# COUNTING THE ORBITS ON FINITE SIMPLE GROUPS UNDER THE ACTION OF THE AUTOMORPHISM GROUP SUZUKI GROUPS VS. LINEAR GROUPS 

Stefan Kohl<br>Mathematisches Institut B, 2. Lehrstuhl<br>Universität Stuttgart<br>70550 Stuttgart, Germany


#### Abstract

We determine the number $\omega(G)$ of orbits on the (finite) group $G$ under the action of $\operatorname{Aut}(G)$ for $G \in\left\{\operatorname{PSL}(2, q), \operatorname{SL}(2, q), \operatorname{PSL}(3,3), \mathrm{Sz}\left(2^{2 m+1}\right)\right\}$, covering all of the minimal simple groups as well as all of the simple Zassenhaus groups. This leads to recursive formulae on the one hand, and to the equation $\omega(\operatorname{Sz}(q))=\omega(\operatorname{PSL}(2, q))+2$ on the other.


MSC 20E32, 20F28, 20G40, 20-04

## 1 INTRODUCTION

For any algebraic structure $A$, let $\omega(A)$ denote the number of orbits on $A$ under the action of its automorphism group $\operatorname{Aut}(A)$. In the following, let $G$ be a finite group. The value of $\omega(G)$ might be considered as a measure of the 'homogeneity' of the group $G$ in a certain sense. An interesting problem arising in this context is to classify those groups $G$ having a prescribed $\omega(G)$ or whose $\omega(G)$ does not exceed a given upper bound. Obviously, $\omega(G)=1$ implies that $G$ is trivial, and it is also not difficult to derive that $\omega(G)=2$ implies that $G$ is isomorphic to $\mathrm{C}_{p}^{k}$ for a prime $p$ and $k \in \mathbb{N}$. The case $\omega(G)=3$ is still tractable (see [1]), but for larger values of $\omega(G)$, the complexity of the classification problem grows rapidly. So it seems sensible to consider reduced problems at first. For example, we can restrict our considerations to the case where $G$ is simple (in this case, the classification problem is solved for $\omega(G) \leq 5$ in [2]). Furthermore, it might be very useful for gaining progress here to explicitly determine the value of $\omega(G)$ for certain 'interesting' types of groups $G$. Surely, the minimal simple groups are interesting in this context (although we have to be a bit careful here, since the invariant $\omega$ is not monotone with respect to inclusions, see Remark 1.8). They are covered by the results of this paper; more precisely, $\omega(G)$ is determined for all $G \in\left\{\operatorname{PSL}(2, q), \operatorname{SL}(2, q), \operatorname{PSL}(3,3), \operatorname{Sz}\left(2^{2 m+1}\right)\right\}$, where $q$ denotes a prime power and $m$ a positive integer.

Apparently, there were not many investigations concerning orbits on finite groups under the action of their whole automorphism group done before; anyway, references to some results about class numbers, especially those of simple groups, should be given here, since these are also interesting in this context. For the groups $\operatorname{GL}(n, q), \mathrm{SL}(n, q), \operatorname{PSL}(n, q), \mathrm{GU}(n, q), \mathrm{SU}(n, q)$ and $\operatorname{PSU}(n, q)$, probably the best reference is [3]. Concerning the symplectic groups and the general orthogonal groups, see [4]. Class number formulas for the Chevalley groups $\mathrm{F}_{4}(q), \mathrm{E}_{6}(q),{ }^{2} \mathrm{E}_{6}(q), \mathrm{E}_{7}(q)$, and $\mathrm{E}_{8}(q)$ are given in [5], for $\mathrm{G}_{2}(q)$ in [6], for ${ }^{2} \mathrm{G}_{2}(q)$ in [7], for ${ }^{2} \mathrm{~F}_{4}(q)$ in [8] and for ${ }^{3} \mathrm{D}_{4}(q)$ in [9]. The number of semisimple conjugacy classes of a simply-connected Chevalley group is given in [10], Theorem 3.7.6. A classification of all finite groups with a given class number $\leq 11$ can be found in [11].

Firstly, we give some introductory information, mainly about the groups under consideration and their automorphisms.
1.1 Lemma Let $M \neq \varnothing$ be a finite set. Then one has

$$
\sum_{\varnothing \neq \tilde{M} \subseteq M}(-1)^{|\tilde{M}|+1}=1+\sum_{\tilde{M} \subseteq M}(-1)^{|\tilde{M}|}=1+0=1
$$

Proof: This assertion is a direct consequence of the fact that $M$ has exactly as many subsets of odd as of even cardinality. Now, the proof is completed by induction over the cardinality of $M$ : in the case $|M|=1$, the assertion is obviously true, and since from every subset $\tilde{M} \subsetneq M$ of cardinality $|M|-1$ you can construct precisely one subset of even as well as of odd cardinality by including or excluding the element of $M \backslash \tilde{M}$, you get the claimed equation.
1.2 Lemma Let $M_{i}, i \in I$ be finitely many finite sets, and let
$M=\bigcup_{i \in I} M_{i}$. Then it holds that

$$
|M|=\sum_{\varnothing \neq J \subseteq I}(-1)^{|J|+1}\left|\bigcap_{i \in J} M_{i}\right| .
$$

Proof: Each element of the union is counted exactly once: Let $m \in M$ be an element of precisely $n$ subsets $M_{i}$. Then for each $k, m$ is an element of exactly $\binom{n}{k}$ intersections of $k$ of these subsets, and the claimed equation is a consequence of $\sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}=1$.
1.3 Lemma Let $n$ be a positive integer and $t \mid n$. Then the cyclic group $\mathrm{C}_{n}$ of order $n$ has precisely one subgroup of order $t$. The automorphisms of $\mathrm{C}_{n}$ are given by $\sigma_{l}: \mathrm{C}_{n} \rightarrow \mathrm{C}_{n}, g \mapsto g^{l}$ for $1 \leq l \leq n-1, \operatorname{gcd}(l, n)=1$. The set of orbits on $\mathrm{C}_{n}$ under the action of $\operatorname{Aut}\left(\mathrm{C}_{n}\right)$ is in natural bijection with the set of divisors of $n$ : for every divisor $t$ of $n$ the set of elements of order $t$ forms an orbit under the action of the automorphism group. In particular it holds that $\left|\operatorname{Aut}\left(\mathrm{C}_{n}\right)\right|=\varphi(n)$ and $\omega\left(\mathrm{C}_{n}\right)=\tau(n)$.
(See for example [12], p. 11, Theorem 2.20 as well as p. 20/21, Theorem 4.6.)
1.4 Lemma Let $p$ be a prime, $k \in \mathbb{N}$ and $\operatorname{GF}\left(p^{k}\right)$ the field with $p^{k}$ elements. Then the following hold:

