***Orbits on k-subsets of 2-transitive Simple Lie-type Groups***

Bradley, Paul and Rowley, Peter

2014

MIMS EPrint: **2014.42**



ISSN 1749-9097

# Orbits on $k$-subsets of 2-transitive Simple Lie-type Groups

Paul Bradley and Peter Rowley

August 7, 2014

**Abstract**

For a finite rank one simple Lie-type group acting 2-transitively on a set $\Omega$ and $k \in \mathbb{N}$ we derive formulae for the number of $G$-orbits on the set of all $k$-subsets of $\Omega$.

## 1 Introduction

Suppose $G$ is a permutation group acting upon a set $\Omega$. Then $G$ has an induced action upon $\mathcal{P}(\Omega)$, the power set of $\Omega$. For $k \in \mathbb{N}$, let $\mathcal{P}_k(\Omega)$ denote all the $k$-subsets of $\Omega$ - clearly $G$ also has an induced action upon $\mathcal{P}_k(\Omega)$. In this paper we shall assume $G$ and $\Omega$ are finite. Let $\sigma_k(G, \Omega)$ denote the number of $G$-orbits on $\mathcal{P}_k(\Omega)$. Questions as to the behaviour of $\sigma_k(G, \Omega)$ as $k$ varies and the relationship between $G$-orbit lengths for various $k$ arise naturally. A contribution to the former type of question is given by the venerable theorem of Livingstone and Wagner [12] which states that for $k \in \mathbb{N}$ with $k \leq |\Omega|/2$,

$$\sigma_{k-1}(G, \Omega) \leq \sigma_k(G, \Omega).$$

Generalizations of this theorem have been obtained by Mnukhin and Siemons [14]. While Bundy and Hart [3] have considered the situation when

$$\sigma_{k-1}(G, \Omega) = \sigma_k(G, \Omega).$$

Results on $G$-orbit lengths are somewhat patchy at present - see Siemons and Wagner [18], [19] and Mnukhin [15]. For the record, we remark there is a considerable literature concerning the infinite case; for a small selection see Cameron [4].

The main aim here is to establish formulae for $\sigma_k(G, \Omega)$ when $G$ is a rank one simple Lie-type group acting 2-transitively on $\Omega$. Thus set $q = p^a$ where

$p$ is a prime and $a \in \mathbb{N}$. Then the possibilities for $G$ are $L_2(q)$ $(q > 3)$, the 2-dimensional projective special linear groups, $Sz(q)$ $(q = 2^{2n+1} > 2)$, the Suzuki groups, $U_3(q)$ $(q > 2)$, the 3-dimensional projective special unitary groups and $R(q)$ $(q = 3^{2n+1} > 3)$, the Ree groups. The corresponding sets $\Omega$ are the projective line (with $|\Omega| = q+1$), the Suzuki oval (with $|\Omega| = q^2+1$), the isotropic 1-spaces of a 3-dimensional unitary space (with $|\Omega| = q^3+1$) and the Steiner system $S(2, q+1, q^3+1)$ (with $|\Omega| = q^3+1$). Before stating our main results we must introduce some notation. For $b, c \in \mathbb{N}$, we use $(b, c)$ to denote the greatest common divisor of $b$ and $c$. For $\ell \in \mathbb{N}$ we let

$$\mathcal{D}(\ell) = \{n \in \mathbb{N} \mid n \text{ divides } \ell\}$$

and $\mathcal{D}^*(\ell) = \mathcal{D}(\ell) \setminus \{1\}$. Euler's phi function $\phi$ (see [17]) will feature in our results. Our final piece of notation concerns partitions. Let $n \in \mathbb{N}$, and let $\pi = \lambda_1\lambda_2...\lambda_r$ where $\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_r$ and $\sum_{i=1}^{r} \lambda_i = n$. Though we will frequently use the more compressed notation $\pi = \mu_1^{a_1}\mu_2^{a_2}...$ where $\mu_1 < \mu_2 < ...$ ($a_i$ being the multiplicity of $\mu_i$ in the partition $\pi$). For $k \in \mathbb{N}$, $\eta_k(\pi)$ is defined to be the number of subsequences $\lambda_{i_1}, \lambda_{i_2}, ..., \lambda_{i_s}$ of $\lambda_1, ..., \lambda_r$ which form a partition of $k$. Since $G$ acts 2-transitively on $\Omega$, we have $\sigma_1(G, \Omega) = \sigma_2(G, \Omega) = 1$, so we shall assume $k \geq 3$. Now we come to our first theorem.

**Theorem 1.1.** *Suppose that $G \cong L_2(q)$ $(q > 3)$ acts upon the projective line $\Omega$, and let $k \in \mathbb{N}$ with $k \geq 3$. Set $d = (2, q-1)$. Then*

$$\begin{aligned}\sigma_k(G, \Omega) &= \frac{d}{q(q+1)(q-1)}\eta_k(1^{q+1}) + \frac{d}{q}\eta_k(1^1 p^{\frac{q}{p}}) \\ &+ \frac{d}{2(q+1)} \sum_{m \in \mathcal{D}^*(\frac{q+1}{d})} \phi(m)\eta_k\left(m^{\frac{q+1}{m}}\right) \\ &+ \frac{d}{2(q-1)} \sum_{m \in \mathcal{D}^*(\frac{q-1}{d})} \phi(m)\eta_k\left(1^2 m^{\frac{q-1}{m}}\right).\end{aligned}$$

In [5] Cameron, Maimani, Omidi and Teyfeh-Razaie give methods for calculating $\sigma_k(L_2(q), \Omega)$, where $\Omega$ is the projective line and $q \equiv 3 \bmod 4$, and Cameron, Omidi and Teyfeh-Razaie [6] follow a similar approach for $\sigma_k(PGL(2, q), \Omega)$, their interest being motivated by a search for 3-designs. Further work is presented by Liu, Tang and Wu [11] and also Chen and Liu [7], in the case when $q \equiv 1 \bmod 4$.

**Theorem 1.2.** *Suppose $G \cong Sz(q)$ ($q = 2^{2n+1} > 2$, $n \in \mathbb{N}$) acts upon the Suzuki oval $\Omega$. Let $r \in \mathbb{N}$ be such that $r^2 = 2q$, and let $k \in \mathbb{N}$ with $k \geq 3$. Then*

$$\begin{aligned}
\sigma(G, \Omega) \quad = \quad & \frac{1}{q^2(q-1)(q^2+1)}\eta_k(1^{q^2+1}) + \frac{1}{q^2}\eta_k(1^1 2^{\frac{q^2}{2}}) \\
& + \frac{1}{q}\eta_k(1^1 4^{\frac{q^2}{4}}) + \frac{1}{2(q-1)} \sum_{m \in \mathcal{D}^*(q-1)} \phi(m)\eta_k(1^2 m^{\frac{q^2-1}{m}}) \\
& + \frac{1}{4(q+r+1)} \sum_{m \in \mathcal{D}^*(q+r+1)} \phi(m)\eta_k(m^{\frac{q^2+1}{m}}) \\
& + \frac{1}{4(q-r+1)} \sum_{m \in \mathcal{D}^*(q-r+1)} \phi(m)\eta_k(m^{\frac{q^2+1}{m}}).
\end{aligned}$$

The corresponding result for $U_3(q)$ is more complicated than for $L_2(q)$ and $Sz(q)$ - see Definitions 3.1, 3.2, 3.3 and 3.4 for an explanation of the notation in the next theorem.

**Theorem 1.3.** *Suppose $G \cong U_3(q)$ ($q > 2$) acts upon $\Omega$, the set of isotropic points of a 3-dimensional unitary space. Let $k \in \mathbb{N}$ with $k \geq 3$, and set $d = (3, q+1)$ and $\ell = \frac{q+1}{d}$. Then*

$$\begin{aligned}
\sigma_k(G, \Omega) \quad = \quad & \frac{d(\eta_k(\pi_1) + \mu_k)}{q^3(q^3+1)(q^2-1)} + \frac{d}{q(q+1)(q^2-1)} \sum_{m \in \mathcal{D}^*(\ell)} \phi(m)\eta_k(\pi_4^{(m)}) \\
& + \frac{d}{q(q+1)(p-1)} \left( \sum_{\substack{m=pj \\ j \in \mathcal{D}^*(\ell)}} \phi(m)\eta_k(\pi_5^{(m)}) \right) + \frac{d\sigma_k(E_0^*, \Omega)}{6(q+1)^2} \\
& + \frac{d}{2(q^2-1)} \sum_{\substack{m \in \mathcal{D}(\frac{q^2-1}{d}) \\ m \notin \mathcal{D}(\ell)}} \phi(m)\eta_k(\pi_7^{(m)}) \\
& + \frac{d(q+1)}{3(q^3+1)} \sum_{m \in \mathcal{D}^*(\frac{q^2-q+1}{d})} \phi(m)\eta_k(\pi_8^{(m)}).
\end{aligned}$$

Lemma 3.9 gives formulae for $\sigma_k(E_0^*, \Omega)$. For corresponding results on the Ree groups see [1].

