An L_2-quotient algorithm for finitely presented groups on arbitrarily many generators

Sebastian Jambor

Abstract

Abstract. We generalize the Plesken-Fabiańska L_2-quotient algorithm for finitely presented groups on two or three generators to allow an arbitrary number of generators. The main difficulty lies in a constructive description of the invariant ring of $\mathrm{GL}(2,K)$ on m copies of $\mathrm{SL}(2,K)$ by simultaneous conjugation. By giving this description, we generalize and simplify some of the known results in invariant theory. An implementation of the algorithm is available in the computer algebra system Magma.

Keywords. Finitely presented groups; quotient algorithm; varieties of representations; invariant theory

2010 Mathematics Subject Classification. 20F05; 13A50

1 Introduction

The Plesken-Fabiańska L_2-quotient algorithm [PF09] takes as input a finitely presented group G on two generators and computes all quotients of G which are isomorphic to $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$. The algorithm finds all possible prime powers q, and also deals with the case when there are infinitely many. This was adapted by Fabiańska [Fab09] to allow finitely presented groups on three generators. In particular, the algorithm can decide whether G has infinitely many quotients isomorphic to $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$, so in some cases it can be used to prove that a finitely presented group is infinite. This has been applied for example in [CHN11]. In this paper, we generalize the algorithm to allow finitely presented groups on an arbitrary number of generators.

The method of Fabiańska and Plesken uses the character of representations $F_2 \to \mathrm{SL}(2,K)$, where F_2 is the free group of rank 2 and K is an arbitrary field. The character is fully determined by the traces of the images of the two generators of F_2 and their product. This observation goes as far back as to Vogt [Vog89] and Fricke and Klein [FK65]. Horowitz [Hor72] gives a rigorous proof of this fact, and generalizes it to representations $F_m \to \mathrm{SL}(2,K)$ for an arbitrary m, by proving that a character is fully determined by 2^m-1 traces. While the traces for $m=2$ are algebraically independent (that is, for every choice of traces for the images of the two generators and their product, there always exists a representation with these traces), this is no longer true for $m>2$. The problem is thus to describe all relations between the traces, or equivalently, to give a presentation for the invariant ring $K[\mathrm{SL}(2,K)^m]^{\mathrm{GL}(2,K)}$, where $\mathrm{GL}(2,K)$ acts on m copies of $\mathrm{SL}(2,K)$ by conjugation. Furthermore, we need this description to be independent of the characteristic of the field K. This problem has a long history. Procesi [Pro76] proves that the invariant ring $K[(K^{n\times n})^m]^{\mathrm{GL}(n,K)}$ is finitely generated if K has characteristic zero, and Donkin [Don92] generalizes this to arbitrary fields K. However, their results are non-constructive. Procesi [Pro84] gives an implicit description of the invariant ring $\mathbb{C}[(\mathbb{C}^{2\times 2})^m]^{\mathrm{GL}(2,\mathbb{C})}$, and Drensky [Dre03] gives an explicit description, however, their results are not valid for fields of characteristic 2. Magnus [Mag80] uses Horowitz's results to to give a description of the quotient ring of the invariant ring.

We will use the approach of Horowitz and Magnus to get a partial description of the invariant ring. The methods are constructive and the arguments are shorter than the original arguments; at the same time we get more precise results, needed for the algorithm. This theory is developed in Section 2.

The author was supported by the Alexander von Humboldt Foundation via a Feodor Lynen Research Fellowship

Sections 3–7 are adaptations of [PF09], where we have to generalize results on characters and traces to work for arbitrarily many generators. Up until the end of Section 7, all results assume that representations restricted to the subgroup generated by the first two generators is absolutely irreducible. The results in Section 8 show how the general case can be reduced to this special case. In Section 9, a new test to recognize epimorphisms onto A_4, S_4, and A_5 is developed, since the test described in [PF09] is inefficient for more than two generators. Section 10 describes the proper notation and theory to deal with an infinite number of L_2-quotients. The algorithm is given in Section 11, with several examples in Section 12.

2 Fricke characters

Througout the paper, K is an arbitrary field and $m \geq 2$ an integer, unless specified otherwise. In this section, we adopt the following notation.

Notation 2.1. Given matrices $A_1, \ldots, A_m \in \mathrm{SL}(2,K)$ and a list $i_1, \ldots, i_k \in \{\pm 1, \ldots, \pm m\}$, we set $t_{i_1,\ldots,i_k} := \mathrm{tr}(A_{i_1} \cdots A_{i_k})$, where $A_{-i} := A_i^{-1}$ for $i \in \{1, \ldots, m\}$. If $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, m\}$ with $i_1 < i_2 < \cdots < i_k$, then $t_I := t_{i_1,\ldots,i_k}$.

Let $A_1, A_2, A_3 \in \mathrm{SL}(2,K)$. The traces satisfy the following basic identities.

$$t_{1,1,2} = t_1 t_{1,2} - t_2, \tag{1}$$
$$t_{-1,2} = t_1 t_2 - t_{1,2}, \tag{2}$$
$$t_{1,2,1,3} = t_{1,2} t_{1,3} + t_{2,3} - t_2 t_3, \tag{3}$$
$$t_{1,3,2} = -t_{1,2,3} + t_1 t_{2,3} + t_2 t_{1,3} + t_3 t_{1,2} - t_1 t_2 t_3. \tag{4}$$

The first two identities are easy consequences of the Cayley-Hamilton Theorem, and the others are easy consequences of the first two (for (3) consider $\mathrm{tr}((A_1A_2)^2(A_2^{-1}A_3))$; for (4) consider $\mathrm{tr}(A_1^{-1}(A_2^{-1}A_3)) = \mathrm{tr}((A_2A_1)^{-1}A_3)$).

We first prove that all traces of words in the A_i are consequences of the t_I with $\emptyset \neq I \subseteq \{1, \ldots, m\}$. This was already observed by Vogt [Vog89] and later by Fricke and Klein [FK65]. The first rigorous proof of this fact was given by Horowitz [Hor72], and a shorter proof by Fabiańska and Plesken [PF09].

Let F_m be the free group of rank m, generated by $g_1, \ldots, g_m$.

Theorem 2.2 ([Hor72, Theorem 3.1], [PF09, Lemma 2.1])**.** *Let $X_m := \{x_I \mid \emptyset \neq I \subseteq \{1, \ldots, m\}\}$ be a set of indeterminates over $\mathbb{Z}$. For every $w \in F_m$ there exists a polynomial $\tau(w) \in \mathbb{Z}[X_m]$, such that for every field K and every m-tuple $A = (A_1, \ldots, A_m) \in \mathrm{SL}(2,K)^m$,*

$$\mathrm{tr}(w(A_1, \ldots, A_m)) = \varepsilon_A(\tau(w)),$$

where $\varepsilon_A \colon \mathbb{Z}[X_m] \to K$ is the evaluation map which sends x_I to t_I.

Since the proof in [Hor72] is lengthy, and the result in [PF09] is not as general, we present a short proof here in its entirety. The basic idea is that of [PF09, Lemma 2.1].

Proof. We assume that w is freely and cyclically reduced and proceed by induction on the length of w. If w is conjugate to $g_i^{-1}w'$ for some $w' \in F_n$ of length $|w| - 1$, set $\tau(w) = \tau(g_iw') - \tau(g_i)\tau(w')$. Thus we may assume that all exponents of w are positive. If w is conjugate to $g_iw'g_iw''$ for some $w', w'' \in F_m$ with $|w'| + |w''| = |w| - 2$, set $\tau(w) = \tau(g_iw')\tau(g_iw'') + \tau(w'w'') - \tau(w')\tau(w'')$. We are left to deal with the case where w is of the form $w = g_{i_1} \cdots g_{i_k}$ where the i_j are pairwise distinct. We may assume $i_1 < i_j$ for all $j \in \{2, \ldots, k\}$. The case $i_1 < \cdots < i_k$ is the induction basis, so there is nothing to do. Otherwise, let j be the smallest index with $i_j > i_{j+1}$. Set $w_1 := g_{i_1} \cdots g_{i_{j-1}}$, $w_2 := g_{i_j}$, and $w_3 := g_{i_{j+1}} \cdots g_{i_k}$, so $w = w_1w_2w_3$. By equation (4) we may set $\tau(w) := -\tau(w_1w_3w_2) + \tau(w_1)\tau(w_2w_3) + \tau(w_2)\tau(w_1w_3) + \tau(w_3)\tau(w_1w_2) - \tau(w_1)\tau(w_2)\tau(w_3)$. Either $w_1w_3w_2$ is of the desired form, or we repeat this process. This terminates after finitely many steps. □

We call $\tau(w)$ the *trace polynomial* of w. If $n > 2$, then $\tau(w)$ is not unique. For example, define the *Fricke polynomial*

$$\begin{aligned}\phi(x_1, x_2, x_3, x_{12}, x_{13}, x_{23}, x_{123}) := x_{123}^2 + (x_1x_2x_3 - x_1x_{23} - x_2x_{13} - x_3x_{12})x_{123} \\ + x_1^2 + x_2^2 + x_3^2 + x_{12}^2 + x_{13}^2 + x_{23}^2 - x_1x_2x_{12} - x_1x_3x_{13} - x_2x_3x_{23} + x_{12}x_{13}x_{23} - 4.\end{aligned}$$

Then $\varepsilon_A(\phi) = 0$ for every choice of A. Proofs appear for example in [Hor72, Section 2] and [Mag80, Lemma 2.2]. We will see below that ϕ is simply a determinant condition (see Proposition 2.4 and Corollary 2.5).

A lot of effort has been put into describing all polynomial relations between the traces. More precisely, let

$$I_m := \{f \in \mathbb{Z}[X_m] \mid \varepsilon_A(f) = 0 \text{ for all } A_1, \dots, A_n \in \mathrm{SL}(2, \mathbb{C})\}$$

and $\Phi_m := \mathbb{Z}[X_m]/I_m$, the *ring of Fricke characters*. It is easy to see that $\varepsilon_A(f) = 0$ for all $A \in \mathrm{SL}(2, K)^m$, so the role of $\mathbb{C}$ is not special. Horowitz [Hor72, Theorem 4.3] proves $I_3 = \langle\phi\rangle$, and Whittemore [Whi73, Theorem 1] proves that I_m is not principal if $m \geq 4$. Magnus [Mag80, Theorem 2.1] shows that Φ_m can be embedded into a finitely generated extension field of $\mathbb{Q}$ of transcendence degree $3m - 3$. Note that $\Phi_m \otimes_{\mathbb{Z}} \mathbb{C}$ is isomorphic to the invariant ring $\mathbb{C}[\mathrm{SL}(2, \mathbb{C})^m]^{\mathrm{GL}(2,\mathbb{C})}$. Procesi [Pro84] gives a description of the invariant ring $\mathbb{C}[(\mathbb{C}^{2\times 2})^m]^{\mathrm{GL}(2,\mathbb{C})}$, and an explicit presentation of the invariant ring with generators and relations is given by Drensky [Dre03, Theorem 2.3]. However, these results are not valid for fields of characteristic 2, and hence cannot be applied to describe Φ_m.

Our first aim is to partially describe Φ_m; we give a presentation of a localisation of Φ_m, which will be enough for our algorithmic applications. By doing that, we will also find new and shorter proofs of some of the results mentioned above.

We will use the following basic result.

Proposition 2.3 ([Mac69, Theorem 2], [Mag80, Equation (2.7)], [BH95, Proposition 4.1], [PF09, Proposition 3.1])**.** *Let $A = (A_1, A_2) \in \mathrm{SL}(2, K)^2$. Then $\langle A_1, A_2\rangle$ is absolutely irreducible if and only if (t_1, t_2, t_{12}) is not a zero of*

$$\rho := x_1^2 + x_2^2 + x_{12}^2 - x_1x_2x_{12} - 4.$$

This is based on the fact that $\langle A_1, A_2\rangle$ is absolutely irreducible if and only if (I_2, A_1, A_2, A_1A_2) is a K-basis of $K^{2\times 2}$ (see for example [PF09]), a result which we will also use several times.

The main result in this section shows that two matrices A_1, A_2 uniquely determine an arbitrary matrix by the specification of four traces; it also shows that the Fricke polynomial is really a determinant condition. The basic idea of the proof has already been used by Brumfiel and Hilden [BH95, Proposition B.4].