1. The field $\mathrm{GF}\left(p^{k}\right)$ is constructed from the prime field $\mathrm{GF}(p)$ by adjunction of an arbitrary element with a minimal polynomial of degree $k$.
2. The subfields of $\mathrm{GF}\left(p^{k}\right)$ are precisely the fields $\mathrm{GF}\left(p^{t}\right)$ with $t \mid k$.
3. For $k_{1}, k_{2} \in \mathbb{N}$ we have $\operatorname{GF}\left(p^{k_{1}}\right) \cap \operatorname{GF}\left(p^{k_{2}}\right)=\operatorname{GF}\left(p^{\operatorname{gcd}\left(k_{1}, k_{2}\right)}\right)$.
4. Let $\sigma: \operatorname{GF}\left(p^{k}\right) \rightarrow \operatorname{GF}\left(p^{k}\right), x \mapsto x^{p}$ be the Frobenius automorphism of $\mathrm{GF}\left(p^{k}\right)$. Then $\operatorname{Aut}\left(\operatorname{GF}\left(p^{k}\right)\right)=\langle\sigma\rangle \cong \mathrm{C}_{k}$.
5. $\mathrm{GF}\left(p^{k}\right)^{*} \cong \mathrm{C}_{p^{k}-1}$.
6. If $p \neq 2$ then in $\operatorname{GF}\left(p^{k}\right) \backslash\{0\}$ there are $\frac{1}{2}\left(p^{k}-1\right)$ squares and the same number of non-squares.
(See for example [13], p. 15, Theorem 1.2.2.)
1.5 Lemma Let $n$ be a positive integer and let $q$ be a prime power.
7. Assume that $G=\mathrm{SL}(n, q)$ and set $\phi: G \rightarrow G, x \mapsto\left(x^{-1}\right)^{t}$. Then we have that

$$
\operatorname{Aut}(G)=\langle\operatorname{P\Gamma L}(n, q), \phi\rangle
$$

In the case $n=2$ one has $\phi \in \operatorname{PGL}(2, q)$, more precisely, it holds for all $x \in G$ that $\phi(x)=x^{\left(\begin{array}{cc}0 & -1 \\ 1 & 0\end{array}\right) \text {. }}$
2. The automorphisms of $\operatorname{SL}(n, q)$ and $\operatorname{PSL}(n, q)$ are in natural bijection with each other; this means that each automorphism of $\operatorname{PSL}(n, q)$ is induced by a uniquely determined automorphism of $\mathrm{SL}(n, q)$.
(For a proof compare with [14], see also [15].)
1.6 Definition and Lemma Let $m$ be a positive integer. We put $q:=2^{2 m+1}$, $r:=2^{m+1}$ and $K:=\operatorname{GF}(q)$. For $a, b \in K$ set

$$
M(a, b):=\left(\begin{array}{llll}
1 & 0 & 0 & 0 \\
a & 1 & 0 & 0 \\
b & a^{r} & 1 & 0 \\
a^{r+2}+a b+b^{r} & a^{r+1}+b & a & 1
\end{array}\right)
$$

and let $S(q)$ denote the group consisting of all of the matrices $M(a, b)$. Matrix multiplication yields $M(a, b) \cdot M(c, d)=M\left(a+c, a^{r} c+b+d\right)$. We associate with each $\kappa \in K \backslash\{0\}$ the diagonal matrix

$$
\left(\begin{array}{cccc}
\kappa^{1+2^{m}} & 0 & 0 & 0 \\
0 & \kappa^{2^{m}} & 0 & 0 \\
0 & 0 & \kappa^{-2^{m}} & 0 \\
0 & 0 & 0 & \kappa^{-1-2^{m}}
\end{array}\right)
$$

Mapping $\kappa$ to this matrix defines an isomorphism from $K^{*}$ onto the group $K(q)$ formed by these matrices. Now $\kappa^{-1} M(a, b) \kappa=M\left(a \kappa, b \kappa^{r+1}\right)$ shows that $K(q)$
normalizes $S(q)$. Hence the group $H(q)$ generated by $S(q)$ and $K(q)$ has order $q^{2}(q-1)$. If we set

$$
T:=\left(\begin{array}{cccc}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0
\end{array}\right)
$$

then the Suzuki Group $\operatorname{Sz}(q)$ is defined as the group generated by $H(q)$ and $T$. For $G:=\mathrm{Sz}(q)$ the following hold:

1. $G$ is a simple group of order $q^{2}(q-1)\left(q^{2}+1\right)$.
2. If $t_{1}$ and $t_{2}$ are divisors of $2 m+1$, then $\mathrm{Sz}\left(2^{t_{1}}\right)$ and $\mathrm{Sz}\left(2^{t_{2}}\right)$ are subgroups of $G$, and we have $\mathrm{Sz}\left(2^{t_{1}}\right) \cap \mathrm{Sz}\left(2^{t_{2}}\right)=\operatorname{Sz}\left(2^{\operatorname{gcd}\left(t_{1}, t_{2}\right)}\right)$.
3. If $b$ is not contained in any proper subfield of $K$, then $G=<M(1, b), T\rangle$.
4. The Sylow 2-subgroups of $G$ are conjugates of $S(q)$. The exponent of $S(q)$ is 4, the normalizer of $S(q)$ in $G$ is $H(q)$.
5. $G$ possesses cyclic subgroups $U_{i}(q), i=1,2$ of order $q+r+1$ and $q-r+1$ respectively. These are Hall subgroups. The conjugates of $S(q), K(q)$, $U_{1}(q)$ and $U_{2}(q)$ form a partition of $G$ in subgroups, and hence are in particular TI-subgroups of $G$.
6. $\left|\mathrm{N}_{G}(K(q)): K(q)\right|=2$, and for $i \in\{1,2\}$, we have $\left|\mathrm{N}_{G}\left(U_{i}\right): U_{i}\right|=4$.
7. There is exactly one conjugacy class of involutions in $G$, and there are two conjugacy classes of elements of order 4 (these do not fuse under any outer automorphism of $G$ ), furthermore there are $\frac{|K(q)|-1}{2}=\frac{q-2}{2}$ conjugacy classes having non-trivial intersection with $K(q)$, and for $i \in\{1,2\}$ there are $\frac{\left|U_{i}\right|-1}{4}=\frac{q \pm r}{4}$ conjugacy classes having non-trivial intersection with $U_{i}(q)$. Together with the class consisting of the neutral element, the group $G$ hence has $1+1+2+\frac{q-2}{2}+\frac{q+r}{4}+\frac{q-r}{4}=q+3$ conjugacy classes.
8. $\operatorname{Out}(G) \cong \operatorname{Aut}(K) \cong \mathrm{C}_{2 m+1}$, more precisely: each element of $\operatorname{Out}(G)$ has a representative which is in a natural way induced by an automorphism of $K$. Let $\varsigma_{q}$ denote the automorphism of $G$ which is induced by the Frobenius automorphism of $K$.
(See [16], in particular sections 13, 16 and 17, [17], chapters XI. 3 and XI. 5 as well as [18], sections 21, 22 and 24.)
1.7 Theorem The minimal simple groups (these are the non-abelian simple groups having no non-solvable proper subgroups) are given by
9. $\operatorname{PSL}\left(2,2^{p}\right)$ for a prime $p$;
10. $\operatorname{PSL}\left(2,3^{p}\right)$ for an odd prime $p$;
11. $\operatorname{PSL}(2, p)$ for a prime $p>3$ with $p^{2}+1 \equiv 0(\bmod 5)$;
12. $\operatorname{PSL}(3,3)$;
13. $\mathrm{Sz}\left(2^{p}\right)$ for an odd prime $p$.
(For a proof, see [19], cp. corollary 1 in section 3 on page 388.)
1.8 Remark The invariant $\omega$ is not monotone with respect to inclusions : we have, for example, $\omega\left(\mathrm{C}_{2} \times \mathrm{C}_{4}\right)=4>3=\omega\left(\mathrm{C}_{4}^{2}\right)$. This remains true when restricting to simple groups, as the example $\operatorname{PSU}(4,2)<\operatorname{PSU}(4,3)$ and $\omega(\operatorname{PSU}(4,2))=15>14=\omega(\operatorname{PSU}(4,3))$ shows.

