On the number of abstract regular polytopes whose automorphism group is a Suzuki simple group Sz(q)

Ann Kiefer and Dimitri Leemans
Université Libre de Bruxelles
Département de Mathématiques - C.P.216
Boulevard du Triomphe
B-1050 Bruxelles

September 27, 2011

Abstract

We determine, up to isomorphism and duality, the number of abstract regular polytopes of rank three whose automorphism group is a Suzuki simple group Sz(q), with q an odd power of 2. No polytope of higher rank exists and, therefore, the formula obtained counts all abstract regular polytopes of Sz(q). Moreover, there are no degenerate polyhedra. We also obtain, up to isomorphism, the number of pairs of involutions.

1 Introduction

In [6], Leemans and Vauthier built an atlas of abstract regular polytopes for small groups. The groups Sz(8) and Aut(Sz(8)) are among the groups analysed. It turns out that, up to isomorphism and duality, Sz(8) has seven polytopes, all of rank three, and that Aut(Sz(8)) has no polytope.

In [3], Leemans proved that, if $G := \mathrm{Sz}(q)$ with $q \neq 2$ an odd power of 2, all the abstract regular polytopes having G as automorphism group are of rank three (and there exists at least one such polytope for each value of q). Moreover, if $\mathrm{Sz}(q) < G \leq \mathrm{Aut}(\mathrm{Sz}(q))$, he showed that G is not a C-group and, therefore, that there cannot exist an abstract regular polytope having G as automorphism group.

In this article, we count, up to isomorphism and duality, the number of polyhedra on which a group Sz(q), with $q = 2^{2e+1}$ and $e > 0$ an integer, acts as a regular flag-transitive automorphism group. To make the proof easier to understand, we split our analysis in two parts. First we look at Sz(q) with q an odd prime power of 2. Then we look at Sz(q) with q an odd power of 2. We first count how many pairs of commuting involutions there are up to isomorphism in a Suzuki simple group. We obtain the following result which is of interest not only for the purpose of this paper, but for group theory in general.

Theorem 1. *Let* $G := \mathrm{Sz}(q)$ *with* $q = 2^{2e+1}$ *and* $e > 0$ *an integer. Up to isomorphism, there are*

$$\frac{1}{2}\sum_{\substack{n|2e+1\\ n\neq 1}} \lambda(n)$$

pairs of commuting involutions in G*, where*

$$\lambda(n) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) \cdot 2^d$$

and μ *is the Möbius function.*

The following result is the main result of this article.

Theorem 2. *Up to isomorphism and duality, a given Suzuki group* $\mathrm{Sz}(q)$*, with* $q = 2^{2e+1}$ *and* $e > 0$ *an integer, acts flag-transitively on*

$$\frac{1}{2}\sum_{2f+1|2e+1} \mu(\frac{2e+1}{2f+1}) \sum_{\substack{n|2f+1\\ n\neq 1}} \lambda(n)\psi(n, 2f+1)$$

polyhedra, where

$$\lambda(n) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) \cdot 2^d \text{ and}$$

$$\psi(n, 2f+1) = \sum_{m|\frac{2f+1}{n}} \frac{\sum_{d|m} \mu(\frac{m}{d})(2^{nd}-1)}{m}.$$

All these polyhedra are non-degenerate, i.e. have a Schläfli symbol with entries ≥ 3.

Observe that Sah [9] and Conder et al. [1] have computed, up to isomorphism, the number of regular hypermaps on which a group of type $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$ acts as a regular automorphism group. We recall that, as seen in [4], the $\mathrm{PSL}(2, q)$ groups act on polytopes of rank at most 4 and that there are only two polytopes of rank 4 having a $\mathrm{PSL}(2, q)$ as flag-transitive regular automorphism group. They are Grünbaum's 11-cells (for $q = 11$) and Coxeter's 57 cells (for $q = 19$). For the $\mathrm{PGL}(2, q)$ groups, the situation is quite similar. In [5], it is shown that these groups act on polytopes of rank at most 4 and that there is a unique polytope of rank 4 having a $\mathrm{PGL}(2, q)$ flag-transitive automorphism group. It is the 4-simplex and the corresponding group is $\mathrm{PGL}(2, 5) \cong Sym(5)$.

Acknowledgements : We thank Wieb Bosma, Francis Buekenhout, Marston Conder and the referees for their interesting comments related to this research. We also acknowledge support by the "Communauté Française de Belgique - Actions de Recherche Concertées".

2 The Suzuki simple groups and their elements

We refer to the definition of the Suzuki groups as given in [7]. The lemmas of this section are all proven in [7] too.

Let $\mathcal{K}$ be a field of characteristic 2 with $\mid \mathcal{K} \mid > 2$. Let σ be an automorphism of $\mathcal{K}$ such that $x^{\sigma^2} = x^2$ for each x in $\mathcal{K}$. Let $\mathcal{B}$ be the 3-dimensional projective space over $\mathcal{K}$ and let (x_0, x_1, x_2, x_3) be the coordinates of a point of $\mathcal{B}$. Let E be the plane defined by the equation $x_0 = 0$ and let $U = (0,1,0,0)\mathcal{K}$. We introduce coordinates in the affine space $\mathcal{B}_E$ by $x = \frac{x_2}{x_0}$, $y = \frac{x_3}{x_0}$ and $z = \frac{x_1}{x_0}$. Finally, let $\mathcal{D}$ be the set of points of $\mathcal{B}$ consisting of U and all those points of $\mathcal{B}_E$ whose coordinates (x, y, z) satisfy the equation

$$z = xy + x^{\sigma+2} + y^{\sigma},$$

where $x^{\sigma+2} = x^{\sigma}x^2$. We denote by $\mathrm{Sz}(\mathcal{K}, \sigma)$ the group of all projective collineations of $\mathcal{B}$ which leave $\mathcal{D}$ invariant.

