A note on cyclic semiregular subgroups of some 2-transitive permutation groups

M. Giulietti and G. Korchmáros

Abstract

We determine the semi-regular subgroups of the 2-transitive permutation groups \( \text{PGL}(2, n) \), \( \text{PSL}(2, n) \), \( \text{PGU}(3, n) \), \( \text{PSU}(3, n) \), \( \text{Sz}(n) \) and \( \text{Ree}(n) \) with \( n \) a suitable power of a prime number \( p \).

2000 Math. Subj. Class.: 14H37

Keywords: 2-transitive permutation groups

1 Introduction

The finite 2-transitive groups play an important role in several investigations in combinatorics, finite geometry, and algebraic geometry over a finite field. With this motivation, the present notes are aimed at providing some useful results on semi-regular subgroups of the 2-transitive permutation groups \( \text{PGL}(2, n) \), \( \text{PSL}(2, n) \), \( \text{PGU}(3, n) \), \( \text{PSU}(3, n) \), \( \text{Sz}(n) \) and \( \text{Ree}(n) \) where \( n \) is a suitable power of a prime number \( p \).

2 The projective linear group

The projective linear group \( \text{PGL}(2, n) \) consists of all linear fractional mappings,

\[
\varphi_{(a,b,c,d)}: \ x \mapsto \frac{ax + b}{cx + d}, \quad ad - bc \neq 0,
\]

with \( a, b, c, d \in \mathbb{F}_n \). The order of \( \text{PGL}(2, n) \) is \( n(n - 1)(n + 1) \).
Let \( \Box \) be the set of all non-zero square elements in \( \mathbb{F}_n \). The special projective linear group \( \text{PSL}(2, n) \) is the subgroup of \( \text{PGL}(2, n) \) consisting of all linear fractional mapping \( \varphi_{(a,b,c,d)} \) for which \( ad - bc \in \Box \). For even \( n \), \( \text{PSL}(2, n) = \text{PGL}(2, n) \). For odd \( n \), \( \text{PSL}(2, n) \) is a subgroup of \( \text{PGL}(2, n) \) of index 2.

For \( n \geq 4 \), \( \text{PSL}(2, n) \) is a non-abelian simple group. For smaller values of \( n \), \( \text{PGL}(2, 2) \cong \text{PSL}(2, 3) \cong \text{Sym}_3 \). For this reason, we only consider the case of \( n \geq 4 \).

The above fractional mapping \( \varphi_{(a,b,c,d)} \) defines a permutation on the set \( \Omega = \mathbb{F}_n \cup \{ \infty \} \) of size \( n + 1 \). So, \( \text{PGL}(2, n) \) can be viewed as a permutation group on \( \Omega \). Such a permutation group is sharply 3-transitive on \( \Omega \), in particular 2-transitive on \( \Omega \), and it is defined to be the natural 2-transitive permutation representation of \( \text{PGL}(2, n) \). In this context, \( \text{PSL}(2, n) \) with \( n \) odd can be viewed as permutation group on \( \Omega \). Such a permutation group is 2-transitive on \( \Omega \), and it is defined to be the natural 2-transitive permutation representation of \( \text{PGL}(2, n) \).

The subgroups of \( \text{PSL}(2, n) \) were determined by Dickson, see [5, Hauptsatz 8.27].

**Theorem 2.1.** Dickson’s classification of subgroups of \( \text{PSL}(2, n) \): If \( U \) is a subgroup of \( \text{PSL}(2, n) \) with \( n = p^r \), then \( U \) is one of the following groups:

1. An elementary abelian \( p \)-group of order \( p^m \) with \( m \leq r \).
2. A cyclic group of order \( z \) where \( z \) is a divisor of \( 2^r - 1 \) or \( 2^r + 1 \), if \( p = 2 \), and a divisor of \( \frac{1}{2}(p^r - 1) \) or \( \frac{1}{2}(p^r + 1) \), if \( p > 2 \).
3. A dihedral group of order \( 2z \) where \( z \) is as in (2).
4. A semidirect product of an elementary abelian \( p \)-group of order \( p^m \) and a cyclic group of order \( t \) where \( t \) is a divisor of \( p^{\gcd(m,r)} - 1 \).
5. A group isomorphic to \( A_4 \). In this case, \( r \) is even, if \( p = 2 \).
6. A group isomorphic to \( S_4 \). In this case, \( p^{2^r} - 1 \equiv 0 \) (mod \( 16 \)).
7. A group isomorphic to \( A_5 \). In this case, \( p^r(p^{2^r} - 1) \equiv 0 \) (mod \( 5 \)).
8. A group isomorphic to \( \text{PSL}(2, p^m) \) where \( m \) divides \( r \).
9. A group isomorphic to \( \text{PGL}(2, p^m) \) where \( 2m \) divides \( r \).
From Dickson’s classification, all subgroups of PGL(2, n) with n odd, can also be obtained, see [11].