## 2 THE LINEAR GROUPS

2.1 Lemma Let $q$ be a prime power and let $G:=\operatorname{SL}(2, q)$.

1. Let

$$
\mathcal{C}:=\mathrm{Z}(\mathrm{SL}(2, q)) \cup\left\{\left.\left(\begin{array}{rr}
0 & -1 \\
1 & a
\end{array}\right) \right\rvert\, a \in \mathrm{GF}(q)\right\} .
$$

Then $\mathcal{C}$ forms a set of representatives for the set of conjugacy classes of $\mathrm{GL}(2, q)$ that lie in $G$, hence there is a set of representatives $\mathcal{R} \subseteq \mathcal{C}$ for the set of the orbits on $G$ under the action of $\operatorname{Aut}(G)$.
2. The set

$$
\mathcal{C}:=\left\{\begin{array}{l}
\left(\begin{array}{lll}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{array}\right),\left(\begin{array}{lll}
1 & 0 & 0 \\
0 & 0 & 2 \\
0 & 1 & 2
\end{array}\right),\left(\begin{array}{lll}
2 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0
\end{array}\right),\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0
\end{array}\right), \\
\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 1
\end{array}\right),\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 2
\end{array}\right),\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 1 \\
0 & 1 & 0
\end{array}\right),\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 1 \\
0 & 1 & 1
\end{array}\right), \\
\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 1 \\
0 & 1 & 2
\end{array}\right),\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 2 \\
0 & 1 & 0
\end{array}\right),\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 2 \\
0 & 1 & 1
\end{array}\right),\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 2 \\
0 & 1 & 2
\end{array}\right)
\end{array}\right\}
$$

is a system of representatives for the set of conjugacy classes of $\mathrm{SL}(3,3)$.
Proof: This result is a direct consequence of the theorem about the rational canonical form of matrices. For the second part, note that in GF(3) there is no non-trivial third root of unity, so that the center of $\operatorname{SL}(3,3)$ is trivial, and that a matrix with $1 \times 1-2 \times 2$ - block structure is in rational canonical form only if the minimal polynomial of the $2 \times 2$ - block is divisible by the one of the $1 \times 1$ - block.
2.2 Lemma Let $n$ be a positive integer, $q$ a prime power and $A \in \operatorname{GL}(n, q)$. If the matrix $A$ is in rational canonical form, then this property remains invariant under applying a fixed automorphism of $\operatorname{GF}(q)$ to each entry.

Proof: According to the theorem about the rational canonical form of matrices it suffices to show that the divisibility relations of the characteristic polynomials of the blocks of $A$ remain invariant. This follows from the fact that field automorphisms of $K$ induce ring automorphisms of the polynomial ring $K[x]$.
2.3 Definition Let $k$ be a positive integer. For a non-empty set $M$ of divisors of $k$ define $T_{k, M}$ by $T_{k, M}:=\operatorname{gcd}_{t \in M} \frac{k}{t}$.
2.4 Lemma Let $p$ be a prime and $k \in \mathbb{N}$. Then we have

$$
\omega\left(\mathrm{GF}\left(p^{k}\right)\right)=\frac{p^{k}}{k}+\sum_{\varnothing \neq M \subseteq \pi(k)}(-1)^{|M|}\left(\frac{p^{T_{k, M}}}{k}-\omega\left(\mathrm{GF}\left(p^{T_{k, M}}\right)\right)\right)
$$

Proof: The set $\operatorname{GF}\left(p^{k}\right)_{\max }$ of elements of $\operatorname{GF}\left(p^{k}\right)$ which are not elements of any proper subfield of $\operatorname{GF}\left(p^{k}\right)$ splits under the action of $\operatorname{Aut}\left(\operatorname{GF}\left(p^{k}\right)\right)$ into orbits of length $k=\left|\operatorname{Aut}\left(\operatorname{GF}\left(p^{k}\right)\right)\right|$, since these elements are zeros of irreducible polynomials of degree $k$ over $\mathrm{GF}(p)$ and the action of the Galois group hence is free. From Lemma 1.4, parts 2 and 3 as well as Lemma 1.2 we conclude that

$$
\begin{aligned}
\left|\mathrm{GF}\left(p^{k}\right)_{\max }\right| & =\left|\operatorname{GF}\left(p^{k}\right)\right|-\left|\bigcup_{t \mid k, t \neq k} \mathrm{GF}\left(p^{t}\right)\right| \\
& =p^{k}-\left|\bigcup_{t \in \pi(k)} \operatorname{GF}\left(p^{\frac{k}{t}}\right)\right| \\
& =p^{k}-\sum_{\varnothing \neq M \subseteq \pi(k)}(-1)^{|M|+1} p^{T_{k, M}}
\end{aligned}
$$

Applying Lemma 1.2 to the sets of the orbits of the maximal subfields of $\operatorname{GF}\left(p^{k}\right)$ yields the claimed assertion.
2.5 Theorem Let $p$ be a prime and $k \in \mathbb{N}$.

