i \le e-3$ . This contradicts (C). Hence  $m_e = 0$ .

**Lemma 3.9:** If  $m_e = 2$ , then the only solution of (A) is given by

$$h = 0, m_i = 1$$
 for  $1 \le i \le e - 2, m_{e-1} = 0$ .

**Proof of Lemma 3.9:** From the list of equations in Lemma 3.8 (Subcase I) it follows that, if  $m_{e-1} \ge 1$ , then  $r_{e-2} \ge 2$  and for the other ones  $r_i \ge 1$ , which contradicts equation (B). If  $m_{e-1} = 0$ , then  $r_i \ge 1$  for  $1 \le i \le e - 1$ . Hence from (B), the only choice is  $r_i = 1$  for  $1 \le i \le e - 1$ . This gives the result from the list of equations given and A.

**Lemma 3.10:** If  $m_e = 0$ , then  $m_1 \le 3$  and h = 0.

**Proof of Lemma 3.10:** If  $m_e = 0$ , then the similar analysis yields  $r'_i \ge 1$  for  $1 \le i \le e - 1$ , and we get the relation

$$e-1 \le r'_1 + r'_2 + \ldots + r'_{e-1}.$$

$$m_e = 0, m_{e-1} = 1, \dots, m_{j+1} = 1,$$

$$m_j = 3, m_{j-1} = 0, m_{j-2} = 1, \dots, m_1 = 1,$$

with the exceptional solutions

$$m_e = 0, m_{e-1} = 3, m_{e-2} = 0, m_{e-3} = 1, \dots, m_1 = 1$$

and

$$m_e = 0, m_{e-1} = 1, \dots, m_2 = 1, m_1 = 3$$

In all these cases, we have h = 0.

**Back to proof of (2):** If  $m_e = 2$ , then  $m_1 = 1, h = 0$  and hence any set  $\mathfrak{G}$  with this datum can generate at most the subgroup  $\langle y \rangle$ . If  $m_e = 0$ , we have h = 0, and hence we need to generate G by the reflections in  $E_{\mathfrak{G},1}$ , which cannot be more than two, hence by Lemma 3.6 are exactly two. Then  $\prod E_{\mathfrak{G},1}$  is an odd power of y, whereas  $\prod_{i\neq 1} \prod E_{\mathfrak{G},i}$  is an even power of y. This contradicts the long relation.  $\Box$ 

# 4 Computation of genus spectra of finite simple groups

We describe how the genus spectrum of a given finite group G can be determined explicitly using tools from computational group theory. To this end, let  $\Delta(G)$  denote the set of non-trivial **periods** of G, that is,  $\Delta(G) := \{|x| \in \mathbb{N} : 1 \neq x \in G\} = \{n_1, \ldots, n_k\}$ , say, for some  $k \in \mathbb{N}_0$ . Then the **Auxiliary Euler-Characteristic Equation (AEC** equation) is defined by

$$2(g-1) = |G| \left( 2(h-1) + \sum_{n \in \Delta(G)} a_n (1-\frac{1}{n}) \right),$$

where  $g, h \in \mathbb{N}_0$ , and  $a_n \in \mathbb{N}_0$  for all  $n \in \Delta(G)$ . Letting  $N_G$  still being the genus increment associated with G, the associated reduced AEC equation is:

$$\tilde{g} := \frac{(g-1)}{N_G} = \frac{|G|}{N_G} \left( (h-1) + \frac{1}{2} \sum_{n \in \Delta(G)} a_n (1-\frac{1}{n}) \right),$$

where  $\tilde{g}$  is called the **reduced genus** corresponding to the genus g.

16

Let  $D(G) := \bigcup_{\tilde{g} \ge 1} D_{\tilde{g}}(G)$ , where for a reduced genus  $\tilde{g} \ge 1$  the set  $D_{\tilde{g}}(G)$  denotes the set of all solutions  $\delta$  of the reduced AEC equation, written as  $\delta := (h; n_1^{[a_1]}, \ldots, n_k^{[a_k]})$ . If  $\delta$  is realized in the group G as described by Riemann's Existence Theorem we notice that the tuple  $\delta$  just is a datum of G. This leads to the following:

**Definition 4.1:** A solution  $\delta \in D_{\tilde{g}}(G)$  to the reduced AEC equation of G is called **bad** if  $\tilde{g} \geq \tilde{\mu}(G) := \frac{\mu(G)-1}{N_G}$ , where the latter number is called the **minimum reduced genus** of G, and  $\delta \notin \mathbb{D}(G)$ , that is  $\delta$  is not a datum.