Proposition 2.4. *Let $A_1, A_2 \in \mathrm{SL}(2, K)$ such that $\langle A_1, A_2\rangle$ is absolutely irreducible, and let $i \geq 3$. Given T_i, T_{1i}, T_{2i}, $T_{12i} \in K$, there exists a unique $A_i \in K^{2\times 2}$ such that $t_I = T_I$ for all $I \in \{\{i\}, \{1, i\}, \{2, i\}, \{1, 2, i\}\}$. Moreover, $\det(A_i) = 1$ if and only if $\phi(t_1, \dots, t_{12i}) = 0$.*

More precisely, let

$$\begin{aligned}\lambda_0^i &:= (x_1^2 + x_2^2 + x_{12}^2 - x_1x_2x_{12} - 2)x_i - x_1x_{1i} - x_2x_{2i} + (x_1x_2 - x_{12})x_{12i}, \\ \lambda_1^i &:= -x_1x_i - x_2x_{12i} + x_{12}x_{2i} + 2x_{1i}, \\ \lambda_2^i &:= -x_2x_i - x_1x_{12i} + x_{12}x_{1i} + 2x_{2i}, \\ \lambda_{12}^i &:= -x_1x_{2i} - x_2x_{1i} - x_ix_{12} + x_1x_2x_i + 2x_{12i};\end{aligned}$$

set $\Lambda_I := \lambda_I^i(t_1, t_2, T_i, t_{12}, T_{1i}, T_{2i}, T_{12i})$ for $I \in \{\{0\}, \{1\}, \{2\}, \{1, 2\}\}$. Then

$$A_i = \frac{1}{\rho(t_1, t_2, t_{12})}(\Lambda_0 I_2 + \Lambda_1 A_1 + \Lambda_2 A_2 + \Lambda_{12} A_1 A_2).$$

Proof. Since $\langle A_1, A_2\rangle$ is absolutely irreducible, (I_2, A_1, A_2, A_1A_2) is a K-basis of $K^{2\times 2}$. Thus if A_i exists as in the statement, then $A_i = \mu_0 I_2 + \mu_1 A_1 + \mu_2 A_2 + \mu_{12} A_1 A_2$ for some $\mu_i \in K$. Multiplying the equation

from the left by the matrices I_2, A_1, A_2, A_1A_2 and taking traces shows that the μ_i are the unique solution of

$$\begin{pmatrix} 2 & t_1 & t_2 & t_{12} \\ t_1 & t_1^2-2 & t_{12} & t_1t_{12}-t_2 \\ t_2 & t_{12} & t_2^2-2 & t_2t_{12}-t_1 \\ t_{12} & t_1t_{12}-t_2 & t_2t_{12}-t_1 & t_{12}^2-2 \end{pmatrix} \begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \mu_{12} \end{pmatrix} = \begin{pmatrix} T_i \\ T_{1i} \\ T_{2i} \\ T_{12i} \end{pmatrix},$$

which is given by $\mu_i = \Lambda_i/\rho(t_1, t_2, t_{12})$. This proves the uniqueness and existence of A_i. It remains to show the determinant condition. We use the idea of [PF09, Proposition 3.1]. Let α be a root of $X^2 - t_1X + 1$; by enlarging K if necessary, we may assume $\alpha \in K$. Let $v_1 \in K^{2\times 1}$ be an eigenvector of A_1 with eigenvalue α. Set $v_2 := A_2v_1$, and let $M \in \mathrm{GL}(2, K)$ be the matrix with columns v_1 and v_2. Set $B_j := M^{-1}A_jM$ for $j \in \{1, 2, i\}$. Then

$$B_1 = \begin{pmatrix} \alpha & t_2(\alpha - t_1) + t_{12} \\ 0 & t_1 - \alpha \end{pmatrix} \quad \text{and} \quad B_2 = \begin{pmatrix} 0 & -1 \\ 1 & t_2 \end{pmatrix}.$$

Since $B_i = 1/\rho(t_1, t_2, t_{12})(\Lambda_0 I_2 + \Lambda_1 B_1 + \Lambda_2 B_2 + \Lambda_{12} B_1 B_2)$,

$$\det(A_i) = \det(B_i) = \frac{\phi(t_1, \ldots, t_{12i}) + \rho(t_1, t_2, t_{12})}{\rho(t_1, t_2, t_{12})},$$

which concludes the proof. □

Corollary 2.5. *Let $A_1, A_2, A_3 \in \mathrm{SL}(2, K)$. The t_I satisfy the Fricke relation, that is, $\phi(t_1, \ldots, t_{123}) = 0$.*

Proof. We may assume without loss of generality that K is algebraically closed. By Proposition 2.4, the statement is true for the Zariski-open subset

$$U = \{(A_1, A_2, A_3) \in \mathrm{SL}(2, K)^3 \mid \rho(\mathrm{tr}(A_1), \mathrm{tr}(A_2), \mathrm{tr}(A_1A_2)) \neq 0\},$$

so by continuity, it is true for all elements in $\mathrm{SL}(2, K)^3$. □

The following is a generalization of [Mag80, Theorem 2.2] and [PF09, Proposition 3.1]. Set

$$\mathcal{I}_m := \{\{i\} \mid 1 \le i \le m\} \cup \{\{i, j\} \mid 1 \le i \le 2, i < j \le m\} \cup \{\{1, 2, k\} \mid 3 \le k \le m\}.$$

Corollary 2.6. *Let $T_I \in K$ for $I \in \mathcal{I}_m$ such that*

$$\rho(T_1, T_2, T_{12}) \neq 0 \quad \textit{and} \quad \phi(T_1, T_2, T_k, T_{12}, T_{1k}, T_{2k}, T_{12k}) = 0 \textit{ for all } 3 \le k \le m.$$

Let L be the splitting field of $X^2 - T_1X + 1 \in K[X]$. There exists $A = (A_1, \ldots, A_m) \in \mathrm{SL}(2, L)^m$ such that $t_I = T_I$ for all $I \in \mathcal{I}_m$, and A is unique up to conjugation by $\mathrm{GL}(2, L)$.

There exists $A \in \mathrm{SL}(2, K)^m$ such that $t_I = T_I$ for all $I \in \mathcal{I}_m$ if and only if $\rho(T_1, T_2, T_{12}) = \mathrm{N}_{L/K}(z)$ for some $z \in L$. In this case, A is unique up to conjugation by $\mathrm{GL}(2, K)$.

Proof. By [PF09, Proposition 3.1], there exists $A' := (A_1, A_2) \in \mathrm{SL}(2, L)^2$ with $t_1 = T_1$, $t_2 = T_2$, and $t_{12} = T_{12}$; furthermore, A' is unique up to L-equivalence, and A' exists in $\mathrm{SL}(2, K)^2$ if and only if $\rho(T_1, T_2, T_{12})$ is a norm, in which case A' is unique up to K-equivalence. By Proposition 2.4, the choice of A' and the T_I uniquely determines the matrices $A_3, \ldots, A_m$. □

This result implies that the traces t_J with $J \notin \mathcal{I}_m$ can be expressed in the traces t_I with $I \in \mathcal{I}_m$ if $\rho(t_1, t_2, t_{12}) \neq 0$. The next result gives the precise formulae.

Proposition 2.7. *Let $A_1, \ldots, A_n \in \mathrm{SL}(2, K)$. Let $3 \le i < n$ and $\emptyset \neq j \subseteq \{i+1, \ldots, n\}$. The tuple $t = (t_I \mid \emptyset \neq I \subseteq \{1, \ldots, n\})$ is a zero of the polynomials*

$$\begin{aligned}
&x_{ij}\rho - (\lambda_0^i x_j + \lambda_1^i x_{1j} + \lambda_2^i x_{2j} + \lambda_{12}^i x_{12j}),\\
&x_{1ij}\rho - (\lambda_0^i x_{1j} + \lambda_1^i (x_1x_{1j} - x_j) + \lambda_2^i x_{12j} + \lambda_{12}^i (x_1x_{12j} - x_{2j})),\\
&x_{2ij}\rho - (\lambda_0^i x_{2j} + \lambda_1^i (-x_{12j} + x_1x_{2j} + x_2x_{1j} + x_jx_{12} - x_1x_2x_j) + \lambda_2^i (x_2x_{2j} - x_j)\\
&\qquad + \lambda_{12}^i (x_{12}x_{2j} - x_1x_j + x_{1j})),\\
&x_{12ij}\rho - (\lambda_0^i x_{12j} + \lambda_1^i (x_{12}x_{1j} - x_2x_j + x_{2j}) + \lambda_2^i (x_2x_{12j} - x_{1j}) + \lambda_{12}^i (x_{12}x_{12j} - x_j)).
\end{aligned}$$

Proof. It is enough to prove the statement if $\rho \neq 0$ (see proof of Corollary 2.5). By Proposition 2.4, we see $A_i = \Lambda_0 I_2 + \Lambda_1 A_1 + \Lambda_2 A_2 + \Lambda_{12} A_1 A_2$. Multiplying from the right by A_j and from the left by $I_2, A_1, A_2, A_1 A_2$ and taking traces yields the result. □

For a ring R and $r \in R$, let R_r denote the localisation of R at the set $\{1, r, r^2, \dots\}$. While we do not have an explicit description of the ring Φ_m of Fricke characters, we have one for a localisation of Φ_m.

Corollary 2.8. *Let*

$$\Phi'_m := (\mathbb{Z}[x_I \mid I \in \mathcal{I}_m]/\langle \phi_{123}, \dots, \phi_{12m} \rangle)_\rho,$$

where $\phi_{12i} := \phi(x_1, x_2, x_i, x_{12}, x_{1i}, x_{2i}, x_{12i})$ *for* $3 \leq i \leq m$ *and* $\rho := \rho(x_1, x_2, x_{12})$. *The ring homomorphism* $\Phi'_m \to (\Phi_m)_\rho$ *defined by* $x_I \mapsto x_I$ *is an isomorphism.*

Proof. Define a ring homomorphism $\alpha \colon \mathbb{Z}[x_I \mid I \in \mathcal{I}_m] \to (\Phi_m)_\rho$ by mapping x_I to x_I. By Proposition 2.7, α is surjective, and by Proposition 2.4, α factors over Φ'_m. But Proposition 2.4 also shows that the induced map is injective (see also Corollary 2.6). □

Corollary 2.9 ([Mag80, Theorem 2.1])**.** *The quotient field of* Φ_m *is isomorphic to a* $(m-2)$*-fold quadratic extension of a rational function field of trancendence degree* $3m-3$ *over* $\mathbb{Q}$.

3 Trace tuples

The ultimate goal is to get a bijection between prime ideals of Φ'_m and equivalence classes of representations $F_m \to \mathrm{SL}(2, K)$, where K ranges over all fields.

Definition 3.1. A tuple $t = (t_I \mid I \in \mathcal{I}_m) \in K^{\mathcal{I}_m}$ is a *trace tuple* if

$$\rho(t_1, t_2, t_{12}) \neq 0 \quad \text{and} \quad \phi(t_1, t_2, t_i, t_{12}, t_{1i}, t_{2i}, t_{12i}) = 0 \text{ for all } 3 \leq i \leq m.$$

If $A \in \mathrm{SL}(2, K)^m$ such that $\langle A_1, A_2 \rangle$ is absolutely irreducible, then the traces $t_I = \mathrm{tr}(A_{i_1} \cdots A_{i_k})$ for $I = \{i_1 < \cdots < i_k\} \in \mathcal{I}_m$ form a trace tuple. We call this the *trace tuple of* A, and A a *realization of* t. The tuple $(t_J \mid \emptyset \neq J \subseteq \{1, \dots, m\})$ is the *full trace tuple of* A.

Definition 3.2. Let Γ be a group generated by $\gamma_1, \dots, \gamma_m$. Let

$$\mathcal{R}(\Gamma, K) := \{\Delta \colon \Gamma \to \mathrm{SL}(2, K) \mid \Delta_{|\langle \gamma_1, \gamma_2 \rangle} \text{ is absolutely irreducible}\}.$$

Remark 3.3. The set $\mathcal{R}(F_m, K)$ is in bijection to the set of matrices $A \in \mathrm{SL}(2, K)^m$ such that $\langle A_1, A_2 \rangle$ is absolutely irreducible, so we may talk about trace tuples of Δ and regard representations as realizations of trace tuples.

We will first prove the results for finite fields and then generalize to arbitrary fields.

3.1 Finite fields

Definition 3.4. Let $t, t' \in \mathbb{F}_q^{\mathcal{I}_m}$ be trace tuples. Let L and L' be the subfields of $\mathbb{F}_q$ generated by t and t', respectively. We say that t and t' are *equivalent* if there exists an isomorphism $\alpha \colon L \to L'$ such that $\alpha(t_I) = \alpha(t'_I)$ for all $I \in \mathcal{I}_m$.

Remark 3.5. By Corollary 2.6, every trace tuple $t \in \mathbb{F}_q^{\mathcal{I}_m}$ has a realization $A \in \mathrm{SL}(2, \mathbb{F}_q)^m$.

Let $t \in \mathbb{F}_q^{\mathcal{I}_m}$ be a trace tuple. Define a ring homomorphism $\alpha_t \colon \Phi'_m \to \mathbb{F}_q$ by $\alpha_t(x_I) := t_I$ for $I \in \mathcal{I}_m$. Then $P_t := \ker(\alpha_t)$ is a maximal ideal of Φ'_m.

Conversely, let $P \in \mathrm{MaxSpec}(\Phi'_m)$, where $\mathrm{MaxSpec}(\Phi'_m)$ denotes the set of maximal ideals of Φ'_m. Let $\mathbb{F}_q = \Phi'_m/P$, and set $(t_P)_I := x_I + P \in \mathbb{F}_q$ for $I \in \mathcal{I}_m$. Then $t_P := ((t_P)_I \mid I \in \mathcal{I}_m) \in \mathbb{F}_q^{\mathcal{I}_m}$ is a trace tuple.

Theorem 3.6. *The maps* $P \mapsto t_P$ *and* $t \mapsto P_t$ *induce mutually inverse bijections between* $\mathrm{MaxSpec}(\Phi'_m)$ *and the set of equivalence classes of trace tuples over finite fields.*

Proof. Let $P \in \mathrm{MaxSpec}(\Phi'_m)$. Since $\alpha_{t_P}(x_I) = x_I + P$ by definition, we see $P = P_{t_P}$. Now let $t \in \mathbb{F}_q^{\mathcal{I}_m}$ be a trace tuple; we may assume that $\mathbb{F}_q$ is generated by t. Then Φ'_m/P_t is a field with q elements. Define a homomorphism $\mathbb{F}_q \to \Phi'_m/P_t$ by $t_I \mapsto x_I + P_t$. By definition of P_t this is well-defined and it is clearly surjective, hence an isomorphism; it maps t to t_{P_t}, so t is equivalent to t_{P_t}. □

If $q|q'$, then we can embedd $\mathcal{R}(F_m, \mathbb{F}_q)$ into $\mathcal{R}(F_m, \mathbb{F}_{q'})$, and we can embedd $\mathcal{R}(F_m, \mathbb{F}_q)/\Gamma\mathrm{L}(2,q)$ into $\mathcal{R}(F_m, \mathbb{F}_{q'})/\Gamma\mathrm{L}(2,q')$ (where $\Gamma\mathrm{L}(2,q)$ acts on $\mathcal{R}(F_m, \mathbb{F}_q)$ by composition).

Corollary 3.7. *There is a bijection between* $\mathrm{MaxSpec}(\Phi'_m)$ *and* $\bigcup_q \mathcal{R}(F_m, \mathbb{F}_q)/\Gamma L(2,q)$*, where* q *ranges over all prime powers.*

Proof. This follows by Theorem 3.6 and Corollary 2.6. □

3.2 Arbitrary fields

Definition 3.8. Let K and K' be fields. Let $t \in K^{\mathcal{I}_m}$ and $t' \in (K')^{\mathcal{I}_m}$ be trace tuples, and let S and S' be the rings generated by t and t', respectively. We say that t and t' are *equivalent* if there exists a ring isomorphism $\alpha\colon S \to S'$ such that $\alpha(t_I) = t'_I$ for all $I \in \mathcal{I}_m$.