1. It holds that

$$
\omega(\mathrm{SL}(2, p))= \begin{cases}3 & \text { if } p=2 \\ p+2 & \text { otherwise }\end{cases}
$$

For $k>1$ we have that

$$
\begin{aligned}
\omega\left(\mathrm{SL}\left(2, p^{k}\right)\right) & =\omega\left(\operatorname{GF}\left(p^{k}\right)\right)+ \begin{cases}1 & \text { if } p=2 \\
2 & \text { otherwise }\end{cases} \\
& =\frac{p^{k}}{k}+\sum_{\varnothing \neq M \subseteq \pi(k)}(-1)^{|M|}\left(\frac{p^{T_{k, M}}}{k}-\omega\left(\operatorname{SL}\left(2, p^{T_{k, M}}\right)\right)\right) .
\end{aligned}
$$

2. For $p=2$ it obviously holds that $\operatorname{PSL}\left(2, p^{k}\right) \cong \mathrm{SL}\left(2, p^{k}\right)$. For odd $p$ we have that

$$
\omega(\operatorname{PSL}(2, p))=\frac{p+3}{2}
$$

and

$$
\begin{aligned}
\omega\left(\operatorname{PSL}\left(2, p^{k}\right)\right) & =\frac{p^{k}+H(p, k)}{2 k} \\
& +\sum_{\varnothing \neq M \subseteq \pi(k)}(-1)^{|M|}\left(\frac{p^{T_{k, M}}}{2 k}-\omega\left(\operatorname{PSL}\left(2, p^{T_{k, M}}\right)\right)\right)
\end{aligned}
$$

where

$$
H(p, k)= \begin{cases}0 & \text { if } 2 \nmid k \\ p^{\frac{k}{2}}-1 & \text { if } k \text { is a power of } 2 \\ p^{\frac{k}{2}}+\sum_{\varnothing \neq M \subseteq \pi(k) \backslash\{2\}}(-1)^{|M|} p^{\operatorname{gcd}_{t \in M} \frac{k}{2 t}} & \text { otherwise. }\end{cases}
$$

Proof: We choose a system of representatives $\mathcal{R}$ for the set of the orbits in $\mathrm{SL}\left(2, p^{k}\right)$ under the action of $\operatorname{Aut}\left(\mathrm{SL}\left(2, p^{k}\right)\right)$ from the set

$$
\mathcal{C}:=\left\{\left(\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right),\left(\begin{array}{rr}
-1 & 0 \\
0 & -1
\end{array}\right)\right\} \cup\left\{\left.\left(\begin{array}{rr}
0 & -1 \\
1 & a
\end{array}\right) \right\rvert\, a \in \mathrm{GF}\left(p^{k}\right)\right\}
$$

(This choice of $\mathcal{R}$ is possible according to Lemma 2.1). We have to determine $|\mathcal{R}|$. The orbit partition induces on $\mathcal{C} \backslash \mathrm{Z}\left(\mathrm{SL}\left(2, p^{k}\right)\right)$ a partition by sets of the form

$$
\mathcal{C}_{a}=\left\{\left.\left(\begin{array}{cc}
0 & -1 \\
1 & a^{p^{i}}
\end{array}\right) \right\rvert\, i=0, \ldots, k-1\right\}
$$

where $a \in \operatorname{GF}\left(p^{k}\right)$, since if $X, Y \in \mathrm{SL}\left(2, p^{k}\right)$ are in rational canonical form and there is an automorphism of $\mathrm{SL}\left(2, p^{k}\right)$ mapping one to the other, then this automorphism is a field automorphism applied to the respective entries: $\left(g^{-1} X g\right)^{\alpha}=Y \Leftrightarrow g^{-1} X g=Y^{\alpha^{-1}} \Longrightarrow X=g^{-1} X g, X^{\alpha}=Y$ (compare with Lemma 1.5). The equation from assertion 1 for prime fields as well as the first equation concerning the case $k>1$ now follow directly from the fact that the two orbits on the center of $\operatorname{SL}\left(2, p^{k}\right)$ fuse in the case $p=2$; from this, we get the remaining equation by Lemma 2.4 and Lemma 1.1.

Now we consider the groups $\operatorname{PSL}\left(2, p^{k}\right)$ for odd primes $p$. Let $\kappa: \mathrm{SL}\left(2, p^{k}\right) \rightarrow$ $\operatorname{PSL}\left(2, p^{k}\right), x \mapsto x \mathrm{Z}\left(\mathrm{SL}\left(2, p^{k}\right)\right)$ denote the canonical projection. We are interested in its behavior on the set $\mathcal{C}$. Computing

$$
\left(\begin{array}{ll}
0 & -1 \\
1 & -a
\end{array}\right)^{\kappa}=\left(\begin{array}{rr}
0 & 1 \\
-1 & a
\end{array}\right)^{\kappa} \quad \text { and } \quad\left(\begin{array}{rr}
0 & 1 \\
-1 & a
\end{array}\right)\left(\begin{array}{rr}
1 & 0 \\
0 & -1
\end{array}\right)=\left(\begin{array}{rr}
0 & -1 \\
1 & a
\end{array}\right)
$$

we see that the sets $\mathcal{C}_{-a}$ and $\mathcal{C}_{a}$ are fused under $\kappa$, as well as the two orbits belonging to the center of $\mathrm{SL}\left(2, p^{k}\right)$. Since the automorphisms of $\mathrm{SL}\left(2, p^{k}\right)$ and $\operatorname{PSL}\left(2, p^{k}\right)$ are in natural bijection with each other (Lemma 1.5, part 2), due to the above we can assume without loss of generality that $a \in \operatorname{GF}\left(p^{k}\right)_{\max }$ and handle the other cases using Lemma 1.2. In the case $a=-a^{p^{i}}$ for an $i \in \mathbb{N}$ it holds that $\mathcal{C}_{-a}=\mathcal{C}_{a}$, hence we get an orbit of length $k$, otherwise one of length $2 k$. Let $H(p, k)$ denote the number of elements belonging to orbits of length $k$. For odd $k$ it obviously holds that $H(p, k)=0$. The case $a=-a^{p^{i}}$ occurs if and only if $a$ and $-a$ are conjugate to each other, hence if they are solutions of an irreducible quadratic equation $(x-a)(x+a)=x^{2}-a^{2}=x^{2}-b=0$ over $\operatorname{GF}\left(p^{\frac{k}{2}}\right)$. We conclude that for each non-square $b \in \operatorname{GF}\left(p^{\frac{k}{2}}\right)$ whose square roots belong to $\mathrm{GF}\left(p^{k}\right)_{\text {max }}$, there are precisely two such elements. According to Lemma 1.4, part 6 there are exactly $\frac{1}{2}\left(p^{t}-1\right)$ non-squares in $\operatorname{GF}\left(p^{t}\right)(t \in \mathbb{N})$, and the mentioned formulas for $H(p, k)$ for even $k$ are a consequence of Lemma 1.4, parts 2 and 3 as well as Lemma 1.2. With the same arguments as in part (1) we now get the claimed assertion.
2.6 Example Since $\mathrm{GF}(729)$ is the smallest field of odd characteristic whose subfield lattice is not totally ordered with respect to the inclusion relation, we determine $\omega(\operatorname{PSL}(2,729))$ as an example in order to illustrate the proof given above.

