INDEPENDENT SETS IN SOME CLASSICAL GROUPS OF DIMENSION THREE

by

PHILIP JAMES KEEN

A thesis submitted to
The University of Birmingham
for the degree of
DOCTOR OF PHILOSOPHY

School of Mathematics
College of Engineering and Physical Sciences
The University of Birmingham
August 2011

Abstract

Given a finite group G, an independent set S in G is a set where no element of S can be written as a word in the other elements of S. A minimax set is an independent generating set for G of largest size in G. This thesis seeks to find a good upper bound for the size of minimax sets in $SL_3(q)$ for odd q. In preparation for this, the sizes of independent sets in $SO_3(q)$ and $SU_3(q)$ are also investigated for odd q.

In each of the cases $G = SO_3(q)$ or $SU_3(q)$, q odd, it is shown that if S is an independent set in G, then either $|S|$ has a particular upper bound, or $\langle S \rangle$ stabilises some sub-structure of the underlying vector space V. These results are then used to help gain upper bounds for minimax sets in $SL_3(q)$.

Further results are shown for finite groups which contain normal, abelian subgroups. These are then used to obtain the size of minimax sets in finite Coxeter groups of types B_n and D_n.

Acknowledgements

I would like to thank my supervisor, Dr. Corneliu Hoffman, for his patient and encouraging support during the course of my PhD studies. I would also like to thank my fellow postgraduate students for helping make my postgraduate years such a fun experience.

Finally, I would like to thank the University of Birmingham for offering me the chance to study there, and EPSRC for funding my research.

CONTENTS

CHAPTER 1

INTRODUCTION

Throughout this thesis, G will generally be used to denote a finite group. Indeed, every group considered in this thesis will be finite.

We begin by defining the notion of *independence*.

Definition 1.0.1. Let G be a finite group and let S be a multiset of elements of G. S is said to be *independent* if for all $g \in S$, $g \notin \langle S \setminus \{g\} \rangle$.

This definition differs from the usual definition of independence in that it makes independence a property of multisets. The usual definition of independence is the same as Definition 1.0.1 except that it assumes that S is a set rather than a multiset (see, for instance, [14]). So the usual definition makes independence a property of sets. This is understandable: Suppose a multiset S in a finite group G is independent according to Definition 1.0.1. Then S can be regarded as a genuine set. Indeed, if a multiset S is independent we will feel free to describe it as "an independent set." So if an independent multiset automatically qualifies as a set, this naturally raises the question of why we have introduced a definition that seeks to apply itself to a wider range of objects.

The reason is that there are some objects that we do *not* wish to be independent. Suppose that G is a finite group, and that $g_1, g_2 \in G$ with $g_1 \notin \langle g_2 \rangle$, $g_2 \notin \langle g_1 \rangle$. We wish to deny that $\{g_1, g_1, g_2\}$ is independent in G. Hence the scope of Definition 1.0.1 is as broad as it is. Suppose that a set S is independent according to the usual definition of independence. We can safely remove repetitions from S, then. Observe that Definition 1.0.1

will now also describe S as independent. The ability to remove repeated elements from sets means that there is broad agreement between the two definitions of independence, and Definition 1.0.1 sits well with the existing results regarding independence.

Definition 1.0.2. Suppose that G is a finite group, and that S is an independent set in G. If $\langle S \rangle = G$ then S is said to be an *independent generating set* for G. An independent generating set for G of largest size is called a *minimax set* for G.

Any generating set T of a finite group G must contain an independent generating set S. Such a set can be found by a process of whittling: At each step, search for any $g \in T$ such that $g \in \langle T \setminus \{g\} \rangle$. If any are found, then take one such g and replace T with $T \setminus \{g\}$. Repeat this step until no such g can be found. Since T is finite, the process must finish. The resulting set S will be independent. At each step, since g can be written as a word in the other elements of T, removing g from T will still result in a generating set for G. Hence S must be an independent generating set for G.

There are two functions that we now introduce.

Definition 1.0.3. Let G be a finite group. $\mu'(G)$ is the size of a largest independent set in G. $\mu(G)$ is the size of a largest independent generating set for G.

It is clear that $\mu(G) \leq \mu'(G)$ for any G. There are examples of finite groups G where $\mu(G) < \mu'(G)$.

Throughout this thesis, we will attempt, for various groups G, to get good upper bounds for $\mu'(G)$ or $\mu(G)$. The interest in these functions arises from work done by Persi Diaconnis and Laurent Saloff-Coste in the study of random generation of group elements [4]. In particular, it arises from their work in studying the running time of the product replacement algorithm. The algorithm runs as follows: For a group G, take an ordered generating set S and append copies of the identity to it, so as to get a tuple $\mathbf{x}$ of length n. The running of the algorithm then consists of repeating the following steps a given number of times: Choose two elements u, v uniformly at random from $\mathbf{x}$ and also choose a random $e \in \{1, -1\}$. Then replace u in $\mathbf{x}$ with uv^e to get a new tuple $\mathbf{x}$. Suppose we

complete the algorithm for some generating set S of a group G. Let uv^e be the element that replaced u in the final step. If the algorithm has run for long enough, then the probability that $uv^e = g$ for $g \in G$ is almost uniform across G. Hence we have generated an almost random element of G. The natural question to ask is: Given G, S and n (the length of $\mathbf{x}$), how long to we have to run the algorithm for in order to produce a random element of G? As Diaconis and Saloff-Coste state, one bound for the running time is $|G|^{O(\mu(G))}n^2 \log n$ [4, p. 254]. Hence the interest in the size of $\mu(G)$.