The proofs of Theorems 1.1, 1.2 and 1.3 all rely upon the orbit counting result commonly referred to as Burnside's Lemma, though this result can be traced back to earlier work of Cauchy and Frobenius. Thus our main task here is to enumerate the cycle types of elements in $G$ in their action on the various $\Omega$. For $G \cong L_2(q)$ or $Sz(q)$ this is straightforward, particularly as $G$ may be partitioned by certain subgroups (see Lemmas 2.5 and 2.6). For $G \cong U_3(q)$ we make use of the description of conjugacy classes obtained in [20]. There the conjugacy classes are divided into a number of types – those of the same type have the same size and fix the same number of points of $\Omega$, $\Omega$ being the set of isotropic 1-spaces of a 3-dimensional unitary space (see Table 2). Using information about the subgroup structure of $G$, in Lemma 3.5 we determine the cycle structures on $\Omega$ of elements in all conjugacy class types except for $\mathcal{C}_6 \cup \mathcal{C}_6'$. This is relatively straightforward. However $\mathcal{C}_6 \cup \mathcal{C}_6'$ is a different kettle of fish – see Table 1 which details the varied cycle structures for such elements in the case of $U_3(71)$ (so $|\Omega| = 357,912$).

| Cycle Type of Conjugacy Class Representative | Number of Classes | Cycle Type of Conjugacy Class Representative | Number of Classes |
|---|---|---|---|
| $2^{36}4^{89460}$ | 1 | $6^{12}12^{29820}$ | 2 |
| $2^{36}8^{44730}$ | 2 | $6^{12}24^{14910}$ | 4 |
| $2^{36}12^{29820}$ | 2 | $6^{12}8^{9}24^{14907}$ | 8 |
| $2^{36}24^{14910}$ | 4 | $8^{9}12^{6}24^{14907}$ | 16 |
| $2^{36}3^{24}6^{59628}$ | 2 | $9^{39768}$ | 3 |
| $3^{24}6^{59640}$ | 1 | $9^{8}18^{19880}$ | 9 |
| $3^{24}12^{29820}$ | 2 | $9^{8}36^{9940}$ | 18 |
| $3^{24}24^{14910}$ | 4 | $9^{8}72^{4970}$ | 36 |
| $3^{24}4^{18}12^{29814}$ | 4 | $12^{6}24^{14910}$ | 8 |
| $3^{24}8^{9}24^{14907}$ | 8 | $18^{4}36^{9940}$ | 18 |
| $4^{18}8^{44730}$ | 4 | $18^{4}72^{4970}$ | 36 |
| $4^{18}24^{14910}$ | 8 | $36^{2}72^{4970}$ | 72 |
| $4^{18}6^{12}12^{29814}$ | 4 | $3^{119304}$ | 1 |

Table 1: Cycle types for $\mathcal{C}_6 \cup \mathcal{C}_6'$ class types in $U_3(71)$

Representatives for all classes of type $\mathcal{C}_6 \cup \mathcal{C}_6'$ are to be found in an abelian subgroup $E$ of $G$ where $E$ is isomorphic to a direct product of cyclic groups of order $(q+1)/d$ and $q+1$ ($d = (3, q+1)$). The key result in enumerating these possible cycle types (and their multiplicities) is Lemma 3.8. With this result to hand, Lemma 3.9 then determines the contribution of the $\mathcal{C}_6 \cup \mathcal{C}_6'$ conjugacy classes to the sum $\sum_{g \in G} |\mathrm{fix}_{\Omega_k}(g)|$ (where $\Omega_k = \mathcal{P}_k(\Omega)$). Combining Lemmas 3.5 and 3.9 yields Theorem 1.3.

It is of interest to examine the number of orbits for these groups on subsets of size 3 (and in the case of $L_2(q)$, size 4), of their respective $G$-sets. The following corollaries can all be derived by appropriate substitutions into Theorems 1.1, 1.2, 1.3 and the corresponding result for the Ree groups as found in [1]. For full details of the proofs see [1].

**Corollary 1.4.** *Let $q = p^a > 2$ where $p$ is a prime and let $\Omega$ be the projective line with $q + 1$ points. Then*

$$\sigma_3(L_2(q), \Omega) = \begin{cases} 2, & \text{if } q \equiv 1 \text{ mod } 4 \\ 1, & \text{if } q \equiv 3 \text{ mod } 4 \end{cases}.$$

**Corollary 1.5.** *Let $L_n = L_2(2^n)$ acting on the projective plane $\Omega_n$, and put $a_n = \sigma_4(L_n, \Omega_n)$. Setting $a_1 = a_2 = 1$, for $n \geq 3$ we have*

$$a_n = a_{n-1} + 2a_{n-2}.$$

**Corollary 1.6.** *Let $q = 2^{2n+1}$ and $\Omega_n$ be the Suzuki oval with $q^2 + 1$ points. Set $a_n = \sigma_3(Sz(q), \Omega_n)$. Then*

$$a_n = \frac{4^n + 2}{3}.$$

**Corollary 1.7.** *Let $q = 3^n$ and $\Omega_n$ be the $q^3 + 1$ isotropic points of a unitary 3-space. Set $a_n = \sigma_3(U_3(q), \Omega_n)$. Then*

$$a_n = \frac{3^n + 3}{2}.$$

**Corollary 1.8.** *Let $q = 3^{2n+1}$ and $\Omega_n$ be the Steiner system on $q^3 + 1$ points. Set $a_n = \sigma_3(R(q), \Omega_n)$. Then*

$$a_n = \frac{(3^{2n+1} + 3)^2}{6}.$$

Two of the sequences found are of interest more generally, the sequence $\{a_n\}$ appearing in Corollory 1.5 is known as the Jacobsthal sequence [21], and the sequence $\{a_n\}$ given in Corollary 1.7 is associated to Sierpinski's Triangle, see [22].

# 2 Background Results

First we recall some background results, starting with the frequently misattributed Burnside's Lemma (see [16]).

**Lemma 2.1.** *Let $H$ be a finite group and $\Omega$ a finite $H$-set. If $t$ is the number of $H$-orbits on $\Omega$, then*
$$t = \frac{1}{|H|}\sum_{h\in H} |\mathrm{fix}_\Omega(h)|.$$

For a partition of $n$, $\pi = \lambda_1\lambda_2...\lambda_r$ (such that $\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_r$ and $\sum_{i=1}^r \lambda_i = n$) we recall from Section 1 that, for $k \in \mathbb{N}$, $\eta_k(\pi)$ is the number of subsequences $\lambda_{i_1}, \lambda_{i_2}, ..., \lambda_{i_s}$ of $\lambda_1, ..., \lambda_r$ which form a partition of $k$. As an example consider $\pi = 11444$ ($= 1^2 4^3$ in compressed form), a partition of $n = 14$. Then $\eta_5(\pi) = 6$, $\eta_6(\pi) = 3$, $\eta_7(\pi) = 0$ and $\eta_8(\pi) = 3$. Our interest in $\eta_k(\pi)$ is because of the following two simple lemmas.

**Lemma 2.2.** *Suppose $g \in Sym(\Lambda)$ where $|\Lambda| = n$, and let $k \in \mathbb{N}$. If $g$ has cycle type $\pi$ on $\Lambda$ (viewed as a partition of $n$), then $g$ fixes (set-wise) $\eta_k(\pi)$ $k$-subsets of $\Lambda$.*

**Lemma 2.3.** *Let $\pi = \mu_1^{a_1}\mu_2^{a_2}...\mu_s^{a_s}$ be a partition of $n$ (in compressed form). Then*
$$\eta_k(\pi) = \prod_{(k_1,k_2,...,k_s)} \binom{a_1}{k_1}\binom{a_2}{k_2}...\binom{a_s}{k_s},$$
*running over all $s$-tuples $(k_1, k_2, ..., k_s)$ with $k_i \geq 0$ and $\mu_1 k_1 + \mu_2 k_2 ... + \mu_s k_s = k$.*

**Lemma 2.4.** *Let $H \cong \mathbb{Z}_n$ and let $m \in \mathbb{N}$, $m \neq 1$, be such that $m \mid n$. If $p_1, p_2, ..., p_r$ are the distinct prime divisors of $m$, then the number of elements in $H$ of order $m$ is*
$$\phi(m) = \frac{m}{p_1 p_2 ... p_r}(p_1 - 1)(p_2 - 1)...(p_r - 1).$$

*Proof.* Since $H$ contains a unique cyclic subgroup $H_0$ of order $m$, all elements of order $m$ in $H$ will be contained in $H_0$. The number of elements of order $m$ in $H_0$ is the number of integers in $\{1, 2, ..., m\}$ which are coprime to $m$ and this, by definition, is $\phi(m)$. The stated formula for $\phi(m)$ is given as Theorem 7.5 in [17]. $\square$

A few well known facts regarding $L_2(q)$ and $Sz(q)$ are given in the next two lemmas.