Thus letting  $\tilde{\sigma}(G) := \frac{\sigma(G)-1}{N_G}$  be the **stable upper reduced genus** of G, describing the spectrum of G completely is equivalent to determining  $\tilde{\mu}(G)$  and  $\tilde{\sigma}(G)$  as well as D(G) and the bad solutions. Note that the bad solutions necessarily belong to the interval  $\tilde{\mu}(G) \leq \tilde{g} \leq \tilde{\sigma}(G)$ .

Now, to determine  $\tilde{\sigma}(G)$  we need to look at a diophantine problem due to Frobenius popularly known as the "Coin Problem": Given positive integers  $n_1, n_2, \ldots, n_k$  having no non-trivial common divisor, consider the linear equation

$$n = n_1 x_1 + n_2 x_2 + \ldots + n_k x_k,$$

and call a non-negative integer n dependent on  $n_1, n_2, \ldots, n_k$  if there exists a solution  $(x_1, x_2, \ldots, x_k)$  of the above equation in the non-negative integers, and independent from  $n_1, n_2, \ldots, n_k$  otherwise. It is known that there is a bound f such that all n exceeding f are dependent, and the largest independent integer  $f = f(n_1, n_2, \ldots, n_k)$  is called the Frobenius number of  $n_1, n_2, \ldots, n_k$ .

There are no formulae known for  $f(n_1, n_2, \ldots, n_k)$  whenever  $k \ge 4$ ; see [1, 27]. But at least it is known that  $f(n_1, n_2) = (n_1 - 1)(n_2 - 1) - 1$ . Our main interest is in the recurrence formula in case there are common divisors for any (k - 1) of the given numbers, which occurs always for the AEC equations.

**Theorem 4.2** [1]: If d divides  $n_2, n_3, \ldots, n_k$ , then

$$f(n_1, n_2, \dots, n_k) = d \cdot f(n_1, \frac{n_2}{d}, \dots, \frac{n_k}{d}) + n_1(d-1).$$

The existence of a datum  $(0; n_1, n_2, n_3) \in \mathbb{D}_3(G)$  can be explicitly computed by the following character sum formula, where  $\operatorname{Irr}(G)$  denotes the set of irreducible complex characters of G:

**Theorem 4.3**, see [11, Thm.2.12]: Let G be a finite group, and let  $C_1, C_2, \ldots, C_k$  denote the conjugacy classes in G, with representatives  $g_1, g_2, \ldots, g_k$ . Then the number of solutions to the equation xyz = 1 in G with  $x \in C_r$  and  $y \in C_s$  and  $z \in C_t$  is given by

$$c_{C_r,C_s,C_t} = \frac{|C_r|.|C_s|.|C_t|}{|G|} \cdot \sum_{\chi \in \operatorname{Irr}(G)} \frac{\chi(g_r)\chi(g_s)\chi(g_t)}{\chi(1)}.$$

The number  $c_{C_r,C_s,C_t}$  is also referred to as the associated **class multiplication coefficient**.

The data extensions are slightly different from what we have done in the previous section. Let  $(h; n_1, n_2, \ldots, n_r) \in \mathbb{D}_r(G)$  denote a datum of G corresponding to the genus  $g \geq 2$ , allowing repetitions of the periods  $n_i$ , with a possible generating sequence  $\{a_1, b_1, \ldots, a_h, b_h; c_1, \ldots, c_r\}$  as in Riemann's Existence Theorem. Let  $c_j = c'_1 c'_2$  where the  $c'_i$  are nontrivial elements of G of order  $n'_i$ . Then replacing  $c_j$  in the long relation by  $c'_1 c'_2$  we see that  $(h; n_1, n_2, \ldots, n_{j-1}, n'_1, n'_2, n_{j+1}, \ldots, n_r)$  is a datum in  $\mathbb{D}_{r+1}(G)$  corresponding to the genus g', where it is straightforward to check that  $g' \geq g$ .