Lemma 1. *Let $e > 0$ be an integer. If $\mathcal{K}$ is isomorphic to $\mathrm{GF}(2^{2e+1})$, then $\mathcal{K}$ admits exactly one automorphism σ with $x^{\sigma^2} = x^2$ for all x in $\mathcal{K}$. If $\mathcal{K}$ is isomorphic to $\mathrm{GF}(2^{2e})$, then $\mathcal{K}$ does not possess an automorphism σ with $x^{\sigma^2} = x^2$ for all x in $\mathcal{K}$.*

This lemma implies that, if $\mathcal{K}$ is isomorphic to $\mathrm{GF}(q)$ with $q = 2^{2e+1}$, we may write $\mathrm{Sz}(q)$ instead of $\mathrm{Sz}(\mathcal{K}, \sigma)$. The groups $\mathrm{Sz}(q)$ are the Suzuki groups named after Michio Suzuki who found them in 1960. The generalizations $\mathrm{Sz}(\mathcal{K}, \sigma)$, where $\mathcal{K}$ is a field of characteristic 2, not necessarily finite, are due to Rimhak Ree and Jacques Tits (see for instance [11]). The set $\mathcal{D}$ is an ovoid as defined below.

Definition 1. *An ovoid is a non-empty point-set of a projective 3-space that satisfies the following three conditions.*

1. *No three points are collinear;*
2. *If $p \in \mathcal{D}$, there exists a plane E of $\mathcal{B}$ with $\mathcal{D} \cap E = \{p\}$;*
3. *If $p \in \mathcal{D}$ and if E is a plane of $\mathcal{B}$ with $\mathcal{D} \cap E = \{p\}$, then all lines l through p which are not contained in E carry a point of $\mathcal{D}$ distinct from p.*

For $a, b \in \mathcal{K}$, we denote by $\tau(a, b)$ the mapping defined by

$$(x, y, z)^{\tau(a,b)} = (x + a, y + b + a^{\sigma}x, z + ab + a^{\sigma+2} + b^{\sigma} + ay + a^{\sigma+1}x + bx),$$

where σ is the involutory automorphism of $\mathcal{K}$ defined above. It follows that $\tau(a, b)\tau(c, d) = \tau(a + c, ac^{\sigma} + b + d)$. For $k \in \mathcal{K}^*$, we define the collineation $\eta(k)$ by

$$(x, y, z)^{\eta(k)} = (kx, k^{\sigma+1}y, k^{\sigma+2}z).$$

A straightforward computation shows that $\tau(a, b)\eta(k) = \eta(k)\tau(ka, k^{\sigma+1}b)$. Let ω be the collineation of $\mathcal{B}$ defined by $(x_0, x_1, x_2, x_3)^{\omega} = (x_1, x_0, x_3, x_2)$ and write $\mathrm{Sz}(\mathcal{K}, \sigma)_U$ for the stabilizer of U in $\mathrm{Sz}(\mathcal{K}, \sigma)$.

Structure	Order	Index	Description
$(E_q\hat{.}E_q) : C_{q-1}$	$q^2 \cdot (q-1)$	q^2+1	Normalizer of a 2-Sylow, stabilizer of a point of the ovoid.
$D_{2(q-1)}$	$2 \cdot (q-1)$	$\frac{(q^2+1)\cdot q^2}{2}$	Stabilizer of a pair of points of the ovoid.
$C_{\alpha_q} : C_4$	$\alpha_q \cdot 4$	$\frac{q^2(q-1)}{4\beta_q}$	Normalizer of a C_{α_q}.
$C_{\beta_q} : C_4$	$\beta_q \cdot 4$	$\frac{q^2(q-1)}{4\alpha_q}$	Normalizer of a C_{β_q}.
$\mathrm{Sz}(2^{2f+1})$ with $2f+1 \mid_M 2e+1$	$(s^2+1) \cdot s^2 \cdot (s-1)$		

Table 1: The maximal subgroups of $\mathrm{Sz}(q)$

Lemma 2. *Let $\mathcal{K}$ be a commutative field of characteristic 2 with $\mid \mathcal{K} \mid > 2$ and assume that $\mathcal{K}$ admits an automorphism σ such that $x^{\sigma^2} = x^2$ for all $x \in \mathcal{K}$. If $\mathcal{D}$ is the point set defined above in the projective space of dimension 3 over $\mathcal{K}$, then $\mathrm{Sz}(\mathcal{K}, \sigma)$ acts doubly transitively on $\mathcal{D}$. Moreover, if $\gamma \in \mathrm{Sz}(\mathcal{K}, \sigma)_U$, then there exists exactly one triple $(k, a, b) \in \mathcal{K}^* \times \mathcal{K} \times \mathcal{K}$ with $\gamma = \eta(k)\tau(a, b)$, and if $\gamma \in \mathrm{Sz}(\mathcal{K}, \sigma) \backslash \mathrm{Sz}(\mathcal{K}, \sigma)_U$, then there exists exactly one 5-tuple $(k, a, b, c, d) \in \mathcal{K}^* \times \mathcal{K} \times \mathcal{K} \times \mathcal{K} \times \mathcal{K}$ with $\gamma = \eta(k)\tau(a, b)\omega\tau(c, d)$.*

