The M"obius Function of the Suzuki Groups, with Applications to Enumeration

Martin Downs and Gareth A. Jones
School of Mathematics
University of Southampton
Southampton SO17 1BJ, U.K.
G.A.Jones@maths.soton.ac.uk

Abstract

We compute the M"obius function for the subgroup lattice of the simple Suzuki group $Sz(q)$; this is used to enumerate normal subgroups of certain Hecke groups with quotients isomorphic to $Sz(q)$.

MSC classification: 20G41 (primary); 05A99, 11A25, 14H57, 20B20, 20H10 (secondary).

Key words: Suzuki group, M"obius function, subgroup lattice, Hecke group.

1 Introduction

Hall’s theory of M"obius inversion in groups \cite{Hall} allows one to enumerate various objects associated with a given finite group $G$. For example, using this method one can compute the number of normal subgroups $N$ of the free group $F_k$ of finite rank $k$ with $F_k/N \cong G$, or equivalently the number of orbits of $\text{Aut} G$ on generating $k$-tuples for $G$. Indeed, both of these numbers are equal to

$$d_k(G) = \frac{1}{|\text{Aut} G|} \sum_{H \leq G} \mu_G(H)|H|^k$$

(1)

where $\mu_G$ is the M"obius function on the lattice of subgroups of $G$, defined recursively by

$$\sum_{K \geq H} \mu_G(K) = \delta_{H,G}.$$  

(2)

Here $\delta_{H,G}$ is the Kronecker delta function, equal to 1 or 0 as $H = G$ or $H < G$.) As examples of this, $d_2(G)$ gives
• the number of isomorphism classes of orientably regular hypermaps with automorphism group $G$;
• the number of regular unbranched coverings of the sphere minus three points (or of the torus minus one point) with covering group $G$;
• the number of regular dessins (in Grothendieck’s terminology [5]) with automorphism group $G$.

Equation (1) is a particular case of the general result that the number $n_{\Gamma}(G)$ of normal subgroups $N$ of a finitely generated group $\Gamma$ with quotient isomorphic to a given finite group $G$ is given by
\[
 n_{\Gamma}(G) = \frac{|Epi(\Gamma, G)|}{|Aut G|} = \frac{1}{|Aut G|} \sum_{H \leq G} \mu_G(H)|\text{Hom}(\Gamma, H)|,
\]
which arises from applying Möbius inversion to the obvious equation
\[
 |\text{Hom}(\Gamma, G)| = \sum_{H \leq G} |Epi(\Gamma, H)|.
\]

A similar principle applies to the enumeration of torsion-free normal subgroups of $\Gamma$ with quotient $G$: one simply counts the smooth homomorphisms and epimorphisms $\Gamma \to H$, those preserving the orders of torsion elements.

Implementing equation (3), as for some other similar results, for a specific group $G$ depends on knowing the value of $\mu_G(H)$ for each subgroup $H \leq G$. Finding these values can be a laborious task, but once it has been done, equation (3) can be applied to $G$ in many different contexts, depending on the choice of $\Gamma$ (see [4, 12], for example). The function $\mu_G$ has been determined for certain groups $G$, including the simple groups $L_2(p) = \text{PSL}_2(p)$ for primes $p \geq 5$, by Hall in [8]. Subsequently the first author extended this in [1] to the groups $L_2(q)$ and $\text{PGL}_2(q)$ for all prime powers $q$: see [2] for full details for $L_2(2^e)$ and a statement of results for $L_2(q)$ with $q$ odd, and [4] for some applications.

The objective of this paper, which is based on an earlier preprint [3] by the first author, is to calculate the Möbius function $\mu_G$ for the family of simple groups $G = Sz(q) = 2B_2(q)$, where $q = 2^e$ for some odd $e > 1$. These groups were discovered in 1960 by Suzuki [14, 15]. We describe $G$ and its subgroups $H$ in Section 2, and give the values of $\mu_G(H)$ in Table 1 in Section 2.4. Specifically, this table gives the values of $\mu_G(H)$ and $|N_G(H)|$ for a set $\mathcal{T}$ of representatives $H$ of the conjugacy classes of subgroups on which $\mu_G$ can take non-zero values. This information is sufficient for applications of equation (3): since $|Aut G| = e|G|$, this now takes the form
\[
 n_{\Gamma}(G) = \frac{1}{e} \sum_{H \in \mathcal{T}} \frac{\mu_G(H)|\text{Hom}(\Gamma, H)|}{|N_G(H)|}.
\]

For example, it follows that for the Suzuki groups $G$ we have
\[
d_2(G) = \frac{1}{e} \sum_{f \mid e} \mu \left( \frac{e}{f} \right) 2^f (2^{4f} - 2^{3f} - 9),
\]
where $\mu$ is the classical Möbius function on $\mathbb{N}$, given by $\mu(n) = (-1)^k$ if $n$ is a product of $k$ distinct primes, and $\mu(n) = 0$ otherwise. See [5] for this result, and for a number of other applications of Hall’s theory to these groups $G$, and see Section 6 for an application to certain Hecke groups $\Gamma$.

This paper, together with its applications in [5], extends work by Silver and the second author [13], where orientably regular maps of type $\{4, 5\}$ with automorphism group $G \cong Sz(q)$ were enumerated, and by Hubard and Leemans [10], where regular maps and polytopes were enumerated. In each case the authors used a restricted form of Möbius inversion, concentrating mainly on subgroups $H \cong Sz(2f)$ where $f$ divides $e$. Here we compute $\mu_G(H)$ for all subgroups $H \leq G$, allowing the enumeration of a wider range of regular objects, including dessins d’enfants, regular or orientably regular maps and hypermaps, and coverings of topological spaces (see [5]).

The method used for calculating the values of $\mu_G$ is as follows. Hall [8, Theorem 2.3] showed that, in any finite group $G$, a subgroup $H$ satisfies $\mu_G(H) = 0$ unless $H$ is an intersection of maximal subgroups of $G$. In our case, with $G = Sz(q)$, instead of directly determining the set $\mathcal{I}$ of such intersections, we first describe, in Section 2.3.3, a more convenient set $\mathcal{S}$ of subgroups of $G$ such that every subgroup in $\mathcal{I}$ is conjugate to a subgroup in $\mathcal{S}$ (see Theorem 3.1). Since $\mu_G$ is invariant under conjugation, it sufficient to find its values on $\mathcal{S}$; then the set $\mathcal{T}$ appearing in equation (5) is simply the subset of $\mathcal{S}$ on which $\mu_G$ can take non-zero values.

For each pair of subgroups $H, K \in \mathcal{S}$, we determine in Table 2 (Section 5) the number $N(H; K)$ of conjugates of $K$ containing $H$. Since $\mu_G(K) = 0$ for all $K \not\in \mathcal{S}$, equation (2) gives

$$\mu_G(H) = -\sum_{H < K \in \mathcal{S}} N(H; K)\mu_G(K)$$

(6)

where $H \in \mathcal{S} \setminus \{G\}$. This allows $\mu_G(H)$ to be calculated recursively, starting with $\mu_G(G) = 1$ and then using the values of $\mu_G(K)$ for the subgroups $K \in \mathcal{S}$ properly containing each $H \in \mathcal{S} \setminus \{G\}$.

**Acknowledgements** The authors are grateful to Dimitri Leemans for some very helpful comments on enumeration with Suzuki groups, and to Nikos Kanakis for help in preparing the TeX file.

## 2 The Suzuki groups and their subgroups

This section is based mainly on Suzuki’s description of the groups $Sz(q)$ in [15]; see also [11, §XI.3] and [16, §4.2] for further information. We have largely followed Suzuki’s notation for elements and subgroups, except that we use the symbol $F$ for the subgroup denoted in [15] by $H$ (a Frobenius group of order $q^2(q - 1)$), while we use $H$ for an arbitrary subgroup of $G$. Also, our rule for distinguishing the subgroups $A_1$ and $A_2$ in §2.1 is non-standard.
2.1 The definition of the Suzuki groups

Let $\mathbb{F} = \mathbb{F}(e)$ be the finite field $\mathbb{F}_q$ of $q = 2^e$ elements for some odd $e \geq 1$, and let $\theta$ be the automorphism $\alpha \mapsto \alpha^r$ of $\mathbb{F}$ where $r = \sqrt{2q} = 2^{(e+1)/2}$, so that $\theta^2$ is the Frobenius automorphism $\alpha \mapsto \alpha^2$.