We now introduce some existing results regarding independent sets.

1.1 Previous Results

1.1.1 Independent Generating Sets and Frattini Subgroups

Suppose that G is a finite group. Let $\Phi(G)$ denote the Frattini subgroup of G. The following proposition is standard:

Proposition 1.1.1. *If $N \leq \Phi(G)$ such that $N \trianglelefteq G$ then $\mu(G) = \mu(G/N)$.*

The proof of Burnside's Basis Theorem uses ideas similar to Proposition 1.1.1.

Theorem 1.1.1 (Burnside's Basis Theorem)**.** *Let G be a p-group with $|G/\Phi(G)| = p^d$. Then $\mu(G) = d$. Furthermore, no independent generating set of G has fewer than d elements.*

There are slightly differing statements of this theorem in [5, p. 31] and [6, p. 199]. The outline of the proof in [6, p. 199] uses an idea similar to Proposition 1.1.1. Indeed, Proposition 1.1.1 can be used to prove a weaker statement of Burnside's Basis Theorem.

1.1.2 Independent Sets in Symmetric Groups

With regard to Symmetric groups, Julius Whiston proved a powerful result in a paper published in 2000 [14]:

Theorem 1.1.2 (J. Whiston)**.** *If T is an independent set inside a symmetric group S_n then $|T| \leq n-1$. Furthermore, if $|T| = n-1$ then $\langle T \rangle = S_n$.*

This gives a useful corollary.

Corollary 1.1.1. *$\mu'(A_n) \leq n-2$.*

It is interesting to note here that the proof of Theorem 1.1.2 depends upon the Classification of the Finite Simple Groups.

1.1.3 Normal Subgroups

In his proof of Theorem 1.1.2, Whiston made implicit use of a particular lemma. This lemma was explicitly written later, in a paper by Peter Cameron and Philippe Cara [3]. We state and prove a particular form of the lemma here. There is some terminology that we should clarify before the statement of the lemma, however.

Definition 1.1.1. Suppose that $N \trianglelefteq G$, and that $S \subseteq G$. Let $\phi : G \to G/N$ be the natural map. Take S' to be the multiset $\{\phi(g) | g \in S\}$. If S' is an independent set in G/N then S is said to be *independent in its action on N*.

Lemma 1.1.1. *Suppose that $N \trianglelefteq G$ and $S = \{g_1, \ldots, g_n\} \subseteq G$ is an independent set in G. Then there are independent sets $S_1, S_2 \subseteq G$ such that*

1. *S_1 is independent in its action on N,*
2. *$S_2 \subseteq N$,*
3. *$|S_1| + |S_2| = |S|$, and*
4. *$\langle S \rangle = \langle S_1, S_2 \rangle$.*

Proof. Consider the image S' of S in G/N. This image S' must generate the image of $\langle S \rangle$ in G/N. So S' contains an independent generating set S_1' for the image of $\langle S \rangle$. Now, there must be $|S_1'|$ elements of $\{g_1, \ldots, g_n\} = S$ such that the image of these elements in

G/N is S_1'. Let $S_1 \subseteq S$ be the subset of these elements. Relabelling the g_i if necessary, we may assume that $S_1 = \{g_1, \ldots, g_m\}$ for some $m \leq n$. Observe that $\langle S_1 \rangle$ provides the action of $\langle S \rangle$ on N. If $S_1 = S$ then we are done, so suppose not.

Since $\langle S_1 \rangle$ provides the action of $\langle S \rangle$ on N, for each $i \geq m+1$ there must be $\omega_i \in \langle S_1 \rangle$ such that $g_i\omega_i \in N$. It may well be that $\omega_i = 1$ for some i. For each $i \geq m+1$, define $h_i := g_i\omega_i$. Let $S_2 := \{h_{m+1}, \ldots, h_n\}$. Clearly $S_2 \subseteq N$ and $|S| = |S_1| + |S_2|$. We wish to argue that S_2 is an independent set. Suppose not. Then there must be some i such that $h_i = h_{j_1}h_{j_2}\ldots h_{j_s}$ where each $j_k \neq i$. So $g_i\omega_i = g_{j_1}\omega_{j_i}g_{j_2}\omega_{j_2}\ldots g_{j_s}\omega_{j_s}$, which implies that $g_i = g_{j_1}\omega_{j_i}g_{j_2}\omega_{j_2}\ldots g_{j_s}\omega_{j_s}\omega_i^{-1}$.

Now, each $g_{j_k} \in \langle S \setminus \{g_i\} \rangle$, as is each ω_k. So $g_i = g_{j_1}\omega_{j_i}g_{j_2}\omega_{j_2}\ldots g_{j_s}\omega_{j_s}\omega_i^{-1} \in \langle S \setminus \{g_i\} \rangle$, which contradicts the independence of S. Thus, for each i, $h_i \notin \langle S_2 \setminus \{h_i\} \rangle$. Therefore S_2 is an independent set in N.