**Lemma 2.5.** *Let $q = p^a > 3$ where $p$ is a prime and $a \in \mathbb{N}$. Suppose $G \cong L_2(q)$, and let $P \in Syl_p(G)$.*

*(i)* $|G| = \frac{q(q+1)(q-1)}{d}$ *where* $d = (2, q-1)$.

*(ii)* *$G$ acts 2-transitively upon the projective line $\Omega$ and $G_\alpha = N_G(P)$ for some $\alpha \in \Omega$.*

*(iii)* *$G$ contains cyclic subgroups $H_- = \langle h_- \rangle$ and $H_+ = \langle h_+ \rangle$ where $|H_-| = \frac{q-1}{d}$ and $|H_+| = \frac{q+1}{d}$. Set $\mathcal{S} = \{P^g, H_-^g, H_+^g \mid g \in G\}$. Then every non-identity element of $G$ belongs to a unique subgroup in $\mathcal{S}$.*

*(iv)* *$h_-$ has cycle type $1^2 \left(\frac{q-1}{d}\right)^d$ on $\Omega$ and $h_+$ has cycle type $\left(\frac{q+1}{d}\right)^d$ on $\Omega$. For $1 \neq x \in P$, $x$ has cycle type $1^1 p^{\frac{q}{p}}$ on $\Omega$.*

*(v)* *The number of elements of order $p$ is $(q-1)(q+1)$.*

*(vi)* *$[G : N_G(H_-)] = \frac{q(q+1)}{2}$ and $[G : N_G(H_+)] = \frac{q(q-1)}{2}$.*

*Proof.* For parts $(i) - (iv)$ see 8.1 Hilfssatz and for $(iii)$, $(iv)$ and $(vi)$ consult 8.3, 8.4, 8.5 Satz of [9]. Part $(v)$ is given in 8.2 Satz (b) and (c) of [9]. □

**Lemma 2.6.** *Let $q = 2^{2n+1}$ where $n \in \mathbb{N}$ and set $r = 2^{n+1}$. Suppose $G \cong Sz(q)$ and let $P \in Syl_2 G$.*

*(i)* *$|G| = q^2(q-1)(q^2+1)$.*

*(ii)* *$G$ acts 2-transitively on the Suzuki oval $\Omega$ and $G_\alpha = N_G(P)$ for some $\alpha \in \Omega$.*

*(iii)* *$G$ contains cyclic subgroups $H_0 = \langle h_0 \rangle$, $H_- = \langle h_- \rangle$ and $H_+ = \langle h_+ \rangle$ where $|H_0| = q-1$, $|H_-| = q-r+1$ and $|H_+| = q+r+1$. Set $\mathcal{S} = \{P^g, H_0^g, H_-^g, H_+^g \mid g \in G\}$. Then every non-identity element of $G$ belongs to a unique subgroup in $\mathcal{S}$.*

*(iv)* *$h_0$ has cycle type $1^2(q-1)^{q+1}$, $h_-$ has cycle type $(q-r+1)^{\frac{q^2+1}{q-r+1}}$ and $h_+$ has cycle type $(q+r+1)^{\frac{q^2+1}{q+r+1}}$ on $\Omega$. For $x \in P$, $x$ has cycle type $1^1 2^{\frac{q^2}{2}}$, respectively $1^1 4^{\frac{q^2}{4}}$, on $\Omega$ if it has order 2, respectively 4.*

*(v)* *$|N_G(H_0)| = 2(q-1)$, $|N_G(H_-)| = 4(q-r+1)$ and $|N_G(H_+)| = 4(q+r+1)$.*

*(vi)* *$P$ contains $q-1$ elements of order 2 and $q^2-q$ elements of order 4.*

*Proof.* Consult Theorem 9 of [23]. □

Next we give a compendium of facts about $U_3(q)$.

**Lemma 2.7.** *Let $q = p^a > 2$ where $p$ is a prime and $a \in \mathbb{N}$, and suppose $G \cong U_3(q)$. Let $P \in Syl_pG$ and set $d = (q+1, 3)$.*

*(i)* $|G| = q^3\frac{(q^2-1)}{d}(q^3+1)$.

*(ii)* *$G$ acts 2-transitively on $\Omega$, the set of isotropic 1-spaces of a unitary 3-space, $|\Omega| = q^3+1$ and $G_\alpha = N_G(P)$ for some $\alpha \in \Omega$. Further for $\beta \in \Omega \setminus \{\alpha\}$, $N_G(P) = PG_{\alpha,\beta}$ with $G_{\alpha,\beta}$ cyclic of order $\frac{q^2-1}{d}$ and $|C_{G_{\alpha,\beta}}(Z(P))| = \frac{(q+1)}{d}$.*

*(iii)* *$P$ has class 2 with $|Z(P)| = q$. If $p$ is odd, then $P$ has exponent $p$ and if $p = 2$ then $P$ has exponent 4 with the set of involutions of $P$ being $Z(P)^\#$.*

*Let ˆdenote the image of subgroups of $SU_3(q)$ in $U_3(q)$ ($\cong G$).*

*(iv)* *$G$ has a maximal subgroup $M$ isomorphic to $\hat{}GU_2(q)$.*

*(v)* *$M$ has a subgroup $E_0$ of shape $\hat{}(q+1)^2$ for which $N_G(E_0) \sim \hat{}(q+1)^2.Sym(3)$ and any subgroup of $G$ of shape $\hat{}(q+1)^2.Sym(3)$ is conjugate to $N_G(E_0)$.*

*(vi)* *$G$ has a cyclic subgroup $C$ of order $\frac{q^2-q+1}{d}$ for which $N_G(C) \sim C.3$ is a Frobenius group.*

*Proof.* For parts $(i)$ to $(iii)$ see Suzuki [23] and Huppert [9]. Part $(iv)$ follows from Mitchell [13] (or Bray, Holt, Roney-Dougal [2]). Also from either [2] or [13] $G$ has one conjugacy class of maximal subgroups of shape $\hat{}(q+1)^2.Sym(3)$ (except when $q = 5$) and $(vi)$ holds (except when $q = 3, 5$). Using the Atlas [8] for these exceptional cases we obtain $(v)$ and $(vi)$. □

From Table 2 in [20] we can extract details of the conjugacy classes of $G = U_3(q)$ as well as some supplementary information which we display in Table 2 ($d = (3, q+1), \ell = \frac{q+1}{d}$ and $\Omega$ as in Lemma 2.7(ii)).

We have used the same notation for the classes as in [20] except we have omitted the superscripts used there as they are of no importance here. Because $U_3(q)$ acts 2-transitively on $\Omega$, by page 69 of [10] the permutation character must be $\chi_1 + \chi_{q^3}$ (as in Table 2 of [20]) which then yields the last column of the table.

| Class Type | Number of Classes of each Type | Centralizer Order | $\lvert\mathrm{fix}_\Omega(g)\rvert$, $g^G \in \mathcal{C}_i$ |
|---|---|---|---|
| $\mathcal{C}_1$ | 1 | $\lvert G\rvert$ | $q^3+1$ |
| $\mathcal{C}_2$ | 1 | $\frac{q^3(q+1)}{d}$ | 1 |
| $\mathcal{C}_3$ | $d$ | $q^2$ | 1 |
| $\mathcal{C}_4$ | $\ell-1$ | $\frac{q(q+1)(q^2-1)}{d}$ | $q+1$ |
| $\mathcal{C}_5$ | $\ell-1$ | $\frac{q(q+1)}{d}$ | 1 |
| $\mathcal{C}_6$ | $\frac{q^2-q+1-d}{6d}$ | $\frac{(q+1)^2}{d}$ | 0 |
| $\mathcal{C}_6'$ | 0 if $d=1$, 1 if $d=3$ | $(q+1)^2$ | 0 |
| $\mathcal{C}_7$ | $\frac{q^2-q-2}{2d}$ | $\frac{q^2-1}{d}$ | 2 |
| $\mathcal{C}_8$ | $\frac{q^2-q+1-d}{3d}$ | $\frac{q^2-q+1}{d}$ | 0 |

Table 2: Conjugacy classes of $U_3(q)$

# 3 The Number of Orbits on $\mathcal{P}_k(\Omega)$

We begin with the

**Proof of Theorem 1.1**. Put $\Omega_k = \mathcal{P}_k(\Omega)$. Suppose $k \in \mathbb{N}$ with $k \geq 3$, and let $1 \neq g \in G$ ($\cong L_2(q)$) be an element of order $m$. Then by Lemma 2.5 $(iii)$ $g$ must be contained (uniquely) in a conjugate of one of $P$, $H_-$ and $H_+$. Since we seek to determine $\lvert\mathrm{fix}_{\Omega_k}(g)\rvert$ we may suppose that $g$ is contained in one of $P$, $H_-$ and $H_+$.