Remark 3.9. By Corollary 2.6, every trace tuple $t \in K^{\mathcal{I}_m}$ has a realization, but in general we must allow field extensions. That is, there exist matrices $A \in \mathrm{SL}(2,L)^m$ with $t_I = \mathrm{tr}(A_{i_1} \cdots A_{i_k})$ for all $I = \{i_1 < \cdots < i_k\} \in \mathcal{I}_m$, where L is either K or a quadratic extension of K.

Let $t \in K^{\mathcal{I}_m}$ be a trace tuple. Define a ring homomorphism $\alpha_t\colon \Phi'_m \to K$ by $\alpha_t(x_I) := t_I$ for $I \in \mathcal{I}_m$. Then $P_t := \ker(\alpha_t)$ is a prime ideal of Φ'_m.

Conversely, let $P \in \mathrm{Spec}(\Phi'_m)$, where $\mathrm{Spec}(\Phi'_m)$ denotes the set of prime ideals of Φ'_m. Let K be the quotient field of Φ'_m/P; set $(t_P)_I := x_I + P \in K$ for $I \in \mathcal{I}_m$. Then $t_P := ((t_P)_I \mid I \in \mathcal{I}_m) \in K^{\mathcal{I}_m}$ is a trace tuple.

Theorem 3.10. *The maps* $P \mapsto t_P$ *and* $t \mapsto P_t$ *induce mutually inverse bijections between* $\mathrm{Spec}(\Phi'_m)$ *and the set of equivalence classes of trace tuples.*

4 Actions

Definition 4.1. Let $\Sigma_m := \{\pm 1\}^m$, the *group of sign changes*. Let $\Delta \in \mathcal{R}(F_m, K)$, and let $\chi\colon F_m \to \mathbb{F}_q\colon w \mapsto \mathrm{tr}(\Delta(w))$ be the character of Δ. Let $t \in K^{\mathcal{I}_m}$ be a trace tuple.

1. Let $\sigma \in \Sigma_m$. Define

$$\begin{aligned} {}^{\sigma}\Delta &\colon F_m \to \mathrm{SL}(2,K)\colon w \mapsto w(\sigma)\Delta(w); \\ {}^{\sigma}\chi &\colon F_m \to K\colon w \mapsto w(\sigma)\chi(w); \text{ and} \\ {}^{\sigma}t_I &:= \Big(\prod_{i\in I} \sigma_i\Big) t_I. \end{aligned}$$

   This defines actions of Σ_m on representations, characters, and trace tuples.

2. Let $\sigma \in \Sigma_m$. Define a ring automorphism on Φ'_m by mapping x_I to $(\prod_{i\in I} \sigma_i) x_I$. This defines an action of Σ_m on Φ'_m by automorphisms, and hence an action on the set of ideals of Φ'_m.

3. Let $\alpha \in \mathrm{Gal}(K)$. Define

$$\begin{aligned} {}^{\alpha}\Delta &\colon F_m \to \mathrm{SL}(2,K)\colon w \mapsto \alpha(\Delta(w)); \\ {}^{\alpha}\chi &\colon F_m \to K\colon w \mapsto \alpha(\chi(w)); \text{ and} \\ {}^{\alpha}t_I &:= \alpha(t_I). \end{aligned}$$

   This defines actions of $\mathrm{Gal}(K)$ on representations, characters, and trace tuples.

Remark 4.2. The actions are compatible with the various bijections. More precisely, let $\Delta \in \mathcal{R}(F_m, K)$, let $t \in K^{\mathcal{I}_m}$ be a trace tuple, and let $P \in \operatorname{Spec}(\Phi'_m)$. Denote by χ_Δ the character of Δ and by t_Δ the trace tuple of Δ. Then

$$\chi_{({}^\sigma\Delta)} = {}^\sigma(\chi_\Delta), \quad t_{({}^\sigma\Delta)} = {}^\sigma(t_\Delta), \quad P_{({}^\sigma t)} = {}^\sigma(P_t), \quad \text{and} \quad t_{({}^\sigma P)} = {}^\sigma(t_P)$$

for all $\sigma \in \Sigma_m$, and

$$\chi_{({}^\alpha\Delta)} = {}^\alpha(\chi_\Delta) \quad \text{and} \quad t_{({}^\alpha\Delta)} = {}^\alpha(t_\Delta)$$

for all $\alpha \in \operatorname{Gal}(K)$.

5 Projective representations and finitely presented groups

Definition 5.1. Let Γ be a group generated by $\gamma_1, \dots, \gamma_m$. Set

$$\mathcal{P}(\Gamma, K) := \{\delta \colon \Gamma \to \operatorname{PSL}(2, K) \mid \delta_{|\langle\gamma_1,\gamma_2\rangle} \text{ is absolutely irreducible}\}.$$

Theorem 5.2. *There is a bijection between* $\operatorname{MaxSpec}(\Phi'_m)/\Sigma_m$ *and* $\bigcup_q \mathcal{P}(F_m, \mathbb{F}_q)/\operatorname{P\Gamma L}(2, q)$*, where* q *ranges over all prime powers.*

Proof. This follows from Corollary 3.7, since two representations $\Delta, \Delta' \colon F_m \to \operatorname{SL}(2, q)$ induce the same projective representation if and only if $\Delta' = {}^\sigma\Delta$ for some $\sigma \in \Sigma_m$. □

Definition 5.3. Let $G = \langle g_1, \dots, g_m \mid w_1, \dots, w_r\rangle$ be a finitely presented group. For $s \in \{\pm 1\}^r$ define

$$\mathrm{I}_s(G) := \langle \tau(w_i b) - s_i \tau(b) \mid 1 \le i \le r,\ b \in \{1, g_1, g_2, g_1 g_2\}\rangle \trianglelefteq \Phi'_m,$$

the *trace presentation ideal of* G with respect to the *sign system* s. (We regard the $\tau(w)$ as elements of Φ'_m via the isomorphism of Corollary 2.8.) Set $\mathrm{I}(G) := \bigcap_{s\in\{\pm1\}^r} \mathrm{I}_s(G)$, the *full trace presentation ideal of* G.

The following result is a reformulation of [PF09, Proposition 3.3].

Proposition 5.4. *Let* G *be a finitely presented group. Let* $\Delta \in \mathcal{R}(F_m, \operatorname{SL}(2, K))$ *with trace tuple* $t \in K^{\mathcal{I}_m}$ *and prime ideal* $P = P_t \in \operatorname{Spec}(\Phi'_m)$*. The following are equivalent:*

1. *The representation* Δ *induces a projective presentation* $\delta \colon G \to \operatorname{PSL}(2, K)$*.*
2. *The trace tuple* t *is a zero of* $\mathrm{I}(G)$*.*
3. *The prime ideal* P *contains* $\mathrm{I}(G)$*.*

Proof. The equivalence of (2) and (3) is immediate. We prove the equivalence of (1) and (2). Let $A_i := \Delta(g_i)$. Then Δ induces a projective representation of G if and only if $w_i(A_1, \dots, A_m) = s_i I_2$ for some $s = (s_1, \dots, s_r) \in \{\pm 1\}^r$. Since the trace bilinear form is non-degenerate, this is equivalent to $\operatorname{tr}(w_i(A_1, \dots, A_m)B) - s_i \operatorname{tr}(B) = 0$, where B runs through a basis of $K^{2\times 2}$. Since $\langle A_1, A_2\rangle$ is absolutely irreducible, we can choose the basis (I_2, A_1, A_2, A_1A_2). □

Corollary 5.5. *There is a bijection between the maximal elements of* $\mathrm{V}(\mathrm{I}(G))/\Sigma_m$*, where* $\mathrm{V}(\mathrm{I}(G)) = \{P \in \operatorname{Spec}(\Phi'_m) \mid \mathrm{I}(G) \subseteq P\}$ *and* $\bigcup_q \mathcal{P}(G, \mathbb{F}_q)/\operatorname{P\Gamma L}(2, q)$*, where* q *ranges over all prime powers.*

6 Subgroups

Corollary 5.5 describes a bijection between classes of maximal ideals and classes of absolutely irreducible projective representations. In this section, we establish criteria to decide whether a maximal ideal is mapped to a *surjective* projective representation.

According to Dickson's classification (see for example [Suz82, Section 3.6]), an absolutely irreducible subgroup $U \lneqq \operatorname{PSL}(2, q)$ is

- isomorphic to A_4, S_4, or A_5, or
- a dihedral group, or
- isomorphic to $\mathrm{PGL}(2,q')$ for some $q'|r$ if $q=r^2$ is a square, or
- isomorphic to $\mathrm{PSL}(2,q')$ for some $q'|q$.

For a finite group H let $J(H) := \bigcap_G \mathrm{I}(G)$, where G ranges over all presentations of G on m generators.

Proposition 6.1. *Let H be a finite group. Set $J'(H) := (J(H) : \left(\bigcap_Q J(Q)\right)^\infty) \trianglelefteq \Phi'_m$, where Q ranges over all proper quotients of H.*

Let $\Delta \in \mathcal{R}(F_m, \mathrm{SL}(2,K))$ with trace tuple $t \in K^{\mathcal{I}_m}$ and prime ideal $P = P_t \in \mathrm{Spec}(\Phi'_m)$. The following are equivalent:

1. *The representation Δ induces a projective presentation δ such that $\mathrm{im}(\delta) \cong H$.*
2. *The trace tuple t is a zero of $J'(H)$.*
3. *The prime ideal P contains $J'(H)$.*

Proof. It suffices to prove the equivalence of (1) and (2). By Proposition 5.4, δ factors over H if and only if t is a zero of $J(H)$, and it factors over Q if and only if t is a zero of $J(Q)$. But t is a zero of $J'(H)$ if and only if it is a zero of $J(H)$ but not a zero of $J(Q)$ for any proper quotient Q of H, which proves the proposition. □

We will later let H be one of the groups A_4, S_4, or A_5, which deals with the first kind of subgroups. We handle the dihedral groups in a slightly more general context.

Lemma 6.2. *Let $t \in K^{\mathcal{I}_m}$ be a trace tuple. Let $\emptyset \neq J \subseteq \{1,\dots,m\}$. If $t_I = 0$ for all $I \in \mathcal{I}_m$ with $|I \cap J|$ odd, then $t_I = 0$ for all $\emptyset \neq I \subseteq \{1,\dots,m\}$ with $|I \cap J|$ odd.*

Proof. Assume $I \notin \mathcal{I}_m$ with $|I \cap J|$ odd. We proceed by induction on $|I|$. We assume that $I \cap \{1,2\} = \emptyset$; the other cases are analogous. Let i be the minimum of I, and let $j := I - \{i\}$. By Proposition 2.7, $t_I = t_{ij} = 1/\rho(t)\big(\lambda_0^i(t)t_j + \lambda_1^i(t)t_{1j} + \lambda_2^i(t)t_{2j} + \lambda_{12}^i(t)t_{12j}\big)$. There are eight cases to consider; we give the proof for two of them, the other six are analogous. The first case is $1,2,i \notin J$; the sets j, $\{1\}\cup j$, $\{2\}\cup j$, and $\{1,2\}\cup j$ have odd intersection with J, thus $t_j = t_{1j} = t_{2j} = t_{12j} = 0$ by induction. The formula for t_{ij} shows that $t_{ij} = 0$. The second case is $1 \in J$ but $2,i \notin J$; now $t_1 = t_2 = t_i = t_{12} = t_{1i} = t_{2i} = t_{12i} = t_j = t_{2j} = t_{12j} = 0$. By Proposition 2.4, $\lambda_1^i(t) = 0$, so $t_{ij} = 0$. □

Let $\Delta \in \mathcal{R}(F_m, K)$; then Δ is *imprimitive* if $K^{2\times 1} = V_1 \oplus V_2$ for one-dimensional subspaces $V_1, V_2 \leq K^{2\times 1}$ such that Δ permutes the V_i transitively.

Proposition 6.3. *Let K be an algebraically closed field. Let $\Delta \in \mathcal{R}(F_m, K)$, and let t be its trace tuple. Then Δ is imprimitive if and only if there exists $\emptyset \neq J \subseteq \{1,\dots,m\}$ such that $t_I = 0$ for all $I \in \mathcal{I}_m$ with $|I \cap J|$ odd.*

Proof. Let $\chi\colon F_m \to \mathbb{F}_q\colon w \mapsto \mathrm{tr}(\Delta(w))$ be the character of Δ. By [Jam14, Theorem 3.3], Δ is imprimitive if and only if there exists an epimorphism $\psi\colon F_m \to \{\pm 1\}$ such that $\psi(w) = -1$ implies $\chi(w) = 0$ for all $w \in F_m$. For $\emptyset \neq J \subseteq \{1,\dots,m\}$ define an epimorphism $\psi_J\colon F_m \to \{\pm 1\}$ by $\psi_J(g_j) = -1$ if $j \in J$ and $\psi_J(g_j) = 1$ otherwise. This yields a bijection between the non-empty subsets of $\{1,\dots,m\}$ and the epimorphisms of F_m onto $\{\pm 1\}$. Let $A_i := \Delta(g_i)$ for $i \in \{1,\dots,m\}$. We show that $\psi_J(w) = -1$ implies $\chi(w)$ for all $w \in F_m$ if and only if $t_I = 0$ for all $I \in \mathcal{I}_m$ with $|I \cap J|$ odd.

The condition is obviously necessary; we show that it is sufficient. By Lemma 6.2 we may assume that $t_I = 0$ for all $\emptyset \neq I \subseteq \{1,\dots,m\}$ with $|I \cap J|$ odd. Let $w \in F_m$ with $\psi_J(w) = -1$. We prove $\chi(w) = 0$ by induction on $|w|$, proceeding along the lines of the proof of Theorem 2.2. Note that $\chi(w) = \varepsilon_A(\tau(w))$, where $A = (\Delta(g_1),\dots,\Delta(g_m))$. If w is conjugate to $g_i^{-1}w'$ for some $i \in \{1,\dots,m\}$ and some $w' \in F_m$ with $|w'| = |w| - 1$, then $\chi(w) = \chi(g_i w') - \chi(g_i)\chi(w')$. By induction, $\chi(w) = \chi(g_i w')$, since either $\psi_J(g_i w')) = -1$ or $\psi_J(g_i) = -1$. Similar considerations apply to the other cases of the proof of Theorem 2.2, so we conclude $\chi(w) = 0$. □

The definition of imprimitivity depends on the field of definition. By abuse of notation we call a representation imprimitive if it is imprimitive after field extension.