Now, for each $i \geq m+1$, $g_i = h_i\omega_i^{-1}$. So $g_{m+1}, \ldots, g_n$ can be recovered from S_2 using $\langle S_1 \rangle$. Hence $\langle S_1, S_2 \rangle = \langle S_1, g_{m+1}, \ldots, g_n \rangle = \langle S \rangle$. The lemma is now proven. □

Corollary 1.1.2. *Suppose $N \trianglelefteq G$. Then*

1. *$\mu'(G) \leq \mu'(G/N) + \mu'(N)$, and*
2. *$\mu(G) \leq \mu(G/N) + \mu'(N)$.*

Proof. Let $S \subseteq G$ be an independent set. By Lemma 1.1.1 there must be independent $S_1, S_2 \subseteq G$ such that $|S_1| + |S_2| = |S|$, the image of S_1 in G/N is independent, and S_2 is an independent set in N. Thus, $|S_1| \leq \mu'(G/N)$ and $|S_2| \leq \mu'(N)$. Therefore $|S| = |S_1| + |S_2| \leq \mu'(G/N) + \mu'(N)$. Assuming that S is of largest size gives us that $\mu'(G) \leq \mu'(G/N) + \mu'(N)$.

Suppose further that S generates G. As $S_2 \subseteq N$, each $g \in S_2$ is mapped to 1 in G/N. Thus the image of $\langle S \rangle$ in G/N must be generated by the image of S_1 in G/N. But the image of $\langle S \rangle$ is G/N. Hence the image of S_1 in G/N is an independent generating set for G/N. Hence $\mu(G) \leq \mu(G/N) + \mu'(N)$. □

We will make frequent use of Corollary 1.1.2 throughout this thesis.

1.1.4 $L_2(q)$

Jan Saxl and Julius Whiston managed to get bounds on $\mu(L_2(q))$ that are tight in some circumstances [12]. We list their results here.

Theorem 1.1.3 (J. Saxl & J. Whiston)**.** *Suppose p is an odd prime. Then $\mu(L_2(p)) \leq 4$. Furthermore, $\mu(L_2(p)) = 3$ if $p \equiv \pm 1$ mod 8.*

Theorem 1.1.4 (J. Saxl & J. Whiston)**.** *Suppose $q = p^r$ is a power of an odd prime. Then $\mu(L_2(q)) \leq \max\{6, \pi(r) + 2\}$ where $\pi(r)$ is the number of distinct prime divisors of r.*

For Theorem 1.1.4 if $\pi(r) + 2 \geq 6$ then the bound is tight.

Saxl and Whiston's results for $L_2(p)$ and $L_2(q)$ are of special interest to us, as we will adopt the strategy used to prove them, with some modifications. We give an outline of the strategy now.

A Proof Strategy

Saxl and Whiston's strategy was as follows: Let G be a finite group such that $Z(G) \leq \Phi(G)$, and let $S := \{g_1, \ldots, g_n\} \subseteq G$ be an independent generating set for G. Suppose we wish to show that there is some m such that $\mu(G) \leq m$. Showing that $|S| \leq m$ will do this.

Suppose further that for any m distinct maximal subgroups $M_1, \ldots, M_m$ of G, either

1. $\mu'(M_i) \leq m - 1$ for some $i \leq m$, or
2. $\bigcap_{i=1}^{m} M_i \leq Z(G)$.

Now, for each $i \leq n$, define $H_i := \langle S \backslash \{g_i\} \rangle$. Observe that each H_i must lie in a maximal subgroup of G. Let $H_1, \ldots, H_n$ lie in maximal subgroups $M_1, \ldots, M_n$ respectively. The M_i must be distinct: If $M_i = M_j$ for some i, j then

$$G = \langle S \rangle = \langle H_i, H_j \rangle \leq \langle M_i, M_j \rangle = M_i,$$

which cannot be.

Now suppose that $\mu'(M_i) \leq m-1$ for some $i \leq n$. Now $S \setminus \{g_i\}$ is an independent set in M_i, so $|S \setminus \{g_i\}| \leq m-1$. Therefore $|S| \leq m$, and we have what we wanted. So suppose there is no such M_i, and that $|S| \geq m+1$. The intersection of any m of the M_i is therefore trivial. Hence

$$g_n \in \bigcap_{i=1}^{m} H_i \leq \bigcap_{i=1}^{m} M_i \leq Z(G).$$

Now we insisted that $Z(G) \leq \Phi(G)$, so $g_n \in \Phi(G)$. But notice that H_n, g_n must both lie in some maximal subgroup M of G. Hence

$$G = \langle S \rangle = \langle H_n, g_n \rangle \leq M \lneqq G,$$

which is absurd. So $|S| \leq m$, and we have what we wanted.