We have to count the sets $\mathcal{C}_{a}$ belonging to $\operatorname{SL}(2,729)$, and use the criterion for the equality of $\mathcal{C}_{a}$ and $\mathcal{C}_{-a}$ mentioned in the proof. We have to separately count the equivalence classes given by $\mathcal{C}_{a} \cup \mathcal{C}_{-a}$ with
$\underbrace{a \in \mathrm{GF}(3)}_{\text {Case } 1}, \underbrace{a \in \mathrm{GF}(9)_{\max }}_{\text {Case } 2}, \underbrace{a \in \mathrm{GF}(27)_{\max }}_{\text {Case } 3}$ as well as $\underbrace{a \in \mathrm{GF}(729)_{\max }}_{\text {Case } 4}$ :

- Case 1 contributes a class of length 1 (for $a=0$ ) and one of length 2.
- It holds that $\left|\mathrm{GF}(9)_{\max }\right|=9-3=6$. In $\mathrm{GF}(3)$ there is one non-square, so case 2 contributes a class of length 2 and one of length 4 .
- It holds that $\left|\mathrm{GF}(27)_{\max }\right|=27-3=24$. Since 27 is no perfect square, case 3 contributes only classes of length 6 , and their number is $\frac{24}{6}=4$.
- It holds that $\left|\mathrm{GF}(729)_{\max }\right|=729-27-9+3=696$. In GF(27) $)_{\text {max }}$ there are $\frac{\left|\operatorname{GF}(27)_{\max }\right|}{2}=12$ non-squares, hence case 4 contributes $\frac{2 \cdot 12}{6}=4$ classes of length 6 and $\frac{696-2 \cdot 12}{12}=56$ classes of length 12 .

Summation of the given numbers of classes and taking the orbit containing the neutral element into account yields the result $\omega(\operatorname{PSL}(2,729))=69$.
2.7 Corollary For a prime $p$ and $k \in \mathbb{N}$, the following hold.
1.

$$
\omega\left(\mathrm{SL}\left(2, p^{k}\right)\right)>\frac{p^{k}}{k}, \quad \omega\left(\operatorname{PSL}\left(2, p^{k}\right)\right)>\frac{p^{k}}{\left(2-\delta_{2, p}\right) k}
$$

2. 

$$
\lim _{k \rightarrow \infty} \frac{\omega\left(\operatorname{SL}\left(2, p^{k}\right)\right)}{\frac{p^{k}}{k}}=\lim _{k \rightarrow \infty} \frac{\omega\left(\operatorname{PSL}\left(2, p^{k}\right)\right)}{\frac{p^{k}}{\left(2-\delta_{2, p}\right)^{k}}}=1
$$

3. Let $p \neq 2$ and $k$ be a prime. Then we have

$$
\omega\left(\mathrm{SL}\left(2, p^{k}\right)\right)=\frac{p^{k}+(k-1) p+2 k}{k}
$$

In the case $k \neq 2$ we have that

$$
\omega\left(\operatorname{PSL}\left(2, p^{k}\right)\right)=\frac{p^{k}+(k-1) p+3 k}{2 k}
$$

## Proof:

1. These assertions hold since no $\mathcal{C}_{a}$ is longer than $k$, the automorphism $\kappa$ never fuses more than two sets $\mathcal{C}_{a}$ and since the orbit of the neutral element is disjoint to all of the sets $\mathcal{C}_{a}$ (compare the proof of the theorem).
2. The number of maximal subfields of $\operatorname{GF}\left(p^{k}\right)$ equals the number of different prime divisors of $k$, hence is not larger than $\log _{2}(k)$. For a maximal subfield $K$ of $\operatorname{GF}\left(p^{k}\right)$ we have $|K| \leq p^{\frac{k}{2}}$, and $\operatorname{SL}(2, K)$ splits under the action of $\operatorname{Aut}\left(\mathrm{SL}\left(2, p^{k}\right)\right)_{\{\mathrm{SL}(2, K)\}}$ into at most $|K|+2$ orbits. Because we have $\left|\mathcal{C}_{a}\right|=k$ for an $a \in \operatorname{GF}\left(p^{k}\right)_{\text {max }}$ (compare the proof of the theorem) it holds that
$\omega\left(\mathrm{SL}\left(2, p^{k}\right)\right) \leq \frac{p^{k}}{k}+\left(p^{\frac{k}{2}}+2\right) \log _{2}(k)+2=(1+\underbrace{\frac{k\left(p^{\frac{k}{2}}+2\right) \log _{2}(k)+2 k}{p^{k}}}_{\rightarrow 0 \text { for } k \rightarrow \infty}) \frac{p^{k}}{k}$,
and using part (1) we get the assertion. The respective assertion concerning $\omega\left(\operatorname{PSL}\left(2, p^{k}\right)\right)$ is shown completely analogously.
3. These equations follow immediately from the formulas in part (1) and part (2) of the theorem, respectively.
2.8 Remark With approximately the same amount of work as required for the proof of Theorem 2.5, it can be shown that for all prime powers $q$, we have $\omega(\operatorname{PGL}(2, q))=\omega(\mathrm{SL}(2, q))$ (see [20], Theorem 2.7). The value of $\omega(\mathrm{GL}(2, p))$ for an odd prime $p$ can also be determined with a comparable effort: we have

$$
\omega(\mathrm{GL}(2, p))=(p+1) \tau(p-1)-\frac{p-1}{2} \tau\left(\frac{p-1}{2}\right)
$$

where $\tau(n)$ denotes the number of divisors of $n$ (see [20], Theorem 2.10). The case of $\mathrm{GL}(2, q)$ for a general prime power $q$ seems to be more difficult due to the intricate interplay between the homomorphisms into the center and the automorphisms induced by field automorphisms of $\mathrm{GF}(q)$, but an efficient algorithm based on the methods used in the proof of Theorem 2.5 can be given anyway (see [20], appendix B).