For any $\alpha, \beta \in \mathbb{F}$ let $(\alpha, \beta)$ denote the $4 \times 4$ matrix

$$(\alpha, \beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \alpha^{\theta+1} + \beta & \alpha^\theta & 1 & 0 \\ \alpha^{\theta+2} + \alpha\beta + \beta^\theta & \beta & \alpha & 1 \end{pmatrix}.$$  

Since $(\alpha, \beta)(\gamma, \delta) = (\alpha + \gamma, \alpha\gamma^\theta + \beta + \delta)$, these matrices $(\alpha, \beta)$ form a group $Q = Q(e)$ of order $q^2$, with identity element $(0, 0)$.

For each $\kappa \in \mathbb{F}^* := \mathbb{F} \setminus \{0\}$ let $a_\kappa$ denote the $4 \times 4$ diagonal matrix with diagonal entries $\zeta_i$ where $\zeta_1 = \kappa^{1+\theta}$, $\zeta_2 = \kappa$, $\zeta_3 = \zeta_2^{-1}$ and $\zeta_4 = \zeta_1^{-1}$. These matrices form a cyclic group $A_0 = A_0(e) \cong \mathbb{F}^*$ of order $q - 1$. Since

$$a_\kappa^{-1}(\alpha, \beta)a_\kappa = (\alpha\kappa, \beta\kappa^{1+\theta}),$$

the group $F = F(e)$ generated by $Q$ and $A_0$ in $GL_4(q)$ is a semidirect product of a normal subgroup $Q$ by a complement $A_0$, so it has order $q^2(q - 1)$.

We define $G = G(e)$ to be the subgroup of $GL_4(q)$ generated by $F$ and the $4 \times 4$ matrix with entries $1$ on the minor diagonal and $0$ elsewhere (denoted by $\tau$ in [15]). This is the Suzuki group associated with $\mathbb{F}_q$, usually denoted by $Sz(q)$ or $2B_2(q)$. It is, in fact, the subgroup of the symplectic group $Sp_4(q) = B_2(q)$ fixed by a certain automorphism of order 2.

In its natural action $g : [v] \mapsto [vg]$ on the projective space $\mathbb{P}^3(\mathbb{F})$, $G$ acts as a doubly transitive permutation group of degree $q^2 + 1$ on the ovoid

$$\Omega = \Omega(e) = \{[\alpha^{\theta+2} + \alpha\beta + \beta^\theta, \beta, \alpha, 1] \mid \alpha, \beta \in \mathbb{F}\} \cup \{\infty\} \subset \mathbb{P}^3(\mathbb{F}),$$

where

$$\infty := [1, 0, 0, 0] \in \mathbb{P}^3(\mathbb{F}).$$

The subgroup $G_\infty$ of $G$ fixing $\infty$ is $F$. This acts as a Frobenius group on $\Omega \setminus \{\infty\}$: its Frobenius kernel is $Q$, acting regularly on $\Omega \setminus \{\infty\}$, and $A_0$ is a Frobenius complement $G_\infty, \omega$, fixing a second point

$$\omega := [0, 0, 0, 1] \in \Omega$$

and acting semiregularly on $\Omega \setminus \{\infty, \omega\}$. Thus the stabiliser of any three points in $\Omega$ is the identity subgroup $I$, so $G$ acts on $\Omega$ as a Zassenhaus group.

There are cyclic subgroups of $G$ of mutually coprime odd orders

$$2^e \pm 2^{(e+1)/2} + 1 = q \pm r + 1,$$
contained in Singer subgroups of $GL_4(q)$: note that since $r = \sqrt{2q}$,

$$(q + r + 1)(q - r + 1) = q^2 + 1,$$

which divides $q^4 - 1$. Let us choose a pair of subgroups $A_1 = A_1(e), A_2 = A_2(e)$ of $G$ of these two orders, indexed according to the rule

$$|A_1(e)| = a_1(e) := 2^e + \chi(e)2^{(e+1)/2} + 1,$$

$$|A_2(e)| = a_2(e) := 2^e - \chi(e)2^{(e+1)/2} + 1,$$

where $\chi(e) = 1$ or $-1$ as $e \equiv \pm 1$ or $\pm 3$ mod (8). (This rule for indexing $A_1$ and $A_2$ differs from that used in [11, 15], where the rule is that $|A_1(e)| > |A_2(e)|$ for all $e$; the rule adopted here has an advantage which will be explained in §2.3.1.)

### 2.2 Basic properties of Suzuki groups

Here we record some basic properties of $G$; see [11, 15] for proofs.

1. $G$ has order $q^2(q^2 + 1)(q - 1)$, and is simple if $e > 1$. (The group $G(1)$ is isomorphic to $AGL_1(5)$, of order 20.)

2. $\text{Aut } G$ is a semidirect product of $\text{Inn } G \cong G$ by a cyclic group of order $e$ acting as the Galois group $\text{Gal } F$ on matrix entries, so $|\text{Aut } G| = e|G|$.

3. Any two subgroups of $G$ conjugate to $Q$ intersect trivially, and any two subgroups conjugate to $F$ have their intersection conjugate to $A_0$.

4. $Q$ is a Sylow 2-subgroup of $G$ of order $q^2$ and of exponent 4. The centre $Z$ of $Q$ consists of the identity and the involutions of $Q$ (the matrices $(0, \beta)$ for $\beta \in F$), with $Z$ and $Q/Z$ elementary abelian of order $q$.

5. $ZA_0 \cong F/Z \cong AGL_1(q)$, with $A_0$ acting regularly by conjugation on the non-identity elements of $Z$ and of $Q/Z$.

6. The involutions of $G$ are all conjugate, as are the cyclic subgroups of order 4; however an element of order 4 is not conjugate to its inverse.

7. All elements of $G$ except those in a conjugate of $Q$ have odd order. Each maximal cyclic subgroup of $G$ of odd order is conjugate to $A_0$, $A_1$ or $A_2$; the intersection of any two of them is trivial.

8. A non-identity element of $G$ has two fixed points on $\Omega$, one fixed point, or none as it is conjugate to an element of $A_0$, of $Q$ or of $A_i$ for $i = 1, 2$, or, equivalently, as it has order dividing $q - 1, 4$ or $q^2 + 1$. 

5
2.3 Some particular subgroups

Here we list some particular subgroups of $G$, in the anticipation that any subgroup $H$ not conjugate to a member of the list satisfies $\mu_G(H) = 0$, and can therefore be ignored in the enumerations mentioned in Section 1. This list enables us to give a statement of all values of the Möbius function, prior to proving it.

2.3.1 Subgroups associated with subfields

If $f$ divides $e$ then restricting matrix entries to the subfield $\mathbb{F}(f)$ of $\mathbb{F}$ of order $2^f$ yields a subgroup $G(f) = Sz(2^f)$ of $G$. This acts doubly transitively, with degree $2^{2f} + 1$, on the subset $\Omega(f)$ of $\Omega$ defined over $\mathbb{F}(f)$. Since the point $\infty$ is defined over the prime field $\mathbb{F}(1)$, its stabiliser in $G(f)$ is $F(f) := F \cap G(f)$, which acts faithfully on $\Omega(f) \setminus \{\infty\}$ as a Frobenius group with kernel $Q(f) := Q \cap G(f) = \{ (\alpha, \beta) | \alpha, \beta \in \mathbb{F}(f) \}$ and complement $A_0(f) := A_0 \cap G(f) = \{ a_\kappa | \kappa \in \mathbb{F}(f)^* \}$. (Note that since $r$ and $r+1$ are coprime to $q-1$, we have $a_\kappa \in G(f)$ if and only if $\kappa \in \mathbb{F}(f)^*$. ) Let $Z(f)$ denote the centre of $Q(f)$, an elementary abelian group of order $2^f$. If $f$ and $h$ are divisors of $e$, and $f$ divides $h$, then

$$G(f) \leq G(h), \ F(f) \leq F(h), \ Q(f) \leq Q(h), \ Z(f) \leq Z(h), \ A_0(f) \leq A_0(h).$$

Indeed, each of these five families of subgroups forms a lattice isomorphic to the lattice $\Lambda(e)$ of divisors of $e$, a fact which is useful in evaluating $\mu_G$.