We now turn to explicit calculations for some finite simple groups. First we consider the infinite family PSL(2, q), where q is a prime power; recall that these groups are simple if and only if  $q \ge 4$ .

**Theorem 4.4**, see [15, Satz.II.8.10]: Let G = PSL(2, q), where  $q = p^f$  is a prime power, and let l be a prime dividing |G|. Then we have:

- (1) If  $2 \neq l \neq p$ , then the Sylow *l*-subgroups of G are cyclic.
- (2) If  $p \neq 2$ , then the Sylow 2-subgroups of G are dihedral.
- (3) The Sylow *p*-subgroups are elementary abelian of order q.

Thus, the genus increment of PSL(2, q), for any odd prime power  $q = p^f$ , equals  $q/p = q^{f-1}$ , while the genus increment of  $PSL(2, 2^f)$  equals  $2^{f-2}$  for  $f \ge 2$ , and that of PSL(2, 2) equals 1. In particular, the genus increment of PSL(2, q), where p is any prime, equals 1.

As for the minimum genus of PSL(2, p), where p is a prime, we have the following results. Recall that  $PSL(2, 4) \cong PSL(2, 5) \cong A_5$  acts on the Riemann sphere, so its genuine minimum genus indeed equals 0, as indicated below, while in our considerations of genus spectra we only look at genera  $g \ge 2$ .

**Theorem 4.5** [13]: For any prime  $p \ge 13$  let

$$d_p := \min\left\{e : e \ge 7, \text{ either } e | \frac{p-1}{2} \text{ or } e | \frac{p+1}{2}\right\}.$$

Then the minimum genus of PSL(2, p), where  $p \ge 5$  is a prime, comes from the following data:

- (1) (0; 2, 3, p) if p = 5, 7, 11,
- (2) (0; 2, 5, 5) if  $p \ge 13$ ,  $p \equiv \pm 1 \mod 5$ ,  $p \not\equiv \pm 1 \mod 8$  and  $d_p \ge 15$ ,
- (3) (0; 3, 3, 4) if  $p \ge 13$ ,  $p \not\equiv \pm 1 \mod 5$ ,  $p \equiv \pm 1 \mod 8$  and  $d_p \ge 12$ ,
- (4) (0; 2, 4, 5) if  $p \ge 13$ ,  $p \equiv \pm 1 \mod 5$ ,  $p \equiv \pm 1 \mod 8$  and  $d_p \ge 9$ ,
- (5)  $(0; 2, 3, d_p)$  in all other cases.

More generally, the minimum genus for PSL(2, q), where q is an arbitrary prime power, has been determined in [12]. Moreover, in [30] there covering groups SL(2, q) have been treated. Thus we ask for the minimum stable genus and the bad solutions. If we restrict ourselves again to the case p a prime, we have the following result:

**Theorem 4.6** [25, Cor.5.10]: Let G = PSL(2, p), where  $p \ge 13$  is a prime. Then for the data spectrum of G we have  $\mathbb{D}(G) = D(G)$ , in particular there are no bad solutions.

Thus, the spectrum of G can be just read off from the solutions of the AEC equation: Letting  $\Delta(G) = \{n_1, \ldots, n_k\}$  be the set of periods of G, then the stable upper genus of G is given as

$$\sigma(G) = 2 + |G| + f(|G|(n_1 - 1)/2n_1, \dots, |G|(n_k - 1)/2n_k),$$

where f denotes the associated Frobenius number.

Actually, it can be checked explicitly that the assertion of Theorem 4.5 also holds for p = 5, 7, 11. Indeed, we take the opportunity to present some details for the case p = 7, in order to indicate the flavor of the computations, and to show how techniques from computational group theory, using the computer algebra system GAP [10] and its character table library [2], come into play:

The group G = PSL(2, 7) has order 168 and periods  $\Delta(G) = \{2, 3, 4, 7\}$ . From Theorem 4.4 we recover the well-known fact that the minimum genus of G equals 3, and corresponds to the datum (0; 2, 3, 7), establishing G as a Hurwitz group. The reduced AEC of G is

$$g - 1 = \tilde{g} = 168(h - 1) + 42a_2 + 56a_3 + 63a_4 + 72a_7$$

The associated Frobenius number being f(168, 42, 56, 63, 72) = 565, we conclude that  $\tilde{g} = 565 - 168 = 397$  is not a reduced genus.