First we consider the case when $g \in H_+$. Since $g$ is some power of $h_+$, by Lemma 2.5$(iv)$, $g$ has cycle type $m^{\frac{q+1}{m}}$. By Lemmas 2.4 and 2.5 $(iv)$ $H_+$ contains $\phi(m)$ elements of order $m$ and there are $\frac{q(q-1)}{2}$ conjugates of $H_+$, whence these elements contribute

$$\frac{q(q-1)}{2} \sum_{m \in \mathcal{D}^*(\frac{q+1}{d})} \phi(m)\eta_k\left(m^{\frac{q+1}{m}}\right)$$

to the sum $\sum_{g\in G} \lvert\mathrm{fix}_{\Omega_k}(g)\rvert$. Now consider the case when $g \in H_-$. As $g$ is a power of $h_-$, by Lemma 2.5 $(iv)$, $g$ has cycle type $1^2 m^{\frac{q-1}{m}}$. Employing Lemmas 2.4 and 2.5 $(iv)$ we obtain

$$\frac{q(q+1)}{2} \sum_{m \in \mathcal{D}^*(\frac{q-1}{d})} \phi(m)\eta_k\left(1^2 m^{\frac{q-1}{m}}\right),$$

in the sum $\sum_{g\in G} \lvert\mathrm{fix}_{\Omega_k}(g)\rvert$. Similar considerations for $g \in P$, using Lemma 2.5, yield

$$(q-1)(q+1)\eta_k(1^1 p^{\frac{q}{p}}).$$

Combining the above with Lemmas 2.1 and 2.5 $(i)$ we obtain the expression for $\sigma_k(G,\Omega)$.

$\square$

The proof of Theorem 1.2 is similar to that of Theorem 1.1 except we use Lemma 2.6 in place of Lemma 2.5. The remainder of this section is devoted to establishing Theorem 1.4. So we assume $G \cong U_3(q)$, $(q = p^a > 2)$ and $\Omega$ is the set of isotropic 1-spaces of a 3-dimensional unitary space.

Before beginning the proof of Theorem 1.4, there are a number of preparatory definitions, notation and lemmas we need. First we describe the partitions that arise in Theorem 1.4. Before we can do that, and introduce $\mu_k$, we require a barrage of notation associated with pairs of natural numbers dividing $\ell'$ where $\ell' \in \mathcal{D}(\ell)$, $\ell = \frac{q+1}{d}$. So let $\ell' \in \mathcal{D}(\ell)$ and

$$(\ell_1, \ell_2) \in \mathcal{D}(\ell') \times \mathcal{D}(\ell'),$$

and let $p_1, .., p_r$ be prime numbers such that $\ell_1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ and $\ell_2 = p_1^{\beta_1} p_1^{\beta_2} ... p_r^{\beta_r}$ where for $i = 1, ..., r$ at least one of the the $\alpha_i$ and $\beta_i$ is non-zero. If $\alpha_i \neq \beta_i$, then define $\gamma_i = max\{\alpha_i, \beta_i\}$. Without loss of generality we shall assume that $\alpha_i = \beta_i$ for $1 \leq i \leq s$ and $\alpha_i \neq \beta_i$ for $s < i \leq r$. Set

$$\begin{aligned} \ell_0 &= p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s} \; (= p_1^{\beta_1} p_2^{\beta_2} ... p_s^{\beta_s}), \\ m_1 &= p_{s+1}^{\alpha_{s+1}} p_{s+2}^{\alpha_{s+2}} ... p_r^{\alpha_r} \text{ and} \\ m_2 &= p_{s+1}^{\beta_{s+1}} p_{s+2}^{\beta_{s+2}} ... p_r^{\beta_r}. \end{aligned}$$

Also set $\ell_* = p_{s+1}^{\gamma_{s+1}} p_{s+2}^{\gamma_{s+2}} ... p_r^{\gamma_r}$ and note that $\ell_1 = \ell_0 m_1$ and $\ell_2 = \ell_0 m_2$. We remark that we do not exclude the possibilities $\ell_1 = \ell_0 = \ell_2$ or $\ell_1 = m_1$ and $\ell_2 = m_2$. Put $\ell_{12} = lcm\{\ell_1, \ell_2\}$. If $\ell_i = 1$ then $\ell_0 = 1 = m_i$ and if $\ell_1 = \ell_2 = 1$ then we set $\ell_* = 1$.

**Definition 3.1.** (i) $\pi_1 = 1^{q^3+1}$.

(ii) $\pi_2 = 1^1 p^{\frac{q^3}{p}}$.

(iii) $\pi_3 = 1^1 4^{\frac{q^3}{4}}$ (only defined for $p = 2$).

(iv) $\pi_4^{(m)} = 1^{q+1} m^{\frac{q^3-q}{m}}$ where $m \in \mathcal{D}^*(\ell)$.

(v) $\pi_5^{(m)} = 1^1 p^{\frac{q}{p}} m^{\frac{q^3-q}{m}}$ where $m = pj$ and $j \in \mathcal{D}^*(\ell)$.

(vi) $\pi_6^{(\ell_1,\ell_2,n)} = \ell_1^{\frac{q+1}{\ell_1}} \ell_2^{\frac{q+1}{\ell_2}} n^{\frac{q+1}{n}} \ell_{12}^{\frac{q^3-3q-2}{\ell_{12}}}$ where $(\ell_1,\ell_2) \in \mathcal{D}^*(\ell) \times \mathcal{D}^*(\ell)$ and $n = n_*\ell_*$, $n_* \in \mathcal{D}(\ell_0)$.

(vii) $\pi_7^{(m)} = 1^2 j^{\frac{q-1}{j}} m^{\frac{q^3-q}{m}}$ where $m \in \mathcal{D}(\frac{q^2-1}{d})$, $m \notin \mathcal{D}(\ell)$, $j = \frac{m}{(m,\ell)}$.

(viii) $\pi_8 = m^{\frac{q^3+1}{m}}$ where $m \in \mathcal{D}^*(q^2-q+1)$.

(ix) When $3^i | q+1$ with $i \in \mathbb{N}$,

$$3^i \pi_6^{(\ell_1,\ell_2,n)} = (3^i\ell_1)^{\frac{q+1}{3^i\ell_1}} (3^i\ell_2)^{\frac{q+1}{3^i\ell_2}} (3^i n)^{\frac{q+1}{3^i n}} (3^i\ell_{12})^{\frac{q^3-3q-2}{3^i\ell_{12}}}$$

where $(\ell_1,\ell_2) \in \mathcal{D}(\ell) \times \mathcal{D}(\ell)$ and $n = n_*\ell_*$, $n_* \in \mathcal{D}(\ell_0)$.

**Definition 3.2.**

$$\mu_k = (q^3+1)(q^3-1)\eta_k(\pi_2)$$

if $p \neq 2$ and

$$\mu_k = (q^3+1)((q-1)\eta_k(\pi_2) + (q^3-q)\eta_k(\pi_3))$$

if $p = 2$.

**Definition 3.3.** Let $k \in \mathbb{N}$, and we continue to set $\ell = \frac{q+1}{d}$. For $(\ell_1,\ell_2) \in \mathcal{D}(q+1) \times \mathcal{D}(q+1)$ we use the notation $\ell_0, m_1, m_2, \ell_*$ as defined earlier.

(i) Let $(\ell_1,\ell_2) \in \mathcal{D}(q+1) \times \mathcal{D}(q+1)$, $n = \ell_* n_*$ with $n_* \in \mathcal{D}(\ell_0)$ and $n_* = p_1^{\delta_1} p_2^{\delta_2} ... p_s^{\delta_s}$. If $\ell_0 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$, then we define

$$f(\ell_1,\ell_2,n) = \phi(m_1)\phi(m_2)\phi(\ell_0) \prod_{\substack{\alpha_j=\delta_j \\ 1\le j\le s}} p_j^{\alpha_j-1}(p_j-2)\phi\left(\prod_{\substack{\alpha_j\neq\delta_j \\ 1\le j\le s}} p_j^{\delta_j}\right).$$

(ii)

$$\lambda_k^*(\ell,\ell) = \sum_{(\ell_1,\ell_2)\in\mathcal{D}^*(\ell)\times\mathcal{D}^*(\ell)} \sum_{\substack{1\neq n=\ell_* n_* \\ n_*\in\mathcal{D}(\ell_0)}} f(\ell_1,\ell_2,n)\eta_k(\pi_6^{(\ell_1,\ell_2,n)}).$$

(iii) For $\ell' \in \mathcal{D}^*(q+1)$ and $i \in \mathbb{N}$ such that $3^i | \ell'$ set

$$\lambda_k(\ell',\ell';i) = \sum_{(\ell_1,\ell_2)\in\mathcal{D}(\ell')\times\mathcal{D}(\ell')} \sum_{\substack{n=\ell_* n_* \\ n_*\in\mathcal{D}(\ell_0)}} f(\ell_1,\ell_2,n)\eta_k(3^i\pi_6^{(\ell_1,\ell_2,n)}).$$

**Definition 3.4.** Let $E_0$ be an abelian subgroup of $G$ isomorphic to the direct product of two cyclic groups of order $\frac{(q+1)}{d}$ and $(q+1)$ with $N_G(E_0) \sim \frac{(q+1)}{d}(q+1).Sym(3)$. Put $E_0^* = (\mathcal{C}_6 \cup \mathcal{C}_6') \cap E_0$, and define

$$\sigma_k(E_0^*, \Omega) = \sum_{g \in E_0^*} |\mathrm{fix}_{\Omega_k}(g)|,$$

where $\Omega_k = \mathcal{P}_k(\Omega)$.