Similarly, we would like to choose cyclic subgroups $A_i(f)$ of $G$ of order

$$|A_i(f)| = a_i(f) = 2^f \pm \chi(f)2^{(f+1)/2} + 1$$

corresponding to $A_i$ for each $i = 1, 2$ so that they also satisfy $A_i(f) \leq A_i(h)$ whenever $f$ divides $h$. The following result allows this:

**Lemma 2.1** For each $i = 1, 2$ and each $f$ dividing $e$ there is a cyclic subgroup $A_i(f)$ of $A_i$ of order $a_i(f)$.

**Proof.** Since $A_i$ is cyclic, it is sufficient to show that if $f$ divides $e$ then $a_i(f)$ divides $a_i(e)$ for $i = 1, 2$. Let $m := 2^{2f} + 1 = a_1(f)a_2(f)$. Then $2^e \equiv -2^{j-2} f \mod (m)$ for all $j \geq 2f$, so

$$2^e \equiv -2^{e-2} f \equiv 2^{e-4} f \equiv \cdots \equiv (-1)^{(e-f)/2} f^{2^f} \mod (m)$$

since $e$ is odd. Now $(e - f)/2f$ is even or odd as $e/f \equiv \pm 1 \mod (4)$, giving $2^e \equiv \pm 2^f \mod (m)$ respectively. Similarly,

$$2^{(e+1)/2} \equiv (-1)^k 2^f \mod (m)$$

where

$$k = \lfloor \frac{e+1}{4f} \rfloor \quad \text{and} \quad 0 \leq l = \frac{e+1}{2} - 2kf < 2f.$$


Now $k$ is even if $e/f \equiv 1$ or $3$ mod $(8)$, and odd if $e/f \equiv -1$ or $-3$ mod $(8)$, while $l = (f+1)/2$ or $(3f+1)/2$ as $e/f \equiv \pm 1$ mod $(4)$.

In the case where $e/f \equiv 1$ mod $(8)$, so that $\chi(e) = \chi(f)$, it follows that

$$a_i(e) = 2^e \pm \chi(e)2^{(e+1)/2} + 1 \equiv 2^f \pm \chi(f)2^{(f+1)/2} + 1 = a_i(f) \mod (m)$$

for $i = 1, 2$; since $a_i(f)$ divides $m$ it divides $a_i(e)$. The argument is essentially the same if $e/f \equiv -3$ mod $(8)$, with a change of sign in the coefficient of $2^{(f+1)/2}$ balanced by a change of sign in $\chi(f)$. If $e/f \equiv 3$ or $-1$ mod $(8)$ a similar argument, using the factorisation

$$-2^f \pm 2^{(3f+1)/2} + 1 = (1 \pm 2^{(f+1)/2})(2^f \mp 2^{(f+1)/2} + 1),$$

gives the result. \hfill \Box

In fact, since $A_i$ is cyclic, this shows that if $f \mid h \mid e$ then $A_i(f) \leq A_i(h)$, so for each $i = 1, 2$ the subgroups $A_i(f)$, where $f$ divides $e$, form a lattice isomorphic to $\Lambda(e)$. This explains our non-standard choice of indexing for these two sets of subgroups. Note, however, that $A_i(f)$ is now not necessarily a subgroup of $G(f)$, though it is conjugate to such a subgroup.

### 2.3.2 The normalisers of some subgroups

The normaliser $B_0$ of $A_0$ in $G$ is a dihedral group of order $2(q-1)$; it is the subgroup $G_{\{\infty, \omega\}}$ of $G$ preserving the subset $\{\infty, \omega\}$ of $\Omega$, with its subgroup $A_0$ fixing these two elements and its involutions transposing them. Let us choose a particular involution $c \in B_0$ and, for each $f$ dividing $e$, define

$$B_0(f) := \langle A_0(f), c \rangle \leq B_0,$$

da dihedral group of order $2(2f-1)$ (so $B_0(1) \cong C_2$). If $f > 1$, then $B_0(f)$ is self-normalising whereas the normaliser of $A_0(f)$ is $B_0$.

For $i = 1, 2$ the normaliser $B_i$ of $A_i$ in $G$ is a semidirect product of $A_i$ and a cyclic group of order $4$ generated by an element $c_i$ satisfying $c_i^{-1} ac_i = a^{2^i}$ for all $a \in A_i$. For each $f$ dividing $e$ let

$$B_i(f) := \langle A_i(f), c_i \rangle \leq B_i,$$

so $|B_i(f)| = 4a_i(f)$, with $B_2(1) \cong C_4$. If $i = 1$ or $f > 1$ then $B_i(f)$ is self-normalising, whereas the normaliser of $A_i(f)$ is $B_i$.

By their construction, these groups $B_i(f)$ are (abstract) Frobenius groups of degree $a_i(f)$, and they satisfy $B_i(f) \leq B_i(h)$ for $i = 0, 1$ and $2$ whenever $f \mid h \mid e$.

### 2.3.3 An important set of subgroups

For each $f$ dividing $e$, we have defined the following subgroups of $G$, with the symbols $(f)$ usually omitted when $f = e$:

\[
G(f), \ F(f), \ Q(f), \ Z(f), \ B_i(f), \ A_i(f) \quad (i = 0, 1, 2).
\] (7)
Let \( S \) denote the set consisting of the subgroups in (7) for all \( f \) dividing \( e \). The conjugacy class in \( G \) of any of these groups will be denoted by changing the appropriate italic capital letter to the corresponding script capital; thus \( \mathcal{G}(f), \mathcal{F}, \ldots \) denote the conjugacy classes containing \( G(f), F, \) and so on.

We note the following coincidences, conjugacies (denoted by \( \sim \)) and isomorphisms:

\[
G(1) \sim B_1(1) \cong AGL(5), \quad F(1) = Q(1) \sim B_2(1) \cong C_4,
\]

\[
B_0(1) \sim Z(1) \cong C_2, \quad A_2(1) = A_0(1) = I.
\]

In addition, if 3 divides \( e \) then

\[
B_1(1) = B_1(3), \quad A_1(1) = A_1(3) \cong C_5.
\]

Apart from these, any two distinct terms in (7) represent non-conjugate subgroups of \( G \). In view of their special role in the following calculations, we will denote the class \( A_2(1) = A_0(1) \) by \( C_1 \), the class \( B_0(1) = Z(1) \) by \( C_2 \), and the class \( F(1) = Q(1) = B_2(1) \) by \( C_4 \), since these consist of the cyclic subgroups of \( G \) of orders 1, 2 and 4.

### 2.4 The Möbius function of a Suzuki group

We can now present the main result of this paper in the form of Table 1, which gives the non-zero values of \( \mu_G(H) \) for the subgroups \( H \) of \( G \); any subgroups \( H \) not appearing in Table 1 (such as \( Q(f) \) and \( Z(f) \) for \( f > 1 \)) satisfy \( \mu_G(H) = 0 \), and can therefore be ignored in applying equations such as (3). Because of the conjugacies listed in §2.3.3, some conjugacy classes appear ‘under an alias’: for instance \( \mathcal{F}(1) \) appears as \( B_2(1) \), and if 3 divides \( e \) then \( G(1) \) and \( B_1(1) \) appear as \( B_1(3) \). In the second column, \( a_i(f) = 2f^t \pm \chi(f)2^{(f+1)/2} + 1 \) for \( i = 1, 2 \) (see [2, 1] and [2, 3, 1]). In the third column, the values of \( |N_G(H)| \) are given for applications of equation (5). In the final column, \( \mu \) is the classical Möbius function on \( \mathbb{N} \), defined by

\[
\sum_{m|n} \mu(m) = \delta_{n,1}
\]

for all \( n \in \mathbb{N} \), with the consequence that \( \mu(n) = (-1)^k \) or 0 as \( n \) is or is not a product of \( k \) distinct primes for some \( k \geq 0 \).

Our aim is to show that the final column of this table is correct, by proving the following theorem:

**Theorem 2.2** Let \( G \) be a Suzuki group \( Sz(2^e) \) for some odd \( e > 1 \), and let \( H \) be a subgroup of \( G \). If \( \mu_G(H) \neq 0 \) then \( \mu_G(H) \) is as given by Table 1.