For this strategy to be implemented for a finite group G, obviously we need a good understanding of its subgroup structure. In particular, we need to know its maximal subgroups. Fortunately, in the case of the classical groups we have a good understanding of their maximal subgroups. For the three classical groups we study, we will use the lists of maximal subgroups of these groups drawn up by John Bray, Derek Holt and Colva Roney-Dougal [8]. These lists use Aschbacher's classification of maximal subgroups of almost simple groups.

Aschbacher's Classes

Aschbacher's classification of the maximal subgroups of almost simple groups can be found in [1], [10]. Let G be a finite classical group. As part of the classification, Aschbacher presents eight classes of maximal subgroups that can be found in almost simple groups. In describing these classes of maximal subgroups of G we suppose that G acts in a natural fashion upon a vector space V of dimension n over field $\mathbb{F}$. Throughout this section, M will be a maximal subgroup of G of geometric nature.

$\mathcal{C}_1$**:** If $M \in \mathcal{C}_1$ then there is some proper, non-trivial subspace U of V such that $M = \mathrm{Stab}_G(U)$. Furthermore, if G stabilises a form on V then U is not isometric to $U^\perp$.

$\mathcal{C}_2$**:** If $M \in \mathcal{C}_2$ then there are some subspaces $U_1, \ldots, U_r \leq V$ such that $r|n$, $\dim(U_i) = \frac{n}{r}$ for all i and $V = U_1 \oplus U_2 \oplus \ldots \oplus U_r$. $M = \mathrm{Stab}_G(U_1 \oplus \ldots \oplus U_r)$.

$\mathcal{C}_3$**:** If $M \in \mathcal{C}_3$ then M stabilises a field extension. More precisely, suppose V is isomorphic to a vector space K over field $\mathbb{F}^p$, where p is a prime dividing n. Then the full stabiliser M in G of the K-structure in V is a maximal subgroup of G.

$\mathcal{C}_4$**:** If $M \in \mathcal{C}_4$ then there is a tensor product decomposition $V = V_1 \otimes V_2$ such that $M = \mathrm{Stab}_G(V_1 \otimes V_2)$.

$\mathcal{C}_5$**:** If $M \in \mathcal{C}_5$ then there is some subfield $\mathbb{F}' \leq \mathbb{F}$ of prime index in $\mathbb{F}$, and some n-dimensional $\mathbb{F}'$ subspace $U \leq V$ such that $M = \mathrm{Stab}_G(U)$.

$\mathcal{C}_6$**:** If $M \in \mathcal{C}_6$ then there is some $R \leq G$ such that R is of symplectic type and $M = N_G(R)$.

$\mathcal{C}_7$**:** Suppose that $n = r^t$. If $M \in \mathcal{C}_7$ then there is a decomposition $V = \bigotimes_{i=1}^t V_i$ where each $\dim(V_i) = r$, such that $M = \mathrm{Stab}_G\left(\bigotimes_{i=1}^t V_i\right)$.

$\mathcal{C}_8$**:** If $M \in \mathcal{C}_8$ then M is isomorphic to a classical group.

1.2 The Results Proved in This Thesis

The main purpose of this thesis is to prove an upper bound for $\mu(SL_3(q))$ for odd q. We prove other results in preparation for this.

In Chapter 2, we establish the following theorem - Theorem 2.3.1, with its accompanying corollary:

Theorem. *Let $S \subseteq SO_3(q)$ be an independent set in $SO_3(q)$. Then either $\langle S \rangle$ is a subspace stabiliser, or*

1. *$|S| \leq 4$ if q is prime, or*

2. $|S| \leq \max\{6, \pi(r)+3\}$ *where* $q = p^r$, p *is a prime.*

Corollary. *If* q *is a prime then* $\mu(SO_3(q)) \leq 4$. *If* $q = p^r$ *for a prime* p *then* $\mu(SO_3(q)) \leq \max\{6, \pi(r)+3\}$.

The strategy used here is essentially the strategy that Saxl and Whiston used in proving Theorems 1.1.3 and 1.1.4. This gives us an upper bound for $\mu(SO_3(q))$, but also enables us to implement Saxl and Whiston's strategy for other classical groups. This is because $SU_3(q)$ contains $SO_3(q)$ as a subfield subgroup and $SL_3(q)$ contains $SO_3(q)$ as a maximal subgroup of type $\mathcal{C}_8$.

In Chapter 3, we establish Theorem 3.3.1. Its statement is:

Theorem. *Let* q *be a power of an odd prime. Suppose* $S \subseteq SU_3(q)$ *is independent. Then one of the following holds:*

1. $\langle S \rangle$ *is a subspace stabiliser, decomposition space stabiliser or field extension stabiliser.*

2. $\langle S \rangle$ *lies in a subfield subgroup.*

3. q *is prime and* $|S| \leq 6$.

4. $q = p^r$ *for some odd prime* p *and* $|S| \leq \max\{8, \pi(r)+3\}$.

Once again, this gives us an upper bound for $\mu(SU_3(q))$, but also enables us to use Saxl and Whiston's strategy for $SL_3(q)$. $SL_3(q)$ contains $SU_3(q)$ subgroups as maximal subgroups of type $\mathcal{C}_8$.