Corollary 6.4. *Let*

$$\mathfrak{D} := \bigcap_{\emptyset \neq J \subseteq \{1,\dots,m\}} \langle x_I \mid I \in \mathcal{I}_m \text{ with } |I \cap J| \text{ odd} \rangle \trianglelefteq \Phi'_m.$$

Let $P \in \operatorname{Spec}(\Phi'_m)$, and let $\Delta \in \mathcal{R}(F_m, K)$ be a realization of t_P, where K is the quotient field of Φ'_m/P. Then Δ is imprimitive if and only if $\mathfrak{D} \subseteq P$.

In other words, the imprimitive representations correspond to the elements of the closed subset

$$\mathrm{V}(\mathfrak{D}) = \{P \in \operatorname{Spec}(\Phi'_m) \mid \mathfrak{D} \subseteq P\}$$

of $\operatorname{Spec}(\Phi'_m)$.

The dihedral subgroups of $\mathrm{PSL}(2,q)$ are precisely the images of imprimitive subgroups of $\mathrm{SL}(2,q)$. Setting $\mathfrak{A}_4 := J'(\mathrm{A}_4)$, $\mathfrak{S}_4 := J'(\mathrm{S}_4)$, and $\mathfrak{A}_5 := J'(\mathrm{A}_5)$, we can formulate the main result of this section.

Theorem 6.5. *Let G be a finitely presented group on m generators. The set of normal subgroups $N \trianglelefteq G$ such that $G/N \cong \mathrm{PSL}(2,q)$ for some prime power $q > 5$ or $G/N \cong \mathrm{PGL}(2,q)$ for some prime power $q > 4$ and such that $\langle g_1 N, g_2 N \rangle$ is absolutely irreducible is in bijection to the set of Σ_m-orbits of maximal ideals of*

$$Q(G) := \mathrm{V}(\mathrm{I}(G)) - \mathrm{V}(\mathfrak{D} \cap \mathfrak{A}_4 \cap \mathfrak{S}_4 \cap \mathfrak{A}_5) \subseteq \operatorname{Spec}(\Phi'_m).$$

7 The PSL-PGL-decision

Definition 7.1. A finite group is of L_2-*type* if it is isomorphic to $\mathrm{PSL}(2,q)$ for some $q > 5$ or to $\mathrm{PGL}(2,q)$ for some $q > 4$. A quotient of a finitely presented group is an L_2-*quotient* if it is of L_2-type.

Theorem 6.5 gives a characterization of L_2-quotients purely in algebro-geometric terms. To decide whether an L_2-quotient is isomorphic to $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$ for some q, we use arithmetic tools.

Let $M \in Q(G)$ be a maximal ideal, and let t_M be the trace tuple defined by M. Let $\Delta\colon F_m \to \mathrm{SL}(2,q)$ be a realization of t_M. The field Φ'_m/M is generated by t_M, so Φ'_m/M is the character field of Δ. Since representations over finite fields can be realized over the character field, we may assume $q = |\Phi'_m/M|$. If q is not a square, then by Dickson's classification Δ induces an epimorphism onto $\mathrm{PSL}(2,q)$, and if $q = r^2$, then Δ induces an epimorphism onto $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,r)$. We give a criterion to decide which case occurs. Note that Δ induces a projective representation onto $\mathrm{PGL}(2,r)$ if and only if the image of Δ is conjugate to a subgroup of $\mathrm{GL}(2,r)\mathbb{F}_q^*$, where $\mathbb{F}_q^*$ is identified with scalar matrices.

Proposition 7.2. *Let $q = r^2$ be a prime power. Let $t \in \mathbb{F}_q^{\mathcal{I}_m}$ be a trace tuple and $\Delta\colon F_m \to \mathrm{SL}(2,q)$ a realization of t, and let α be a generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_r)$. The image of Δ is conjugate to a subgroup of $\mathrm{GL}(2,r)\mathbb{F}_q^*$ if and only if ${}^{\sigma}t = {}^{\alpha}t$ for some $\sigma \in \Sigma_m$.*

Proof. Let $\chi\colon F_m \to \mathbb{F}_q\colon w \mapsto \operatorname{tr}(\Delta(w))$ be the character of Δ. By [Jam14, Theorem 4.1], the image of Δ is conjugate to a subgroup of $\mathrm{GL}(2,r)\mathbb{F}_q^*$ if and only if there exists $\sigma \in \Sigma_m$ with ${}^{\sigma}\chi = {}^{\alpha}\chi$. Using Lemma 6.2 and the construction of the $\tau(w)$ in the proof of Theorem 2.2, we can show as in the proof of Proposition 6.3 that this is equivalent to ${}^{\sigma}t_I = {}^{\alpha}t_I$ for all $I \in \mathcal{I}_m$. □

Remark 7.3. Let $M \trianglelefteq \Phi'_m$ be a maximal ideal, and let $\sigma \in \operatorname{Stab}_{\Sigma_m}(M)$. Then $\Phi'_m/M \to \Phi'_m/M\colon x_I + M \mapsto {}^{\sigma}x_I + M$ defines a Galois automorphism.

Corollary 7.4. *Let $M \trianglelefteq \Phi'_m$ be a maximal ideal such that $|\Phi'_m/M| = q = r^2$ is a square. Let $t = t_M$ be the trace tuple of M, and let $\Delta\colon F_m \to \mathrm{SL}(2,q)$ be a realization of t_M. The image of Δ is conjugate to a subgroup of $\mathrm{GL}(2,r)\mathbb{F}_q^*$ if and only if M has a non-trivial stabilizer in Σ_m.*

Together with Theorem 6.5 we get the following result.

Theorem 7.5. *Let G be a finitely presented group on m generators. The set of normal subgroups $N \trianglelefteq G$ such that $G/N \cong \mathrm{PSL}(2,q)$ for some odd $q > 5$ with $\langle g_1N, g_2N\rangle$ absolutely irreducible is in bijection to the regular Σ_m-orbits of maximal ideals of $Q(G)$. The set of normal subgroups $N \trianglelefteq G$ such that $G/N \cong \mathrm{PGL}(2,q)$ for some $q > 4$ with $\langle g_1N, g_2N\rangle$ absolutely irreducible is in bijection to the Σ_m-orbits of maximal ideals of $Q(G)$ with a stabilizer of order 2.*

When dealing with infinitely many L_2-quotients, the following reformulation in terms of trace tuples if often useful.

Corollary 7.6. *Let G be a finitely presented group on m generators, and let $q = p^d$ be a prime power. If $q > 5$ is odd, then the set of normal subgroups $N \trianglelefteq G$ such that $G/N \cong \mathrm{PSL}(2,q)$ with $\langle g_1N, g_2N\rangle$ absolutely irreducible is in bijection to the regular $\Sigma_m \times \mathrm{Gal}(\mathbb{F}_q)$-orbits of zeroes $t \in \mathbb{F}_q^{\mathcal{I}_m}$ of $Q(G)$ with $\mathbb{F}_q = \mathbb{F}_p[t]$. If $q > 4$, then the set of normal subgroups $N \trianglelefteq G$ such that $G/N \cong \mathrm{PGL}(2,q)$ with $\langle g_1N, g_2N\rangle$ absolutely irreducible is in bijection to the $\Sigma_m \times \mathrm{Gal}(\mathbb{F}_{q^2})$-orbits of zeroes $t \in \mathbb{F}_{q^2}^{\mathcal{I}_m}$ of $Q(G)$ with $\mathbb{F}_{q^2} = \mathbb{F}_p[t]$ having stabilizer of order 2.*

Let G/N_1 and G/N_2 be L_2-quotients of G with $N_1 \neq N_2$. What is the isomorphism type of $G/N_1 \cap N_2$? Clearly, if G/N_1 or G/N_2 is simple, then $G/N_1 \cap N_2 \cong G/N_1 \times G/N_2$. This leaves the case that both G/N_i are non-simple, that is, $G/N_i \cong \mathrm{PGL}(2,q_i)$ for some prime powers q_i.

Proposition 7.7. *Let G be a finitely presented group on m generators. Let M_1 and M_2 be maximal ideals of $Q(G)$ with stabilizers $\langle \sigma^{(i)}\rangle \leq \Sigma_m$ of order 2, and let $N_1, N_2 \trianglelefteq G$ be normal subgrops corresponding to M_1, M_2 in the bijection of Theorem 7.5. Let q_1, q_2 be prime powers with $G/N_i \cong \mathrm{PGL}(2,q_i)$. If $N_1 \neq N_2$, then*

$$G/N_1 \cap N_2 \cong \begin{cases} \mathrm{PGL}(2,q_1) \wr^{\mathrm{C}_2} \mathrm{PGL}(2,q_2) & \text{if } \sigma^{(1)} = \sigma^{(2)}, \\ \mathrm{PGL}(2,q_1) \times \mathrm{PGL}(2,q_2) & \text{otherwise.} \end{cases}$$

Proof. Let $\delta_i \colon G \to \mathrm{PSL}(2,q_i^2)$ be a realization of M_i; define $\delta_1 \times \delta_2 \colon G \to \mathrm{PSL}(2,q_1^2) \times \mathrm{PSL}(2,q_2^2) \colon g \mapsto (\delta_1(g), \delta_2(g))$. The image H of $\delta_1 \times \delta_2$ is a subdirect product of $\mathrm{PGL}(2,q_1) \times \mathrm{PGL}(2,q_2)$. Since $N_1 \neq N_2$, this subdirect product is amalgamated either in C_2 or in the trivial group, and in the latter case the product is direct. There is a unique epimorphism $\varepsilon_i \colon \mathrm{PGL}(2,q_i) \to \mathrm{C}_2$, where $\varepsilon_i(\delta(g_j)) = 1$ if and only if $\delta_i(g_j) \in \mathrm{PSL}(2,q_i)$. By the proof of [Jam14, Theorem 4.1], this is equivalent to $\sigma_j^{(i)} = 1$. Hence $\varepsilon_1(\delta_1(g_j)) = \varepsilon_2(\delta_2(g_j))$ if and only if $\sigma^{(1)} = \sigma^{(2)}$, which proves the proposition. □

8 Arbitrary representations

Until now, we only considered representations $\Delta \colon F_m \to \mathrm{SL}(2,K)$ such that $\Delta_{|\langle g_1,g_2\rangle}$ is absolutely irreducible. We now show how the case of arbitrary absolutely irreducible representations can be reduced to this one.

Proposition 8.1. *Let $\Delta \colon F_m \to \mathrm{SL}(2,K)$ be a representation. For $1 \leq i,j,k \leq m$ set $\Delta_{i,j} := \Delta_{|\langle g_i,g_j\rangle}$ and $\Delta_{i,jk} := \Delta_{|\langle g_i,g_jg_k\rangle}$. Then Δ is absolutely irreducible if and only if one of $\Delta_{i,j}$ with $1 \leq i < j \leq m$, $\Delta_{1,2i}$ with $3 \leq i \leq m$, or $\Delta_{2,ij}$ with $3 \leq i < j \leq m$ is absolutely irreducible.*

Proof. We generalize [Fab09, Lemma 3.4.4] and so strenghten [BH95, Proposition B.7]. We may assume that K is algebraically closed, so absolute irreducibility coincides with irreducibility. Clearly if some restriction of Δ is irreducible, then Δ is irreducible. So assume now that all given restrictions are reducible. We show that Δ is reducible. Since $\Delta_{i,j}$ is reducible, $\Delta(g_i)$ and $\Delta(g_j)$ have a common eigenspace. If the minimal polynomial of some $\Delta(g_i)$ is not square-free, then $\Delta(g_i)$ has a unique eigenspace of dimension 1, which has to be a common eigenspace for all $\Delta(g_j)$. Thus Δ is reducible. So assume now that the minimal polynomials of all $\Delta(g_i)$ are square-free. We may further assume that all $\Delta(g_i)$ have two distinct eigenvalues; for if $\Delta(g_i)$ is a scalar matrix, then Δ is reducible if and only if $\Delta_{|\langle g_1,\dots,\widehat{g_i},\dots,g_m\rangle}$ is reducible. Let E_i be the set of eigenspaces of Δ_i and $\mathcal{E} := \{E_i \mid 1 \leq i \leq m\}$. By our hypothesis, $|E_i \cap E_j| \geq 1$ for all i,j. Note that $|E_i| = 2$, so if $|\mathcal{E}| \geq 4$, then the E_i must have a common element, that is, the matrices have a common eigenspace. The same is trivially true if $|\mathcal{E}| \leq 2$. Assume now that $|\mathcal{E}| = 3$. Consider first the case $E_1 \neq E_2$. Let $E_1 = \{\langle v_1\rangle, \langle v_2\rangle\}$ and $E_1 \cap E_2 = \{\langle v_1\rangle\}$. We claim that $\langle v_1\rangle$ is a common

eigenspace for all $\Delta(g_i)$. For suppose that $\langle v_1\rangle$ is not an eigenspace of $\Delta(g_i)$ for some i; then $\langle v_2\rangle$ must be an eigenspace of $\Delta(g_i)$, since $|E_1 \cap E_i| \geq 1$. Since $\Delta_{1,2i}$ is reducible, $\Delta(g_1)$ and $\Delta(g_2 g_i)$ have a common eigenspace. This is either $\langle v_1\rangle$ or $\langle v_2\rangle$. In the first case, $\Delta(g_2 g_i)$ and $\Delta(g_2)$ have eigenspace $\langle v_1\rangle$, so $\Delta(g_i)$ has eigenspace $\langle v_1\rangle$, contradicting our assumption. In the second case, $\Delta(g_2 g_i)$ and $\Delta(g_i)$ have eigenspace $\langle v_2\rangle$, so $\Delta(g_2)$ has eigenspace $\langle v_2\rangle$, again a contradiction. Thus the assumption that $\langle v_1\rangle$ is not an eigenspace of $\Delta(g_i)$ is impossible. We conclude the proof by showing that $E_1 = E_2$ is not possible. Since $|\mathcal{E}| = 3$, there exist $i < j$ with $\mathcal{E} = \{E_1, E_i, E_j\}$. All sets have at least one element in common, so we may assume $E_1 = \{\langle v_1\rangle, \langle v_2\rangle\}$, $E_i = \{\langle v_1\rangle, \langle v_3\rangle\}$, and $E_j = \{\langle v_2\rangle, \langle v_3\rangle\}$. Since $\Delta_{2,ij}$ is reducible, $\Delta(g_2)$ and $\Delta(g_i g_j)$ have a common eigenspace. Assume that this is $\langle v_1\rangle$; then $\langle v_1\rangle$ is also an eigenspace of $\Delta(g_j)$, a contradiction. If it is $\langle v_2\rangle$, then $\langle v_2\rangle$ is also an eigenspace of $\Delta(g_i)$, also a contradiction. Thus $E_1 = E_2$ is impossible. □

Let

$$U_m := \{(\{i\},\{j\}) \mid 1 \leq i < j \leq m\} \cup \{(\{1\},\{2,j\}) \mid 3 \leq j \leq m\} \cup \{(\{2\},\{i,j\}) \mid 3 \leq i < j \leq m\}.$$

For every $u = (u_1, u_2) \in U_m$, let $\alpha_u \in \mathrm{Aut}(F_m)$ with $\alpha_u(g_{u_1}) = g_1$ and $\alpha_u(g_{u_2}) = u_2$, where $g_v := g_{v_1} \cdots g_{v_k}$ for $v = \{v_1 < \cdots < v_k\}$. Thus $\Delta\colon F_m \to \mathrm{SL}(2,K)$ is absolutely irreducible if and only if $(\Delta \circ \alpha_u^{-1})_{|\langle g_1, g_2\rangle}$ is absolutely irreducible for some $u \in U_m$.