Let $\mathrm{PG}(3, q)$ be the projective space over the field $\mathrm{GF}(q)$ and let $\mathcal{D}$ be an ovoid of $\mathrm{PG}(3, q)$. If Π is a plane of $\mathrm{PG}(3, q)$ such that $\mid \Pi \cap \mathcal{D} \mid > 1$, we call $\Pi \cap \mathcal{D}$ a *circle*. The following lemma ensures that every circle has the same number of points and, moreover, that these circles are ovals.

Lemma 3. *If $\mathcal{D}$ is an ovoid in $\mathrm{PG}(3, q)$, then $\mid \mathcal{D} \mid = q^2 + 1$. If E is a plane of $\mathrm{PG}(3, q)$, then E is either a tangent plane of $\mathcal{D}$ or $E \cap \mathcal{D}$ consists of the $q + 1$ points of an oval of E.*

3 The maximal subgroups of $\mathrm{Sz}(q)$

There are four numbers that play an important role in the subgroup structure of $\mathrm{Sz}(q)$. They are respectively q, $q - 1$, $q + r + 1$ and $q - r + 1$ where $r = \sqrt{2q}$. We write $q + r + 1 =: \alpha_q$ and $q - r + 1 =: \beta_q$. In [2], the following lemma is proven.

Lemma 4. *The numbers $q - 1$, α_q and β_q are pairwise coprime.*

Table 1 gives the maximal subgroups of a Suzuki group. These have been computed by Suzuki in [10]. We write $m \mid_M n$ when m is a proper maximal divisor of n. The groups E_n are elementary abelian groups of order n. The groups C_n are cyclic groups of order n. The groups D_{2n} are dihedral groups of order $2n$. The symbols $\hat{.}$ and : stand for non-split and split extensions.

4 Abstract regular polytopes and string C-groups

Thin regular residually connected geometries with a linear diagram, abstract polytopes and string C-groups are the same mathematical objects. The link between these objects may be found for instance in [8]. We take here the viewpoint of string C-groups because it is the easiest and the most efficient one to define abstract regular polytopes.

As defined for instance in [8], a C-group is a group G generated by pairwise distinct involutions $\rho_0, \ldots, \rho_{n-1}$, which satisfy the following property, called the *intersection property*.

$$\forall J, K \subseteq \{0, \ldots, n-1\}, \langle \rho_j \mid j \in J \rangle \cap \langle \rho_k \mid k \in K \rangle = \langle \rho_j \mid j \in J \cap K \rangle$$

A C-group $(G, \{\rho_0, \ldots, \rho_{n-1}\})$ is a string C-group if its generators satisfy the following relations.

$$(\rho_j \rho_k)^2 = 1_G \; \forall \, j, k \in \{0, \ldots n-1\} \; with \; \mid j-k \mid \geq 2$$

5 Suzuki groups and polytopes

In [3], the following result is proven.

Theorem 3. *Let* $\mathrm{Sz}(q) \leq G \leq \mathrm{Aut}(\mathrm{Sz}(q))$ *with* $q = 2^{2e+1}$ *and* $e > 0$ *an integer. Then* G *is a C-group if and only if* $G = \mathrm{Sz}(q)$*. Moreover, if* $(G, \{\rho_0, \ldots, \rho_{n-1}\})$ *is a string C-group, then* $n = 3$*.*

We may translate this theorem in abstract regular polytope theory. If $\mathrm{Sz}(q) < G \leq \mathrm{Aut}(\mathrm{Sz}(q))$, then G is not the automorphism group of an abstract regular polytope. If $G = \mathrm{Sz}(q)$, there exists an abstract regular polytope $\mathcal{P}$ such that $G = \mathrm{Aut}(\mathcal{P})$. Moreover, if $\mathcal{P}$ is an abstract regular polytope such that $G = \mathrm{Aut}(\mathcal{P})$, then $\mathcal{P}$ must be an abstract polyhedron, i.e. a rank three polytope.

Let $G := \mathrm{Sz}(q)$ with $q = 2^{2e+1}$ and $e > 0$ an integer. We consider that a polytope and its dual are the same object. In order to determine, up to isomorphism and duality, the number of abstract regular polytopes whose automorphism group is G, we must count, up to isomorphism, the number of unordered triples of involutions $\{\rho_0, \rho_1, \rho_2\}$ in G, such that $(\rho_0\rho_2)^2 = 1_G$ and $\langle \rho_0, \rho_1, \rho_2 \rangle = G$. To do this, we first count the number of ordered triples of involutions $[\rho_0, \rho_1, \rho_2]$. This is done in 3 steps. In step 1, we count the number of non-isomorphic choices for ρ_0. In step 2, we fix ρ_0 and look at the number of non-isomorphic choices for an ordered pair of involutions $[\rho_0, \rho_2]$, where ρ_2 has to commute with ρ_0. In step 3, we suppose ρ_0 and ρ_2 fixed and we count the number of possibilities left to choose ρ_1 in order to obtain an ordered triple of involutions $[\rho_0, \rho_1, \rho_2]$ satisfying the given properties. Finally, we divide the result by two, as no polyhedron of $\mathrm{Sz}(q)$ is self-dual. The intersection property is automatically satisfied thanks to Lemma 4.