In Chapter 4, we establish the main result of this thesis:

Theorem. *Let* q *be the power of an odd prime. Then*

1. $\mu(SL_3(q)) \leq 6$ *if* q *is a prime.*

2. $\mu(SL_3(q)) \leq \max\{10, \pi(r)+6\}$ *if* $q = p^r$ *for an odd prime* p.

Once again, we use Saxl and Whiston's strategy in order to do this.

In the later chapters, we take up a proof strategy that was used in Chapter 3 and apply it to groups with proper, normal, abelian subgroups. In Chapter 5, given a group G with a proper, normal, abelian subgroup N, we provide an expression for $\mu(G)$ in terms of $\mu(G/N)$ and the action of G on N. We use this result in Chapter 6 to find $\mu(G)$ for some finite Coxeter groups G. The main result established here is:

Proposition. *Suppose G is a finite, irreducible Coxeter group with n vertices in its Coxeter diagram, such that G is not of type E_6, E_7 or E_8. If G is not dihedral then $\mu(G) = n$ or $n+1$.*

1.3 A Note on the Text

Throughout this thesis,we will endeavour to use ATLAS notation when referring to group structure. We note some of the features of this notation. $SO_n(q), SU_n(q), SL_n(q)$ refer to the n-dimensional special orthogonal, special unitary and special linear groups respectively. Most textbooks would agree with this use of notation. However, $U_n(q)$ is taken to be equivalent to $PSU_n(q)$, $L_n(q)$ is equivalent to $PSL_n(q)$ and $O_n(q)$ is equivalent to $P\Omega_n(q)$.

If a group G is written as $A : B$ then this means that G is the semi-direct product $A \rtimes B$ for some $A, B \leq G$. If G is written as $A.B$ then this means that G is a non-split extension of A by B. If G is written as $A.B$ then this means that $A \trianglelefteq G$ and $G/A \cong B$, with no specific claim being made of the nature of the extension.

Single integers a may be used to refer to the cyclic group C_a. a^b will refer to the direct product $\underbrace{C_a \times \ldots \times C_a}_{b}$ of b copies of C_a. It should be obvious from context when a or a^b refer to groups, and when they refer to genuine numbers. We also note here that 1 may be used to refer to the identity element of a group. Once again, it should be obvious from the context whether 1 refers to an identity element or the integer 1. r^{1+2m} will denote a group of symplectic type.

For any classical group G that we consider, we will automatically assume that it acts in a natural fashion on an underlying vector space V, defined over an appropriate field. Also, for any sort of group action, we will make the group act on the right. So we treat V as a set of row vectors, and multiply vectors on the right by matrices.

CHAPTER 2

INDEPENDENT SETS IN 3-DIMENSIONAL SPECIAL ORTHOGONAL GROUPS OVER FIELDS OF ODD CHARACTERISTIC

In this chapter, we wish to place bounds on the size of independent set S within $SO_3(q)$ for odd q. We will eventually arrive at a result that says that either $|S|$ must be bounded, or the nature of $\langle S \rangle$ is limited. This will enable us to place bounds on $\mu(SO_3(q))$. However, it is a result that will prove useful in later chapters as well.

The approach is a simple development of the one described in the introduction. We let $S = \{g_1, \ldots, g_n\}$ be an independent set inside $SO_3(q)$, q odd, and for each non-empty $T \subsetneqq S$, define $H_T := \langle S \setminus T \rangle$. Observe that H_T must be a proper subgroup of $SO_3(q)$. For each $T \subsetneqq S$, define $K_T := H_T \cap \Omega_3(q)$ - the intersection of H_T with the derived subgroup of $SO_3(q)$. Note that $|H_T : K_T| \leq 2$ for each T.

We will use K_T to determine the nature of H_T. If $K_T \neq \Omega_3(q)$ then K_T must lie in a maximal subgroup of $\Omega_3(q)$. The maximal subgroups of $\Omega_3(q)$, where $q \geq 5$ is odd, are described in Table 2.1. The information on Table 2.1 is drawn from [8].

For the most part, we will be interested in the groups $H_{\{g_i\}}$, $g_i \in S$. If any $\mu'(K_{\{g_i\}})$ is small (at most 3), then $\mu'(H_{\{g_i\}})$ will be small as well (at most 4). If this is not the case, we will see that the nature of $H_{\{g_i\}}$ is limited.

Throughout, we will assume that each $SO_3(q)$ acts on a vector space V of dimension 3 over the field of order q.

Class	Isomorphism Type	Conditions
$\mathcal{C}_1$	$E_q : \frac{q-1}{2}$	
	D_{q-1}	$q \neq 5, 7, 9, 11$
	D_{q+1}	$q \neq 7, 9$
$\mathcal{C}_2$	$2^2 : S_3$	$q = p \equiv \pm 1 \bmod 8$
	$2^2 : 3$	$q = p \equiv \pm 3, 5, \pm 13 \bmod 40$
$\mathcal{C}_5$	$\Omega_3(q_0).(r, 2)$	$q = q_0^r$, r prime
$\mathcal{S}_1$	A_5	$q = p \equiv \pm 1 \bmod 10$
		$q = p^2$, $p \equiv \pm 3 \bmod 10$

Table 2.1: The maximal subgroups of $\Omega_3(q)$ for $q \geq 5$ odd

2.1 Independent sets in $SO_3(q)$ for q an odd prime

Let S and the H_T, K_T be as already defined. So $S = \{g_1, \ldots, g_n\}$ is an independent set in $SO_3(q)$. We make a further assumption that q is an odd prime. We prove some lemmas before proving the main result of this section.