By abuse of notation, if $\alpha \in \mathrm{Aut}(F_m)$ and G is a group generated by elements $g_1, \ldots, g_m$, then we denote the automorphism of G defined by $g_i \mapsto \alpha(g_i)$ for $1 \leq i \leq m$ again by α. Fix a total order $<$ on U_m. Set

$$\mathrm{I}_u(G) := \mathrm{I}(\alpha(G)) + \langle \rho(x_{v_1}, x_{v_2}, x_{v_1 \cup v_2}) \mid v \in U_m, v < u\rangle.$$

For a maximal ideal $M \in \mathrm{V}(\mathrm{I}_u(G))$ let t_M be the trace tuple, and let $\Delta_M\colon F_m \to \mathrm{SL}(2,q)$ be a realization of t_M, where $q = |\Phi'_m/M|$. The projective representation induced by $\Delta_M \circ \alpha_u$ factors over G; denote this projective representation by $\delta_{M,u}$, and define $N_M := \ker(\delta_{M,u}) \trianglelefteq G$. Note that N_M is constant on the Σ_m-orbit of M.

Conversely, let $N \trianglelefteq G$ such that G/N is of L_2-type. Let $\delta\colon G \to \mathrm{PSL}(2,q)$ with $\ker(\delta) = N$, and let $\Delta\colon F_m \to \mathrm{SL}(2,q)$ be a lift of δ. Set $t = t_\Delta$ and $M_N := P_t$; then M_N is a maximal L_2-ideal. Note that M_N is only well-defined up to the action of Σ_m. If $u \in U_m$ is minimal such that $(\Delta \circ \alpha_u^{-1})|_{|\langle g_1, g_2\rangle}$ is absolutely irreducible, then $M_N \in \mathrm{V}(\mathrm{I}_u(G))$.

For $u \in U_m$ set

$$Q_u(G) := \mathrm{V}(\mathrm{I}_u(G)) - V(\mathfrak{D} \cap \mathfrak{A}_4 \cap \mathfrak{S}_4 \cap \mathfrak{A}_5).$$

We now present the main result.

Theorem 8.2. *Let G be a finitely presented group on m generators. The maps $M \mapsto N_M$ and $N \mapsto M_N$ induce mutually inverse bijections between Σ_m-orbits of maximal ideals of $\biguplus_{u \in U_m} Q_u(G)$ and normal subgroups $N \trianglelefteq G$ such that G/N is of L_2-type (where $\biguplus$ denotes the disjoint union).*

Proof. This follows by Proposition 8.1 and Theorem 7.5. □

9 Subgroup tests

Proposition 6.1 allows us to test whether a realization $\Delta\colon F_m \to \mathrm{SL}(2,K)$ of a prime ideal $P \trianglelefteq \Phi'_m$ maps projectively onto A_4, S_4, or A_5, using the ideals $J'(\mathrm{A}_4)$, $J'(\mathrm{S}_4)$, and $J'(\mathrm{A}_5)$. These ideals are easily computed if $m = 2$, since there are only 4 presentations of A_4 on two generators, 9 for S_4, and 19 for A_5; see [PF09, Lemmas 3.7–3.9]. However, this approach is no longer efficient if $m \geq 3$. For example, there are 65 presentations of A_4 on three generators, 420 for S_4, and 1688 for A_5.

In this section, we describe a more efficient test, using the absolutely irreducible subgroups of A_4, S_4, and A_5. Set $A_i := \Delta(g_i)$ and let $a_i \in \mathrm{PSL}(2,K)$ be the projective image, for $1 \leq i \leq m$. We assume that $\langle A_1, A_2\rangle$ is absolutely irreducible. Define $H := \langle a_1, \ldots, a_m\rangle$. If $H \cong \mathrm{A}_4$, then $\langle a_1, a_2\rangle \in \{\mathrm{V}_4, \mathrm{A}_4\}$; if $H \cong \mathrm{S}_4$, then $\langle a_1, a_2\rangle \in \{\mathrm{V}_4, \mathrm{S}_3, \mathrm{D}_8, \mathrm{A}_4, \mathrm{S}_4\}$; and if $H \cong \mathrm{S}_4$, then $\langle a_1, a_2\rangle \in \{\mathrm{V}_4, \mathrm{S}_3, \mathrm{D}_{10}, \mathrm{A}_4, \mathrm{S}_4\}$. It is easy to check whether $\langle a_1, a_2\rangle \in \{\mathrm{V}_4, \mathrm{S}_3, \mathrm{D}_8, \mathrm{D}_{10}, \mathrm{A}_4, \mathrm{S}_4, \mathrm{A}_5\}$; for example, $\langle a_1, a_2\rangle = \mathrm{V}_4$ if and only if $\mathrm{tr}(A_1) = \mathrm{tr}(A_2) = \mathrm{tr}(A_1 A_2) = 0$. If $\langle a_1, a_2\rangle$ is one of the seven groups, then we can always find matrices $B_1 = w_1(A_1, A_2), B_2 = w_2(A_1, A_2)$ such that $\mathrm{tr}(B_1) = \mathrm{tr}(B_2) = 0$ and $\langle w_1(a_1, a_2), w_2(a_1, a_2)\rangle$

is a dihedral group of order 4, 6, or 10. In the latter two cases we may also assume that $\mathrm{tr}(B_1B_2) = 1$ or $\mathrm{tr}(B_1B_2)$ is a root of $X^2 + X - 1$, respectively.

For $B = (B_1, B_2) \in \mathrm{SL}(2,q)^2$ and $X \in \mathrm{SL}(2,q)$ let

$$\theta_B(X) := (\mathrm{tr}(X), \mathrm{tr}(B_1X), \mathrm{tr}(B_2X), \mathrm{tr}(B_1B_2X)) \in \mathbb{F}_q^4.$$

If $\langle B_1, B_2\rangle$ is absolutely irreducible, then X is uniquely determined by $\theta_B(X)$, see Proposition 2.4.

We give details of an A_4-test. Fix B, and let $b_i \in \mathrm{PSL}(2,q)$ be the projective image of B_i. Assume $\langle b_1, b_2\rangle \cong \mathrm{V}_4$; let $\langle b_1, b_2\rangle \le \Gamma \le \mathrm{PSL}(2,q)$ with $\Gamma \cong \mathrm{A}_4$ and let $\widetilde{\Gamma} \le \mathrm{SL}(2,q)$ be the full preimage of Γ. Now $X \in \mathrm{SL}(2,q)$ maps onto an element of Γ if and only if $\theta_B(X) \in \theta_B(\widetilde{\Gamma}) = \{\theta_B(Y) \mid Y \in \widetilde{\Gamma}\}$, thus for an effective subgroup test it is enough to compute the sets $\theta_B(\widetilde{\Gamma})$. The subgroups of $\mathrm{PSL}(2,q)$ isomorphic to A_4 are all conjugate in $\mathrm{PGL}(2,q)$, and $\theta_{({}^MB)}(\widetilde{\Gamma}) = \theta_B({}^{M^{-1}}\widetilde{\Gamma})$ for all $M \in \mathrm{GL}(2,q)$, so it is enough to compute $\theta_B(\widetilde{\Gamma})$ for a fixed Γ and all possible B. Furthermore, $\theta_{({}^MB)}(\widetilde{\Gamma}) = \theta_B(\widetilde{\Gamma})$ for all $M \in \mathrm{N}_{\mathrm{GL}(2,q)}(\widetilde{\Gamma})$, so it suffices to compute $\theta_B(\widetilde{\Gamma})$ for a fixed Γ and all $\mathrm{N}_{\mathrm{GL}(2,q)}(\widetilde{\Gamma})$-conjugacy classes of pairs $B \in \widetilde{\Gamma}$ mapping onto generators for V_4. Finally, the subgroups $\widetilde{\Gamma}$ are up to conjugation images of $\mathrm{SL}(2,3) \le \mathrm{SL}(2,\mathbb{Z}[i])$ modulo a prime ideal of $\mathbb{Z}[i]$, so $\theta_B(\widetilde{\Gamma})$ can be computed uniformly for all prime powers q by a single computation over $\mathbb{Z}$.

Summarizing, we get the following result.

Proposition 9.1. *Let $G = \mathrm{PSL}(2,q)$ for an odd prime power q, let $a_1, a_2 \in G$ be generators of a Klein four group V, and let $z \in G$. Let $A_i \in \mathrm{SL}(2,q)$ be a preimage of A_i, and let $Z \in \mathrm{SL}(2,q)$ be a preimage of z.*

There is a unique $H \le G$ isomorphic to A_4 which contains V, and $z \in H$ if and only if $\theta_B(Z)$ is one of the 24 elements

$$\Theta_4 := \{(\pm2,0,0,0), (0,\pm2,0,0), (0,0,\pm2,0), (0,0,0,\pm2), (\pm1,\pm1,\pm1,\pm1)\}.$$

Proposition 9.2. *Let $A_1, \ldots, A_m \in \mathrm{SL}(2,q)$ such that $\langle A_1, A_2\rangle$ is absolutely irreducible. Let $t = (\mathrm{tr}(A_1), \mathrm{tr}(A_2), \mathrm{tr}(A_1A_2))$, and let $a_i \in \mathrm{PSL}(2,q)$ be the image of A_i. Set $B := (A_1, A_2)$. Then $\langle a_1, \ldots, a_m\rangle$ is isomorphic to A_4 if and only if one of the following conditions is satisfied.*

1. *$t = (0,0,0)$ and $\theta_B(A_i) \in \Theta_4$ for all $3 \le i \le m$, where $B = (A_1, A_2)$, and at least one $\theta_B(A_i) = (\pm1,\pm1,\pm1,\pm1)$.*
2. *$t = (0,\pm1,\pm1)$ and $\theta_B(A_i) \in \Theta_4$ for all $3 \le i \le m$, where $B = (A_1, A_2^{-1}A_1A_2)$.*
3. *$t = (\pm1,0,\pm1)$ and $\theta_B(A_i) \in \Theta_4$ for all $3 \le i \le m$, where $B = (A_2, A_1^{-1}A_2A_1)$.*
4. *$t = (\pm1,\pm1,0)$ and $\theta_B(A_i) \in \Theta_4$ for all $3 \le i \le m$, where $B = (A_1A_2, A_2A_1)$.*
5. *$t = (\pm1,\pm1,\pm1)$ with an even number of -1's, and $\theta_B(A_i) \in \Theta_4$ for all $3 \le i \le m$, where $B = (A_1A_2^{-1}, A_2^{-1}A_1)$.*

Proof. The only absolutely irreducible subgroups of A_4 are the Klein four group and A_4. If $t = (0,0,0)$, then $\langle a_1, a_2\rangle$ is a Klein four group, and the claim follows by Proposition 9.1. If $t = (0,\pm1,\pm1)$, then $\langle a_1, a_2\rangle = \mathrm{A}_4$, and $\langle a_1, a_2^{-1}a_1a_2\rangle$ generate the subgroup of order 4; again, the claim follows by Proposition 9.1. The other cases correspond to the other three presentations of A_4 and are handled similarly. □

It is straight-forward to give similar conditions for S_4 and A_5, utilizing the subgroups S_3 and D_{10} in addition to V_4.

10 L_2-ideals

Definition 10.1. An L_2-*ideal* is a prime ideal $P \in \mathrm{Spec}(\Phi'_m) - \mathrm{V}(\mathfrak{D} \cap \mathfrak{A}_4 \cap \mathfrak{S}_4 \cap \mathfrak{A}_5)$. Let $P \cap \mathbb{Z} = \langle p\rangle$, and let d be the Krull dimension of P.

1. If $d = 0$, that is, P is a maximal ideal, let $k := \dim_{\mathbb{F}_p}(\Phi'_m/P)$. Then P is of type $\mathrm{L}_2(p^k)$ if $\mathrm{Stab}_{\Sigma_m}(P)$ is trivial, and of type $\mathrm{PGL}(2,p^{k/2})$ otherwise.

2. If $d > 0$ and $p \neq 0$, then P is of type $\mathrm{L}_2(p^{\infty^d})$, or of type $\mathrm{L}_2(p^\infty)$ if $d = 1$.