STEP 1

The following lemma is given without proof since it is well known and easy to prove.

Lemma 5. *In* $\mathrm{Sz}(q)$*, there are* $(q^2+1)(q-1)$ *involutions that are all pairwise conjugate.*

Therefore, up to conjugacy (and hence up to isomorphism), there is a unique choice for ρ_0 in G.

STEP 2

Suppose that ρ_0 is fixed. Since ρ_2 commutes with ρ_0, we have $\rho_2 \in C_G(\rho_0) \cong E_q \dot{} E_q \leq E_q \dot{} E_q : C_{q-1}$. Obviously, in $C_G(\rho_0)$, there are $q-1$ involutions, namely ρ_0 and $q-2$ others. All of the $q-1$ involutions are in a subgroup of G isomorphic to $\mathrm{AGL}(1,q)$. These involutions correspond to translations of $\mathrm{AGL}(1,q)$. Under conjugation in G, the stabilizer of ρ_0 fixes all the involutions of the centralizer, as the $\mathrm{AGL}(1,q)$ subgroup does. So, up to conjugacy, there are $q-2$ ordered pairs of commuting involutions in $\mathrm{Sz}(q)$. We now look at the action of $\mathrm{Aut}(G) = G : C_{2e+1}$ on these involutions. It amounts to looking at the action of $\mathrm{Aut}(\mathrm{AGL}(1,q)) = \mathrm{AGL}(1,q) : C_{2e+1}$.

Elements of $\mathrm{AGL}(1,q)$ may be written as follows.

$$\alpha(a,b) : \mathrm{GF}(q) \to \mathrm{GF}(q) : x \to ax+b \text{ with } a \neq 0, a, b \in \mathrm{GF}(q).$$

The involutions are the $\alpha(1,b)$ with $b \neq 0$, i.e. the translations of the affine line $\mathrm{AGL}(1,q)$. Without loss of generality we may suppose $\rho_0 = \alpha(1,1)$ and $\rho_2 = \alpha(1,b)$, with $b \neq 1$. There are $q-2$ possible values for b.

In $\mathrm{Aut}(\mathrm{AGL}(1,q))$, the set of field automorphisms is added. These automorphisms are as follows.

$$\sigma_n : \mathrm{GF}(q) \to \mathrm{GF}(q) : x \to x^n \text{ where } n = 2^m \text{ with } m = 0, \cdots, 2e.$$

Recall that the involutions in $\mathrm{AGL}(1,q)$ are the mappings $\alpha_a : \mathrm{AGL}(1,q) \to \mathrm{AGL}(1,q) : x \to x+a$ with $a \in \mathrm{GF}(q)^*$. We look at the action of $\mathrm{Aut}(\mathrm{AGL}(1,q))$ on the set of involutions $\Omega := \{\alpha_a \mid a \in \mathrm{GF}(q)^*\})$. We want to know how many orbits of ordered pairs of involutions $[\alpha_a, \alpha_b]$ ($\alpha_a, \alpha_b \in \Omega$), there are under the action of $\mathrm{Aut}(\mathrm{AGL}(1,q))$.

Since $\mathrm{Aut}(\mathrm{AGL}(1,q))$ is transitive on Ω, there is a unique choice for α_a. Assume $a=1$. Take $H := \mathrm{Aut}(\mathrm{AGL}(1,q))_{\alpha_1} = \{\sigma_n | n = 2^m, m = 0, \cdots, 2e\}$. Then $|H| = 2e+1$. Let us study the action of H on $\Omega \backslash \{\alpha_1\}$. We distinguish between the case where $2e+1$ is a prime and the case where $2e+1$ is not a prime.

5.1 $q = 2^{2e+1}$ with $2e+1$ a prime

Here, $|H| = |H_{\alpha_b}| \cdot |H(\alpha_b)|\ \forall \alpha_b \in \Omega$. Since $2e+1$ is a prime, the orbits have length 1 or $2e+1$. There is one orbit of length 1, namely $\{\alpha_1\}$. The remaining $q-2$ involutions of Ω are split in $\frac{q-2}{2e+1}$ orbits of length $2e+1$. The following lemma ensures that $\frac{q-2}{2e+1}$ is a natural number.

Lemma 6 (Fermat, 1640)**.** *If p is a prime number then p divides $2^p - 2$.*

The discussion above implies that, up to isomorphism, there are $\frac{q-2}{2e+1}$ ordered pairs of commuting involutions in G, and $\frac{q-2}{2(2e+1)}$ unordered pairs. This settles Theorem 1 when $2e+1$ is a prime.