**Remark 1.** Subgroups such as $E_0$ in Definition 3.4 exist by Lemma 2.7($v$), and $\sigma_k(E_0^*, \Omega)$ is the contribution of $E_0^*$ to the sum $\sum_{g \in G} |\mathrm{fix}_{\Omega_k}(g)|$.

**Lemma 3.5.** *The cycle type for elements in the classes of type $\mathcal{C}_i$ for $i \neq 6$ are given in Table 3.*

| Class Type | Order of $g$ | Cycle type of $g$ |
|---|---|---|
| $\mathcal{C}_1$ | 1 | $\pi_1$ |
| $\mathcal{C}_2$ | $p$ | $\pi_2$ |
| $\mathcal{C}_3$ | $4\ (p = 2)$<br>$p\ (p \neq 2)$ | $\pi_3$<br>$\pi_2$ |
| $\mathcal{C}_4$ | $m,\ (m \in \mathcal{D}^*(\ell))$ | $\pi_4^{(m)}$ |
| $\mathcal{C}_5$ | $px,\ (x \in \mathcal{D}^*(\ell))$ | $\pi_5^{(m)}$ |
| $\mathcal{C}_7$ | $m = js,\ (j \in \mathcal{D}^*(q-1),$<br>$s \in \mathcal{D}(\ell))$ | $\pi_7^{(m)}$ |
| $\mathcal{C}_8$ | $m, (m \in \mathcal{D}^*(q^2 - q + 1))$ | $\pi_8$ |

Table 3: Cycle Types

*Proof.* Let $X = g^G$ be a conjugacy class of type $\mathcal{C}_i$, $i \in \{1, ..., 8\} \setminus \{6\}$, and let $P \in Syl_p(G)$. If $i = 1$, then clearly $g = 1$. From the centralizer sizes in Table 2, for $i = 2$ we must have $X$ is the conjugacy class containing $Z(P)^{\#}$, while classes of type $\mathcal{C}_3$ are the conjugacy classes of elements in $P \setminus Z(P)$. If $p$ is odd, then by Lemma 2.7($iii$) the elements in classes of type $\mathcal{C}_3$ all have order $p$ whence, as elements in classes of types $\mathcal{C}_2$ and $\mathcal{C}_3$ fix just one element of $\Omega$, their cycle type is $\pi_2$. If $p = 2$, then for $i = 2$, we also have cycle type $\pi_2$ and for $i = 3$ as the elements of order 4 must square to involutions in $Z(P)$, their cycle type must be $\pi_3$.

From Lemma 2.7($iv$) $G$ possesses a maximal subgroup $M \cong \hat{\ }GU_2(q)$. Further, $Z(M)$ is cyclic of order $\ell = \frac{q+1}{d}$. It is straightforward to check that no two elements in $Z(M)^{\#}$ are $G$-conjugate. So we see, using the centralizer sizes in Table 2, $Z(M)^{\#}$ supplies representatives for all the conjugacy classes of type $\mathcal{C}_4$. Choose $h$ to be an element of order $p$ in $M$ (in fact $h$ is $G$-conjugate to an element in $Z(P)$, this can be seen as these elements must have centralizer with order divisible by $|Z(M)| = \frac{q+1}{d}$, hence cannot be in classes $\mathcal{C}_3$). By the structure of $M$, for any $h' \in Z(M)^{\#}$, $|C_G(hh')| = \frac{q(q+1)}{d}$. (We note that no element of $G \setminus M$ centralizes $M$ and that $h, h' \in M$, both are centralized by $Z(P) < M$ and $Z(M) < M$). Also for $h', h'' \in Z(M)^{\#}$ with $h' \neq h''$ we see that $hh'$ and $hh''$ are not $G$-conjugate. Therefore $\{hh' \mid h' \in Z(M)^{\#}\}$ gives representatives for all conjugacy classes of type $\mathcal{C}_5$. Now $|\mathrm{fix}_\Omega(g')| = q + 1$ for all $g' \in Z(M)^{\#}$. So for $h' \in Z(M)^{\#}$ of order $m$, $h'$ will have cycle type $\pi_4^{(m)}$ on $\Omega$. Similarly for $hh'$, $h' \in Z(M)^{\#}$ with $h'$ of order $m$, as $|\mathrm{fix}_\Omega(h)| = 1$, we infer that $hh'$ has cycle type $\pi_5^{(m)}$. So we have dealt with classes of type $\mathcal{C}_4$ and $\mathcal{C}_5$.

Next we look at classes of type $\mathcal{C}_7$. Since $|\mathrm{fix}_\Omega(g)| = 2$, we may suppose $g \in G_{\alpha,\beta}$ $(\cong \frac{q^2-1}{d})$, where $\alpha, \beta \in \Omega$, $\alpha \neq \beta$. We may also suppose $Z(M)(\cong \frac{q+1}{d}) \leq G_{\alpha,\beta}$ where $M$ is a maximal subgroup of $G$ isomorphic to $\hat{\ } GU_2(q)$. Since $|\mathrm{fix}_\Omega(g')| = q + 1$ for all $g' \in Z(M)^{\#}$, $g \in G_{\alpha,\beta} \setminus Z(M)$. Let $g$ have order $m$ and let $j$ be the smallest natural number such that $g^j \in Z(M)$. Then $m = (m, \ell)j$ where $j \in \mathcal{D}^*(q-1)$ (note that $j = 1$, as $G_{\alpha,\beta} \cong \frac{(q+1)}{d}$ contains a unique subgroup, $Z(M)$, of order $\frac{q+1}{d} = \ell$, would mean $g \in Z(M)$). So $j = \frac{m}{(m,\ell)}$ and hence $g$ has cycle type $\pi_7^{(m)}$.

Finally we look at those of type $\mathcal{C}_8$. From Lemma 2.7($vi$) $G$ has a cyclic subgroup $C \cong \frac{(q^2-q+1)}{d}$ with $N_G(C) \sim C.3$ being a Frobenius group. Now $C^{\#}$ has $(|C|-1)/3$ $N_G(C)$-conjugacy classes and it can be seen that no two of these are $G$-conjugate. Hence we have that the $N_G(C)$-conjugacy class representatives of $C^{\#}$ give us representatives for all of the classes of type $\mathcal{C}_8$. So, as $|\mathrm{fix}_\Omega(h)| = 0$ for all $h \in C^{\#}$, the elements in $C^{\#}$ has cycle type $\pi_8$ on $\Omega$, which completes the proof of Lemma 3.5.

□

We now turn our attention to the delicate process of dissecting the classes of type $\mathcal{C}_6 \cup \mathcal{C}_6'$.

**Lemma 3.6.** *Suppose $A \cong \mathbb{Z}_e \times \mathbb{Z}_e$ with $A$ containing three subgroups $A_i \cong \mathbb{Z}_e$ $(i = 1, 2, 3)$, such that $A_i \cap A_j = 1$ for $i \neq j$. Then there exists $a_1 \in A_1$, $a_2 \in A_2$ such that $A_1 = \langle a_1 \rangle$, $A_2 = \langle a_2 \rangle$ and $A_3 = \langle a_1 a_2 \rangle$.*

*Proof.* Since $A_1 \cap A_2 = 1$ and $A_1 \cong \mathbb{Z}_e$, $A = A_1 A_2$. Let $A_3 = \langle c \rangle$. Then $c = a_1 a_2$ where $a_i \in A_i$, $i = 1, 2$. Suppose $a_i$ has order $e_i$, $i = 1, 2$ and, without loss that, $e_1 \leq e_2$. Then $c^{e_1} = a_1^{e_1} a_2^{e_1} = a_2^{e_1} \in A_2 \cap A_3 = 1$. So

$e_2 \le e_1$ and hence $e_1 = e_2$. Since $c = a_1 a_2$ has order $e$, we must have that $e_1 = e_2 = e$, so proving the lemma. $\square$

**Hypothesis 3.7.** Suppose that $A_0$ is an abelian group containing a subgroup $A$ with $[A_0 : A] = 1$ or 3. Also suppose that $A$ has order $e^2$ and contains three subgroups $A_1, A_2, A_3$ with $A_i \cong \mathbb{Z}_e$ $(i = 1, 2, 3)$.