3. If $d = 1$ and $p = 0$, let $k := \dim_{\mathbb{Q}}(\Phi'_m \otimes_{\mathbb{Z}} \mathbb{Q}/P \otimes_{\mathbb{Z}} \mathbb{Q})$. Then P is of type $\mathrm{L}_2(\infty^k)$.

4. If $d > 1$ and $p = 0$, then P is of type $\mathrm{L}_2(\infty^{\infty^{d-1}})$, or of type $\mathrm{L}_2(\infty^\infty)$ if $d = 2$.

For an L_2-ideal P let t_P be the trace tuple, Δ_P a realization of t_P, and δ_P the projective representation induced by Δ_P.

Proposition 10.2. *Let P be an L_2-ideal.*

1. *If P is of type $\mathrm{L}_2(p^k)$, then the image of δ_P is isomorphic to $\mathrm{L}_2(p^k)$; if P is of type $\mathrm{PGL}(2, p^k)$, then the image of δ_P is isomorphic to $\mathrm{PGL}(2, p^k)$.*

2. *If P is of type $\mathrm{L}_2(\infty^k)$, then every maximal L_2-ideal containing P is of type $\mathrm{L}_2(p^\ell)$ or $\mathrm{PGL}(2, p^{\ell/2})$ with $\ell \leq k$. Moreover, the set of maximal elements of $\mathrm{V}(P)$ which are not L_2-ideals is finite.*

3. *If P is of type $\mathrm{L}_2(p^{\infty^d})$, then there are infinitely many $k \in \mathbb{N}$ such that $\mathrm{V}(P)$ contains L_2-ideals of type $\mathrm{L}_2(p^k)$. Moreover, the set of prime ideals in $\mathrm{V}(P)$ which are not L_2-ideals form a closed set of dimension at most $d - 1$.*

4. *If P is of type $\mathrm{L}_2(\infty^{\infty^{d-1}})$, then for all but finitely many primes p there exist infinitely many $k \in \mathbb{N}$ such that $\mathrm{V}(P)$ contains L_2-ideals of type $\mathrm{L}_2(p^k)$. Moreover, the set of prime ideals in $\mathrm{V}(P)$ which are not L_2-ideals form a closed set of dimension at most $d - 1$.*

Proof. First note that the set of prime ideals in $\mathrm{V}(P)$ which are not L_2-ideals are precisely the elements of the set $\mathrm{V}(P) \cap \mathrm{V}(\mathfrak{D} \cap \mathfrak{A}_4 \cap \mathfrak{S}_4 \cap \mathfrak{A}_5) = \mathrm{V}(P + \mathfrak{D} \cap \mathfrak{A}_4 \cap \mathfrak{S}_4 \cap \mathfrak{A}_5)$. Since P does not contain $\mathfrak{D} \cap \mathfrak{A}_4 \cap \mathfrak{S}_4 \cap \mathfrak{A}_5$ and P is prime, $P \subsetneqq P + \mathfrak{D} \cap \mathfrak{A}_4 \cap \mathfrak{S}_4 \cap \mathfrak{A}_5$, so the Krull dimension of the latter ideal is smaller than that of P. This settles all claims about the size of $\mathrm{V}(P)$.

We prove the other claims.

1. This follows by Theorem 7.5.

2. The first point follows since $\dim_{\mathbb{F}_p}(\Phi'_m \otimes_{\mathbb{Z}} \mathbb{F}_p/P \otimes_{\mathbb{Z}} \mathbb{F}_p) \leq \dim_{\mathbb{Q}}(\Phi'_m \otimes_{\mathbb{Z}} \mathbb{Q}/P \otimes_{\mathbb{Z}} \mathbb{Q})$ for all primes p, and the maximal ideals of Φ'_m containing P and p are in bijection to the maximal ideals of $\Phi'_m \otimes_{\mathbb{Z}} \mathbb{F}_p$ containing $P \otimes_{\mathbb{Z}} \mathbb{F}_p$. For the second point, note that a set of dimension zero is finite.

3. Since Φ'_m is finitely generated, there are only finitely many epimorphisms of Φ'_m onto $\mathbb{F}_{p^k}$ for every k. But there are infinitely many primes containing P.

4. In this case, $(\Phi'_m/P) \otimes_{\mathbb{Z}} \mathbb{Q}$ has algebraically independent elements, so there are epimorphisms onto number fields of arbitrarily high degrees. Let $\alpha\colon \Phi'_m \otimes_{\mathbb{Z}} \mathbb{Q} \to K$ be an epimorphism onto a number field K of degree k such that α factors over $\Phi'_m \otimes_{\mathbb{Z}} \mathbb{Q}$; set $Q := \ker(\alpha_{|\Phi'_m}) \trianglelefteq \Phi'_m$. Then $Q \supseteq P$; if Q is an L_2-ideal, then it is of type $\mathrm{L}_2(\infty^k)$. But the prime ideals which are not L_2-ideals form a set of Krull-dimension $d - 1$, so this approach yields an L_2-ideal for almost all Q. The result now follows by part (2). □

11 The algorithm

Definition 11.1. Let $G = \langle g_1, \ldots, g_m \mid w_1(g_1, \ldots, g_m), \ldots, w_r(g_1, \ldots, g_m) \rangle$ be a finitely presented group. Then Σ_m acts on the set $\{\pm 1\}^r$ of sign systems by

$$^\sigma s := (w_1(\sigma_1, \ldots, \sigma_m)s_1, \ldots, w_r(\sigma_1, \ldots, \sigma_m)s_r)$$

for $\sigma \in \Sigma_m$ and $s \in \{\pm 1\}^r$.

Remark 11.2. A prime ideal $P \in \mathrm{Spec}(\Phi'_m)$ contains $\mathrm{I}_s(G)$ if and only if $^\sigma P$ contains $\mathrm{I}_{(^\sigma s)}(G)$. Let T be the kernel of the action and S a set of representatives of the orbits; then the Σ_m-orbits of $\mathrm{V}(\mathrm{I}(G))$ are in bijection to the T-orbits of $\mathrm{V}(\bigcap_{s \in S} \mathrm{I}_s(G))$.

This allows us to reduce the computations by a factor up to 2^m.

Algorithm 11.3 (`L2Quotients`)**.**
Input: A finitely presented group G.
Output: For every $u \in U_m$, a set of representatives for the Σ_m-orbits of minimal L_2-ideals of $Q_u(G)$.

1. Set $A := U_m$ and $\mathcal{R} := \emptyset$.
2. Let u be the smallest element in A. Let T be the kernel and S a set of representatives for the orbits of the action of Σ_m on the sign systems of $\alpha_u(G)$.
3. Let $\mathcal{P}$ be the set of minimal elements in $\bigcup_{s\in S} \mathrm{MinAss}(\mathrm{I}_s^u(G))$, where $\mathrm{MinAss}(I)$ denotes the minimal associated prime ideals of I. Remove from $\mathcal{P}$ all elements which contain one of the ideals $\mathfrak{D}$, $\mathfrak{A}_4$, $\mathfrak{S}_4$, or $\mathfrak{A}_5$.
4. Choose a set $\mathcal{P}'$ of representatives of T-orbits on $\mathcal{P}$.
5. Add $(\mathcal{P}', u)$ to $\mathcal{R}$, and remove u from A. If $A \neq \emptyset$, go to step 2; otherwise return $\mathcal{R}$.

Remark 11.4.
1. The output of the algorithm describes the L_2-quotients of G as follows. For every $N \trianglelefteq G$ with G/N of L_2-type there exists $u \in U_m$ and $\sigma \in \Sigma_m$ such that $M_N \supseteq P$ for some P. Conversely, if $M \supseteq P$ is a maximal L_2-ideal for some P, then $N_M \trianglelefteq G$ with G/N_M of L_2-type.
2. If all prime ideals returned by the algorithm are maximal, then G has only finitely many L_2-quotients, and the normal subgroups $N \trianglelefteq G$ with G/N of L_2-type are in bijection to the maximal ideals.
3. If the algorithm returns at least one prime ideal of positive Krull dimension, then G has infinitely many L_2-quotients.

The algorithm has been implemented in Magma [BCP97].

Remark 11.5.
1. The ring Φ'_m is very useful for the theoretical description of the algorithm. However, in practice the localization at ρ slows down computations considerably. Instead, we work with the preimage of $\mathrm{I}_s^u(G)$ in $\mathbb{Z}[x_J \mid \emptyset \neq J \subseteq \{1,\dots,m\}]$, and remove all prime components containing ρ.
2. The implementation uses Gröbner bases to handle the ideals $\mathrm{I}_s^u(G)$. However, Gröbner basis computations over the integers can be very slow, especially as m grows. The algorithm in [Jam11] to compute the minimal associated primes of an ideal replaces Gröbner basis computations over the integers by several Gröbner basis computations over prime fields, resulting in a much faster algorithm.

11.1 Adaptation to Coxeter groups

Coxeter groups are a special class of finitely presented groups, where the only relations are $(g_i g_j)^{C_{ij}} = 1$ for a symmetric matrix $C = (C_{ij}) \in (\mathbb{Z} \cup \{\infty\})^{m\times m}$ with 1's along the diagonal (if $C_{ij} = \infty$, then we simply omit the relation). We call C a *Coxeter matrix* and denote the finitely presented group by G_C. We are often only interested in smooth quotients of Coxeter groups, that is, those for which the images also have the prescribed orders (unless the prescribed order is ∞). In this case, the L_2-quotient algorithm can be simplified, which also results in a considerable speed-up of the computation. This is based on the following.

For $n \in \mathbb{N}$ let $\zeta_n \in \mathbb{C}$ be a primitive n-th root of unity. Set $\eta_n := \zeta_n + \zeta_n^{-1}$, and let $\Psi_n \in \mathbb{Z}[T]$ be the minimal polynomial of η_n. For convenience, we define $\Psi_\infty := 0$.

Remark 11.6. Let $A \in \mathrm{SL}(2, K)$ where k is a field of characteristic $p \geq 0$, and let $n \in \mathbb{N}$.

1. If $p = 0$ or $(n, p) = 1$, then $\Psi_n(\mathrm{tr}(A)) = 0$ if and only if $|A| = n$.
2. If $n = p$, then $\Psi_n(\mathrm{tr}(A)) = 0$ if and only if $|A| \in \{1, p\}$.
3. If $n = 2p \neq 4$, then $\Psi_n(\mathrm{tr}(A)) = 0$ if and only if $|A| \in \{2, 2p\}$.

For a Coxeter matrix $C \in (\mathbb{Z} \cup \{\infty\})^{m\times m}$ set

$$\mathrm{I}(C) := \langle x_1, \ldots, x_m\rangle + \langle \Psi_{2C_{ij}}(x_{ij}) \mid 1 \le i < j \le m \text{ with } C_{ij} \text{ even}\rangle \\ + \langle \Psi_{C_{ij}}(x_{ij})\Psi_{2C_{ij}}(x_{ij}) \mid 1 \le i < j \le m \text{ with } C_{ij} \text{ odd}\rangle \trianglelefteq \Phi'_m,$$

where $x_{ij} = \rho^{-1}(\lambda_0^i x_j + \lambda_1^i x_{1j} + \lambda_2^i x_{2j} + \lambda_{12}^i x_{12j})$.

Remark 11.7. Let $a_1, a_2 \in \mathrm{L}_2(q)$ with $|a_1| = |a_2| = 2$ and $|a_1a_2| \neq 1$. Then $\langle a_1, a_2\rangle$ is absolutely irreducible if and only if $(q, |a_1a_2|) = 1$.

Theorem 11.8. *Let $C \in (\mathbb{Z} \cup \{\infty\})^{m\times m}$ be a Coxeter matrix.*

1. *Let $q = p^d$, and let $\Delta\colon F_m \to \mathrm{SL}(2,q)$ be a representation which induces a smooth projective representation $\delta\colon G_C \to \mathrm{PSL}(2,q)$ such that $\delta(G_C)$ is of L_2-type. Let $t := t_\Delta$ and $P := P_t$. If $|\delta(g_1g_2)| \neq p$, then $P \supseteq \mathrm{I}(C)$.*
2. *Let $M \supseteq \mathrm{I}(C)$ be a maximal L_2-ideal and $\Delta = \Delta_M\colon F_m \to \mathrm{SL}(2,q)$ a realization. Then Δ induces a projective representation $\delta\colon G_C \to \mathrm{PSL}(2,q)$ such that $\delta(G_C)$ is of L_2-type. If $(q, 2C_{ij}) = 1$ for all $1 \le i < j \le m$, then δ is smooth.*

Proof. This follows easily by the preceeding remarks. □

This can be easily turned into an algorithm. We leave the details to the reader.

11.2 Computing realizations

The L_2-quotient algorithm returns a set of L_2-ideals, which contain a lot of information, for example, the isomorphism types and number of L_2-images. However, in certain cases one will want to compute an explicit epimorphism $G \to \mathrm{PSL}(2,q)$ encoded by an L_2-ideal. We now present an algorithm to accomplish that. This algorithm works for representations of arbitrary degree, so we present it in this generality.

Proposition 11.9. *Let G be a finitely generated group, and let $\chi\colon G \to K$ be the character of an absolutely irreducible representation Δ of degree n. There is a probabilistic algorithm with input χ and n which constructs an extension field L/K of degree at most n and a representation $\Delta'\colon G \to \mathrm{GL}(n,L)$, such that Δ' is equivalent to Δ. If K is finite, then we can choose $L = K$.*

Proof. We assume first that $G = F_m$ is a free group on $g_1, \ldots, g_m$. We first find words $w_1, \ldots, w_{n^2} \in F_m$ such that $(\Delta(w_1), \ldots, \Delta(w_{n^2}))$ is a basis of $K^{n\times n}$. Let $W_i := \{w \in F_m \mid |w| \le i\}$, where $|w|$ denotes the length of the word w. For $X \subseteq K^{n\times n}$ denote by $\langle X\rangle_K$ the K-span of X. Note that $\langle\Delta(W_{i+1})\rangle_K = \langle\Delta(W_i)\rangle_K$ for some i implies $\langle\Delta(W_j)\rangle_K = \langle\Delta(W_i)\rangle_K$ for all $j \ge i$. In particular, the chain

$$\langle\Delta(W_0)\rangle_K \subseteq \langle\Delta(W_1)\rangle_K \subseteq \cdots$$

stabilizes after at most n^2 steps, so $\Delta(W_{n^2-1})$ is a generating set of $K^{n\times n}$. Let C be a subset of W_{n^2-1} of n^2 elements; define the matrix $\Sigma := (\chi(v,w))_{v,w}$, where v and w run through C. Since the trace bilinear form $S\colon K^{n\times n} \times K^{n\times n} \to K\colon (V,W) \mapsto \mathrm{tr}(VW)$ is non-degenerate, $\Delta(C)$ is a basis of $K^{n\times n}$ if and only if Σ is non-singular. By running through all n^2-element subsets of W_{n^2-1} we can find the $w_1, \ldots, w_{n^2}$.