Note that when \( H \) is the identity subgroup, the value of \( \mu_G(H) \) is \( |G|\mu(e) \), supporting a conjecture of Conder that this value is divisible by \( |G| \) whenever \( G \) is an almost simple group, that is, \( S \leq G \leq \text{Aut} S \) for some non-abelian finite simple group \( S \). By [2, 3] this is true when \( G = L_2(q) \) or \( PGL_2(q) \), and computer calculations have verified the conjecture when \( S \) is one of the smaller alternating or sporadic simple groups.
### Table 1: Information about the subgroups $H$ with non-zero values for $\mu_G(H)$

| Conjugacy class of $H$ | $|H|$ | $|N_G(H)|$ | $\mu_G(H)$ |
|------------------------|------|----------|------------|
| $G(f)$, $1 < f | e$   | $2^{2j}(2^{2j} + 1)(2^j - 1)$ | $|H|$ | $\mu(e/f)$ |
| $F(f)$, $1 < f | e$   | $2^{2j}(2^j - 1)$ | $|H|$ | $-\mu(e/f)$ |
| $B_0(f)$, $1 < f | e$ | $2(2^j - 1)$ | $|H|$ | $-\mu(e/f)$ |
| $A_0(f)$, $1 < f | e$ | $2^j - 1$ | $2(q - 1)$ | $2^{(2^j - 1)/2} \mu(e/f)$ |
| $B_1(f)$, $1 < f | e$ | $4a_1(f)$ | $|H|$ | $-\mu(e/f)$ |
| $B_2(f)$, $1 < f | e$ | $4a_2(f)$ | $|H|$ | $-\mu(e/f)$ |
| $B_2(1) = C_4$     | 4    | $2q$     | $-2^{e-1} \mu(e)$ |
| $B_0(1) = C_2$     | 2    | $q^2$    | $-2^{e-1} \mu(e)$ |
| $A_0(1) = C_1$     | 1    | $|G|$     | $|G| \mu(e)$ |

3 **Subgroups $H$ with $\mu_G(H) \neq 0$**

As a first step towards proving Theorem 2.2 in this section we find some necessary conditions for a subgroup $H$ of $G$ to satisfy $\mu_G(H) \neq 0$.

3.1 **Maxint subgroups**

If $G$ is any finite group, we shall say that a subgroup $H$ of $G$ is maxint if it is the intersection of a set of maximal subgroups of $G$ (when $H = G$ this set is empty). The set of maxint subgroups of $G$ will be denoted by $\mathcal{I}$. Hall proved in [8, Theorem 2.3] that if $H \notin \mathcal{I}$ then $\mu_G(H) = 0$, so in determining $\mu_G$ one may restrict attention to the subgroups $H \in \mathcal{I}$.

Since $\mu_G$ is preserved under conjugacy, it is sufficient to consider a set of representatives of the conjugacy classes of subgroups in $\mathcal{I}$. The main step in the proof of Theorem 2.2 is to show that if $G$ is a Suzuki group $G(e)$ then the set $\mathcal{S}$ defined in §2.3.3 contains such a set of representatives:

**Theorem 3.1** If $H \in \mathcal{I}$ then $H$ is conjugate in $G$ to a subgroup in $\mathcal{S}$, that is, $\mathcal{I}$ is contained in the union of the conjugacy classes

$$G(f), F(f), Q(f), Z(f), B_i(f), A_i(f)$$

of subgroups of $G$, where $f$ divides $e$ and $i = 0, 1$ or 2.

The rest of this section is devoted to a proof of this theorem. We will use the following criterion for a subgroup $H$ of $G$ to be in $\mathcal{I}$. Let $\mathcal{M}$ denote the set of all maximal subgroups of $G$, and let $\mathcal{M}(H)$ denote the set of those containing a particular subgroup $H$ of $G$. Then the following, valid for any finite group $G$, is evident:
Lemma 3.2  Let $H \leq G$. Then

$$H \leq \bigcap_{M \in \mathcal{M}(H)} M,$$

with equality if and only if $H \in \mathcal{I}$.

3.2 Maximal subgroups

We will systematically apply Lemma 3.2 to the various subgroups $H$ of $G$, using the following result:

Proposition 3.3  The set $\mathcal{M}$ of maximal subgroups of $G$ is given by

$$\mathcal{M} = \bigcup_{e/f \text{ prime}} \mathcal{G}(f) \cup \mathcal{F} \cup \mathcal{B}_0 \cup \mathcal{B}_1 \cup \mathcal{B}_2.$$

This result is an immediate consequence of the following classification, due to Suzuki [15, Theorems 9 and 10]:

Proposition 3.4  If $H \leq G$ then either $H \in \mathcal{G}(f)$ for some $f$ dividing $e$, or $H$ is a subgroup of a group in $\mathcal{F}$ or in $\mathcal{B}_i$ for some $i = 0, 1$ or 2.

In the first case $H$ is either simple or isomorphic to $G(1) \cong AGL_1(5)$, and in the second case $H$ is solvable. Finite solvable groups $H$ all satisfy Hall’s theorems [7] on the existence and conjugacy of Hall $\pi$-subgroups for any set $\pi$ of primes, generalising Sylow’s theorems for single primes. We will use this fact, mainly with $\pi$ the set $2'$ of odd primes.

Since $G(f) \in \mathcal{S}$ for each $f$ dividing $e$, it follows from Proposition 3.4 that, in proving Theorem 3.1 it is sufficient to assume that $H$ is a subgroup of a group in $\mathcal{F}$ or $\mathcal{B}_i$ for $i = 0, 1$ or 2. We will deal with these cases in turn.

In preparation for applying Lemma 3.2 in the first case, we will consider how the various maximal subgroups of $G$ intersect $F$.

3.3 Point-stabilisers in maximal subgroups

Recall that $F$ is the stabiliser in $G$ of the point $\infty \in \Omega$. If $H \leq F$ then

$$\bigcap_{M \in \mathcal{M}(H)} M = \bigcap_{M \in \mathcal{M}(H)} (M \cap F),$$

so in applying Lemma 3.2 to $H$ one can restrict attention to the stabilisers $M_{\infty} = M \cap F$ of $\infty$ for the various maximal subgroups $M$ of $G$. The following result describes the possibilities for these stabilisers.

Lemma 3.5  Let $M$ be a maximal subgroup of $G$.

1. If $M = F^g \in \mathcal{F}$, then $M \cap F = F$ or $M \cap F = G_{\infty, \infty, g} \in \mathcal{A}_0$ as $g \in F$ or not.
2. If $M = G(f)^q \in \mathcal{G}(f)$ for some $f|e$, then $M \cap F = F(f)^q \in \mathcal{F}(f)$ or $M \cap F = I \in C_1$ as $g \in G(f)F$ or not.

3. If $M \in \mathcal{B}_0$ then $M \cap F \in \mathcal{A}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2$.

4. If $M \in \mathcal{B}_i$ for $i = 1, 2$ then $M \cap F \in \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_4$.

In order to prove part (2), we first need the following lemma:

**Lemma 3.6** If $f$ divides $e$ then $G(f)$ acts semi-regularly on $\Omega \setminus \Omega(f)$.

**Proof.** By §2.2(8), a non-identity element of $G$ fixes 2, 1 or 0 elements of $\Omega$ as it has order dividing $q - 1, 4$ or $q^2 + 1$. Similarly, a non-identity element of $G(f)$ fixes 2, 1 or 0 elements of $\Omega(f)$ as it has order dividing $2^f - 1, 4$ or $2^{2f} + 1$ respectively. Since $2^f - 1$ divides $q - 1$, and $2^{2f} + 1$ divides $q^2 + 1$, a non-identity element of $G(f)$ can have no further fixed points in $\Omega \setminus \Omega(f)$. Thus all orbits of $G(f)$ on this set are regular, with point-stabilisers $G(f) \cap G_\alpha = I$ for $\alpha \in \Omega \setminus \Omega(f)$. □

**Proof of Lemma 3.6** The maximal subgroups $M$ of $G$ are given by Proposition 3.3.

1. This part is trivial, since $F$ and $M$ are the stabilisers in $G$ of $\infty$ and $\infty g$, and $G$ is doubly transitive on $\Omega$.