Let $n \geq 5$ odd. Then the subgroups listed in (1) and (2) form a partition of PSL(2, n), that is, every non-trivial element of PSL(2, n) belongs exactly one of those subgroups, see [10]. This has the following corollary.

**Proposition 2.2.** Let $n \geq 5$ odd. Any two maximal cyclic subgroups of PSL(2, n) have trivial intersection.

If $n \geq 5$ is odd, the number of involutions in PGL(2, n) is equal to $n^2$.

**Proposition 2.3.** Let $n \geq 5$ be odd.

(I) $\varphi_{(a,b,c,d)} \in \text{PGL}(2, n)$ is an involution if and only if $a + d = 0$.

(II) If $n \equiv 1 \pmod{4}$, then PSL(2, n) has $\frac{1}{2}n(n + 1)$ involutions. Each has exactly exactly two fixed points on Ω, while no involution in PGL(2, n) \ PSL(2, n) has a fixed point on Ω.

(III) If $n \equiv 3 \pmod{4}$, then PSL(2, n) has $\frac{1}{2}n(n - 1)$ involutions. Each has exactly two fixed points on Ω.

**Proof.** A direct computation shows that $\varphi_{(a,b,c,d)} \in \text{PGL}(2, n)$ is an involution if and only if $b(a + d) = 0$ and $c(a + d) = 0$. The latter condition is satisfied when either $a + d = 0$ or $b = c = 0$. Furthermore, since $\varphi_{(a,0,0,d)}$ is an involution if and only if $a^2 = d^2$ but $a \neq d$, assertion (I) follows.

To show (II) and (III) take an involution $\varphi_{(a,b,c,-a)} \in \text{PGL}(2, n)$. A direct computation shows that $\varphi_{(a,b,c,-a)}$ has two or zero fixed points on Ω according as $-(a^2 - bc)$ is in □ or not. Since $-1 \in □$ if and only if $n \equiv 1 \pmod{4}$, assertions (II) and (III) follow. □

**Proposition 2.4.** Let $n \geq 5$ odd.

(x) The elements of PGL(2, n) of order $p$ are contained in PSL(2, n).

(xx) Any two elements of PSL(2, n) of order $p$ are conjugate in PGL(2, n).

.xxx) The elements of PSL(2, n) of order $p$ form two different conjugacy classes in PSL(2, n).
Proof. In the natural 2-transitive permutation representation, the elements \( \varphi_{(a,b,c,d)} \) with \( a = d = 1, c = 0 \) and \( b \in \mathbb{F}_n \) form a Sylow \( p \)-subgroup \( S_p \) of \( \text{PGL}(2, n) \). Actually, all such elements \( \varphi_{(a,b,c,d)} \) are in \( \text{PSL}(2, n) \).

To show (x), it is enough to observe that \( \text{PSL}(2, n) \) is self-conjugate in \( \text{PGL}(2, n) \) and that any two Sylow \( p \)-subgroups are conjugate in \( \text{PGL}(2, n) \).

Take two non-trivial elements in \( S_p \), say \( \varphi_1 = \varphi_{(1,b,0,1)} \) and \( \varphi_2 = \varphi_{(1,b',0,1)} \). Let \( a = b'/b \), and \( \varphi = \varphi_{(a,0,0,1)} \). Then \( \varphi_2 = \varphi \varphi_1 \varphi^{-1} \) showing that \( \varphi_2 \) is conjugate to \( \varphi_1 \) in \( \text{PGL}(2, n) \). This proves (xx). Note that if \( a \in \Box \), then \( \varphi_2 \) is conjugate to \( \varphi_1 \) in \( \text{PSL}(2, n) \).

Take any two distinct elements of \( \text{PSL}(2, n) \) of order \( n \). Every element of \( \text{PGL}(2, n) \) of order \( p \) has exactly one fixed point in \( \Omega \) and \( \text{PSL}(2, n) \) is transitive on \( \Omega \). Therefore, to show (xxx), we may assume that both elements are in \( S_p \). So, they are \( \varphi_1 \) and \( \varphi_2 \) with \( b, b' \in \mathbb{F}_n \setminus \{0\} \). Assume that \( \varphi_2 \) is conjugate to \( \varphi_1 \) under an element \( \varphi \in \text{PSL}(2, n) \). Since \( \varphi \) fixes \( \infty \), we have that \( \varphi = \varphi_{(a,u,0,1)} \) with \( a, u \in \mathbb{F}_n \) and \( a \neq 0 \). But then \( a = b'/b' \). Therefore, \( \varphi_2 \) is conjugate to \( \varphi_1 \) under \( \text{PSL}(2, n) \) if and only if \( b'/b \in \Box \). This shows that \( \varphi_1 \) and \( \varphi_2 \) are in the same conjugacy class if and only if \( b \) and \( b' \) have the same quadratic character in \( \mathbb{F}_n \). This completes the proof.