Now let $V := K^{n\times 1}$ be the KF_m-module induced by Δ. We first construct the KF_m-module $V^n = V \oplus \cdots \oplus V \equiv K^{n\times n}$. To determine the action of F_m on $K^{n\times n}$, it is enough to determine values $\lambda_{jk}^i \in K$ such that $\Delta(g_i)\Delta(w_j) = \sum_k \lambda_{jk}^i \Delta(w_k)$, where $1 \le i \le m$ and $1 \le j,k \le n^2$. Since S is non-degenerate, each λ_{jk}^i is uniquely determined by the n^2 equations

$$\chi(g_iw_jw_\ell) = S(\Delta(g_i)\Delta(w_j), \Delta(w_\ell)) = S(\sum_k \lambda_{jk}^i \Delta(w_k), \Delta(w_\ell)) = \sum_{k=1}^{n^2} \lambda_{jk}^i \chi(w_k \cdot w_\ell),$$

where $1 \le \ell \le n^2$. By solving the linear equations, we can construct the KF_m-module $V^n \equiv K^{n\times n}$.

Let $\Gamma\colon F_m \to \mathrm{GL}(K^{n\times n})$ be the representation on $V^n \equiv K^{n\times n}$. We denote the extensions of Δ and Γ to the group algebras again by Δ and Γ, respectively. Let $v = (v_1, \ldots, v_n) \in K^{n\times n}$, where the v_i are

the columns of v. Then $\Gamma(a)v = (\Delta(a)v_1, \ldots, \Delta(a)v_n)$ for $a \in KF_m$. In particular, $\Gamma(a)$ and $\Delta(a)$ have the same minimal polynomial, and if $c \in K[x]$ is the characteristic polynomial of $\Delta(a)$, then c^n is the characteristic polynomial of $\Gamma(a)$.

We now use an adaptation of [GLGO06] to find a simple factor of the KF_m-module $K^{n\times n}$. If K is finite, choose random elements $a \in KF_m$ until $\Gamma(a)$ has an eigenspace of dimension n. Since the image of Δ is isomorphic to $K^{n\times n}$, this terminates with high probability by a result of Holt and Rees (see [HR94, Section 2.3]). Set $L := K$, and let $\lambda \in L$ be an eigenvalue of $\Gamma(a)$ of multiplicity n. If K is infinite, then choose random $a \in KF_m$ until the characteristic polynomial of $\Gamma(a)$ is an n-th power of a separable polynomial (that is, the characteristic polynomial of $\Delta(a)$ is separable). The characteristic polynomial of a matrix is inseparable if and only if its discriminant is zero, so the set of matrices with inseparable characteristic polynomial is Zariski closed in $K^{n\times n}$. Thus the matrices with separable characteristic polynomial are Zariski dense in $K^{n\times n}$. Since the image of Δ is isomorphic to $K^{n\times n}$, the probability of finding a suitable a is very high. Let L/K be a field extension such that the characteristic polynomial has a root λ in L.

Let $v \in L^{n\times n}$ be an eigenvector of $\Gamma(a)$ with eigenvalue λ. Then

$$\Gamma(a)v = (\Delta(a)v_1, \ldots, \Delta(a)v_n) = \lambda v = (\lambda v_1, \ldots, \lambda v_n).$$

We may assume without loss of generality that v_1 is non-zero. Since the λ-eigenspace of $\Delta(a)$ is one-dimensional, there exist $\xi_2, \ldots, \xi_n \in L$ such that $v_i = \xi_i v_1$ for $i > 1$. Thus $v = (v_1, \xi_2 v_1, \ldots, \xi_n v_1)$ and $\Gamma(a)v = (\Delta(a)v_1, \xi_2\Delta(a)v_1, \ldots, \xi_n\Delta(a)v_1)$, so $LF_m v$ is isomorphic to $LF_m v_1 \cong L \otimes_K V$. Now choose $w_1, \ldots, w_n \in F_m$ such that $B := (\Gamma(w_1)v, \ldots, \Gamma(w_n)v)$ is a basis of $LF_m v$. For every generator g_i of F_m let $\Delta'(g_i)$ be the representation matrix of g_i on $LF_m v$ with respect to B. By construction, Δ' is equivalent to Δ. This concludes the proof if $G = F_m$ is a free group.

Now assume that G is an arbitrary finitely generated group generated by m elements, and let $\nu\colon F_m \to G$ be an epimorphism. Let $\widehat{\Delta} := \Delta \circ \nu$ and $\widehat{\chi} := \chi \circ \nu$. We construct an extension field L/K and a representation $\widehat{\Delta}'$ such that $\widehat{\Delta} \sim \widehat{\Delta}'$. But then $\Delta'\colon G \to \mathrm{GL}(n, F)$ defined by $\Delta'(g) := \widehat{\Delta}'(\widetilde{g})$, where $\widetilde{g} \in F_m$ with $\nu(\widetilde{g}) = g$ is arbitrary, is a representation of G, equivalent to Δ. □

In our special setting, we can use the trace polynomials to compute all character values. Furthermore, we always assume that $\Delta_{\langle g_1, g_2\rangle}$ is absolutely irreducible, so we can choose $(w_1, \ldots, w_4) = (1, g_1, g_2, g_1g_2)$ in the first part of the algorithm.

12 Examples

For the results in this section we use our implementation of the L_2-quotient algorithm in Magma [BCP97].

12.1 Groups with finitely many L_2-quotients

In [Cox39], Coxeter defines three families of presentations:

$$\begin{aligned}(\ell, m|n, k) &= \langle a, b \mid a^\ell, b^m, (ab)^n, (a^{-1}b)^k\rangle,\\ (\ell, m, n; q) &= \langle a, b \mid a^\ell, b^m, (ab)^n, [a, b]^q\rangle,\\ G^{m,n,p} &= \langle a, b \mid a^m, b^n, c^p, (ab)^2, (ac)^2, (bc)^2, (abc)^2\rangle.\end{aligned}$$

These groups have been intensively studied, see [EJ08] for an overview. After recent work of Havas and Holt [HH10], only for four of these groups is it not known whether they are finite or infinite, namely $(3, 4, 9; 2)$, $(3, 4, 11; 2)$, $(3, 5, 6; 2)$, and $G^{3,7,19}$. We study these groups and their low-index subgroups [Sim94] using the L_2-quotient algorithm.

Proposition 12.1. *Let $G = (3, 4, 9; 2)$. Then G has seven conjugacy classes of subgroups of index ≤ 50. For $1 \leq i \leq 50$ let $H_i \leq G$ with $[G : H_i] = i$, if such a group exists. The only L_2-quotient of H_i for $i \in \{1, 3, 4, 12\}$ is $\mathrm{L}_2(89)$; the group H_6 has a quotient $\mathrm{L}_2(89) \times (\mathrm{PGL}(2, 5) \wr^{\mathrm{C}_2} \mathrm{PGL}(2, 5))$; and H_{30} and H_{36} have a quotient $\mathrm{L}_2(89) \times \mathrm{PGL}(2, 5)$.*

Let $G = (3, 5, 6; 2)$. Then G has two conjugacy classes of subgroups of index ≤ 50, a group of index 3 and G itself. Both groups have the single L_2-quotient $\mathrm{L}_2(61)$.

The groups $(3,4,11;2)$ *and* $G^{3,7,19}$ *do not have non-trivial subgroups of index* ≤ 50*. Both groups have a single* L_2*-quotient, namely* $(3,4,11;2)$ *has* $\mathrm{L}_2(769)$*, and* $G^{3,7,19}$ *has* $\mathrm{L}_2(113)$*.*

The next result concerns a question of Conder [Con92], asking whether a group has non-trivial finite quotients.

Proposition 12.2. *The group*

$$\begin{aligned} G = \langle A,B,C,D,E,F \mid & A^3, B^3, C^2, D^2, E^2, F^2, (AC)^3, (AD)^3, (AE)^3, (AF)^3, \\ & (BC)^3, (BD)^3, (BE)^3, (BF)^3, (ABA^{-1}C)^2, (ABA^{-1}D)^2, (A^{-1}BAE)^2, \\ & (A^{-1}BAF)^2, (BAB^{-1}C)^2, (B^{-1}ABD)^2, (BAB^{-1}E)^2, (B^{-1}ABF)^2 \rangle \end{aligned}$$

has no quotients isomorphic to $\mathrm{L}_2(q)$ *or* $\mathrm{PGL}(2,q)$ *for any prime power* q*.*

12.2 Groups with L_2-ideals of type $\mathrm{L}_2(\infty^k)$

If the algorithm returns an ideal of type $\mathrm{L}_2(\infty^k)$, then the group has infinitely many L_2-quotients, finitely many in every characteristic. Using algebraic number theory, the precise quotient types can be determined as already outlined in [PF09, Example 8.1]. We illustrate the process by relaxing the conditions of the Coxeter presentation $G^{3,7,19}$.

Proposition 12.3. *Let* $G = \langle a,b,c \mid a^3, b^7, (ab)^2, (ac)^2, (bc)^2, (abc)^2 \rangle$*. Then* G *has finitely many* L_2*-quotients in every characteristic.*

More precisely, let $K/\mathbb{Q}$ *be the splitting field of* $X^6-4X^4+3X^2+1$ *with Galois group* $\Gamma = \mathrm{Gal}(K/\mathbb{Q}) \cong \langle (1,4), (1,2,3)(4,5,6) \rangle = \mathrm{C}_2 \wr \mathrm{C}_3$*. For a prime* $p \neq 2,7$ *denote by* $\varphi_p \in \Gamma$ *the Frobenius automorphism mod* p*. The* L_2*-quotient in characteristic* p *is*

1. $\mathrm{L}_2(p)^3$ *if* $\varphi_p = ()$*;*
2. $\mathrm{L}_2(p)^2 \times \mathrm{PGL}(2,p)$ *if* $\varphi_p \sim (1,4)$*;*
3. $\mathrm{L}_2(p) \times \mathrm{PGL}(2,p) \leftthreetimes^{\mathrm{C}_2} \mathrm{PGL}(2,p)$ *if* $\varphi_p \sim (1,4)(2,5)$*;*
4. $\mathrm{PGL}(2,p) \leftthreetimes^{\mathrm{C}_2} \mathrm{PGL}(2,p) \leftthreetimes^{\mathrm{C}_2} \mathrm{PGL}(2,p)$ *if* $\varphi_p \sim (1,4)(2,5)(3,6)$*;*
5. $\mathrm{L}_2(p^3)$ *if* $\varphi_p \sim (1,2,3)(4,5,6)^{\pm 1}$*;*
6. $\mathrm{PGL}(2,p^3)$ *if* $\varphi_p \sim (1,2,3,4,5,6)^{\pm 1}$*;*

Moreover, G *has quotients* $\mathrm{L}_2(2^3)$ *and* $\mathrm{PGL}(2,7)$*.*

In this case, we do not need the precise conjugacy type of the Frobenius automorphism, the decomposition of $X^6-4X^4+3x^2+1$ is enough. For example, taking $p = 65537$, we see that $X^6-4X^4+3X^2+1 \in \mathbb{F}_p[X]$ has two irreducible factors of degree 3; this shows that G has a quotient $\mathrm{L}_2(65537^3)$. Taking $p = 8388617$ we see that $X^6-4X^4+3X^2+1 \in \mathbb{F}_p[X]$ has two linear factors and two factors of degree 2; this shows that G has quotient $\mathrm{L}_2(8388617) \times \mathrm{PGL}(2,8388617) \leftthreetimes^{\mathrm{C}_2} \mathrm{PGL}(2,8388617)$, that is, there is precisely one $N \trianglelefteq G$ with $G/N \cong \mathrm{L}_2(8388617)$, precisely two $N \trianglelefteq G$ with $G/N \cong \mathrm{PGL}(2,8388617)$, and no other $N \trianglelefteq G$ with $G/N \cong \mathrm{L}_2(8388617^k)$ or $G/N \cong \mathrm{PGL}(2,8388617^k)$ for some $k \in \mathbb{N}$.

Proof. The algorithm returns the single L_2-ideal $P = \langle x_1+1, x_2^3+x_2^2-2x_2-1, x_3^2+x_2^2-3, x_{12}, x_{13}, x_{23}, x_{123} \rangle$ of type $\mathrm{L}_2(\infty^6)$. The zeroes are

$$t = (-1, -\xi^4+3\xi^2-1, \xi, 0, 0, 0, 0) \in \mathbb{F}_q,$$

where ξ is a root of $X^6-4X^4+3X^2+1$. We assume $\mathbb{F}_q = \mathbb{F}_p[\xi]$. Let $\delta\colon G \to \mathrm{PSL}(2,q)$ be a realization of t. There is no characteristic such that $-\xi^4+3\xi^2-1 = 0$ or $\xi = 0$, so Δ is never imprimitive, by Proposition 6.3. Furthermore, ξ is never a root of Ψ_k for $k \in \{3,4,5,6,8,10\}$, so $|\delta(c)| > 5$ for all q (see Remark 11.6), hence the image of δ cannot be A_4, S_4, or A_5. Thus $\mathrm{im}(\delta) \in \{\mathrm{L}_2(q), \mathrm{PGL}(2,\sqrt{q})\}$. The precise isomorphism type depends on the action of the Galois group. Note that ${}^{\alpha}t = {}^{\sigma}t$ for a Galois automorphism α and a non-trivial sign system σ if and only if $\sigma = (1,1,-1)$ and $\alpha(\xi) = -\xi$. The result for $p \neq 2,7$ now follows by Corollary 7.6 and the fact that the Galois automorphism in characteristic p is determined by the Frobenius automorphism. For $p \in \{2,7\}$ the result can be verified directly. □

12.3 Groups with L_2-ideals of type $\mathrm{L}_2(p^\infty)$

The other kind of L_2-ideals of Krull dimension 1 are the ones containing a prime p. They seem to occur far less frequently in practice than ideals of type $\mathrm{L}_2(\infty^k)$. However, when they occur, we can again make precise statements about the quotients.