2. If $M = G(f)^q \in \mathcal{G}(f)$ then Lemma 3.6 shows that $M$ acts doubly transitively on $\Omega(f)g$, and semiregularly on its complement. Thus $M \cap F = F(f)^q$ or $I$ as $\infty \in \Omega(f)g$ or not, that is, as $g \in G(f)F$ or not.

3. Each $M \in \mathcal{B}_0$ is the subgroup $G_{\{\alpha, \beta\}}$ of $G$ preserving an unordered pair $\{\alpha, \beta\} \subset \Omega$. If $\infty \notin \{\alpha, \beta\}$ then since $G_{\alpha, \beta, \infty} = I$ we have $|M \cap F| \leq 2$, whereas if $\infty = \alpha$ or $\beta$ then $M \cap F = G_{\alpha, \beta} \in \mathcal{A}_0$.

4. If $M \in \mathcal{B}_i$ for $i = 1$ or 2 then $M = N_{G(A)} \cong A \times C_4$ for some $A \in \mathcal{A}_i$; since $A$ acts without fixed points, $M \cap F$ is isomorphic to a subgroup of $C_4$, so it is in $C_m$ for $m = 1, 2$ or 4. □

### 3.4 Subgroups $H$ of $F$

We first prove Theorem 3.1 for subgroups $H \in \mathcal{I}$ which are contained in groups in $\mathcal{F}$. Replacing $H$ with a conjugate, we may assume that $H \leq F$.

#### 3.4.1 Preliminaries

Here we record some observations and simplifications which will be used in the proof.

(a) Lemma 3.3 shows that each $M \in \mathcal{M}(H)$ satisfies $M \cap F \in \mathcal{X}_M$ where $\mathcal{X}_M = \mathcal{F}(f_M)$ for some $f_M$ dividing $e$ (depending on $M$), or $\mathcal{X}_M = \mathcal{A}_0$, or $\mathcal{X}_M = \mathcal{C}_m$ for some $m$ dividing 4. If $\mathcal{X}_M = \mathcal{C}_m$ for some $m$, then since $H \leq M \cap F$ we have $H \in \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_4$, so $H$ is as required, i.e. conjugate to an element of $\mathcal{S}$; we may therefore assume that for each $M \in \mathcal{M}(H) \setminus \{F\}$ we have $\mathcal{X}_M = \mathcal{F}(f_M)$ for some $f_M$ or $\mathcal{X}_M = \mathcal{A}_0$, with $M \in \mathcal{G}(f_M)$ or $\mathcal{F}$ respectively.
(b) Since $F$ is solvable, Hall’s theorems \([7]\) imply that a Hall $2'$-subgroup $A$ of $H$ is contained in one of the Hall $2'$-subgroups of $F$. These are the conjugates of $A_0$, and $Q$ permutes them regularly by conjugation, so by conjugating $H$ with a suitable element of $Q$ we may assume that $A \leq A_0$.

(c) If $H$ has even order it contains an involution. The involutions in $F$ (the non-identity elements of $Z$) are all conjugate under $A_0$, so in this case, by conjugating $H$ with an element of $A_0$ we may also assume that $H$ contains $z := (0, 1)$.

(d) If any $M \in \mathcal{M}(H) \setminus \{F\}$ satisfies $M = G(f_M)^g \in G(f_M)$ for some $g \in G$, then since $M \cap F \in F(f_M)$ we have $g \in G(f_M)F$ by Lemma 3.5. Without loss of generality we can therefore choose this conjugating element $g$ to be in $F$. Then

$$F(f_M)^g = (G(f_M) \cap F)^g = G(f_M)^g \cap F = M \cap F.$$  

Thus $z \in M \cap F$, so $z^{g^{-1}} \in F(f_M)$. Since $F = A_0Q$ we can write $g = ab$ where $a \in A_0$ and $b \in Q$. Since $z$ is in the centre $Z$ of $Q$ we have

$$z^{g^{-1}} = (z^{b^{-1}})^{a^{-1}} = z^{a^{-1}},$$

so $z^{a^{-1}} \in F(f_M)$. Since $z \in F(1)$ and $A_0$ acts regularly by conjugation on the involutions in $Z$, this implies that $a \in A_0(f_M)$. Thus $g = ab$ with $a \in F(f_M)$, so each $M \in \mathcal{M}(H) \setminus \{F\}$ satisfies

$$M \cap F = F(f_M)^g = F(f_M)^b$$

for some $f_M$ dividing $e$, with $b \in Q$.

(e) We claim that if $f \mid h \mid e$ then the set

$$Q(f, h) := \{g \in Q \mid Q(f)^g \leq Q(h)\}$$

is the union of the cosets $(\alpha, 0)Z$ of $Z$ in $Q$ where $\alpha \in \mathbb{F}(h)$.

Clearly this set consists of complete cosets of $Z$ in $Q$. The elements $(\alpha, 0)$ where $\alpha \in \mathbb{F}$ are representatives of these cosets, since there is an epimorphism $(\alpha, \beta) \mapsto \alpha$ from $Q$ to the additive group of $\mathbb{F}$, with kernel $Z$. Therefore it suffices to show that $g := (\alpha, 0) \in Q(f, h)$ if and only if $\alpha \in \mathbb{F}(h)$.

If $\alpha \in \mathbb{F}(h)$ then $g \in Q(h)$; since $Q(f) \leq Q(h)$ we have $Q(f)^\alpha \leq Q(h)$ and hence $g \in Q(f, h)$. For the converse, note that $(1, 0) \in Q(f)$. A simple calculation shows that

$$(1, 0)^g = (1, \alpha + \alpha^\theta),$$

so if $g \in Q(f, h)$ then $\alpha + \alpha^\theta \in \mathbb{F}(h)$. The function $\phi : x \mapsto x + x^\theta$ maps each subfield $\mathbb{K}$ of $\mathbb{F}$ into itself. Composing $\phi$ with itself gives a quadratic polynomial

$$\phi^2 : x \mapsto (x + x^\theta) + (x + x^\theta)^\theta = x + x^{\theta^2} = x + x^2$$

defined over the prime field, so if $\beta \in \mathbb{K}$ then any element of $\phi^{-2}(\beta)$ has degree at most 2 over $\mathbb{K}$. Since $\epsilon$ is odd, $\mathbb{F}$ contains no quadratic extensions, so $\phi^{-2}(\mathbb{K}) \subseteq \mathbb{K}$ and hence $\phi^{-1}(\mathbb{K}) \subseteq \mathbb{K}$. In particular, since $\phi(\alpha) \in \mathbb{F}(h)$ we have $\alpha \in \mathbb{F}(h)$.

We can now start the case-by-case analysis of maxint subgroups $H \leq F$. 

12
3.4.2 Subgroups $H \leq F$ which are not 2-groups

First suppose that $H$ is not a 2-group, or equivalently the Hall 2'-subgroup $A \leq A_0$ of $H$ is not the identity subgroup, so that $C_G(A) = A_0$. For each $M \in \mathcal{M}$, $A$ is contained in a maximal cyclic subgroup $A_M$ of $M$, which has order $2^{fM}-1$ if $M \in \mathcal{G}(f)$, and order $2^k - 1$ if $M \in \mathcal{F}$. This subgroup $A_M$ centralises $A$, so it is contained in $A_0$; thus $A = A_0(f_M)$, where we take $f_M = e$ when $M \in \mathcal{F}$, since this is the unique subgroup of $A_0$ of order $2^{fM}-1$. Now $H$ is the intersection of these subgroups $M$, so $A$ is the intersection of the corresponding subgroups $A_M$; it therefore has the form $A = A_0(f)$ where $f$ is the highest common factor of the divisors $f_M$ of $e$.

If $H$ has odd order then this gives $H = A \in A_0(f)$, one of the types allowed for in Theorem 3.1, so we may assume that $H$ has even order. As noted in §3.4.1(c), this allows us to assume that $z \in H$. This also implies that each $M \in \mathcal{M}(H) \setminus \{F\}$ is in $\mathcal{G}(f_M)$ for some $f_M$, for otherwise $M \in \mathcal{F}$ and so $H$ is a subgroup of a two-point stabiliser $M \cap F$, which has odd order. As shown in §3.4.1(d), it follows that such subgroups $M$ satisfy $M \cap F = F(f_M)^b$ for some $b \in Q$.