Since GAP [10] shows that for the class multiplication coefficients in G we  $c_{7,7,i} \neq 0$ , for all  $i \in \Delta(G)$ , the extension principle shows that all tuples  $(h; 2^{[a_2]}, 3^{[a_3]}, 4^{[a_4]}, 7^{[a_7]})$  with  $h \geq 0, a_2 \geq 1, a_3 \geq 1, a_4 \geq 0, a_7 \geq 1$  are actually data of G. Thus all  $\tilde{g} > 565 - 168 + (42 + 56 + 72) = 567$  are reduced genera of G. We will prove that all integers  $\tilde{g}$  with  $398 \leq \tilde{g} \leq 567$  are genera of G, and thus in particular are solutions of the reduced AEC, implying that  $\sigma(G) - 1 = \tilde{\sigma}(G) = 398$ . Moreover, we will prove that all solutions of the reduced AEC come from data of G, so that there are no bad solution.

Using GAP [10] we verify that the above assertions follow from the extension principle, as soon as we have shown that the following actually are data: (Indeed, we cannot do with less.)

> (0; 2, 4, 7), (0; 2, 7, 7), (0; 3, 3, 4), (0; 3, 3, 7), (0; 3, 4, 4),(0; 3, 4, 7), (0; 3, 7, 7), (0; 4, 4, 4), (0; 4, 7, 7), (0; 7, 7, 7).

To this end, firstly GAP [10] shows that all the relevant class multiplication coefficients are non-zero. Hence for any case there are triples of elements fulfilling the associated long relation. Next, recall that, by [4], G has precisely our conjugacy classes of maximal subgroups, these consist of groups of shape  $S_4$  (order 24), 7 : 3 (order 21),  $D_8$  (order 8),  $D_6$  (order 6), respectively. In particular, the only maximal subgroup having order divisible by 7 is of shape 7 : 3, which moreover has a normal Sylow 7-subgroup. Hence triples corresponding to (0; 2, 4, 7), (0; 2, 7, 7), (0; 3, 4, 7), (0; 3, 7, 7) and (0; 4, 7, 7) necessarily generate G.

Moreover, from  $c_{7X,7X,7X} = c_{7Y,7X,7X} = c_{7X,7Y,7X} = 24$  and  $c_{7Y,7Y,7X} = 216$ , where  $\{X, Y\} = \{A, B\}$ , we conclude that there are 576 triples associated with (0; 7, 7, 7). If such a triple does not generate G, then it necessarily generates a cyclic group of order 7. But there are precisely eight such subgroups in PSL(2, 7), each of which contains 30 such triples. Hence there are generating triples of this shape. Similarly, there are 1008 triples in G associated with (0; 3, 3, 7), but in any of the eight subgroups isomorphic to 7 : 3 there are precisely 84 such triples; hence there are triples of this shape generating G.

Next we consider (0; 3, 3, 4): Assume a corresponding triple does not generate G, then it necessarily generates a subgroup isomorphic to  $S_4$ , but since elements of order 4 in  $S_4$  are odd permutations while elements of order 3 are even, this is a contradiction. Hence all such triples necessarily generate G. Similarly, a non-generating triple associated with (0; 4, 4, 4) generates a subgroup isomorphic to a subgroup of  $S_4$  or  $D_8$ , but since elements of order 4 in  $S_4$  are odd, and  $D_8$  has a unique cyclic subgroup of order 4, this is a contradiction as well, implying that triples of this shape are necessarily generating.