3 The projective unitary group

Let \( \mathcal{U} \) be the classical unital in \( \text{PG}(2, n^2) \), that is, the set of all self-conjugate points of a non-degenerate unitary polarity \( \Pi \) of \( \text{PG}(2, n^2) \). Then \( |\mathcal{U}| = n^3 + 1 \), and at each point \( P \in \mathcal{U} \), there is exactly one 1-secant, that is, a line \( \ell_P \) in \( \text{PG}(2, n^2) \) such that \( |\ell_P \cap \mathcal{U}| = 1 \). The pair \( (P, \ell_P) \) is a pole-polar pair of \( \Pi \), and hence \( \ell_P \) is an absolute line of \( \Pi \). Each other line in \( \text{PG}(2, n^2) \) is a non-absolute line of \( \Pi \) and it is an \((n+1)\)-secant of \( \mathcal{U} \), that is, a line \( \ell \) such that \( |\ell \cap \mathcal{U}| = n + 1 \), see [4, Chapter II.8].

An explicit representation of \( \mathcal{U} \) in \( \text{PG}(2, n^2) \) is as follows. Let
\[
M = \{m \in \mathbb{F}_{n^2} \mid m^n + m = 0\}.
\]
Take an element \( c \in \mathbb{F}_{n^2} \) such that \( c^n + c + 1 = 0 \). A homogeneous coordinate system in \( \text{PG}(2, n^2) \) can be chosen so that
\[
\mathcal{U} = \{X_\infty\} \cup \{U = (1, u, u^{n+1} + c^{-1}m) \mid u \in \mathbb{F}_{n^2}, m \in M\}.
\]
Note that \( \mathcal{U} \) consists of all \( \mathbb{F}_{n^2} \)-rational points of the Hermitian curve of homogeneous equation \( cX_0^nX_2 + cX_0X_2^n + X_1^{n+1} = 0 \).
The **projective unitary group** $\text{PGU}(3, n)$ consists of all projectivities of $\text{PG}(2, n^2)$ which commute with $\Pi$. $\text{PGU}(3, n)$ preserves $\mathcal{U}$ and can be viewed as a permutation group on $\mathcal{U}$, since the only projectivity in $\text{PGU}(3, n)$ fixing every point in $\mathcal{U}$ is the identity. The group $\text{PGU}(3, n)$ is a 2-transitive permutation group on $\Omega$, and this is defined to be the **natural 2-transitive permutation representation of $\text{PGU}(3, n)$**. Furthermore, $|\text{PGU}(3, n)| = (n^3 + 1)n^3(n^2 - 1)$.

With $\mu = \gcd(3, n+1)$, the group $\text{PGU}(3, n)$ contains a normal subgroup $\text{PSU}(3, n)$, the **special unitary group**, of index $\mu$ which is still a 2-transitive permutation group on $\Omega$. This is defined to be the **natural 2-transitive permutation representation of $\text{PSU}(3, n)$**.

For $n > 2$, $\text{PSU}(3, n)$ is a non-abelian simple group, but $\text{PSU}(3, 2)$ is a solvable group.

The maximal subgroups of $\text{PSU}(3, n)$ were determined by Mitchell [9] for $n$ odd and by Hartley [2] for $n$ even, see [3].

**Theorem 3.1.** The following is the list of maximal subgroups of $\text{PSU}(3, n)$ with $n \geq 3$ up to conjugacy:

(i) the one-point stabiliser of order $n^3(n^2 - 1)/\mu$;

(ii) the non-absolute line stabiliser of order $n(n^2 - 1)(n + 1)/\mu$;

(iii) the self-conjugate triangle stabiliser of order $6(n + 1)^2/\mu$;

(iv) the normaliser of a cyclic Singer group of order $3(n^2 - n + 1)/\mu$;

further, for $n = p^k$ with $p > 2$,

(v) $\text{PGL}(2, n)$ preserving a conic;

(vi) $\text{PSU}(3, p^m)$, with $m \mid k$ and $k/m$ odd;

(vii) the subgroup containing $\text{PSU}(3, p^m)$ as a normal subgroup of index 3 when $m \mid k$, $k/m$ is odd, and 3 divides both $k/m$ and $q + 1$;

(viii) the Hessian groups of order 216 when $9 \mid (q + 1)$, and of order 72 and 36 when $3 \mid (q + 1)$;

(ix) $\text{PSL}(2, 7)$ when either $p = 7$ or $\sqrt{-7} \notin \mathbb{F}_q$;
(x) the alternating group $A_6$ when either $p = 3$ and $k$ is even, or $\sqrt{5} \in \mathbb{F}_q$ but $\mathbb{F}_q$ contains no cube root of unity;

(xi) the symmetric group $S_6$ for $p = 5$ and $k$ odd;

(xii) the alternating group $A_7$ for $p = 5$ and $k$ odd;

for $n = 2^k$,

(xiii) $\text{PSU}(3, 2^m)$ with $k/m$ an odd prime;

(xiv) the subgroups containing $\text{PSU}(3, 2^m)$ as a normal subgroup of index 3 when $k = 3m$ with $m$ odd;

(xv) a group of order 36 when $k = 1$.