We have $A_0(f_M) = A \leq A_M \leq M \cap F = F(f_M)^b$, so $A_0(f_M)$ and $A_0(f_M)^{b^{-1}}$ are both point-stabilisers in $F(f_M)$; because $F(f_M)$ acts as a Frobenius group on $\Omega(f)$, its kernel $Q(f_M)$ permutes these point-stabilisers regularly by conjugation, so $A_0(f_M) = A_0(f_M)^{b^{-1}c}$ for some $c \in Q(f_M)$. Thus the element $b^{-1}c$ of $Q$ normalises $A_0(f_M)$, so it also normalises $C_G(A_0(f_M)) = A_0$. However, $Q$ permutes the conjugates of $A_0$ regularly by conjugation (since it is also a Frobenius group), so $b^{-1}c = 1$ and hence $b = c \in Q(f_M)$.

Thus $M \cap F = F(f_M)^b = F(f_M)$ for each $M \in \mathcal{M}(H) \setminus \{F\}$, so $H$, being the intersection of such subgroups $F(f_M)$, together with $F$, has the form $F(f) \cap F = F(f)$ for some divisor $f$ of $e$, giving $H \in \mathcal{F}(f)$ as required.

3.4.3 Subgroups $H \leq F$ which are 2-groups

Now suppose that $H$ is a 2-group, so $H \leq Q$. By §3.4.1(a), for each $M \in \mathcal{M}(H) \setminus \{F\}$ either $M \cap F \in \mathcal{F}(f_M)$ for some $f_M$ dividing $e$, or $M \cap F \in A_0$, with $M \in \mathcal{G}(f_M)$ or $\mathcal{F}$ respectively. We may assume that $H \neq I$, so $H$ has even order and hence (as in §3.4.2) the second possibility cannot arise. Thus $M \cap F = F(f_M)^b$ for some $b \in Q$, as shown in §3.4.1(d). As $Q$ is normal in $F$, and is a Sylow 2-subgroup of $F$, we have $M \cap Q = Q(f_M)^b$; comparing centres, we see that $M \cap Z = Z(f_M)^b = Z(f_M)$ since $Z(f_M)$, being central in $Q$, is normalised by $b$. Thus if $H \leq Z$ then

$$H = \bigcap_{M \in \mathcal{M}(H)} M = \bigcap_{M \in \mathcal{M}(H)} (M \cap Z) = \bigcap_{M \in \mathcal{M}(H)} Z(f_M) = Z(f),$$

where $f$ is the highest common factor of the integers $f_M$, so $H \in Z(f)$.

We may therefore assume that $H \nleq Z$, so $H$ contains an element of order 4. Since $F$ has a single conjugacy class of cyclic subgroups of order 4, we may assume that $H$ contains the subgroup $Q(1) = \{1, z, y^\pm 1\}$ where $y := (1,0)$. Then $Q(1) \leq H \leq M \cap Q = Q(f_M)^b$, so by §3.4.1(e) we have $b^{-1} \in (\alpha, 0)Z$ for some $\alpha \in \mathcal{F}(f_M)$. This shows that $M \cap Q =$
\( Q(f_M)^h = Q(f_M) \) for each \( M \in \mathcal{M}(H) \setminus \{F\} \), so taking the intersection over all such \( M \) gives \( H = Q(f) \in \mathcal{Q}(f) \) where \( f \) is the highest common factor of the integers \( f_M \).

### 3.5 Subgroups \( H \) of \( B_i \)

Now suppose that \( H \) is a subgroup of a group in \( B_i \) for some \( i = 0, 1 \) or 2, and is maxint. Without loss of generality we may assume that \( H \leq B_i \).

#### 3.5.1 Subgroups \( H \) of \( B_0 \)

Suppose that \( H \leq B_0 \). The subgroup \( A := H \cap A_0 = H \cap F \) is maxint, since \( H \) is, it is contained in \( F \), and it has odd order, so by an argument in §3.4.2 we see that \( A = A_0(f) \) for some \( f \) dividing \( e \). Now \( H \) contains \( A \) with index at most 2, so either \( H = A_0(f) \), or \( H \) is a dihedral subgroup of \( B_0 \) conjugate (since \( |A_0| \) is odd) to \( B_0(f) \). Thus \( H \) is in \( A_0(f) \) or \( B_0(f) \).

#### 3.5.2 Subgroups \( H \) of \( B_i \) for \( i = 1 \) or 2

Suppose that \( H \leq B_i \) where \( i = 1 \) or 2. Let \( A := H \cap A_i \). If \( |A| = 1 \) then \( H \) is isomorphic to a subgroup of \( B_i/A_i \cong C_4 \), so \( H \) is in \( C_m \) for some \( m = 1, 2 \) or 4. We may therefore assume that \( |A| > 1 \). Any subgroup \( M \in \mathcal{M}(H) \setminus \{B_i\} \) contains \( A \), which has order dividing \( q^2 + 1 \), so it follows from the classification of the maximal subgroups in Proposition 3.3 that \( M \) must be in \( B_i \) or in \( G(f_M) \) for some \( f_M \) dividing \( e \). The first possibility can be dismissed, since distinct subgroups in \( B_i \) have intersections of order dividing 4, so \( M \in G(f_M) \). We can now argue as in §3.4.2, by considering subgroups centralising \( A \), to show that \( A = A_i(f) \) for some \( f \) dividing \( e \).

Now \( |H : A| \) divides \( |B_i : A_i| = 4 \). If \( |H : A| = 1 \) then \( H = A_i(f) \in A_i(f) \), as required. If \( |H : A| = 4 \) then \( H \) is a subgroup of \( B_i \) of order \( 4a_i(f) \); all subgroups of this order are conjugate in \( B_i \) to \( B_i(f) \), so \( H \in B_i(f) \). We will show that the remaining case \( |H : A| = 2 \), where \( |H| = 2a_i(f) \), cannot arise.

In a Suzuki group \( Sz(q) \), any subgroup \( K \) of order \( 2m \), where \( m \) divides \( q^2 + 1 \), is contained in a unique subgroup \( K^* \) of order \( 4m \). (This is because \( A_i < KA_i < B_i \) for \( i = 1 \) or 2, up to conjugacy, and the complements for \( A_i \) in \( B_i \) have mutually trivial intersections.) Applying this to the subgroup \( K = H \), firstly as a subgroup of \( G \), and then as a subgroup of each of the Suzuki subgroups \( M \cong G(f) \) in \( \mathcal{M}(H) \), we see that there is a subgroup \( H^* \leq B_i \), containing \( H \) with index 2, such that \( H^* \leq M \) for all \( M \in \mathcal{M}(H) \). Lemma 3.2 then shows that \( H \notin T \).

This completes the proof of Theorem 3.1. \( \square \)

### 4 Size of conjugacy classes

An important step in proving the statement of the Möbius function of \( G \) in Theorem 2.2 is to determine the number of conjugates of each subgroup \( H \in \mathcal{S} \), equal to the index in
$G$ of its normaliser $N_G(H)$. The orders of some of these normalisers are noted in Table 1.

**Theorem 4.1** Let $f$ divide $e$. Then

1. $N_G(G(f)) = G(f)$ and $|G(f)| = |G|/|G(f)|$;
2. $N_G(F(f)) = F(f)$ and $|F(f)| = |G|/|F(f)|$ if $f > 1$;
3. $|N_G(Q(f))| = 2^{e+f}(2^f - 1)$ and $|Q(f)| = |G|/2^{e+f}(2^f - 1)$ if $f > 1$;
4. $N_G(Z(f)) = QA_0(f)$ and $|Z(f)| = |G|/2^{e-f}(2^f - 1)$ if $f > 1$;
5. $N_G(B_i(f)) = B_i(f)$ and $|B_i(f)| = |G|/|B_i(f)|$ if $i = 1$, or if $i = 0$ or 2 and $f > 1$;
6. $N_G(A_i(f)) = B_i$ and $|A_i(f)| = |G|/|B_i|$ if $i = 1$, or if $i = 0$ or 2 and $f > 1$;
7. $|N_G(B_2(1))| = 2q$ and $|B_2(1)| = q(q^2 + 1)(q - 1)/2$;
8. $|N_G(B_0(1))| = q^2$ and $|B_0(1)| = (q^2 + 1)(q - 1)$.