STEP 3

Now we count the number of possibilities for choosing ρ_1. As seen before, there are $q-1$ involutions of G in $C_G(\rho_0)$. So there are $q^2(q-1)$ involutions in G that are non-commuting with ρ_0. Step 2 gives $I := \mathrm{Aut}(G)_{[\rho_0,\rho_2]} \cong C_G(\rho_0) \cong C_G(\rho_2)$. Clearly, each involution in $C_G(\rho_0)$ is fixed by I. By definiton, none of the $q^2(q-1)$ involutions not in $C_G(\rho_0)$ are fixed by I. Hence, for every possible ρ_1, $|I_{\rho_1}| = 1$. As $C_G(\rho_0) \cong E_q \dot{} E_q$, $|I| = |C_G(\rho_0)| = q^2$. So $|I(\rho_1)| = q^2$ for every possible ρ_1. Therefore, the length of the orbit of ρ_1 under the action of $C_G(\rho_0)$ is

q^2 and $C_G(\rho_0)$ splits the $q^2(q-1)$ involutions in $q-1$ orbits of length q^2 each. The action of $\mathrm{Inn}(\mathrm{AGL}(1,q))$ on the involutions that are non-commuting with ρ_0 gives $q-1$ non-conjugate choices for ρ_1. The outer automorphisms do not fix ρ_0 and ρ_2 at the same time. Since we want both involutions to be fixed, we cannot apply an outer automorphism in this case. So we have $q-1$ non-isomorphic choices for ρ_1.

Finally, in $\mathrm{Sz}(q)$, up to isomorphism, there are $\frac{q-2}{2e+1}(q-1)$ ordered triples of involutions $[\rho_0, \rho_1, \rho_2]$ such that $(\rho_0\rho_2)^2 = 1_{\mathrm{Sz}(q)}$ and $\langle \rho_0, \rho_1, \rho_2 \rangle = \mathrm{Sz}(q)$. Since ρ_0 and ρ_2 commute and have the same property, we can exchange them. The polytopes yielded by $[\rho_0, \rho_1, \rho_2]$ and by $[\rho_2, \rho_1, \rho_0]$ are dual. None of these polytopes may be self-dual. Indeed, suppose $[\rho_0, \rho_1, \rho_2]$ gives a self-dual polyhedron. Then, there must be an involution $g \in \mathrm{Aut}(G)$ such that $g(\rho_0) = \rho_2$, $g(\rho_2) = \rho_0$ and $g(\rho_1) = \rho_1$. The last condition implies that $g \in C_G(\rho_1)$. Therefore, g cannot swap ρ_0 and ρ_2. Hence, up to isomorphism and duality, there are $\frac{q-2}{2(2e+1)}(q-1)$ triples of involutions $\{\rho_0, \rho_1, \rho_2\}$ such that $(\rho_0\rho_2)^2 = 1_{\mathrm{Sz}(q)}$ and $\langle \rho_0, \rho_1, \rho_2 \rangle = \mathrm{Sz}(q)$. All these triples satisfy the intersection property by Lemma 4 and the subgroup structure of $\mathrm{Sz}(q)$. It is obvious that all polyhedra of $\mathrm{Sz}(q)$ are non-degenerate for, otherwise, $\mathrm{Sz}(q) \cong 2 \times D_{2n}$ for some integer n. In other words, we get the following theorem.

Theorem 4. *A given Suzuki group $\mathrm{Sz}(q)$, with $q = 2^{2e+1}$ and $2e+1$ a prime, acts flag-transitively on $\frac{q-2}{2(2e+1)}(q-1)$ polyhedra up to isomorphism and duality. All these polyhedra are non-degenerate.*

5.2 $q = 2^{2e+1}$ with $2e+1$ not a prime

We are in the same situation as above section 5.1. Recall that STEP 1 gives us only one choice for ρ_0.

STEP 2 (Continued)

We want to count the number of orbits of ordered pairs of involutions $[\alpha_1, \alpha_b]$, with $\alpha_b \in \Omega\backslash\{\alpha_1\}$, under the action of $\mathrm{Aut}(\mathrm{AGL}(1,q))$. Let $H := \mathrm{Aut}(\mathrm{AGL}(1,q))_{\alpha_1} = \{\sigma_n \mid n = 2^m, m = 0, \cdots, 2e\}$. Since $2e+1$ is no longer a prime, the orbits yielded by the field automorphisms may have a length other than 1 or $2e+1$. In fact they can have any length n, with $n \mid 2e+1$. Let $\lambda(n)$ be the number of orbits of length n under the action of H on $\Omega \cup \{1_G\}$. To determine $\lambda(n)$, we use the Möbius function.

Definition 2. *The Möbius function is the function μ on the positive integers given by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 \cdots p_k, \text{ where } p_1, \cdots, p_k \text{ are pairwise distinct primes}, \\ 0 & \text{if } n \text{ is not squarefree}. \end{cases}$$

The Möbius function has the following important property, also known as *Möbius inversion.*

Lemma 7. *Let F and G be functions on the positive integers. If*

$$G(n) = \sum_{d|n} F(d),$$

then

$$F(n) = \sum_{d|n} \mu(\frac{n}{d}) G(d),$$

and conversely.

Using this definition and this lemma, we get the following result.