### 2.9 Theorem It holds that $\omega(\operatorname{PSL}(3,3))=9$.

Proof: Set $G:=\operatorname{SL}(3,3)$. Since $\mathrm{Z}(G)$ is trivial (see the proof of Lemma 2.1), we have $G \cong \operatorname{PSL}(3,3)$. Let $\phi$ be as in Lemma 1.5 and $\mathcal{C}$ be the set of representatives for the conjugacy classes of $G$ given in Lemma 2.1. According to Lemma 1.5 it suffices to investigate which conjugacy classes are fused by $\phi$. Since $\phi$ acts on $1 \times 1$ - blocks as the identity and on $2 \times 2$ - blocks as a conjugation, it is sufficient to consider the effect of $\phi$ on the conjugacy classes whose elements have a rational canonical form $A$ consisting of a single $3 \times 3$ - block. If we have

$$
A=\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & b \\
0 & 1 & a
\end{array}\right)
$$

then it holds that $\chi(A)=x^{3}-a x^{2}-b x-1$, and $\phi(A)$ is conjugate to the companion matrix of $\chi(\phi(A))=-x^{3}\left(\chi(A)\left(\frac{1}{x}\right)\right)=-x^{3}\left(\left(\frac{1}{x}\right)^{3}-a\left(\frac{1}{x}\right)^{2}-b\left(\frac{1}{x}\right)-1\right)=$ $x^{3}+b x^{2}+a x-1$ :

$$
\phi(A) \sim\left(\begin{array}{rrr}
0 & 0 & 1 \\
1 & 0 & -a \\
0 & 1 & -b
\end{array}\right)
$$

and if we now consider the set of representatives $\mathcal{C}$ for the conjugacy classes of $G$, then we recognize that of the nine conjugacy classes in question six are fused in pairs under automorphisms of $G$. Hence we have that $\omega(G)=|\mathcal{C}|-\frac{6}{2}=$ $12-3=9$.
2.10 Remark The group $\operatorname{PSL}(3,3) \cong \mathrm{SL}(3,3)=: G$ has order

$$
\frac{1}{2}\left(3^{3}-1\right)\left(3^{3}-3\right)\left(3^{3}-3^{2}\right)=2^{4} \cdot 3^{3} \cdot 13=5616
$$

and contains elements of orders $1,2,3,4,6,8$ and 13 . If we convert the representatives constructed in the proof of the theorem to some nice form, then we get the following set of representatives for the set of orbits on the group $G$ under the action of $\operatorname{Aut}(G)$ :
(The orbit lengths were computed using GAP (see [21]).)

## 3 THE SUZUKI GROUPS

In this section, we implicitly refer to Lemma 1.6 and use the notation introduced there.
3.1 Lemma Let $n$ be odd, $s \mid n$ and $q=2^{n}=\tilde{q}^{s}$. Then $\operatorname{gcd}\left(q^{2}+1,|\operatorname{GL}(4, \tilde{q})|\right)$ divides $\tilde{q}^{2}+1$.

Proof: Obviously it holds that

$$
\begin{aligned}
|\operatorname{GL}(4, \tilde{q})| & =\left(\tilde{q}^{4}-1\right)\left(\tilde{q}^{4}-\tilde{q}\right)\left(\tilde{q}^{4}-\tilde{q}^{2}\right)\left(\tilde{q}^{4}-\tilde{q}^{3}\right) \\
& =\tilde{q}^{6}(\tilde{q}-1)^{2}\left(\tilde{q}^{2}-1\right)^{2}\left(\tilde{q}^{2}+1\right)\left(\tilde{q}^{2}+\tilde{q}+1\right),
\end{aligned}
$$

hence it is sufficient to show that $q^{2}+1=\tilde{q}^{2 s}+1$ is coprime to $\tilde{q}-1, \tilde{q}^{2}-1$ and $\tilde{q}^{2}+\tilde{q}+1$ :

- Since $\tilde{q}-1$ divides $\tilde{q}^{2 s}-1$, we have $\tilde{q}^{2 s}+1 \equiv 2(\bmod (\tilde{q}-1))$. The coprimality condition is satisfied since $\tilde{q}-1$ is odd.
- Replacing $\tilde{q}-1$ by $\tilde{q}^{2}-1$ yields the required assertion for the second one of the mentioned factors.
- Dividing $\tilde{q}^{2 s}+1$ by $\tilde{q}^{2}+\tilde{q}+1$ as polynomials yields for $s \equiv 0(\bmod 3)$ the residue 2 , for $s \equiv 1(\bmod 3)$ the residue $-\tilde{q}$ and for $s \equiv 2(\bmod 3)$ the residue $\tilde{q}+1$. Since the residue and the divisor are coprime in any case, we get the claimed assertion.


### 3.2 Definition Let

1. $\Sigma$ denote the cyclic group generated by $\varsigma_{q}$, where we identify the automorphism $\varsigma_{q}$ of $\mathrm{Sz}(q)$ with its natural extension to $\mathrm{GL}(4, q)$,
2. $\mathrm{Sz}(q)_{\text {max }}$ denote the set of all elements of $\mathrm{Sz}(q)$, which are not conjugate to an element of any Suzuki subgroup $\operatorname{Sz}(\tilde{q}) \lesseqgtr \operatorname{Sz}(q)$ (with $\tilde{q}=2^{t}$ for a divisor $t$ of $n)\left(\mathrm{Sz}(q)_{\max } \subset \mathrm{Sz}(q)\right.$ is obviously characteristic and we have $\left.S(q) \cap \mathrm{Sz}(q)_{\max }=\varnothing\right)$,
3. $\mathcal{C}_{K(q)_{\max }}$ denote the set of conjugacy classes of $\mathrm{Sz}(q)$, whose intersection with $K(q)_{\max }:=K(q) \cap \mathrm{Sz}(q)_{\max }$ is not empty and
4. $\mathcal{C}_{U_{i}(q)_{\max }}(i=1,2)$ denote the set of the conjugacy classes of $\mathrm{Sz}(q)$, whose intersection with $U_{i}(q)_{\max }:=U_{i}(q) \cap \mathrm{Sz}(q)_{\max }$ is not empty.
3.3 Lemma The group $\Sigma$ acts semiregularly on the sets
$\mathcal{C}_{K(q)_{\text {max }}}$ and $\mathcal{C}_{U_{i}(q)_{\text {max }}}(i=1,2)$.
Proof: Since reversing the order of application of automorphisms and exponentiation leaves the result unchanged, the group $\Sigma$ acts on $K(q)$ as $\operatorname{Aut}(K)$ on $K \backslash\{0\}$, and hence also on $K(q)_{\max }$ as $\operatorname{Aut}(K)$ on $K_{\max }$. Because $K(q)$ is a TI-subgroup of $\mathrm{Sz}(q)$ and because we have $\left|\mathrm{N}_{\mathrm{Sz}(q)}(K(q)): K(q)\right|=2$, at most two elements of $K(q)_{\max } \subseteq K(q) \backslash\{1\}$ lie in each of the considered conjugacy classes. Since we have $\kappa^{T}=\kappa^{-1}$ for $\kappa \in K(q)$, there are also at least two elements in each of them, in particular, pairs of the form $\left(\kappa, \kappa^{-1}\right)$. Since the set of pairs $\left(\kappa, \kappa^{-1}\right)$ lying in $K(q)_{\max }$ forms a block system for the action of $\Sigma$ on $K(q)_{\max }$ and $n$ is odd, $\Sigma$ acts semiregularly on $\mathcal{C}_{K(q)_{\max }}$, as claimed.