Further suppose that $\Omega$ is an $A_0$-set such that

(i) for $1 \ne g \in A_0$, $\mathrm{fix}_\Omega(g) = \emptyset$ if $g \notin A_1 \cup A_2 \cup A_3$ and $\mathrm{fix}_\Omega(g) = \mathrm{fix}_\Omega(A_i)$ if $g \in A_i$;

(ii) $\mathrm{fix}_\Omega(A_i) \cap \mathrm{fix}_\Omega(A_j) = \emptyset$ for $1 \le i \ne j \le 3$; and

(iii) for $i = 1, 2, 3$, $|\mathrm{fix}_\Omega(A_i)| = q + 1$.

Set $\Lambda_i = \mathrm{fix}_\Omega(A_i)$ for $i = 1, 2, 3$ and $\Lambda = \Omega \setminus (\Lambda_1 \cup \Lambda_2 \cup \Lambda_3)$ and so, by $(ii)$, $\Omega$ is the disjoint union

$$\Lambda_1 \cup \Lambda_2 \cup \Lambda_3 \cup \Lambda.$$

Moreover, by $(i)$, $A_0$ acts regularly on $\Lambda$ and for $i = 1, 2, 3$, $A_0/A_i$ acts regularly on $\Lambda_i$.

We shall encounter Hypothesis 3.7 both in a recursive setting and in the group $A_0 = \mathbb{Z}_{q+1} \times \mathbb{Z}_\ell$ (where $\ell = \frac{q+1}{d}$, $d = (3, q+1)$). For this $A_0$ we have $e = \ell$ and $A$ would be the subgroup of $A_0$ generated by the elements of $A_0$ of order $\ell$. Then $[A_0 : A] = d$.

**Lemma 3.8.** *Assume Hypothesis 3.7 holds and use the notation $A_0, A$ and $A_i$ in the hypothesis. Let $(\ell_1, \ell_2) \in \mathcal{D}(e) \times \mathcal{D}(e)$ where $e \in \mathcal{D}(\ell)$. The cycle structure on $\Omega$ of the elements $g = g_1 g_2 \in A$ where $g_i \in A_i$ $(i = 1, 2)$ with $g_i$ of order $\ell_i$ is*

$$(\ell_1)^{\frac{q+1}{\ell_1}} (\ell_2)^{\frac{q+1}{\ell_2}} (n)^{\frac{q+1}{n}} (\ell_{12})^{\frac{|\Lambda|}{\ell_{12}}},$$

*where $n = \ell_* n_*$ with $n_* \in \mathcal{D}(\ell_0)$ and $\ell_{12} = lcm(\ell_1, \ell_2)$. This cycle structure, as $g_1$ and $g_2$ ranges over the elements of order (respectively) $\ell_1$ and $\ell_2$ occurs*

$$\phi(m_1)\phi(m_2)\phi(\ell_0) \prod_{\substack{\alpha_j = \delta_j \\ 1 \le j \le s}} p_j^{\alpha_j - 1}(p_j - 2)\phi\left(\prod_{\substack{\alpha_j \ne \delta_j \\ 1 \le j \le s}} p_j^{\delta_j}\right)$$

*times, where $n_* = p_1^{\delta_1} ... p_s^{\delta_s}$.*

*Proof.* By Hypothesis 3.7 $(i)$ and $(ii)$ $A_i \cap A_j = 1$ for $i \neq j$. Hence, by Lemma 3.5 we may select $a_1 \in A_1$, $a_2 \in A_2$ so as to have $A_1 = \langle a_1 \rangle$, $A_2 = \langle a_2 \rangle$ and $A_3 = \langle a_1 a_2 \rangle$. Additionally we may identify $A$ with $A_1 A_2$. Let $g = g_1 g_2$ where $g_i \in A_i$ and $g_i$ has order $\ell_i$, $i = 1, 2$. The smallest $k \in \mathbb{N}$ such that $g^k \in A_2$ is clearly $\ell_1$ and, likewise, the smallest $k \in \mathbb{N}$ such that $g^k \in A_1$ is clearly $\ell_2$. Hence, as $A/A_2$ acts regularly on $\Lambda_2$, $g$ in its action on $\Lambda_2$ must be the product of disjoint cycles of length $\ell_1$. Similarly $g$ acts upon $\Lambda_1$ as a product of disjoint cycles each of length $\ell_2$. Concerning the action of $g$ on $\Lambda$, as $A_0$ acts regularly on $\Lambda$ and $\ell_{12} = lcm\{\ell_1, \ell_2\}$ is the order of $g$, $\Lambda$ is a disjoint union of $\frac{|\Lambda|}{\ell_{12}}$ length cycles of $g$.

Since $A_3 = \langle a_1 a_2 \rangle$ to find the lengths of $g$'s cycles on $\Lambda_3$, we must determine the smallest $k \in \mathbb{N}$ such that $g^k \in \langle a_1 a_2 \rangle$. For $i = 1, 2$ let $k_i \in \mathbb{N}$ with $k_i \leq e$ be such that $g_i = a_i^{k_i}$. So $g = a_1^{k_1} a_2^{k_2}$ and, we recall, $\ell_i = e/(e, k_i)$ for $i = 1, 2$. Thus we seek the smallest $k \in \mathbb{N}$ for which

$$g^k = (a_1^{k_1} a_2^{k_2})^k = a_1^{k_1 k} a_2^{k_2 k} = (a_1 a_2)^j$$

for some $j$, $0 \leq j < e$. This is the smallest $k \in \mathbb{N}$ such that $k_1 k \equiv k_2 k \bmod e$ which is $k = \frac{e}{(k_1 - k_2, e)}$.

Let $C$ be a cyclic group isomorphic to $\mathbb{Z}_e$ with generator $c$. Now for $i = 1, 2$ the order of $c^{k_i}$ is $\frac{e}{(e, k_i)} = \ell_i$ and the order of $c^{k_1}(c^{k_2})^{-1}$ is $k$. Thus to enumerate the possibilities for $k$ (recall $(\ell_1, \ell_2)$ is a fixed ordered pair) we look at the order of $c^{k_1}(c^{k_2})^{-1}$ as we run through the ordered pairs $(c^{k_1}, c^{k_2})$ of elements of $C$ of order, respectively, $\ell_1$ and $\ell_2$. In doing this there no loss in supposing $C = \langle c \rangle$ has order $lcm\{\ell_1, \ell_2\}$.

For $i = 1, ..., r$, let $P_i \in Syl_{p_i}(C)$. Since the order of elements in $C$ is the product of their orders in the projections into $P_i$ for $i = 1, ..., r$, we first consider the special case when $C = P_i \neq 1$, for some $i \in \{1, ..., r\}$. So $\ell_1 = p_i^{\alpha_i}$ and $\ell_2 = p_i^{\beta_i}$.

**(3.8.1)** If $\alpha_i \neq \beta_i$, then for all choices of $(c^{k_1}, c^{k_2})$, of which there are $\phi(p_i^{\alpha_i})\phi(p_i^{\beta_i})$, the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\gamma_i}$.

Recalling that by definition $\gamma_i = max\{\alpha_i, \beta_i\}$ we see that the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\gamma_i}$ as asserted.

Now we turn to the case when $\alpha_i = \beta_i$. Here we have $\phi(p_i^{\alpha_i})^2$ possible choices for $(c^{k_1}, c^{k_2})$. Let $C_1$ be the unique subgroup of $C$ of order $p_i^{\alpha_i - 1}$ (and note $c^{k_1}$ and $c^{k_2}$ are in $C \setminus C_1$). Should $c^{k_1}$ and $c^{k_2}$ be in different $C_1$ cosets of $C$, then $c^{k_1}(c^{k_2})^{-1}$ is not in $C_1$ whence $c^{k_1}(c^{k_2})^{-1}$ has order $p_i^{\alpha_i}$. This will happen $\phi(p_i^{\alpha_i}) p_i^{\alpha_i - 1}(p_i - 2)$ times. The number of ordered pairs $(c^{k_1}, c^{k_2})$ for which $c^{k_1}$ and $c^{k_2}$ are in the same $C_1$ coset of $C$ is $\phi(p_i^{\alpha_i}) p_i^{\alpha_i - 1}$. In this situation, for a fixed $c^{k_1}$, $c^{k_1}(c^{k_2})^{-1}$ runs through all the elements of $C_1$ thus yielding $\phi(p_i^{\alpha_i - 1})$ of order $p_i^{\alpha_i - 1}$, $\phi(p_i^{\alpha_i - 2})$ of order $p_i^{\alpha_i - 2}$, and so on. To summarize we have the following.

**(3.8.2)** Suppose $\alpha_i = \beta_i$. Then for $\phi(p_i^{\alpha_i})p_i^{\alpha_i-1}(p_i-2)$ of the ordered pairs $(c^{k_1}, c^{k_2})$ the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\alpha_i}$ and, for $j = 1, ..., \alpha_i$, $\phi(p_i^{\alpha_i})\phi(p_i^{\alpha_i-j})$ of the ordered pairs $(c^{k_1}, c^{k_2})$ the order of $c^{k_1}(c^{k_2})^{-1}$ is $p_i^{\alpha_i-j}$.