Lemma 2.1.1. *Let $H \leq GO_3(q)$, and let $K \leq H$ such that $|H : K| \leq 2$. If K is a subspace stabiliser then H is a subspace stabiliser.*

Proof. If $H = K$ then the conclusion is immediate. So suppose not. Let $g \in H \setminus K$. So $H = \langle K, g \rangle$ since $|H : K| = 2$.

Let U be a subspace stabilised by K. If $\dim(U) = 1$, then we are satisfied. So suppose not. Since $GO_3(q)$ acts on a 3-dimensional vector space, it must be that $dim(U) = 2$. But then K also stabilises 1-dimensional $U^\perp$. Hence we can always suppose that K stabilises a 1-dimensional space U.

If g fixes U then $H = \langle K, g \rangle$ is a subspace stabiliser. So suppose $U^g \neq U$. Now, since $|H : K| = 2$, it must be that $g^2 \in K$. Thus $U^{g^2} = U$. This means that g fixes $U \oplus U^g$. Now consider the action of K on U^g. For any $k \in K$,

$$(U^g)^k = U^{gkg^{-1}g} = U^g,$$

where the second equality follows from the fact that $gkg^{-1} \in K$. So K stabilises both U and U^g. But then K must stabilise $U \oplus U^g$. Hence $H = \langle K, g \rangle$ stabilises $U \oplus U^g$, and we

have what we want. □

Lemma 2.1.2. *For each H_T, $T \subsetneq S$, either H_T contains at most 3 elements of S, $H_T = \Omega_3(q)$, or H_T is a subspace stabiliser.*

Proof. Suppose that $K_T = \Omega_3(q)$. The only subgroup of $SO_3(q)$ that contains $\Omega_3(q)$ as a proper subgroup is $SO_3(q)$. So, given that H_T is an overgroup of K_T, it must be that $H_T = \Omega_3(q)$ or $H_T = SO_3(q)$. But H_T must be a proper subgroup of $SO_3(q)$, so $H_T = \Omega_3(q)$. So we suppose that $K_T \neq \Omega_3(q)$. Hence each K_T must lie in a maximal subgroup of $\Omega_3(q)$. We consider all possible cases.

Case: K_T lies in an $\mathcal{S}_1$ subgroup

In this case K_T is isomorphic to a subgroup of A_5. Now, if $g \in SO_3(q)$ normalises $A_5 \leq SO_3(q)$ then $g \in A_5$ [8]. So if $K_T \cong A_5$ then $H_T = K_T$. So $\mu'(H_T) = \mu'(A_5) = 3$. Thus H_T contains at most 3 elements of S. Hence suppose K_T is isomorphic to a proper subgroup of A_5. So K_T is isomorphic to a subgroup of S_3, A_4 or D_{10}, since these are maximal subgroups of A_5. But it is easy to check that

$$\mu'(S_3) = \mu'(A_4) = \mu'(D_{10}) = 2.$$

If $H_T = K_T$ then $\mu'(H_T) = \mu'(K_T) \leq 2$. If $H_T = K_T.2$ then

$$\mu'(H_T)\mu'(K_T.2) \leq \mu(K_T) + \mu'(2) \leq 2 + 1 = 3,$$

where the second equality follows from Corollary 1.1.2. So H_T contains at most 3 elements of S.

Case: K_T lies in a $\mathcal{C}_2$ subgroup

In this case K_T is isomorphic to a subgroup of $2^2 : S_3 \cong S_4$. If $K_T \cong 2^2 : S_3$ then $N_{SO_3(q)}(K_T) = K_T$ [8]. In that case $H_T = K_T$ and so $\mu'(H_T) \leq \mu'(S_4) = 3$. Then H_T contains at most 3 elements of S. So suppose K_T is isomorphic to a proper subgroup of $2^2 : S_3 \cong S_4$. But then Whiston's result regarding independent sets in symmetric

groups (Theorem 1.1.2) tells us that any such group contains independent sets of at most $\mu'(S_4) - 1 = 2$ elements. Hence $\mu'(K_T) \leq 2$. Therefore

$$\mu'(H_T) \leq \mu'(K_T) + 1 \leq 3,$$

and so H_T contains at most 3 elements of S.

Case: K_T lies inside a $\mathcal{C}_1$ subgroup

In this case we wish to argue that H_T stabilises a subspace. If $H_T = K_T$ then H_T is a subspace stabiliser. So suppose K_T is of index 2 in H_T. But K_T stabilises a subspace, so we may apply Lemma 2.1.1 to H_T, K_T to get that H_T is a subspace stabiliser.