It remains to look at (0; 3, 4, 4): The relevant class multiplication coefficient equals  $c_{3,4,4} = 672$ . If an associated triple does not generate G, then it necessarily generates a subgroup isomorphic to  $S_4$ . Now the class multiplication coefficient in  $S_4$  equals  $c_{3,4,4} = 42$ , and since there precisely 7 subgroups in PSL(2, 7) isomorphic to  $S_4$ , we conclude that there are generating triples of this shape.  $\Box$ 

Elaborating on the techniques indicated above, and also using GAP [10], we have done a few computations towards an understanding of the minimum stable genus and the bad solutions in the general case. The explicit results are shown in Table 4; recall again the exceptions  $PSL(2,2) \cong S_3$  and  $PSL(2,3) \cong A_4$ , as well as  $PSL(2,4) \cong PSL(2,5) \cong A_5$ , and that we are only considering genera  $g \ge 2$  here.

p	$N_G$	$\mu(G)$	$\sigma(g)$	bad
2	1	2	2	0
4	1	3	63	0
8	2	7	1,453	0
16	4	205	32,153	1
32	8	1,241	517, 617	0
64	16	11,761	1,386,081	12
3	1	3	3	0
9	3	16	505	1
27	9	118	61,696	0
81	27	15,499	5,371,111	6
5	1	3	63	0
25	5	326	52,111	3
125	25	11,626	9,886,176	4
7	1	3	399	0
49	7	2,451	337, 359	7
		TABL	Е 4	

These data imply that a straightforward generalization of Theorem 4.5 cannot possibly hold, leading to the following question:

**Question 6:** Give a closed formula for the stable upper genus of PSL(2,q), and find a combinatorial description of the bad solutions.

Finally, similarly, and still employing GAP [10], we have calculated the stable upper genus and the bad solutions for the first thirteen sporadic simple groups. The result is given in Table 5, together with the respective genus increments and number of bad solutions.

G	$N_G$	$\mu(G)$	$\sigma(g)$	bad
M <sub>11</sub>	3	631	48,511	2
M <sub>12</sub>	36	3,169	510,841	4
J <sub>1</sub>	2	2,091	2,749,249	0
M <sub>22</sub>	24	34,849	3,856,897	1
$J_2$	360	7,201	1,905,841	3
M <sub>23</sub>	24	1,053,361	176,488,081	2
HS	2,400	1,680,001	335,793,601	3
J <sub>3</sub>	216	1,255,825	880, 271, 713	1
M <sub>24</sub>	576	10,200,961	4,063,754,881	0
McL	16,200	78, 586, 201	6,587,730,001	1
He	141,120	47,980,801	36,015,517,441	1
Ru	115,200	1,737,216,001	2,658,295,065,601	0
Suz	622,080	11, 208, 637, 441	5,213,968,496,641	0
		<b>T</b>	-	

TADDE 0
TUDDE O

This leads to the following question:

**Question 7:** Compute the stable upper genus and the number of bad solutions for the remaining sporadic simple groups.

#### References

- A. Brauer, J.E. Shockley, On a problem of Frobenius, J. Reine Angew Math., 211 (1962), 215-220.
- [2] T. Breuer: GAP package CTblLib The GAP Character Table Library, Version 1.1.3, http://www.gap-system.org/Packages/ctbllib.html.
- [3] T. Breuer: Characters and automorphism groups of compact Riemann surfaces, London Math. Soc. Lecture Note Series 280, Cambridge Univ. Press, (2000).
- [4] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R. A. Wilson: An ATLAS of finite groups, Oxford University Press, Oxford (1985).
- [5] M.D.E. Conder: The symmetric genus of alternating and symmetric groups, J. Combin. Theory Ser. B, 39 (1985), 179–186.
- [6] M.D.E. Conder: The symmetric genus of the Mathieu groups, Bull. London Math. Soc. 23 (1991), 445–453.
- [7] M.D.E. Conder, Hurwitz groups: A Brief Survey, Bulletin (New Series) of the American Mathematical Society, 23 no. 2 (1990), 359–370.
- [8] M.D.E. Conder, An update on Hurwitz groups, Groups Complex. Cryptol. 2 (2010), 35–49.
- [9] M.D.E. Conder, R.A. Wilson, A.J. Woldar: The symmetric genus of sporadic groups, *Proceedings of the American Math. Soc.* **116**, no. 3 (1992), 653–663.
- [10] The GAP Group: GAP Groups, Algorithms, Programming a System for Computational Discrete Algebra, Version 4.5.4, (2012), http://www.gapsystem.org.
- [11] D. Gorenstein: Finite Groups, AMS Chelsea Publishing, American Math. Soc., Reprint (2007).
- [12] H. Glover, D. Sjerve: The genus of PSl<sub>2</sub>(q), J. Reine Angew. Math. 380 (1987), 59-86.
- [13] H. Glover, D. Sjerve, Representing PSL<sub>2</sub>(p) on a Riemann surface of least genus, *Enseign Math.*, **31** (1985) 305-325.
- [14] W.J. Harvey: Cyclic groups of automorphisms of a compact Riemann surface, Quart. J. Math. Oxford Ser. (2) 17 (1966), 86–97.
- [15] B. Huppert: Endliche Gruppen I, Grundlehren der mathematischen Wissenschaften 134, Springer, 1983.
- [16] A. Hurwitz: Uber algebraische Gebilde mit eindeutigen Transformationen in sich, Math. Ann. 41, (1893), 403–442.
- [17] R. Kulkarni: Symmetries of surfaces, *Topology* 26, (1987), 195–203.
- [18] R. Kulkarni, C. Maclachlan: Cyclic *p*-groups of symmetries of surfaces, *Glas-gow Math. J.* 33, (1991), 213–221.
- [19] C. Leedham-Green, S. McKay: The structure of groups of prime power order, London Math. Soc. Monographs, New Ser. 27, 2002.
- [20] S.A. Linton, R.J. Wilson, The Maximal Subgroups of the Fischer Groups  $Fi_{24}$  and  $Fi'_{24}$ , Proc. London Math. Soc. (3) 63 (1991), 113–164.
- [21] C. Maclachlan: Abelian groups of automorphisms of compact Riemann surfaces, Proc. London Math. Soc. (3) 15 (1965), 699–712.
- [22] A.A. George Michael: Metacyclic groups of automorphisms of compact Riemann surfaces, *Hiroshima Math. J.* **31** (2001), 117–132.
- [23] J. Müller, S. Sarkar: On p-groups of Gorenstein-Kulkarni Type, preprint (2012), arXiv:1208.3566v1 [math.GR].

- [24] C. Maclachlan, Y. Talu: p-Groups of symmetries of surfaces, Michigan Math. J. 45, (1998), 315–332.
- [25] M. Özaydin, C. Simmons, J. Taback: Surface symmetries and PSL<sub>2</sub>(p), Trans. Amer. Math. Soc. (5) 359 (2007), 2243–2268.
- [26] C. O'Sullivan, A. Weaver: A Diophantine-Frobenius Problem Related to Riemann Surfaces, *Glagow Mathematical Journal*, 53 (2011), 501–522.
- [27] O.J. Rödseth, On a linear Diophantine problem of Frobenius, J. Reine Angew Math., 301 (1978), 171-178.
- [28] S. Sarkar: On the genus spectrum for p-groups of exponent p and p-groups of maximal class, J. Group Theory 12 (2009), 39–54.
- [29] Y. Talu: Abelian p-groups of symmetries of surfaces, Taiwanese J. Math., 15, no. 3 (2011), 1129–1140.
- [30] S. Voon: The genus of  $SL_2(F_q)$ , Michigan Math. J. 40 (1993), no. 3, 527-544.
- [31] A. Weaver, Genus Spectra for Split Metacyclic Groups, Glasgow Mathematical Journal, Vol. 43 (2001), 209–218.
- [32] R.J. Wilson, The Symmetric Genus of the Baby Monster, Quart. J. Math. Oxford (2), 44 (1993), 513–516.
- [33] R. J. Wilson, The Symmetric Genus of the Fischer Group *Fi*<sub>23</sub>, *Topology*, **36**, no. 2 (1997), 379–380.
- [34] R.J. Wilson, The Monster is a Hurwitz Group, J. Group Theory, 4 (2001), 367–374.

J.M.: LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN TEMPLERGRABEN 64, D-52062 AACHEN, GERMANY juergen.mueller@math.rwth-aachen.de

S.S.: MATHEMATICS DEPARTMENT, IISER BHOPAL INDORE BY-PASS ROAD, BHAURI BHOPAL 462030 (M.P.), INDIA sidhu@iiserb.ac.in