**Proposition 3.2.** Let $n \geq 3$ be odd. Let $U$ be a cyclic subgroup of $\text{PSU}(3, n)$ which contains no non-trivial element fixing a point on $\Omega$. Then $|U|$ divides either $\frac{1}{2}(n + 1)$ or $(n^2 - n + 1)/\mu$.

**Proof.** Fix a projective frame in $\text{PG}(2, n^2)$ and define the homogeneous point coordinates $(x, y, z)$ in the usual way. Take a generator $u$ of $U$ and look at the action of $u$ in the projective plane $\text{PG}(2, \mathbb{K})$ over the algebraic closure $\mathbb{K}$ of $\mathbb{F}_{n^2}$. In our case, $u$ fixes no line point-wise. In fact, if a collineation point-wise fixed a line $\ell$ in $\text{PG}(2, \mathbb{K})$, then $\ell$ would be a line $\text{PG}(2, n^2)$. But every line in $\text{PG}(2, n^2)$ has a non-trivial intersection with $\Omega$, contradicting the hypothesis on the action of $U$.

If $u$ has exactly one fixed point $P$, then $P \in \text{PG}(2, n^2)$ but $P \notin \Omega$. Then the polar line $\ell$ of $P$ under the non-degenerate unitary polarity $\Pi$ is a $(n + 1)$-secant of $\Omega$. Since $\Omega \cap \ell$ is left invariant by $U$, it follows that $|U|$ divides $n + 1$. Since every involution in $\text{PSU}(3, n)$ has a fixed point on $\Omega$, the assertion follows.

If $u$ has exactly two fixed points $P, Q$, then either $P, Q \in \text{PG}(2, n^2)$, or $P, Q \in \text{PG}(2, n^4) \setminus \text{PG}(2, n^2)$ and $Q = \Phi^{(2)}(P)$, $P = \Phi^{(2)}(Q)$ where

$$\Phi^{(2)} : (x, y, z) \rightarrow (x^{n^2}, y^{n^2}, z^{n^2})$$

is the Frobenius collineation of $\text{PG}(2, n^4)$ over $\text{PG}(2, n^2)$. In both cases, the line $\ell$ through $P$ and $Q$ is a line $\ell$ of $\text{PG}(2, n^2)$. As $u$ has no fixed point in $\Omega$, $\ell$ is not a 1-secant of $\Omega$, and hence it is a $(n + 1)$-secant of $\Omega$. Arguing as before shows that $|U|$ divides $\frac{1}{2}(n + 1)$.
If $U$ has exactly three points $P, Q, R$, then $P, Q, R$ are the vertices of a triangle. Two cases can occur according as $P, Q, R \in PG(2, n^2)$ or $P, Q, R \in PG(2, n^6) \setminus PG(2, n^2)$ and $Q = \Phi(3)(P), R = \Phi(3)(Q), P = \Phi(3)(R)$ where
\[
\Phi(3): (x, y, z) \rightarrow (x^{n^2}, y^{n^2}, z^{n^2})
\]
is the Frobenius collineation of $PG(2, n^6)$ over $PG(2, n^2)$.

In the former case, the line through $P, Q$ is a $(n + 1)$-secant of $\Omega$. Again, this implies that $|U|$ divides $\frac{1}{2}(n + 1)$.

In the latter case, consider the subgroup $\Gamma$ of $PGL(3, n^2)$, the full projective group of $PG(2, n^2)$, that fixes $P, Q$ and $R$. Such a group $\Gamma$ is a Singer group of $PG(2, n^2)$ which is a cyclic group of order $n^4 + n^2 + 1$ acting regularly on the set of points of $PG(2, n^2)$. Therefore, $U$ is a subgroup of $\Gamma$. On the other hand, the intersection of $\Gamma$ and $PSU(3, n)$ has order $(n^2 - n + 1)/\mu$, see case (iv) in Proposition 2.4.

4 The Suzuki group

A general theory on the Suzuki group is given in [6, Chapter XI.3].

An ovoid $\mathcal{O}$ in $PG(3, n)$ is a point set with the same combinatorial properties as an elliptic quadric in $PG(3, n)$; namely, $\Omega$ consists of $n^2 + 1$ points, no three collinear, such that the lines through any point $P \in \Omega$ meeting $\Omega$ only in $P$ are coplanar.

In this section, $n = 2n_0^2$ with $n_0 = n^s$ and $s \geq 1$. Note that $x^{\varphi} = x^{2q_0}$ is an automorphism of $F_n$, and $x^{\varphi^2} = x^2$.