Let $i \in\{1,2\}$ and $g$ be an element of $U_{i}(q)_{\max }$. Firstly, we show that $g$ as an element of $\mathrm{GL}(4, q)$ is not conjugate to an element of any subgroup $\mathrm{GL}(4, \tilde{q}) \lesseqgtr \mathrm{GL}(4, q)$ (with $\tilde{q}=\sqrt[s]{q}$ for a divisor $s$ of $n$ ). Since $U_{i}(q)$ as a cyclic group has precisely one subgroup of order $t$ for each divisor $t$ of the group order according to Lemma 1.3, the order of $g$ does certainly not divide the order of $U_{i}(\tilde{q}) \leq U_{i}(q)$, and since $\operatorname{gcd}\left(\left|U_{1}(q)\right|,\left|U_{2}(q)\right|\right)=1$ and $\left|U_{3-i}(\tilde{q})\right|$ divides $\left|U_{3-i}(q)\right|$ the order of $g$ also does not divide $\left|U_{1}(\tilde{q})\right| \cdot\left|U_{2}(\tilde{q})\right|=\tilde{q}^{2}+1$. Because we have $\left|U_{1}(q)\right| \cdot\left|U_{2}(q)\right|=q^{2}+1, \operatorname{ord}(g)$ divides $q^{2}+1$, but according to Lemma 3.1 it does not divide the order of $\operatorname{GL}(4, \tilde{q})$. Hence $g$ is not conjugate to an element of $\operatorname{GL}(4, \tilde{q})$, as claimed, and so the rational canonical form of $g$ contains an entry from $\mathrm{GF}(q)_{\max }$. Its orbit under the action of $\Sigma$ thus clearly has length $n$, and the elements of this orbit are also in rational canonical form according to Lemma 2.2, so they all lie in different conjugacy classes according to the definition of the rational canonical form. Hence $\Sigma$ also acts semiregularly on the set $\mathcal{C}_{U_{i}(q)_{\max }}$, as claimed.
3.4 Main Theorem Let $m \in \mathbb{N}, n:=2 m+1$ and $q:=2^{n}$. Then we have

$$
\omega(\operatorname{Sz}(q))=\omega(\operatorname{PSL}(2, q))+2
$$

Proof: Due to technical reasons, we also admit the construction of $\mathrm{Sz}(q)$ for $q=2$ (then it holds that $\mathrm{Sz}(2) \cong\langle(2435),(12)(34)\rangle)$. Now, let $q>2$ and $g \in \mathrm{Sz}(q)_{\max }$. Then, $g$ is not conjugate to any of its images under a power of the automorphism $\varsigma_{q}$ which is not equal to the identity $\left(g \sim \varsigma_{q}^{k}(g) \Rightarrow n \mid k\right)$, since the conjugates of $S(q), K(q), U_{1}(q)$ and $U_{2}(q)$ form a partition of $\mathrm{Sz}(q)$ into subgroups, $S(q) \cap \mathrm{Sz}(q)_{\max }=\varnothing$ and the group $\Sigma$ acts semiregularly on the sets $\mathcal{C}_{K(q)_{\max }}$ and $\mathcal{C}_{U_{i}(q)_{\max }}(i=1,2)$, according to Lemma 3.3. Because the set of elements of $\Sigma$ gives rise to a set of representatives for the set of the elements of $\operatorname{Out}(\operatorname{Sz}(q))=\operatorname{Aut}(\operatorname{Sz}(q)) / \operatorname{Inn}(\operatorname{Sz}(q))$, under the action of $\operatorname{Aut}(\operatorname{Sz}(q))$ each conjugacy class belonging to $\mathrm{Sz}(q)_{\max }$ is fused with $n-1$ others. Since an arbitrary Suzuki subgroup $\operatorname{Sz}(\tilde{q}) \leq \mathrm{Sz}(q)$ has a total of $\tilde{q}+3$ conjugacy classes, this leads with nearly the same argument as in the proof of Lemma 2.4 to the formula

$$
\omega(\operatorname{Sz}(q))=\frac{q+3}{n}+\sum_{\varnothing \neq M \subseteq \pi(n)}(-1)^{|M|}\left(\frac{2^{T_{n, M}}+3}{n}-\omega\left(\operatorname{Sz}\left(2^{T_{n, M}}\right)\right)\right)
$$

Since the summand $\frac{3}{n}$ is added exactly as often as it is subtracted according to Lemma 1.1, we get the claimed result because of $\omega(\operatorname{Sz}(2))=5=\omega(\operatorname{PSL}(2,2))+2$ (compare with Remark 3.6) by comparison with the result concerning PSL(2,q) in Theorem 2.5.

In addition to the assertion stated in the main theorem, as an immediate consequence of its proof we see the following.
3.5 Corollary The partitions of the sets of the elements of the groups $\mathrm{Sz}(q)$ resp. $\operatorname{PSL}(2, q)$ which are not conjugate to an element of $\mathrm{Sz}(2)$ resp. $\operatorname{PSL}(2,2)$ are in the following sense in bijective correspondence with each other: if we denote the set of elements of $\operatorname{PSL}(2, q)$ which are not conjugate to an element of a subgroup $\operatorname{PSL}(2, \tilde{q}) \lesseqgtr \operatorname{PSL}(2, q)$ by $\operatorname{PSL}(2, q)_{\max }$, then $\operatorname{Sz}(q)_{\max }$ splits under the action of $\operatorname{Aut}(\operatorname{Sz}(q))$ into the same number of orbits as $\operatorname{PSL}(2, q)_{\text {max }}$ under that of $\operatorname{Aut}(\operatorname{PSL}(2, q))$; the same certainly holds also for any pair of corresponding subgroups over arbitrary subfields.