Lemma 8. *With the notations as above, for every $n \mid 2e+1$,*

$$\lambda(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) \cdot 2^d.$$

Proof. By the definiton of $\lambda(n)$, for every $n \mid 2e+1$, there are $\lambda(n)$ orbits of length n. So, in each of the $\lambda(n)$ orbits, there are exactly n elements. If we sum up $d \cdot \lambda(d)$ for every $d \mid n$, we get all the elements that are split up in orbits of length $\leq n$. In fact, we get all the elements of a subgroup $E_{2^n} \leq \mathrm{AGL}(1,q)$ corresponding to the subfield $\mathrm{GF}(2^n)$ of $\mathrm{GF}(2^{2e+1})$. Since there are 2^n elements in $\mathrm{GF}(2^n)$, we have the following.

$$2^n = \sum_{d|n} d \cdot \lambda(d)$$

If we take $G(n) = 2^n$, $F(d) = d \cdot \lambda(d)$, and apply Lemma 7, we get $n \cdot \lambda(n) = \sum_{d|n} \mu(\frac{n}{d}) 2^d$. □

To get the final number of orbits, we have to sum up all the orbits for $n \mid 2e+1, n \neq 1$. The only element of Ω that is in an orbit of length 1 is α_1. So, ρ_2 has to be chosen in an orbit of length $\neq 1$. If follows that the number of orbits is $\sum_{\substack{n|2e+1 \\ n\neq 1}} \lambda(n)$. This gives us the number of non-isomorphic ordered pairs of involutions $[\rho_0, \rho_2]$. Therefore, the number of non-isomorphic unordered pairs of involutions $\{\rho_0, \rho_2\}$ is $\frac{1}{2} \sum_{\substack{n|2e+1 \\ n\neq 1}} \lambda(n)$ as stated in Theorem 1.

STEP 3 (Continued)

To choose ρ_1, we cannot apply exactly the same argument as in section 5.1. In STEP 2 we fix the two involutions ρ_0 and ρ_2. Applying the same computation as in the case 5.1, there are, up to isomorphism, at most $q-1$ choices for ρ_1. However, this time, the stabilizer of ρ_0 and ρ_2 in $\mathrm{Aut}(G)$ is not necessarily $C_G(\rho_0)$. Let us illustrate this with the following example.

Example 1. *Take* $\mathrm{GF}(2^{15})^*$. *A subgroup of this group is* $\mathrm{GF}(2^3)^* = \mathrm{GF}(8)^*$. *We can write* $\mathrm{GF}(2^{15})^* = \left\{1, i, i^2, \cdots, i^{2^{15}-2}\right\}, i \neq 1$ *and* $i^{2^{15}-1} = 1$. *Then,* $\mathrm{GF}(8^*) = \{1, i^{4681}, i^{4681 \cdot 2}, \cdots\}$ *because* $2^{15} - 1 = 32767$ *and* $32767/(8-1) = 4681$. *So* $\mathrm{GF}(8)^* =< i^{4681} >$ *and* $\sigma_8(i^{4681}) = i^{4681}$. *If we let* $\rho_0 := \alpha_1$ *and* $\rho_2 := \alpha_{i^{4681}}$, σ_8 *is an automorphism that fixes the two involutions but not every element of* Ω. *For instance,* $\sigma_8(\alpha_{i^2}) \neq \alpha_{i^2}$.

This example shows that the $q-1$ non-conjugated choices for ρ_1 give, in certain cases, less than $q-1$ choices up to isomorphism. It depends on the choice of ρ_2. Indeed, if we pick ρ_2 in an orbit of length $< 2e+1$, the stabilizer of ρ_0 and ρ_2 is a proper overgroup of $C_G(\rho_0)$. This latter subgroup fuses some of the $q-1$ orbits of length q^2 together. To obtain the number of ordered triples of involutions $[\rho_0, \rho_1, \rho_2]$, we cannot just multiply the number of possibilities for $[\rho_0, \rho_2]$ by a fixed number of possibilities for ρ_1. In fact, as $C_{Aut(G)}(?0)nC_{Aut(G)}(?2) = E_q\hat{.}E_q : C_{\frac{2e+1}{n}}$, we have to multiply every single $\lambda(n)$ by a number depending on $2e+1$ and n.

Lemma 9. *Let $\psi(n, 2e+1)$ be the number of candidates for ρ_1 up to isomorphism, provided there are $\lambda(n)$ possibilities for ρ_2. Then,*

$$\psi(n, 2e+1) = \sum_{m|\frac{2e+1}{n}} \frac{\sum_{d|m} \mu(\frac{m}{d})(2^{nd}-1)}{m}.$$

Proof. If there are $\lambda(n)$ possibilities for choosing ρ_2, then ρ_2 is in an orbit of length $n \mid 2e+1$ and $C_{\mathrm{Aut}(G)}(\rho_0) \cap C_{\mathrm{Aut}(G)}(\rho_2) = E_q\hat{.}E_q : C_{\frac{2e+1}{n}} =: S$. This group S acts on the $q^2(q-1)$ involutions in $G \setminus C_G(\rho_0)$ that are the candidates for ρ_1. Up to conjugacy, these $q^2(q-1)$ involutions are in $q-1$ orbits of length q^2. Let us look at the action of the $\frac{2e+1}{n}$ outer automorphisms in S, namely $C_{\frac{2e+1}{n}}$, on the $q-1$ orbits. At first sight, any divisor m of $\frac{2e+1}{n}$ is a candidate for an orbit length. Orbits of length m are obtained in $\mathrm{Sz}(2^{nm})$. However, the only involutions that are in orbits of length m are those in $\mathrm{Sz}(2^{nm})$ that are not in a Suzuki-subgroup of the form $\mathrm{Sz}(2^{nd})$, with $d \mid m$. These last involutions will be in orbits of length d. Let $\alpha(m)$ be the number of candidates for ρ_1 in $\mathrm{Sz}(2^{mn})$ that are in no Suzuki-subgroup of the form $\mathrm{Sz}(2^{nd})$, with $d \mid m$. If we sum up all the $\alpha(d)$ for every $d \mid m$ we get all the involutions that are non-commuting with ρ_0 in $\mathrm{Sz}(2^{nm})$. As we have already seen, there are exactly $2^{nm}-1$ such involutions. So $\sum_{d|m} \alpha(d) = 2^{nm}-1$. If we take $G(m) = 2^{nm}-1$, $F(d) = \alpha(d)$ and apply Lemma 7, we get the following expression for $\alpha(m)$.