Proposition 12.4. *Let $G = \langle a, b, c \mid a^3 = 1, [a, c] = [c, a^{-1}], aba = bab, abac^{-1} = caba\rangle$. There exist epimorphisms $G \to \mathrm{L}_2(q)$ if and only if $q = 3^k$ for some $k \in \mathbb{N}$. Similarly, there exist epimorphisms $G \to \mathrm{PGL}(2, q)$ if and only if $q = 3^k$ for some $k \in \mathbb{N}$.*

Proof. The algorithm returns the single L_2-ideal

$$P = \langle 3, x_1 + 1, x_2 + 1, x_{12} - 1, x_{13} - x_3, x_{23} - x_3, x_{123}^2 - x_3x_{123} + 1\rangle$$

of type $\mathrm{L}_2(3^\infty)$, so L_2-quotients can only occur in characteristic 3, proving the 'only if' parts. It remains to show that every 3-power occurs. The zeroes of P are the trace tuples of the form

$$t = (t_1, t_2, t_3, t_{12}, t_{13}, t_{23}, t_{123}) = (2, 2, \xi + \xi^{-1}, 1, \xi + \xi^{-1}, \xi + \xi^{-1}, \xi)$$

with $\xi \in \overline{\mathbb{F}_3}$. Let $k = [\mathbb{F}_3[\xi] : \mathbb{F}_3]$, and let $\delta\colon G \to \mathrm{PSL}(3, 3^k)$ be a realization of t. If $k = 2\ell$ and $\xi^{3^\ell} = -\xi$, then the Galois automorphism $\alpha = (x \mapsto x^{3^\ell})$ and the sign system $\sigma = (1, 1, -1)$ induce the same action on t, so the image of δ is $\mathrm{PGL}(2, 3^\ell)$, by Proposition 7.2. Otherwise, the image is $\mathrm{L}_2(3^k)$. □

Variations of the presentation yield similar results. We omit the easy proof.

Proposition 12.5. *Let $H = \langle a, b, c \mid [a, c][a^{-1}, c], [b, a]ba^{-1}, a^{-1}c^{-1}abac^{-1}a^{-1}b^{-1}\rangle$.*

1. *Let $G = H/\langle a^5\rangle^H$. Then $\mathrm{L}_2(q)$ and $\mathrm{PGL}(2, q)$ are quotients of G if and only if $q = 5^k$ for some $k \in \mathbb{N}$.*
2. *Let $G = H/\langle a^7, (ab^{-1})^8\rangle^H$. Then $\mathrm{L}_2(q)$ and $\mathrm{PGL}(2, q)$ are quotients of G if and only if $q = 7^k$ for some $k \in \mathbb{N}$.*
3. *Let $G = H/\langle a^{11}, (ab^{-1})^5\rangle^H$. Then $\mathrm{L}_2(q)$ and $\mathrm{PGL}(2, q)$ are quotients of G if and only if $q = 11^k$ for some $k \in \mathbb{N}$.*
4. *Let $G = H/\langle a^{19}, (ab^{-1})^9\rangle^H$. Then $\mathrm{L}_2(q)$ is a quotient of G if and only if $q = 19^k$ for some $k \in \mathbb{N}$ or $q = 37$; and $\mathrm{PGL}(2, q)$ is a quotient of G if and only if $q = 19^k$ for some $k \in \mathbb{N}$.*

12.4 Coxeter groups

Example 12.6. Let

$$C := \begin{pmatrix} 1 & 8 & 3 & 2 \\ 8 & 1 & 5 & 5 \\ 3 & 5 & 1 & 13 \\ 2 & 5 & 13 & 1 \end{pmatrix} \in \mathbb{Z}^{4\times 4}.$$

Then $\mathrm{L}_2(q)$ is a smooth quotient of G_C if and only if q is one of the five primes

$$79,\ 6\,449,\ 699\,127\,441,\ 8\,438\,303\,591\,453\,175\,937\,527\,551,\ 518\,103\,478\,579\,218\,726\,546\,844\,118\,197\,999.$$

Similarly, $\mathrm{PGL}(2, q)$ is a smooth quotient of G_C if and only if q is one of the six primes

$$11\,311,\ 28\,081,\ 68\,466\,319,\ 24\,005\,442\,449,\ 13\,345\,982\,337\,089,\ 408\,327\,690\,683\,773\,678\,271.$$

Definition 12.7. A *C-group representation* of rank m is a pair $\mathcal{C} = (H, S)$ such that $S = \{a_1, \ldots, a_m\}$ is a generating set of involutions of H which satisfy the *intersection property*

$$\langle a_i \mid i \in I\rangle \cap \langle a_j \mid j \in J\rangle = \langle a_k \mid k \in I \cap J\rangle \quad \text{for all } I, J \subseteq \{1, \ldots, m\}.$$

Example 12.8. Let

$$C := \begin{pmatrix} 1 & 2 & 3 & 3 \\ 2 & 1 & 3 & 4 \\ 3 & 3 & 1 & 2 \\ 3 & 4 & 2 & 1 \end{pmatrix} \in \mathbb{Z}^{4\times 4}.$$

Then $\mathrm{L}_2(7)$ is the only smooth quotient of G_C of L_2-type. A realization is given by

$$S = \left\{ \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 6 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 0 & 5 \\ 4 & 0 \end{pmatrix} \right\},$$

and it is easy to check that this generating set satisfies the intersection property.

The intersection property can be checked easily if G_C only has finitely many L_2-quotients. Infinitely many quotients can be handled as well, but require a little more work, as shown in the following result.

Proposition 12.9. *The only finite group of* L_2*-type having a C-group representation of rank* 4 *such that* $(|a_1a_2|, |a_1a_3|, |a_1a_4|, |a_2a_3|, |a_3a_4|) = (2, 3, 2, 3, 3)$ *is* $\mathrm{PGL}(2, 5)$.

Proof. The algorithm returns only one L_2-ideal P of type $\mathrm{L}_2(\infty^2)$. Let $P \subseteq M \trianglelefteq \Phi'_m$ be a maximal ideal containing P, and let $t = t_M \in \mathbb{F}_q^{15}$ be the corresponding full trace tuple (see Theorem 3.6). Let $H = \langle a_1, \ldots, a_4 \rangle \leq \mathrm{PSL}(2, q)$ be the image of the induced projective representation. Then

$$\begin{aligned} t &= (t_1, t_2, t_3, t_4, t_{12}, \ldots, t_{1234}) \\ &= \left(0, 0, 0, 0, 0, -1, 0, -1, \frac{2}{3}, -1, \eta_4, \frac{4}{3}\eta_4, \eta_4, -\frac{2}{3}\eta_4, \frac{1}{3}\right), \end{aligned}$$

where $\eta_4^2 - 2 = 0$. The induced trace tuple for $H_1 = \langle a_2, a_3, a_4 \rangle$ is

$$\theta := (t_2, t_3, t_4, t_{23}, t_{24}, t_{34}, t_{234}) = \left(0, 0, 0, -1, \frac{2}{3}, -1, -\frac{2}{3}\eta_4\right).$$

We determine the isomorphism type of H_1. By Proposition 6.3, H_1 is dihedral if and only if $t_{234} = 0$, that is, if and only if $2 \mid q$. The alternating group of degree 4 is not generated by involutions, and using the methods of Section 9 it is easy to check that $H_1 \cong \mathrm{S}_4$ if and only if $5 \mid q$; furthermore, $H_1 \ncong \mathrm{A}_5$ for all q. So if $(q, 30) = 1$, then H_1 is of L_2-type. More precisely, if $X^2 - 2$ has a solution mod p, then $\eta_4 \in \mathbb{F}_p$, so $H_1 = \mathrm{PSL}(2, p)$. If $X^2 - 2$ has no solution mod p, then η_4 is a generator of $\mathbb{F}_{p^2}/\mathbb{F}_p$, and the Galois group acts by the automorphism α which maps η_4 to $-\eta_4$. In particular, ${}^{\alpha}\theta = {}^{\sigma}\theta$ for $\sigma = (-1, -1, -1)$, so $H_1 = \mathrm{PGL}(2, p)$ by Proposition 7.2.

We now determine the isomorphism type of H. If $2 \mid q$, then H is dihedral; in fact, in this case $\eta_4 = 0$, so $t \in \mathbb{F}_2^{15}$, that is, $H = \mathrm{PSL}(2, 2) = \mathrm{S}_3 = H_1$. If $X^2 - 2$ has a solution mod p, then $H = \mathrm{PSL}(2, p)$; otherwise, ${}^{\alpha}t = {}^{s}t$ for $s = (-1, -1, -1, -1)$ with α as above, hence $H = \mathrm{PGL}(2, p)$. In any case, unless $5 \mid q$ we see $H = H_1$, so the generating set does not satisfy the intersection property. We compute the realization

$$A = \left(\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 4\eta_4 + 2 \\ 4\eta_4 + 3 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2\eta_4 + 2 \\ 2\eta_4 + 3 & 0 \end{pmatrix} \right) \in \mathrm{SL}(2, 5^2)^4$$

of the unique trace tuple in characteristic 5, and it is easy to check that the induced projective tuple satisfies the intersection property. □

In this way, the L_2-quotient algorithm can be used in the classification of all C-group representations of $\mathrm{L}_2(q)$ and $\mathrm{PGL}(2, q)$ of rank 4 ([CJL14]).

13 Acknowledgments

I thank Eamonn O'Brien for comments on an early version of the paper.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BH95] G. W. Brumfiel and H. M. Hilden. SL(2) *representations of finitely presented groups*, volume 187 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1995.

[CHN11] Marston Conder, George Havas, and M. F. Newman. On one-relator quotients of the modular group. In *Groups St Andrews 2009 in Bath. Volume 1*, volume 387 of *London Math. Soc. Lecture Note Ser.*, pages 183–197. Cambridge Univ. Press, Cambridge, 2011.

[CJL14] Thomas Connor, Sebastian Jambor, and Dimitri Leemans. C-groups of $\mathrm{PSL}(2, q)$ and $\mathrm{PGL}(2, q)$. Preprint, 2014.

[Con92] Marston Conder. Group actions on the cubic tree. *J. Algebraic Combin.*, 1(3):209–218, 1992.

[Cox39] H. S. M. Coxeter. The abstract groups $G^{m,n,p}$. *Trans. Amer. Math. Soc.*, 45(1):73–150, 1939.

[Don92] Stephen Donkin. Invariants of several matrices. *Invent. Math.*, 110(2):389–401, 1992.

[Dre03] Vesselin Drensky. Defining relations for the algebra of invariants of 2×2 matrices. *Algebr. Represent. Theory*, 6(2):193–214, 2003.

[EJ08] M. Edjvet and A. Juhász. The groups $G^{m,n,p}$. *J. Algebra*, 319(1):248–266, 2008.

[Fab09] Anna Fabiańska. *Algorithmic analysis of presentations of groups and modules*. PhD thesis, RWTH Aachen University, 2009.

[FK65] Robert Fricke and Felix Klein. *Vorlesungen über die Theorie der automorphen Funktionen. Band 1: Die gruppentheoretischen Grundlagen. Band II: Die funktionentheoretischen Ausführungen und die Andwendungen*, volume 4 of *Bibliotheca Mathematica Teubneriana, Bände 3*. Johnson Reprint Corp., New York, 1965.

[GLGO06] S. P. Glasby, C. R. Leedham-Green, and E. A. O'Brien. Writing projective representations over subfields. *J. Algebra*, 295(1):51–61, 2006.

[HH10] George Havas and Derek F. Holt. On coxeter's families of group presentations. *J. Algebra*, 324(5):1076–1082, 2010.

[Hor72] Robert D. Horowitz. Characters of free groups represented in the two-dimensional special linear group. *Comm. Pure Appl. Math.*, 25:635–649, 1972.

[HR94] Derek F. Holt and Sarah Rees. Testing modules for irreducibility. *J. Austral. Math. Soc. Ser. A*, 57(1):1–16, 1994.

[Jam11] Sebastian Jambor. Computing minimal associated primes in polynomial rings over the integers. *Journal of Symbolic Computation*, 46(10):1098–1104, 2011.

[Jam14] Sebastian Jambor. Determining Aschbacher classes using characters. 2014, arXiv:1402.6395.

[Mac69] A. M. Macbeath. Generators of the linear fractional groups. In *Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967)*, pages 14–32. Amer. Math. Soc., Providence, R.I., 1969.

[Mag80] Wilhelm Magnus. Rings of Fricke characters and automorphism groups of free groups. *Math. Z.*, 170(1):91–103, 1980.

[PF09] Wilhelm Plesken and Anna Fabiańska. An L_2-quotient algorithm for finitely presented groups. *J. Algebra*, 322(3):914–935, 2009.

[Pro76] C. Procesi. The invariant theory of $n \times n$ matrices. *Advances in Math.*, 19(3):306–381, 1976.

[Pro84] C. Procesi. Computing with 2×2 matrices. *J. Algebra*, 87(2):342–359, 1984.

[Sim94] Charles C. Sims. *Computation with finitely presented groups*, volume 48 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994.

[Suz82] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

[Vog89] H. Vogt. Sur les invariants fondamentaux des équations différentielles linéaires du second ordre. *Ann. Sci. École Norm. Sup. (3)*, 6:3–71, 1889.

[Whi73] Alice Whittemore. On special linear characters of free groups of rank $n \geq 4$. *Proc. Amer. Math. Soc.*, 40:383–388, 1973.

Department of Mathematics
The University of Auckland
Prive Bag 92019
Auckland
New Zealand
E-mal address: `s.jambor@auckland.ac.nz`