**Proof.** (1) Let $H = G(f)$ where $f$ divides $e$. If $f > 1$, then since $N_G(G(f))$ contains $G(f)$ it cannot be solvable, so by Proposition 3.4 it must be conjugate to $G(h)$ for some multiple $h$ of $f$. Since $G(h)$ is simple, we must have $h = f$ and $N_G(H) = H$, giving $|G(f)| = |G|/|H|$. The case $f = 1$ is dealt with in (5), since $G(1)$ is conjugate to $B_1(1)$.

(4) It is convenient to prove (4) before (2) and (3). Let $f > 1$. Any element of $G$ normalising $Z(f)$ must fix its unique fixed point $\infty$, so $N_G(Z(f)) \leq F$. By §2.2(4), $F = QA_0$. Now $Z(f)$ is centralised by $Q$ since it lies in the centre $Z$ of $Q$, and §2.2(5) implies that $N_G(Z(f)) \cap A_0 = A_0(f)$, so $N_G(Z(f)) = QA_0(f)$, of order $|Q||A_0(f)| = q^2(2^f - 1) = 2^{e-f}(2^f - 1)$.

(3) Any element of $G$ normalising $Q(f)$ must normalise its characteristic subgroup $Z(f)$, so $N_G(Q(f)) \leq N_G(Z(f)) = QA_0(f)$. Now $A_0(f) \leq F(f) \leq N_G(Q(f))$, and §3.4.1(e) shows that $N_G(Q(f)) = \bigcup_{\alpha \in \mathbb{F}} Z$ with the union over all $\alpha \in \mathbb{F}$, so $N_G(Q(f))$ has order $|Z|2^f|A_0(f)| = 2^{e+f}(2^f - 1)$.

(2) Clearly $N_G(F(f)) \leq N_G(Q(f)) \leq QA_0(f)$, and $A_0(f) \leq N_G(F(f))$. Since $Z$ acts semi-regularly on $\Omega \setminus \{\infty\}$, it acts semi-regularly by conjugation on the subgroups of $F$ in the conjugacy class $A_0$, so $N_G(F(f)) \cap Z = Z(f)$. Hence, using the proof of part (3), we see that $N_G(F(f)) \leq F \cap G(f) = F(f)$. Thus $F(f)$ is self-normalising.

(5, 6) See §2.3.2.

(7, 8) For $i = 0$ and 2 the subgroups in $B_i(1)$ are cyclic groups of orders 2 and 4 respectively, so they are contained in Sylow 2-subgroups of $G$. There are $q^2 + 1$ Sylow 2-subgroups, each conjugate to $Q$ and containing $q - 1$ subgroups of order 2, and containing $(q^2 - q)/2$ of order 4. Since distinct Sylow 2-subgroups have trivial intersection, there are $(q^2 + 1)(q - 1)$ and $(q^2 + 1)(q^2 - q)/2$ such subgroups in $G$. In each case such subgroups are all conjugate, so their normalisers have order $q^2$ and $2q$. \qed
5 Calculating values of $\mu_G$

We can now complete the proof of Theorem 2.2 by calculating $\mu_G(H)$ for each subgroup $H \in S$. In order to use equation (6) for this (see §1), we first need to know, for each pair of subgroups $H, K \in S$, the number $N(H; K)$ of conjugates in $G$ of $K$ containing $H$. If $M(H; K)$ denotes the number of conjugates in $G$ of $H$ contained in $K$, then a simple double counting argument gives

$$M(H; K)M(K; G) = M(H; G)N(H; K)$$

for all $H, K \in S$. This allows $N(H; K)$ to be determined from the values of the function $M$. Now $M(H; G) = |H|$ and $M(K; G) = |K|$, where $H$ and $K$ are the conjugacy classes of subgroups of $G$ containing $H$ and $K$, so these values are given by Theorem 4.1. The values of $M(H; K)$ for $K \neq G$ can be found by using arguments similar to those used in proving Theorem 4.1, so details are omitted.

| $G(h)$ | $F(h)$ | $Q(h)$ | $Z(h)$ | $B_0(h)$ | $A_0(h)$ |
|--------|--------|--------|--------|----------|----------|
| $G(f)$ | 1      |        |        |          |          |
| $F(f)$ | 1      | 1      |        |          |          |
| $Q(f)$ | $2^{e-h}$ | $2^{e-h}$ | 1      |          |          |
| $Z(f)$ | $2^{2(e-h)}$ | $2^{2(e-h)}$ | $2^{e-h}$ | 1        |          |
| $B_0(f)$ | 1      |        |        |          |          |
| $A_0(f)$ | $(2^{e-1})$ | $(2^{e-1})$ | $(2^{e-1})$ | 1        |          |
| $B_1(f), f \geq 1$ | 1      |        |        |          |          |
| $B_2(f)$ | 1      |        |        |          |          |
| $A_1(f), f \geq 1$ | $a_1(h)$ |        |        |          |          |
| $A_2(f)$ | $a_2(h)$ |        |        |          |          |
| $B_2(1) \cong C_4$ | $2^{e-h}$ | $2^{e-h}$ | 1      |          |          |
| $B_0(1) \cong C_2$ | $2^{2(e-h)}$ | $2^{2(e-h)}$ | $2^{e-h}$ | 1        | $2^{2e-1}$ |

Table 2: Values of $N(H; K)$ where $H, K \in S$. 

| $B_1(h)$ | $B_2(h)$ | $A_1(h)$ | $A_2(h)$ | $B_2(1)$ | $B_0(1)$ |
|----------|----------|----------|----------|----------|----------|
| $B_1(f), f \geq 1$ | 1      |        |          |          |          |
| $B_2(f)$ |        | 1      |          |          |          |
| $A_1(f), f \geq 1$ | $a_1(h)$ |        |          |          |          |
| $A_2(f)$ | $a_2(h)$ |        |          |          |          |
| $B_2(1) \cong C_4$ | $2^{e-1}$ | $2^{e-1}$ | 1      |          |          |
| $B_0(1) \cong C_2$ | $2^{2(e-1)}$ | $2^{2(e-1)}$ | $2^{e-1}$ | 1        |          |
The non-zero values of \(N(H; K)\) resulting from \(\mathbb{N}\) are given in Table 2, where the rows and columns are indexed by the subgroups \(H\) and \(K\) respectively; the row corresponding to the identity subgroup \(H = A_0(1) = A_2(1)\) is omitted since in this case \(N(H; K) = |\mathcal{K}|\), given by Theorem 4.1 for all \(K \in \mathcal{S}\). The table is split into two parts, the second part giving further entries for the last six rows of the first part. We assume that \(f\) divides \(h\) and that \(f > 1\) unless otherwise stated. Thus \(G(1)\) is represented by its conjugate \(B_1(1)\), while \(F(1)\) and \(Q(1)\) are represented by \(B_2(1)\), and \(Z(1)\) by \(B_0(1)\) (see §2.3.3 and the comments in §2.4).

Given Table 2, one can systematically use equation (3) to calculate \(\mu_G(H)\) for each \(H \in \mathcal{S}\), starting with \(H = G(f)\) in the first row, and working downwards through the table. For instance, if \(H = G(f)\) then the subgroups \(K \in \mathcal{S}\) with \(N(H; K) \neq 0\) are those of the form \(K = G(h)\) where \(f \mid h \mid e\); under inclusion, these form a lattice isomorphic to the lattice \(\Lambda(e/f)\) of all divisors \(h/f\) of \(e/f\), with \(\mu_G(K) = 1\) when \(h = e\), so we find that \(\mu_G(H) = \mu(e/f)\), as in Table 1. Next, if \(H = F(f)\) we consider the subgroups \(K = G(h)\) and \(F(h)\) where \(f \mid h \mid e\); these form a lattice isomorphic to \(\Lambda(2e/f)\) since \(e\) is odd, giving \(\mu_G(H) = \mu(2e/f) = -\mu(e/f)\). Similar arguments show that if \(f > 1\) then \(\mu_G(B_i(f)) = -\mu(e/f)\) for \(i = 0, 1, 2\), and \(\mu_G(Q(f)) = \mu_G(Z(f)) = \mu_G(A_i(f)) = 0\) for \(i = 1, 2\). This process continues until \(\mu_G(H)\) is evaluated for all \(H \in \mathcal{S}\). The method is essentially the same as that described fully in [2, §4] for the groups \(G = L_2(2^6)\), so the remaining details are omitted.