These are all the possible cases, so the lemma has been established. □

We now prove a lemma regarding the intersection of subspace stabilisers. However, we widen our assumptions. In this chapter we deal with the case that $G = SO_3(q)$ stabilises some bilinear form on V. If we allow the possibility that $G = SU_3(q)$ stabilises an hermitian form on V then we will have a result useful in this chapter and the next. We use the fact that any subspace stabiliser in $SO_3(q)$ or $SU_3(q)$ must stabilise both a 2-dimensional subspace U and a 1-dimensional subspace $U^\perp$.

Lemma 2.1.3. *Suppose $G = SO_3(q)$ or $SU_3(q)$ and $S \subseteq G$ is independent. Suppose $T_1, T_2, T_3 \subsetneq S$ are non-empty such that $T_i \cap T_j = \varnothing$ for all distinct i, j. Suppose further that $H_{T_1}, H_{T_2}, H_{T_3}$ are subspace stabilisers, stabilising 2-dimensional U_1, U_2, U_3 respectively. Then either $\langle S \rangle$ stabilises a subspace or $\bigcap_{i=1}^{3} H_{T_i} \leq Z(G)$.*

Proof. Suppose $U_i = U_j$ for some distinct i, j. Let $g_k \in S$. If $g_k \notin T_i$ then $g_k \in S \setminus T_i$. In this case, $g_k \in H_{T_i}$. If $g_k \in T_i$ then $g_k \notin T_j$ as $T_i \cap T_j = \varnothing$. In this case, $g_k \in H_{T_j}$. So each $g_k \in S$ lies in one of H_{T_i}, H_{T_j}. Thus, $\langle S \rangle = \langle H_{T_i}, H_{T_j} \rangle$ stabilises $U_i = U_j$. So suppose the U_i are mutually distinct.

Now suppose that $U_1 \cap U_2 \cap U_3 \neq \{\mathbf{0}\}$. Then $U_1 \cap U_2 = U_1 \cap U_3 = U_2 \cap U_3$ since the U_i are distinct. Now, $H_{T_1} \cap H_{T_2}$ stabilises $U_1 \cap U_2$, while $H_{T_1} \cap H_{T_3}$ stabilises $U_1 \cap U_3 = U_1 \cap U_2$ and $H_{T_2} \cap H_{T_3}$ stabilises $U_2 \cap U_3 = U_1 \cap U_2$. But now take any $g_i \in S$. If $g_i \notin T_1 \cup T_2$ then g_i

lies in both $S \setminus T_1, S \setminus T_2$. In this case $g_i \in H_{T_1} \cap H_{T_2}$. If $g_i \in T_1 \cup T_2$ then it cannot be that $g_i \in T_3$ as $T_1 \cap T_3, T_2 \cap T_3 = \varnothing$. Note also that either $g_i \notin T_1$ or $g_i \notin T_2$ since $T_1 \cup T_2$ is a disjoint union. But then g_i must lie either in both $S \setminus T_1, S \setminus T_3$ or $S \setminus T_2, S \setminus T_3$. Therefore g_i lies in one of $H_{T_1} \cap H_{T_3}, H_{T_2} \cap H_{T_3}$ in this case. Hence any $g_i \in S$ lies in at least one of $H_{T_1} \cap H_{T_2}, H_{T_1} \cap H_{T_3}, H_{T_2} \cap H_{T_3}$. But then $\langle S \rangle = \langle H_{T_1} \cap H_{T_2}, H_{T_1} \cap H_{T_3}, H_{T_2} \cap H_{T_3} \rangle$ must stabilise $U_1 \cap U_2$. So suppose that $U_1 \cap U_2 \cap U_3 = \{\mathbf{0}\}$.

Let $W_{12} := U_1 \cap U_2, W_{13} := U_1 \cap U_3, W_{23} := U_2 \cap U_3$. Now $V = W_{12} \oplus W_{13} \oplus W_{23}$ with $\bigcap_{i=1}^3 H_{T_i}$ stabilising each subspace in this decomposition. Now $\bigcap_{i=1}^3 H_{T_i}$ also stabilises each 1-dimensional $U_1^\perp, U_2^\perp, U_3^\perp$. Note that $U_i^\perp \neq U_j^\perp$ for all distinct i, j otherwise $U_i = U_j$ for some i, j. We consider all possibilities for the $U_i^\perp$ and argue in each case that either $\bigcap_{i=1}^3 H_{T_i} \leq Z(G)$, $\langle S \rangle$ is a subspace stabiliser, or the case is impossible.

Suppose that some $U_i^\perp \not\leq W_\alpha \oplus W_\beta$ for any $\alpha, \beta = 12, 13$ or 23. Then any $g \in \bigcap_{j=1}^3 H_{T_j}$ must fix each of $W_{12}, W_{13}, W_{23}, U_i^\perp$ and in so doing, be scalar. Hence $\bigcap_{j=1}^3 H_{T_j} \leq Z(G)$. So suppose that for each $U_i^\perp$ there is some α, β such that $U_i^\perp \leq W_\alpha \oplus W_\beta$. It must be that $W_\alpha \oplus W_\beta = U_j$ for some j. Hence we may assume that for each i there is some j such that $U_i^\perp \leq U_j$.