Let $\Omega$ be the Suzuki–Tits ovoid in $PG(3, n)$, which is the only known ovoid in $PG(3, n)$ other than an elliptic quadric. In a suitable homogeneous coordinate system of $PG(3, q)$ with $Z = (0, 0, 0, 1)$,
\[
\Omega = \{Z \in \Omega \}_{(1, u, v, w + u^{2q + 2}v^{\varphi}) | u, v \in F_n}.
\]

The Suzuki group $Sz(n)$, also written $B_2(q)$, is the projective group of $PG(3, n)$ preserving $\Omega$. The group $Sz(n)$ can be viewed as a permutation group on $\Omega$ as the identity is the only projective transformation in $Sz(n)$ fixing every point in $\Omega$. The group $Sz(n)$ is a 2-transitive permutation group on $\Omega$, and this is defined to be the natural 2-transitive permutation representation of $Sz(n)$. Furthermore, $Sz(n)$ is a simple group of order $(n^2 + 1)n^2(n - 1)$.

The maximal subgroups of $Sz(n)$ were determined by Suzuki, see also [6, Chapter XI.3].
Proposition 4.1. The following is the list of maximal subgroups of $Sz(n)$ up to conjugacy:

(i) the one-point stabiliser of order $n^2(n-1)$;
(ii) the normaliser of a cyclic Singer group of order $4(n+2n_0+1)$;
(iii) the normaliser of a cyclic Singer group of order $4(n-2n_0+1)$;
(iv) $Sz(n')$ for every $n'$ such that $n = n^m$ with $m$ prime.

Proposition 4.2. The subgroups listed below form a partition of $Sz(n)$:

(v) all subgroups of order $n^2$;
(vi) all cyclic subgroups of order $n-1$;
(vii) all cyclic Singer subgroups of order $n + 2n_0 + 1$;
(viii) all cyclic Singer subgroups of order $n - 2n_0 + 1$.

Proposition 4.3. Let $U$ be a cyclic subgroup of $Sz(n)$ which contains no non-trivial element fixing a point on $\Omega$. Then $|U|$ divides either $n - 2n_0 + 1$ or $(n + 2n_0 + 1)$.

Proof. Take a generator $u$ of $U$. Then $u$, and hence $U$, is contained in one of the subgroups listed in Proposition 4.2. More precisely, since $u$ fixes no point, such a subgroup must be of type (v) or (vi). \qed

5 The Ree group

The Ree group can be introduced in a similar way using the combinatorial concept of an ovoid, this time in the context of polar geometries, see for instance [2, Chapter XI.13].

An ovoid in the polar space associated to the non-degenerate quadric $Q$ in the space $PG(6,n)$ is a point set of size $n^3 + 1$, with no two of the points conjugate with respect to the orthogonal polarity arising from $Q$.

In this section, $n = 3n_0^2$ and $n_0 = 3^s$ with $s \geq 0$. Then $x^\varphi = x^{3n_0}$ is an automorphism of $\mathbb{F}_n$, and $x^{\varphi^2} = x^3$. 

8
Let $\Omega$ be the Ree–Tits ovoid of $\mathbb{Q}$. In a suitable homogenous coordinate system of $\text{PG}(6, n)$ with $Z_\infty = (0, 0, 0, 0, 0, 1)$, the quadric is defined by its homogenous equation $X_3^2 + X_0X_6 + X_1X_5 + X_2X_4 = 0$, and

$$\Omega = \{ Z_\infty \} \cup \{ (1, u_1, u_2, u_3, v_1, v_2, v_3) \},$$

with

$$v_1(u_1, u_2, u_3) = u_1^2u_2 - u_1u_3 + u_2^\varphi - u_1^{\varphi+3},$$

$$v_2(u_1, u_2, u_3) = u_1^\varphi u_2^2 - u_3^\varphi + u_1u_2^2 + u_2u_3 - u_1^{2\varphi+3},$$

$$v_3(u_1, u_2, u_3) = u_1u_3^\varphi - u_1^{\varphi+1}u_2^\varphi + u_1^{\varphi+3}u_2 + u_1^2u_2^2 - u_2^{\varphi+1} - u_3^2 + u_1^{2\varphi+4},$$

for $u_1, u_2, u_3 \in \mathbb{F}_n$.

The Ree group $\text{Ree}(n)$, also written $^2G_2(n)$, is the projective group of $\text{PG}(6, n)$ preserving $\Omega$. The group $\text{Ree}(n)$ can be viewed as a permutation group on $\Omega$ as the identity is the only projective transformation in $\text{Ree}(n)$ fixing every point in $\Omega$. The group $\text{Ree}(n)$ is a 2-transitive permutation group on $\Omega$, and this is defined to be the natural 2-transitive permutation representation of $\text{Ree}(n)$. Furthermore, $|\text{Ree}(n)| = (n^3 + 1)n^3(n - 1)$. For $n_0 > 1$, the group $\text{Ree}(n)$ is simple, but $\text{Ree}(3) \cong \text{PGL}(2, 8)$ is a non-solvable group with a normal subgroup of index 3.