We now consider the general situation for $\ell_1 = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ and $\ell_2 = p_1^{\beta_1}p_1^{\beta_2}...p_r^{\beta_r}$. Looking at all those $i$ for which $\alpha_i \neq \beta_i$ (just for the moment considering the projections onto $P_{s+1}, ..., P_r$) we obtain that $c^{k_1}(c^{k_2})^{-1}$ has order $p_{s+1}^{\gamma_{s+1}}...p_r^{\gamma_r} = \ell_*$ for

$$\prod_{i=s+1}^{r} \phi(p_i^{\alpha_i})\phi(p_i^{\beta_i}) = \phi(m_1)\phi(m_2)$$

pairs $(c^{k_1}, c^{k_2})$ by (3.8.1) We now wish to enumerate the pairs $(c^{k_1}, c^{k_2})$ for which the order of $c^{k_1}(c^{k_2})^{-1}$ is $n$, where $n = \ell_* n_*$, $n_* \in \mathcal{D}(\ell_0)$ and $n_* = p_1^{\delta_1}p_2^{\delta_2}...p_s^{\delta_s}$. Using (3.8.2) and by just considering the projections on $P_1, ..., P_s$ we see this occurs for

$$\begin{aligned}
&\prod_{\alpha_i=\delta_i} \phi(p_i^{\alpha_i})p_i^{\alpha_i-1}(p_i-2) \prod_{\alpha_i\neq\delta_i} \phi(p_i^{\alpha_i})\phi(p_i^{\delta_i}) \\
&= \prod_{1\leq i\leq s} \phi(p_i^{\alpha_i}) \prod_{\alpha_i=\delta_i} p_i^{\alpha_i-1}(p_i-2) \prod_{\alpha_i\neq\delta_i} \phi(p_i^{\delta_i}) \\
&= \phi(\ell_0) \prod_{\alpha_i=\delta_i} p^{\alpha_i-1}(p_i-2)\phi\left(\prod_{\alpha_i\neq\delta_i} p_i^{\delta_i}\right)
\end{aligned}$$

pairs. Combining this with the projection onto $P_{s+1}, ..., P_r$ yields Lemma 3.8. $\square$

**Lemma 3.9.** *Let $E_0$ be an abelian subgroup of $G$ isomorphic to the direct product of two cyclic groups of order $\frac{(q+1)}{d}$ and $(q+1)$ with $N_G(E_0) \sim \frac{(q+1)}{d}(q+1).Sym(3)$. Also let $E$ be the subgroup of $E_0$ generated by the elements of $E_0$ of order $\ell = \frac{(q+1)}{d}$. Then*

*(i)* $\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell)$ *if* $d = 1$*;*

*(ii)* $\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2\lambda_k(\ell, \ell; 1)$ *if* $d = 3$ *and* $3 \nmid |E|$*; and*

*(iii)* $\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2.9^{b-1}\lambda_k(\frac{q+1}{3^b}, \frac{q+1}{3^b}; b)$ *if* $d = 3$, $3\big||E|$ *and* $3^b$ *is the largest power of* $3$ *dividing* $q+1$.

*Proof.* By Lemma 2.7(*iv*),(*v*) $G$ contains a subgroup $M$ with $M \sim\hat{}GU_2(q)$ and $E_0 \leq M$. From the structure of $N_G(E_0)$ and $\hat{}GU_2(q)$, $Z(M) \leq E_0$ with $Z(M) \cong \frac{q+1}{d}(= \ell)$. Let $h \in N_G(E_0)$ be an element of order 3. Because

$[N_M(E_0) : E_0] = 2$, $h \notin M = N_G(Z(M))$. In order to key in with the notation of Hypothesis 3.7, principally as we shall employ Lemma 3.8, we set $A_0 = E_0$ and $A = E$. Further, we set $A_1 = Z(M)$, $A_2 = Z(M)^h$ and $A_3 = Z(M)^{h^2}$. Since $\mathrm{fix}_\Omega(h) = \mathrm{fix}_\Omega(Z(M))$ for all $h \in Z(M)^{\#}$, it follows that $\mathrm{fix}_\Omega(A_i) \cap \mathrm{fix}_\Omega(A_j) = \emptyset$ for $1 \leq i \neq j \leq 3$. We also have $|\mathrm{fix}_\Omega(A_i)| = q+1$ and, by Table 2, $\mathrm{fix}_\Omega(g) = \emptyset$ if $g \in A_0 \setminus (A_1 \cup A_2 \cup A_3)$. Now $A$ is the subgroup of $A_0$ generated by the elements of $A_0$ of order $\ell$ and $A_i \cong \ell$. So we have $A_i \leq A$, $i = 1, 2, 3$ and $[A : A_0] = d$ $(= 1$ and $3)$. Hence Hypothesis 3.7 holds with $e = \ell$.

Suppose $d = 1$. Then $A = A_0$. Using Lemma 3.8 and Definition 3.3($ii$) we obtain $\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell)$. (Note the condition in Definition 3.3($ii$) on the outer sum that $(\ell_1, \ell_2) \in \mathcal{D}^*(\ell) \times \mathcal{D}^*(\ell)$ and on the inner sum that $n \neq 1$ prevents the counting of elements in $\mathcal{C}_4$.) So Lemma 3.9 holds in this case.

So we now investigate the case when $d = 3$. Hence $[A_0 : A] = 3$. Let $\theta : A_0 \mapsto A_0$ be defined by $\theta : g \mapsto g^3$. Then, as $A_0$ is abelian, $\theta$ is a homomorphism with $im\theta \leq A$ and $ker\theta = \{x \in A_0|$ order of $x$ is 1 or 3$\}$.

Further assume that $3 \nmid |E|$ (so $3 \nmid \ell$). Then, as $|A| = \ell^2$, $3 \nmid |A|$. Also we have $|ker\theta| = 3$ and therefore, by orders, $im\theta = A$. For every $g \in A_0 \setminus A$, the smallest power of $g$ contained in $A_i$ $(i = 1, 2, 3)$ will be three times the corresponding power for $h = g^3 = \theta(g)$. Now $3 \nmid |A|$ means that $\theta$ restricted to $A$ is a one-to-one map, and so the inverse image of $h$ contains two elements of $A_0 \setminus A$. Hence, using Lemma 3.8, the elements of $A_0 \setminus A$ contribute $2\lambda_k(\ell, \ell, 1)$ to the sum $\sum_{g \in G} |\mathrm{fix}_{\Omega_k}(g)|$. Thus, using Lemma 3.8 again, $\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2\lambda_k(\ell, \ell; 1)$, as stated.

The last case to be considered is when, as well as $d = 3$, we have $3\big||E|$. So $3|\ell$. As a consequence $|ker\theta| = 3^2$ and thus $[A : im\theta] = 3$. We seek to pinpoint $im\theta$. Now let $A_i^3$ denote the unique subgroup of $A_i$ of index 3 $(i = 1, 2, 3)$. Let $B$ be the subgroup of $A$ generated by the elements of $A$ of order $\ell/3$. Then $[A : B] = 3^2$ and, for $1 \leq i < j \leq 3$, $B = A_i^3 A_j^3$. Also observe that $im\theta \geq B$. Set $N = N_G(A_0)$, and recall that $N \sim (\frac{q+1}{d}(q+1)).Sym(3)$. Also the $N$-conjugacy class of $A_1$ is $\{A_1, A_2, A_3\}$. Hence $N$ normalizes $B$ $(= A_i^3 A_j^3, 1 \leq i < j \leq 3)$ and the $N$-conjugacy of $A_1 B$ is $\{A_1 B, A_2 B, A_3 B\}$. Moreover $A_i B \neq A_j B$ for $1 \leq i < j \leq 3$ (as $A = A_i A_j$). Evidently $im\theta$ is a normal subgroup of $N$ and therefore $\{im\theta, A_1 B, A_2 B, A_3 B\}$ comprise the four subgroups of index 3 in $A$ which contain $B$. Observe that the inverse image under $\theta$ of $B$ is $A$. Since, by Lemma 3.8, $\lambda_k^*(\ell, \ell)$ is the count for the contribution of elements in $A$, we are looking to determine the contribution from the elements in $A_0 \setminus A$. Thus for $h \in im\theta \setminus B$, $\theta^{-1}(\{h\}) \subseteq A_0 \setminus A$ with $|\theta^{-1}(\{h\})| = 9$. For $g \in \theta^{-1}(\{h\})$, $h = g^3 \in im\theta$ and so we must multiply the cycle lengths of $h$ by 3 and their multiplicities by 9 to count the contribution of $\theta^{-1}(\{h\})$.