Since \(\mu_G(H) = 0\) whenever \(H = Q(f), Z(f), A_1(f)\) or \(A_2(f)\) for any \(f > 1\), we may disregard these subgroups, and let \(\mathcal{T}\) denote the remaining set of subgroups \(H \in \mathcal{S}\), namely those of the form

\[
G(f), F(f), B_i(f) \ (i = 0, 1, 2), A_0(f), B_2(1), B_0(1), A_0(1),
\]

where \(1 < f \mid e\). This is a set of representatives for the conjugacy classes in Table 1; by the construction of \(\mathcal{T}\), every subgroup \(H\) of \(G\) with \(\mu_G(H) \neq 0\) must belong to one of these classes. This fact, together with the values of \(|H|, |N_G(H)|\) and \(\mu_G(H)\) determined earlier, justifies the entries in Table 1 and in particular proves Theorem 2.2.

Each conjugacy class in Table 1 contains \(|G|/|N_G(H)|\) subgroups, and \(|\text{Aut } G| = e|G|\) by (2,2,2), so equation (3) takes the form

\[
n_T(G) = \frac{1}{e} \sum_{\Gamma \in \mathcal{T}} \frac{\mu_G(H)|\text{Hom}(\Gamma, H)|}{|N_G(H)|},
\]
as in equation (5). Table 1 gives the values of \(\mu_G(H)\) and \(|N_G(H)|\), so in order to apply this equation to a particular group \(\Gamma\) one needs only to count the homomorphisms \(\Gamma \rightarrow H\) for each \(H \in \mathcal{T}\). We will illustrate this in the case of certain Hecke groups \(\Gamma\) in Section 4.

## 6 Application to Hecke groups

In [2], the first author used Möbius inversion to enumerate the normal subgroups of the modular group \(\Gamma = PSL_2(\mathbb{Z}) \cong C_2 \ast C_3\) with quotient group isomorphic to \(L_2(q)\) for any
given prime power \( q \). There are no normal subgroups of \( \Gamma \) with quotient group \( G = S\ell_2(q) \), since Suzuki groups have no elements of order 3, but instead one can apply the same method to Hecke groups other than \( \Gamma \).

For each integer \( k \geq 3 \) the Hecke group \( H_k \), introduced by Hecke in connection with Dirichlet series \([9]\), is the subgroup of \( \text{PSL}_2( \mathbb{R} ) \) generated by the Möbius transformations

\[
X : z \mapsto z + \lambda_k \quad \text{and} \quad Y : z \mapsto -\frac{1}{z}
\]

of the upper half plane, where \( \lambda_k = 2 \cos(\pi/k) \). This group is a free product of cyclic groups of orders 2 and \( k \) generated by \( Y \) and \( XY \). In particular, \( H_3 \) is the modular group.

The torsion-free normal subgroups of \( H_k \) with a given finite quotient group \( G \) correspond bijectively to the orbits of \( \text{Aut} \ G \) on generating pairs for \( G \) of orders 2 and \( k \). By equation \( (5) \) the number of these orbits is

\[
\frac{1}{|\text{Aut} \ G|} \sum_{H \leq G} \mu_G(H)|H_2||H|_k = \frac{1}{e} \sum_{H \in \mathcal{T}} \mu_G(H)|H_2||H|_k \div |N_G(H)|,
\]

(10)

where \( |H|_n \) is the number of elements of order \( n \) in each subgroup \( H \) of \( G \). Table 3 gives \( |H|_n \) for subgroups \( H \in \mathcal{T} \) in the cases \( n = 2, 4 \) and 5; here \( q = 2^e \) and \( 1 < f \mid e \).

| \( H \)   | \( |H|_2 \)       | \( |H|_4 \)       | \( |H|_5 \)       |
|---------|-----------------|-----------------|-----------------|
| \( G(f) \) | \( (2^f-1)(2^{2f}+1) \) | \( 2^f(2^{2f}+1)(2^f-1) \) | \( 2^{2f}(2^f-1)a_2(f) \) |
| \( F(f) \) | \( 2^f-1 \)      | \( 2^f(2^f-1) \)  | 0               |
| \( B_0(f) \) | \( 2^f-1 \)      | 0               | 0               |
| \( A_0(f) \) | 0               | 0               | 0               |
| \( B_1(f) \) | \( a_1(f) \)    | \( 2a_1(f) \)   | 4               |
| \( B_2(f) \) | \( a_2(f) \)    | \( 2a_2(f) \)   | 0               |
| \( B_2(1) \) | 1               | 2               | 0               |
| \( B_0(1) \) | 1               | 0               | 0               |
| \( A_0(1) \) | 0               | 0               | 0               |

Table 3: Values of \( |H|_n \) for \( n = 2, 4 \) and 5.

With this information, together with Table 1, one finds from equation \( (10) \) that the numbers of (necessarily torsion-free) normal subgroups of \( H_4 \) and of \( H_5 \) with quotient group \( S\ell_2(q) \) are respectively

\[
\frac{1}{e} \sum_{f \mid e} \mu \left( \frac{e}{f} \right) 2^f(2^f - 2)
\]

(11)

and

\[
\frac{1}{e} \sum_{f \mid e} \mu \left( \frac{e}{f} \right) (2^f - 1)a_2(f),
\]

(12)

where \( a_2(f) = |A_2(f)| = 2^f - \chi(f)2^{(f+1)/2} + 1 \) (see \([2,1]\)).
One can apply similar arguments for odd \( k > 5 \). For instance, \( G \) contains elements of order 7 if and only if \( e \) is divisible by 3, in which case they form three conjugacy classes, represented by elements of \( A_0 \). It follows that the number of normal subgroups of \( H_7 \) with quotient group \( Sz(q) \) is

\[
3 \sum_{e \mid f} \mu \left( \frac{e}{f} \right) (2^{2f} - 2). \tag{13}
\]

These enumerations have applications in other areas, such as topological graph theory. For instance, formulae (11), (12) and (13) give the numbers of orientably regular \( k \)-valent maps with automorphism group \( Sz(q) \) for \( k = 4, 5 \) and 7 (see [5] for these and other examples).

References

[1] M. L. N. Downs, PhD thesis, University of Southampton, 1988.

[2] M. L. N. Downs, The Möbius function of \( PSL_2(q) \), with application to the maximal normal subgroups of the modular group, *J. London Math. Soc.* 43 (1991), 61–75.

[3] M. L. N. Downs, The Möbius function of the Suzuki groups, preprint, 1993.

[4] M. L. N. Downs and G. A. Jones, Enumerating regular objects with a given automorphism group, *Discrete Math.* 64 (1987), 299–302.

[5] M. L. N. Downs and G. A. Jones, Enumerating regular objects associated with Suzuki groups, [arXiv:1309.5215][math.GR], 2013.

[6] A. Grothendieck, Esquisse d’un Programme, in *Geometric Galois Actions I, Around Grothendieck’s Esquisse d’un Programme* (ed. P. Lochak and L. Schneps) London Math. Soc. Lecture Note Ser. 242 (Cambridge University Press, Cambridge, 1997), 5–48.

[7] P. Hall, A note on soluble groups, *J. London Math. Soc.* 3 (1928), 98–105.

[8] P. Hall, The Eulerian functions of a group, *Q. J. Math.* 7 (1936), 134–151.

[9] E. Hecke, Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung, *Math. Ann.* 112 (1936), 664–699.

[10] I. Hubard and D. Leemans, Chiral polytopes and Suzuki simple groups, in eds. R. Connelly, W. Whitely, A. Weiss, *Rigidity and Symmetry*, Fields Inst. Commun., to appear, 20 pages.

[11] B. Huppert and N. Blackburn, *Finite Groups III*, Springer-Verlag, Berlin – Heidelberg – New York, 1982.
[12] G. A. Jones, Enumeration of homomorphisms and surface-coverings, *Q. J. Math.* 46 (1995), 485–507.

[13] G. A. Jones and S. A. Silver, Suzuki groups and surfaces, *J. London Math. Soc.* (2) 48 (1993), 117–125.

[14] M. Suzuki, A new type of simple groups of finite order, *Proc. Nat. Acad. Sci. U.S.A.* 46 (1960), 868–870.

[15] M. Suzuki, On a class of doubly transitive groups, *Ann. of Math.* (2) 75 (1962), 105–145.

[16] R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Math. 251, Springer, London, 2009.