For every prime $d > 3$, the Sylow $d$-subgroups of $\text{Ree}(n)$ are cyclic, see [6] Theorem 13.2 (g)]. Put

$$w_1(u_1, u_2, u_3) = -u_1^{\varphi+2} + u_1u_2 - u_3,$$

$$w_2(u_1, u_2, u_3) = u_1^{\varphi+1}u_2 + u_1^\varphi u_3 - u_2^2,$$

$$w_3(u_1, u_2, u_3) = u_3^\varphi + (u_1u_2)^\varphi - u_1^{\varphi+2}u_2 - u_1u_2^2 + u_2u_3 - u_1^{\varphi+1}u_3 - u_1^{2\varphi+3},$$

$$w_4(u_1, u_2, u_3) = u_1^{\varphi+3} - u_2^2u_2 - u_2^\varphi - u_1u_3.$$

Then a Sylow 3-subgroup $S_3$ of $\text{Ree}(n)$ consists of the projectivities represented by the matrices:

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
a & 1 & 0 & 0 & 0 & 0 & 0 \\
b & a^\varphi & 1 & 0 & 0 & 0 & 0 \\
c & b - a^{\varphi+1} & -a & 1 & 0 & 0 & 0 \\
v_1(a, b, c) & w_1(a, b, c) & -a^2 & -a & 1 & 0 & 0 \\
v_2(a, b, c) & w_2(a, b, c) & ab + c & b & -a^\varphi & 1 & 0 \\
v_3(a, b, c) & w_3(a, b, c) & w_4(a, b, c) & c & -b + a^{\varphi+1} & -a & 1
\end{bmatrix}$$
for $a, b, c \in \mathbb{F}_n$. Here, $S_3$ is a normal subgroup of $\text{Ree}(n)_{Z_\infty}$ of order $n^3$ and regular on the remaining $n^3$ points of $\Omega$. The stabiliser $\text{Ree}(n)_{Z_\infty, O}$ with $O = (1, 0, 0, 0, 0, 0)$ is the cyclic group of order $n - 1$ consisting of the projectivities represented by the diagonal matrices,

$$\text{diag}(1, d, d^{\phi+1}, d^{\phi+2}, d^{\phi+3}, d^{2\phi+3}, d^{2\phi+4})$$

for $d \in \mathbb{F}_n$. So the stabiliser $\text{Ree}(n)_{Z_\infty}$ has order $n^3(n - 1)$.

The group $\text{Ree}(n)$ is generated by $S_3$ and $\text{Ree}(n)_{Z_\infty, O}$, together with the projectivity $W$ of order 2 associated to the matrix,

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix},$$

that interchanges $Z_\infty$ and $O$. Here, $W$ is an involution and it fixes exactly $n + 1$ points of $\Omega$. Furthermore, $\text{Ree}(n)$ has a unique conjugacy classes of involutions, and hence every involution in $\text{Ree}(n)$ has $n + 1$ fixed points in $\Omega$.

Assume that $n = n''$ with an odd integer $t = 2v + 1$, $v \geq 1$. Then $\mathbb{F}_n$ has a subfield $\mathbb{F}_n'$, and PG$(6, n)$ may be viewed as an extension of PG$(6, n')$. Doing so, $Q$ still defines a quadric in PG$(6, n')$, and the points of $\Omega$ contained in PG$(6, n')$ form an ovoid, the Ree-Tits ovoid of $Q$ in PG$(6, n')$. The associated Ree group $\text{Ree}(n')$ is the subgroup of $\text{Ree}(n)$ where the above elements $a, b, c, d$ range over $\mathbb{F}_n'$.

The maximal subgroups of $\text{Ree}(n)$ were determined by Migliore and, independently, by Kleidman [8, Theorem C], see also [1, Lemma 3.3].

**Proposition 5.1.** The following is the list of maximal subgroups of $\text{Ree}(n)$ with $n > 3$ up to conjugacy:

(i) the one-point stabiliser of order $n^3(n - 1)$;

(ii) the centraliser of an involution $z \in \text{Ree}(n)$ isomorphic to $\langle z \rangle \times \text{PSL}(2, n)$ of order $n(n - 1)(n + 1)$;
(iii) a subgroup of order $6(n + 3n_0 + 1)$, the normaliser of a cyclic Singer group of order $n + 3n_0 + 1$;

(iv) a subgroup of order $6(n - 3n_0 + 1)$, the normaliser of a cyclic Singer group of order $6(n - 3n_0 + 1)$;

(v) a subgroup of order $6(n + 1)$, the normaliser of a cyclic subgroup of order $n + 1$;

(vi) $\text{Ree}(n')$ with $n = n'^a$ and $t$ prime.

**Proposition 5.2.** Let $U$ be a cyclic subgroup of $\text{Ree}(n)$ with $n > 3$ which contains no non-trivial element fixing a point on $\Omega$. Then $|U|$ divides either $\frac{1}{2}(n + 1)$, or $n - 3n_0 + 1$ or $n + 3n_0 + 1$.

**Proof.** Every involution in $\text{Ree}(n)$ has exactly $n+1$ fixed points on $\Omega$, and every element in $\text{Ree}(n)$ whose order is 3 fixes exactly one point in $\Omega$. Therefore, neither 3 nor 2 divides $|U|$. Furthermore, if $U$ is contained in a subgroup (iii), then $U$ preserves the set of fixed points of $z$, and hence $|U|$ divides $\frac{1}{2}(n + 1)$.