$$\alpha(m) = \sum_{d|m} \mu(\frac{m}{d})(2^{nd}-1)$$

There are $\alpha(m)$ involutions that are split up in orbits of length m. This gives $\frac{\alpha(m)}{m}$ orbits of $m \cdot q^2$ candidates for ρ_1. Every candidate has to be in exactly one orbit of length m with $m \mid \frac{2e+1}{n}$. Involutions that are in a same orbit are equivalent by isomorphism. So to get the complete number of candidates for ρ_1, once ρ_2 is fixed in an orbit of length n, we have to count the number of orbits in which the $q^2(q-1)$ involutions of $G \setminus C_G(\rho_0)$ are split up, for a fixed n. The complete number of orbits is obtained by summing up all the $\frac{\alpha(m)}{m}$ for every possible $m \mid \frac{2e+1}{n}$. Therefore, up to isomorphism, the number of choices for ρ_1 is the following.

$$\psi(n, 2e+1) = \sum_{m|\frac{2e+1}{n}} \frac{\alpha(m)}{m} = \sum_{m|\frac{2e+1}{n}} \frac{\sum_{d|m} \mu(\frac{m}{d})(2^{nd}-1)}{m}$$

□

Combining Lemma 8 and Lemma 9, there are $\sum_{\substack{n|2e+1 \\ n\neq 1}} \lambda(n) \cdot \psi(n, 2e+1)$ non-isomorphic ordered triple of involutions $[\rho_0, \rho_1, \rho_2]$. As in section 5.1, this number has to be divided by 2 and so we get

$$\frac{1}{2}\sum_{\substack{n|2e+1\\ n\neq 1}} \lambda(n)\cdot\psi(n,2e+1) \tag{1}$$

triples of involutions $\{\rho_0,\rho_1,\rho_2\}$, up to isomorphism and duality. However, since $2e+1$ is no longer a prime, $\mathrm{Sz}(q)$ has subgroups that are Suzuki groups too. Therefore it might be that the three involutions generate a sub-Suzuki group, not the full $\mathrm{Sz}(q)$. In section 3, it was shown that $\mathrm{Sz}(q')$, with $q'=s$, is a subgroup of $\mathrm{Sz}(q)$, with $q=2e+1$, if $s|2e+1$ and $s>2$. Take an example, say $\mathrm{Sz}(2^{15})$, to illustrate this idea.

Example 2. *The divisors of 15 are 1, 3, 5 and 15. By Lemma 8, there are 2 orbits of length 3, 6 of length 5 and 2182 of length 15. Lemma 9 gives*

$$\begin{aligned}
\psi(3,15) &= \frac{2^3-1}{1}+\frac{2^{15}-1-(2^3-1)}{5} = 7+\frac{2^{15}-2^3}{5} = 7+6552 = 6559,\\
\psi(5,15) &= \frac{2^5-1}{1}+\frac{2^{15}-1-(2^5-1)}{3} = 31+\frac{2^{15}-2^5}{3} = 31+10912 = 10943, \textit{ and}\\
\psi(15,15) &= \frac{2^{15}-1}{1} = 2^{15}-1 = 32767.
\end{aligned}$$

Formula (1) gives $\frac{1}{2}(\lambda(3)\psi(3,15)+\lambda(5)\psi(5,15)+\lambda(15)\psi(15,15)) = 35788185$. *So, up to isomorphism and duality, there are 35788185 triples* $\{\rho_0,\rho_1,\rho_2\}$. *We know that* $\mathrm{Sz}(2^{15})$ *has subgroups isomorphic to* $\mathrm{Sz}(2^3)$ *and* $\mathrm{Sz}(2^5)$. *Therefore, some triples will not generate* $\mathrm{Sz}(2^{15})$*, but a subgroup isomorphic to* $\mathrm{Sz}(2^3)$ *or* $\mathrm{Sz}(2^5)$. *We have to subtract these triples from all the triples of involutions we have found. Since 3 and 5 are prime numbers, we can use Theorem 4 to compute theses triples.*

Definition 3. $\mathrm{Inv}(q)$ *is the number of orbits of* $\mathrm{Aut}(\mathrm{Sz}(q))$ *on the set*

$$\left\{\{\rho_0,\rho_1,\rho_2\} \mid \rho_0^2=\rho_1^2=\rho_2^2=(\rho_0\rho_2)^2=1_{\mathrm{Sz}(q)}, \langle\rho_0,\rho_1,\rho_2\rangle = \mathrm{Sz}(q)\right\}.$$