Now $im\theta$ contains $B = A_i^{(3)}A_j^{(3)}$ $(1 \leq i \neq j \leq 3)$ as a subgroup of index 3, and clearly $A_i \cap im\theta \geq A_i^{(3)}$, $(1 \leq i \leq 3)$. If $A_i \cap im\theta \neq A_i^{(3)}$, then, as $[A_i : A_i^{(3)}] = 3$, we get $A_i \leq im\theta$. But then

$$im\theta \geq A_i A_j^{(3)} = A_i A_i^{(3)} A_j^{(3)} = A_i B$$

whence $im\theta = A_i B$. This is impossible as $im\theta \neq A_i B$ and so we conclude that $A_i \cap im\theta = A_i^{(3)}$ for $1 \leq i \leq 3$. Hence we have that $im\theta$ satisfies Hypothesis 3.7 with $B$ playing the role of $A$ and $A_i \cap im\theta$ $(1 \leq i \leq 3)$ the role of the $A_i$. Further $B$ itself satisfies Hypothesis 3.7 with $B$ playing the role also of $A$ and the $A_i^{(3)}$ $(1 \leq i \leq 3)$ the role of the $A_i$. We may repeat this process for $im\theta \setminus B$ (note $b \geq 2$ in this case), each time we multiply cycle lengths by 3 and the multiplicity by 9. Eventually we arrive at $im(\theta^{b-1})$, containing a subgroup $B^*$ of index 3. Observe that the count for $im(\theta^{b-1}) \cong \frac{q+1}{3^{b-1}} \times \frac{q+1}{3^b}$ is given by part $(ii)$ (with $\ell = \frac{q+1}{3^{b-1}}$) and the count for $B^* \cong \frac{q+1}{3^b} \times \frac{q+1}{3^b}$ with $(\ell = \frac{q+1}{3^b})$. Keeping track of changes in cycle length and multiplicity we obtain

$$9^{b-1}\big(\lambda_k^*(\frac{q+1}{3^{b-1}}, \frac{q+1}{3^{b-1}}) + 2\lambda_k(\frac{q+1}{3^b}, \frac{q+1}{3^b}; b) - \lambda_k^*(\frac{q+1}{3^{b-1}}, \frac{q+1}{3^{b-1}})\big)$$

$$= 2.9^{b-1}\lambda_k(\frac{q+1}{3^b}, \frac{q+1}{3^b}; b)$$

which is the contribution for $A_0 \setminus A$. Consequently

$$\sigma_k(E_0^*, \Omega) = \lambda_k^*(\ell, \ell) + 2.9^{b-1}\lambda_k(\frac{q+1}{3^b}, \frac{q+1}{3^b}; b),$$

and the proof of Lemma 3.9 is complete. □

We are now in a position to prove Theorem 1.3.

**Proof of Theorem 1.3** Again we apply Lemma 2.1 using the information on cycle types given in Lemmas 3.5 and 3.9. The size of a given conjugacy class is obtained using the centralizer orders displayed in Table 2. So the conjugacy classes in $\mathcal{C}_i$ for a fixed $i$ all have the same size hence using their multiplicity in each $\mathcal{C}_i$ together with Lemmas 3.5 and 3.9 we obtain $\sigma_k(G, \Omega)$, so proving Theorem 1.3.

□

**Remark 2.** Type $\mathcal{C}_6'$ classes only arise when $d = 3$ (and then there is only one conjugacy class of this type) and consists of elements of order 3 with no fixed points, and is one third the size of the type $\mathcal{C}_6$ classes. When $d = 3$ we include this class along with the other type $\mathcal{C}_6$ classes in $\sigma_k(E_0^*, \Omega)$. It occurs as the case $\ell_1 = \ell_2 = n = 3$ and appears $f(3, 3, 3) = 2$ times. As the size of this class is divided by 6, this corrects the size of this class in our count.

# 4 Magma Code for $L_2(q)$

In this section we give a MAGMA implementation for the formula in Theorem 1.1.

```
PSLsig:=procedure(q,k,~sigma);
Z:=Integers();d:=GreatestCommonDivisor(q-1,2);
p:=Factorisation(q)[1,1];sig:=0;
I:=(d/(q*(q+1)*(q-1)))*Binomial(Z!(q+1),k);
CC:=[]; Append(~CC,[<(d/q),1>,<p,Z!(q/p)>,<1,1>]);
for m in Divisors(Z!((q+1)/d)) do if m ne 1 then
Append(~CC,[<(d/(2*(q+1))),EulerPhi(m)>,<m,Z!((q+1)/m)>]);
end if;end for;
for m in Divisors(Z!((q-1)/d)) do if m ne 1 then
Append
(~CC,[<(d/(2*(q-1))),EulerPhi(m)>,<m,Z!((q-1)/m)>,<1,2>]);
end if;end for; a:=0;
for i:=1 to #CC do Cg:=CC[i];S:={Z!(Cg[i][1]): i in [2..#Cg]};
RPg:=RestrictedPartitions(k,S);
for l:=1 to #RPg do p:=RPg[l];np:=1;
for j:=2 to #Cg do
pj:=#{m:m in [1..#p] |p[m] eq Cg[j][1]};
np:=np*Binomial(Cg[j][2],pj);   end for;
a:=a + np*(Cg[1][1]*Cg[1][2]);end for;end for;
sigma:=a+I;end procedure;
```

Code implementing the formula for $U_3(q)$ is available from the authors.

# References


[1] Bradley, P. PhD. Thesis University of Manchester, in preparation.

[2] Bray, J. N.; Holt, D. F.; Roney-Dougal, C. M. *The maximal subgroups of the low-dimensional finite classical groups.* London Mathematical Society Lecture Note Series, 407. *Cambridge University Press, Cambridge*, 2013. xiv+438 pp.

[3] Bundy, D.; Hart, S. *The case of equality in the Livingstone-Wagner theorem.* J. Algebraic Combin. 29(2009), no. 2, 215–227.

[4] Cameron, P. J. *On an algebra related to orbit-counting.* J. Group Theory 1(1998), no. 2, 173–179.

[5] Cameron, P. J.; Maimani, H. R.; Omidi, G. R.; Tayfeh-Rezaie, B. *3-designs from PSL(2,q).* Discrete Math. 306(2006), no. 23, 3063–3073.

[6] Cameron, P. J.; Omidi, G. R.; Tayfeh-Rezaie, B. *3-designs from PGL(2,q).* Electron. J. Combin. 13(2006), no. 1, Research Paper 50, 11.

[7] Chen, J.; Liu, W. J. 3-*designs from* $PSL(2,q)$ *with* $q = 1(mod 4)$ . Util. Math. 88(2012), 211–222.

[8] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray.* Oxford University Press, Eynsham, 1985.

[9] Huppert, B. *Endliche Gruppen. I.* (German) Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York 1967.

[10] Isaacs, I. M. *Character theory of finite groups.* Pure and Applied Mathematics, No. 69. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976.

[11] Liu, W. J.; Tang, J. X.; Wu, Y. X. *Some new* 3-*designs from* $PSL(2,q)$ *with* $q = 1(mod\ 4)$ Sci. China Math. 55(2012), no. 9, 1901–1911.

[12] Livingstone, D.; Wagner, A. *Transitivity of finite permutation groups on unordered sets.* Math. Z. 90(1965) 393–403.

[13] Mitchell, H. H. *Determination of the ordinary and modular ternary linear groups* Trans. Amer. Math. Soc 12(1911), 207–242.

[14] Mnukhin, V. B.; Siemons, I. J. *On the Livingstone-Wagner theorem.* Electron. J. Combin. 11(2004), no. 1, Research Paper 29, 8.

[15] Mnukhin, V. B. *Some relations for the lengths of orbits on k -sets and (k-1) -sets.* Arch. Math. (Basel) 69(1997), no. 4, 275–278.

[16] Neumann, P. M. *A lemma that is not Burnside's.* Math. Sci. 4 (1979), no. 2, 133–141.

[17] Rosen, K. H. *Elementary number theory and its applications.* Second edition. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1988. xiv+466 pp.

[18] Siemons, J.; Wagner, A. *On finite permutation groups with the same orbits on unordered sets.* Arch. Math. (Basel) 45(1985), no. 6, 492–500.

[19] Siemons, J.; Wagner, A. *On the relationship between the lengths of orbits on k -sets and (k+1) -sets.* Abh. Math. Sem. Univ. Hamburg 58(1988), 267–274.

[20] Simpson, W. A.; Frame, J. S. *The character tables for* $SL(3,q)$, $SU(3,q^2)$ *,*$PSL(3,q)$*,* $PSU(3,q^2)$. Canad. J. Math. 25(1973), 486–494.

[21] Sloane, N. J. A. *Jacobsthal sequence (or Jacobsthal numbers)* Available: `http://oeis.org`

[22] Sloane, N. J. A. *Number of vertices in Sierpinski triangle of order n* Available: `http://oeis.org`

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