Now, assume that $U$ is contained in a subgroup (iii) or (iv), say $N$. Let $S$ be the cyclic Singer subgroup of $N$. We show that $U$ is contained in $S$. Suppose on the contrary that $S \cap U \neq U$. Then $SU/S$ is a non-trivial subgroup of factor group $N/S$. Hence either 2 or 3 divides $|SU/S|$. Since $|SU/S| = |S| \cdot |U|/|S \cap U|$ and neither 2 nor 3 divides $|S|$, it follows that either 2 or 3 divides $|U|$. But this is impossible by the preceding result.

If $U$ is contained in a subgroup (v), say $N$, we may use the preceding argument. Let $S$ be the cyclic subgroup of $N$. Arguing as before, we can show that $U$ is a subgroup of $S$.

Finally, we deal with the case where $U$ is contained in a subgroup (vi) which may be assumed to be $\text{Ree}(n')$ with

$$n = n'^{(2v+1)}, \ v \geq 1;$$

equivalently

$$s = 2uv + u + v.$$ 

Without loss of generality, $U$ may be assumed not be contained in any subgroup $\text{Ree}(n'')$ of $\text{Ree}(n')$.

If $n' = 3$ then $U$ is a subgroup of $\text{Ree}(3) \cong \text{PGL}(2,8)$. Since $|\text{PGL}(2,8)| = 2^3 \cdot 3^3 \cdot 7$, and neither 2 nor 3 divides $|U|$, this implies that $|U| = 7$. On the
other hand, since \( n = 3^k \) with \( k \) odd, 7 divides \( n^3 + 1 \). Therefore, 7 divides \( n^3 + 1 = (n + 1)(n + 3n_0 + 1)(n - 3n_0 + 1) \) whence the assertion follows.

For \( n' > 3 \), the above discussion can be repeated for \( n' \) in place of \( n \), and this gives that \(|U|\) divides either \( n' + 1 \) or \( n' + 3n'_0 + 1 \) or \( n' + 3n'_0 + 1 \). So, we have to show that each of these three numbers must divide either \( n + 1 \), or \( n + 3n_0 + 1 \), or \( n - 3b_0 + 1 \).

If \( U \) divides \( n' + 1 \) then it also divide \( n + 1 \) since \( n \) is an odd power of \( n' \).

For the other two cases, the following result applies for \( n_0 = k \) and \( n'_0 = m \).

**Claim 5.3.** [12, V. Vigh] Fix an \( u \geq 0 \), and let \( m = 3^u \), \( d^+ = 3m^2 + 3m + 1 \).

For a non-negative integer \( v \), let \( s = 2uv + u + v \), \( k = 3^s \), and

\[
M_1(v) = 3k^2 + 3k + 1, \quad M_2(v) = 3k^2 + 1, \quad M_3(v) = 3k^2 - 3k + 1.
\]

Then for all \( v \geq 0 \), \( d^+ \) divides at least one of \( M_1(v) \), \( M_2(v) \) and \( M_3(v) \).

We prove the claim for \( d^+ = d = 3m^2 + 3m + 1 \), the proof for other case \( d^- = m^2 - 3m + 1 \) being analog.

We use induction on \( v \). We show first that the claim is true for \( v = 0, 1, 2 \), then we prove that the claim holds true when stepping from \( v \) to \( v + 3 \).

Since \( M_1(0) = d \), the claim trivially holds for \( v = 0 \).

For \( v = 1 \) we have the following equation:

\[(3^{2u+1} + 3^u + 1)(3^{4u+2} - 3^{3u+2} + 3^{2u+2} - 3^{2u+1} - 3^{u+1} + 1) = 3^{6u+3} + 1,
\]

whence

\[3^{2u+1} + 3^u + 1 = d \mid M_2(1) = 3^{6u+3} + 1. \tag{1}\]

Similarly,

\[(3^{2u+1} + 3^u + 1)(3^{8u+4} - 3^{7u+4} + 3^{6u+4} - 3^{6u+3} - 3^{5u+3}) = 3^{10u+5} - 3^{5u+3} + 1 - (3^{6u+3} + 1).
\]

On the other hand, using (1) we obtain that

\[3^{2u+1} + 3^u + 1 = d \mid M_3(2) = 3^{10u+5} - 3^{5u+3} + 1,
\]

which gives the claim for \( v = 2 \).