This is illustrated in fig. 1 for $q=2^{n}, n=p_{1}^{k_{1}} p_{2}^{k_{2}}\left(p_{1}, p_{2}\right.$ odd primes, $k_{1}, k_{2} \in \mathbb{N}$ ). In this figure, the squares represent the equally-sized sets of orbits into which the sets of elements being conjugate to an element of the mentioned sets split under the action of $\operatorname{Aut}(\operatorname{Sz}(q))$ resp. $\operatorname{Aut}(\operatorname{PSL}(2, q))$. The restriction to exponents with only two different prime factors is arbitrary and only forced by the dimension of the paper.
3.6 Remark We would like to compare the orbit partitions of the groups $\mathrm{Sz}(2) \cong \operatorname{AGL}(1,5)$ and $\operatorname{PSL}(2,2) \cong \operatorname{AGL}(1,3)$.

For better legibility, we use the permutation representation of $\mathrm{Sz}(2)$ mentioned above: a group isomorphism of $\mathrm{Sz}(2)$ onto $G:=\langle(2435),(12)(34)\rangle$ is given


Figure 1: Orbits on $\operatorname{Sz}\left(2^{p_{1}^{k_{1}} p_{2}^{k_{2}}}\right)$ vs. orbits on $\operatorname{PSL}\left(2,2^{p_{1}^{k_{1}} p_{2}^{k_{2}}}\right)$
by $f: M(1,1) \mapsto(2435), T \mapsto(12)(34)$. The group $G$ splits under the action of its automorphism group into the following 5 orbits:

$$
\begin{aligned}
& \{()\}, \\
& \{(23)(45),(12)(34),(13)(25),(14)(35),(15)(24)\}, \\
& \{(2435),(1254),(1345),(1423),(1532)\}, \\
& \{(2534),(1235),(1324),(1452),(1543)\}, \\
& \{(12453),(13542),(14325),(15234)\} .
\end{aligned}
$$

The orbits on the group $\operatorname{SL}(2,2) \cong \operatorname{PSL}(2,2) \cong \operatorname{AGL}(1,3) \cong S_{3}$ under the action of its automorphism group are

$$
\left\{\left(\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right)\right\},\left\{\left(\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right),\left(\begin{array}{ll}
1 & 0 \\
1 & 1
\end{array}\right),\left(\begin{array}{ll}
1 & 1 \\
0 & 1
\end{array}\right)\right\},\left\{\left(\begin{array}{ll}
0 & 1 \\
1 & 1
\end{array}\right),\left(\begin{array}{ll}
1 & 1 \\
1 & 0
\end{array}\right)\right\} .
$$

Hence we see that the sets of orbits consisting of elements of orders 1 and 2 are in a certain way in direct correspondence to each other, that the orbit consisting of elements of order 5 on $\mathrm{Sz}(2)$ plays a role similar to that of the orbit consisting of elements of order 3 on $\operatorname{PSL}(2,2)$ and that the 'additional' orbits on $\mathrm{Sz}(2)$ are those consisting of elements of order 4.

## 4 ACKNOWLEDGEMENTS

The author would like to thank Markus Stroppel for his valuable support in preparing this paper. Furthermore, he would like to thank Robert A. Wilson for the part of Remark 1.8 concerning simple groups.

## References

[1] Mäurer, Helmut; Stroppel, Markus. Groups that are almost homogeneous. Geom. Ded., 1997, 68, 229-243.
[2] Stroppel, Markus. Finite simple groups with few orbits under automorphisms. Preprint, 1999.
[3] Macdonald, I. G. Numbers of conjugacy classes in some finite classical groups. Bull. Austral. Math. Soc. 1981, 23, 23-48.
[4] Wall, G. E. On the conjugacy classes in the unitary, symplectic and orthogonal groups. J. Austral. Math. Soc. 1963, 3, 1-62.
[5] Fleischmann, Peter; Janiszczak, Ingo. On the computation of conjugacy classes of Chevalley groups. Appl. Alg. in Eng., Comm. and Comp. 1996, $7(3), 221-234$.
[6] Chang, Bomshik. The conjugate classes of Chevalley groups of type $G_{2} . J$. Algebra 1968, 9, 190-211.
[7] Ward, H. N. On Ree's series of simple groups. Trans. Amer. Math. Soc. 1966, 121, 62-89.
[8] Shinoda, Ken-ichi. The conjugacy classes of the finite Ree groups of type F4. J. Fac. Sci. Univ. Tokyo Sect. I A Math. 1975, 22, 1-15.
[9] Deriziotis, D. I.; Michler, G. O. Character table and blocks of finite simple triality groups ${ }^{3} D_{4}(q)$. Trans. Amer. Math. Soc. 1987, 303, 39-70.
[10] Carter, Roger W. Finite Groups of Lie Type. Wiley Classics Library Edition. John Wiley \& Sons, 1993.
[11] Vera Lopez, Antonio; Vera Lopez, Juan. Classification of finite groups according to the number of conjugacy classes. Isr. J. Math., 1985, 51, 305-338.
[12] Huppert, Bertram. Endliche Gruppen I. Band 134 der Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1967.
[13] Jungnickel, Dieter. Finite Fields. BI - Wissenschaftsverlag, 1993.
[14] Dieudonne, Jean. On the automorphisms of the classical groups. Mem. Amer. Math. Soc., 2, 1951.
[15] Dieudonne, Jean. La geometrie des groupes classiques. Ergebnisse der Mathematik und ihrer Grenzgebiete, 5, 1963.
[16] Suzuki, Michio. On a class of doubly transitive groups. Ann. Math. 1962, 75, 105-145.
[17] Huppert, Bertram; Blackburn, Norman. Finite Groups III. Band 243 der Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1982.
[18] Lüneburg, Heinz. Translation Planes. Springer-Verlag, 1980.
[19] Thompson, John G. Nonsolvable finite groups all of whose local subgroups are solvable. Bull. Amer. Math. Soc. 1968, 74, 383-437.
[20] Kohl, Stefan. Über die Anzahl der Bahnen in endlichen Gruppen unter der Operation ihrer Automorphismengruppe - Suzuki-Gruppen vs. lineare Gruppen. Diplomarbeit, Universität Stuttgart, 2000.
[21] The GAP Group, Aachen, St Andrews. GAP - Groups, Algorithms, and Programming, Version 4.2, 2000. (http://www.gap-system.org).