In our example,

$$\begin{aligned}
\mathrm{Inv}(2^{15}) &= \frac{1}{2}\Big(\sum_{\substack{n|15\\ n\neq 1}}\lambda(n)\psi(n,15) - \frac{2^5-2}{5}(2^5-1) - \frac{2^3-2}{3}(2^3-1)\Big)\\
&= 35788185 - 93 - 7\\
&= 35788085.
\end{aligned}$$

For $\mathrm{Sz}(2^{15})$, we get 35788085 triples of involutions $\{\rho_0,\rho_1,\rho_2\}$ such that $(\rho_0\rho_2)^2 = 1_{\mathrm{Sz}(2^{15})}$ and $\langle\rho_0,\rho_1,\rho_2\rangle = \mathrm{Sz}(2^{15})$. Therefore, up to isomorphism and duality, $\mathrm{Sz}(2^{15})$ acts flag-transitively on 35788085 polyhedra.

This example shows clearly that (1) is not our final result. For the moment, the only thing we have is the following lemma.

Lemma 10. *Let $e > 0$ be an integer. Up to isomorphism and duality, there are*

$$\frac{1}{2}\sum_{\substack{n|2e+1\\ n\neq 1}} \lambda(n)\psi(n, 2e+1)$$

triples of involution $\{\rho_0, \rho_1, \rho_2\}$ in $\mathrm{Sz}(2^{2e+1})$, such that $(\rho_0\rho_2)^2 = 1_{\mathrm{Sz}(q')}$ and $\langle \rho_0, \rho_1, \rho_2\rangle = \mathrm{Sz}(q')$, with $q' = 2^{2f+1}$, $2f+1 \mid 2e+1$ and $f \neq 0$.

Remark 1. *The reader may easily check that this formula is the one given in Theorem 4 if $2e+1$ is a prime.*

To obtain the final formula, we subtract from (1) the number of triples of involutions which generate a sub-Suzuki-group of the given Suzuki group. As Lemma 10 states,

$$\frac{1}{2}\sum_{\substack{n|2e+1\\ n\neq 1}} \lambda(n)\psi(n, 2e+1) = \sum_{d|2e+1} \mathrm{Inv}(2^d).$$

Let us take $F(d) = \mathrm{Inv}(2^d)$ and $G(2e+1) = \frac{1}{2}\sum_{\substack{n|2e+1\\ n\neq 1}} \lambda(n)\psi(n, 2e+1)$. By Lemma 7, we get

$$\begin{aligned}
F(2e+1) &= \sum_{d|2e+1} \mu(\frac{2e+1}{d})G(d)\\
\Rightarrow \mathrm{Inv}(2^{2e+1}) &= \sum_{d|2e+1} \mu(\frac{2e+1}{d})\frac{1}{2}\sum_{\substack{n|d\\ n\neq 1}} \lambda(n)\psi(n, d)\\
&= \frac{1}{2}\sum_{d|2e+1} \mu(\frac{2e+1}{d})\sum_{\substack{n|d\\ n\neq 1}} \lambda(n)\psi(n, d).
\end{aligned}$$

Therefore, up to isomorphism and duality, there are

$$\frac{1}{2}\sum_{d|2e+1} \mu(\frac{2e+1}{d})\sum_{\substack{n|d\\ n\neq 1}} \lambda(n)\psi(n, d)$$

triples of involutions $\{\rho_0, \rho_1, \rho_2\}$ such that $(\rho_0\rho_2)^2 = 1_{\mathrm{Sz}(q)}$ and $\langle \rho_0, \rho_1, \rho_2\rangle = \mathrm{Sz}(q)$. They are all non-degenerate for, otherwise, $\mathrm{Sz}(q) \cong 2 \times D_{2n}$ for some integer n. They all satisfy the intersection property by Lemma 4 and the subgroup structure of $\mathrm{Sz}(q)$. This finishes the proof of Theorem 2.

References

[1] M. Conder, P. Potočnik, and J. Širáň, *Regular hypermaps over projective linear groups*, J. Aust. Math. Soc. **85** (2008), no. 2, 155–175.

[2] D. Leemans, *The rank 2 geometries of the simple Suzuki groups Sz(q)*, Beiträge Algebra Geom. **39** (1998), no. 1, 97–120.

[3] ———, *Almost simple groups of Suzuki type acting on polytopes*, Proc. Amer. Math. Soc. **134** (2006), no. 12, 3649–3651 (electronic).

[4] D. Leemans and E. Schulte, *Groups of type $PSL(2,q)$ acting on polytopes*, Adv. Geom **7** (2007), 529–539.

[5] ———, *Polytopes with groups of type* $\mathrm{PGL}(2,q)$, Ars Math. Contemp. **2** (2009), 163–171.

[6] D. Leemans and L. Vauthier, *An atlas of abstract regular polytopes for small groups*, Aequationes Math. **72** (2006), no. 3, 313–320.

[7] H. Lüneburg, *Translation planes*, Springer-Verlag, Berlin, 1980.

[8] P. McMullen and E. Schulte, *Abstract regular polytopes*, Encyclopedia of Mathematics and its Applications, vol. 92, Cambridge University Press, Cambridge, 2002.

[9] C.-H. Sah, *Groups related to compact Riemann surfaces*, Acta Math. **123** (1969), 13–42.

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

[11] J. Tits, *Ovoïdes et groupes de Suzuki*, Arch. Math. **13** (1962), 187–198.