Furthermore, using (1) together with

\[M_2(v+3) - M_2(v) = (3^{4uv+14u+2v+7} + 1) - (3^{4uv+2u+2v+1} + 1) = 3^{4uv+2u+2v+1}(3^{u+3} + 1)(3^{u+3} - 1)
\]

12
we obtain that
\[ d \mid M_2(v + 3) - M_2(v). \] (2)

Now, direct calculation shows that
\[ M_1(v + 3) - M_3(v) = M_2(v + 3) - M_2(v) + 3^{2uv^2+u+v+1} \cdot M_2(1). \]

From (1) and (2),
\[ d \mid M_1(v + 3) - M_3(v). \]

Similarly,
\[ M_3(v + 3) - M_1(v) = M_2(v + 3) - M_2(v) - 3^{2uv^2+u+v+1} \cdot M_2(1), \]
and so
\[ d \mid M_3(v + 3) - M_1(v). \]

This finishes the proof of the Claim and hence it completes the proof of Proposition 5.2. \( \Box \)

One may ask for a proof that uses the structure of \( \text{Ree}(n) \) in place of the above number theoretic Claim. This can be done as follows.

Take a prime divisor \( d \) of \( |U| \). As we have pointed out at the beginning of the proof of Proposition 5.2 \( U \) has no elements of order 2 or 3. This implies that \( d > 3 \). In particular, the Sylow \( d \)-subgroups of \( \text{Ree}(n) \) are cyclic and hence are pairwise conjugate in \( \text{Ree}(n) \).

Since \( |U| \) divides \( n^3 + 1 \), and \( n^3 + 1 \) factorizes into \( (n + 1)(n + 3n_0 + 1)(n - 3n_0 + 1) \) with pairwise co-prime factors, \( d \) divides just one of this factors, say \( v \). From Proposition 5.1 \( \text{Ree}(n) \) has a cyclic subgroup \( V \) of order \( v \). Since \( d \) divides \( v \), \( V \) has a subgroup of order \( d \). Note that \( V \) is not contained in \( \text{Ree}(n') \) as \( v \) does not divide \( |\text{Ree}(n')| \).

Let \( D \) be a subgroup of \( U \) of order \( d \). Then \( D \) is conjugate to a subgroup of \( V \) under \( \text{Ree}(n) \). We may assume without loss of generality that \( D \) is a subgroup of \( V \).

Let \( C(D) \) be the centralizer of \( D \) in \( \text{Ree}(n) \). Obviously, \( C(D) \) is a proper subgroup of \( \text{Ree}(n) \). Since both \( U \) and \( V \) are cyclic groups containing \( D \), they are contained in \( C(D) \). Therefore, the subgroup \( W \) generated by \( U \) and \( V \) is contained in \( C(D) \). To show that \( U \) is a subgroup of \( V \), assume on the contrary that the subgroup \( W \) of \( C(D) \) generated by \( U \) and \( V \) contains \( V \) properly. From Proposition 5.1 the normalizer \( N(V) \) is the only maximal subgroup containing \( V \). Therefore \( W \) is a subgroup of \( N(V) \) containing \( V \),
and \( W = UV \). The factor group \( W/V \) is a subgroup of the factor group \( \mathcal{N}(V)/V \). From Proposition 5.1, \( |W/V| \) divides 6. On the other hand,

\[
|W/V| = \frac{|U||V|}{|U \cap V||V|} = \frac{|U|}{|U \cap V|}.
\]

But then \( |U| \) has to divide 6, a contradiction.

References

[1] X.G. Fang, C.H. Li, C.E. Praeger, The locally 2-arc transitive graphs admitting a Ree simple group. \textit{J. Algebra} \textbf{282} (2004), 638–666.

[2] R.W. Hartley, Determination of the ternary collineation groups whose coefficients lie in \( GF(2^h) \), \textit{Ann. of Math.} \textbf{27} (1926), 140-158.

[3] A.R. Hoffer, On unitary collineation groups, \textit{J. Algebra} \textbf{22} (1972), 211–218.

[4] D.R. Hughes and F.C. Piper, \textit{Projective Planes}, Graduate Texts in Mathematics \textbf{6}, Springer, New York, 1973, x+291 pp.

[5] B. Huppert, \textit{Endliche Gruppen. I}, Grundlehren der Mathematischen Wissenschaften \textbf{134}, Springer, Berlin, 1967, xii+793 pp.

[6] B. Huppert and B.N. Blackburn, \textit{Finite groups. III}, Grundlehren der Mathematischen Wissenschaften \textbf{243}, Springer, Berlin, 1982, ix+454 pp.

[7] W.M. Kantor, M. O’Nan and G.M. Seitz, 2-transitive groups in which the stabilizer of two points is cyclic, \textit{J. Algebra} \textbf{21} (1972), 17–50.

[8] P.B. Kleidman, The maximal subgroups of the Chevalley groups \( G_2(q) \) with \( q \) odd, the Ree groups \( ^2G_2(q) \), and their automorphism groups, \textit{J. Algebra} \textbf{117} (1988), 30–71.

[9] H.H. Mitchell, Determination of the ordinary and modular linear group, \textit{Trans. Amer. Math. Soc.} \textbf{12} (1911), 207-242.

[10] M. Suzuki, On a finite group with a partition, \textit{Arch. Math.} \textbf{12} (1961), 241–254.
[11] R.C. Valentini and M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, *J. Reine Angew. Math.* **318** (1980), 156–177.

[12] V. Vígh, On a divisibility problem, *Private comunication*, 2008.