Suppose that two distinct $U_i^\perp, U_j^\perp$ are contained within the same U_k. Suppose, to begin with, that the indices i, j, k are distinct. Note that $U_k = U_i^\perp \oplus U_j^\perp$. Then $H_{T_i} \cap H_{T_j}$ stabilises $U_i^\perp \oplus U_j^\perp = U_k$. But then $\langle S \rangle = \langle H_{T_i} \cap H_{T_j}, H_{T_k} \rangle$ stabilises U_k. So suppose that $U_i^\perp, U_j^\perp \leq U_i$. Without loss of generality, we suppose that $U_1^\perp, U_2^\perp \leq U_1$. The other cases will be similar.

Now, $U_2^\perp \leq U_1$ so it must be that $U_1^\perp \leq (U_2^\perp)^\perp = U_2$. Therefore $U_1^\perp$ lies in both U_1, U_2. Hence $U_1^\perp = W_{12}$. Now consider $U_3^\perp$. It cannot be that $U_3^\perp \leq U_2$ as then $U_1^\perp, U_3^\perp \leq U_2$ and we have already dealt with this case. Also, it cannot be that $U_3^\perp \leq U_1$ as then $U_2^\perp, U_3^\perp \leq U_1$. So $U_3^\perp \leq U_3$. Note that $U_3 \neq W_{13}, W_{23}$ since $U_3^\perp \not\leq U_1, U_2$.

But now consider $U_2^\perp$. Suppose $U_2^\perp \leq U_3$. But then $U_3^\perp \leq (U_2^\perp)^\perp = U_2$, which does not happen. So $U_2^\perp \not\leq U_3$. Therefore $U_2^\perp \neq W_{12}, W_{13}$ as $U_2^\perp \neq U_1^\perp = W_{12}$ and $U_2^\perp \not\leq U_3$. But now take any $g \in \bigcap_{i=1}^3 H_{T_i}$. g fixes each of W_{12}, W_{13}, W_{23}, $U_2^\perp$, $U_3^\perp$. Therefore g

fixes each of the three distinct points $W_{12}, W_{13}, U_2^\perp$ within U_1 and fixes each of the three distinct points $W_{13}, W_{23}, U_3^\perp$ within U_3. Hence both $g|_{U_1}, g|_{U_3}$ are scalar. But then g itself must be scalar. Hence $\bigcap_{i=1}^3 H_{T_i} \leq Z(G)$. So we suppose that for each U_i, U_i contains at most one $U_j^\perp$.

But now suppose that some $U_i^\perp = W_\alpha$ for some i, α. Then $U_i^\perp$ lies in two U_j. Without loss of generality, suppose $U_i^\perp \leq U_1, U_2$. Then neither of the other two U_j can lie in U_1 or U_2, as then U_1 or U_2 contain two $U_k^\perp$. Therefore the other two $U_j^\perp$ lie in U_3 since we have assumed that each $U_j^\perp$ lies in some U_k. But by assumption, it cannot be that the other two $U_j^\perp \leq U_3$. Therefore $U_i^\perp \neq W_\alpha$ for all i, α. Therefore W_{12}, W_{13} and one of the $U_i^\perp$ form three distinct points in U_1. Also W_{12}, W_{23} and one of the remaining $U_j^\perp$ must form three distinct points within U_2. But now take $g \in \bigcap_{i=1}^3 H_{T_i}$. g fixes each of $W_{12}, W_{13}, W_{23}, U_1^\perp, U_2^\perp, U_3^\perp$. Therefore it must fix the three distinct points we found within U_1 as well as the three distinct points we found within U_2. Therefore both $g|_{U_1}, g|_{U_2}$ are scalar, and so g itself is scalar. Therefore $\bigcap_{i=1}^3 H_{T_i} \leq Z(G)$.

This establishes the proposition. □

We return to our more restrictive assumption that $S \subseteq SO_3(q)$.

Corollary 2.1.1. *Suppose $H_{\{g_1\}}, H_{\{g_2\}}, H_{\{g_3\}}$ are subspace stabilisers. Then $\langle S \rangle$ is a subspace stabiliser or $\bigcap_{i=1}^3 H_{\{g_i\}} = \{1\}$.*

Proof. For each $i \leq 3$, let $T_i = \{g_i\}$. Observe that $T_i \cap T_j = \varnothing$ for all distinct i, j. So applying Lemma 2.1.3 to T_1, T_2, T_3 in this case, and using the fact that $Z(SO_3(q)) = \{1\}$, gives us the corollary. □

We are now able to prove the main result of this section.

Proposition 2.1.1. *With S as defined, either $|S| \leq 4$, or $\langle S \rangle$ is a subspace stabiliser.*

Proof. Table 2.1 covers only the cases where $q \geq 5$, so we must cover the case that $S \subseteq SO_3(3)$ separately. But $SO_3(3) \cong S_4$, so $\mu'(SO_3(3)) = \mu'(S_4) \leq 3$. So suppose that $q \geq 5$.

We now consider the $H_{\{g_i\}}$ as defined previously. If any $H_{\{g_i\}}$ contains at most three elements of S then we are done, so suppose that each $H_{\{g_i\}}$ contains at least four elements of S. Observe that this means that there are at least five $H_{\{g_i\}}$, since $H_{\{g_1\}}$ must contain the elements $g_2, g_3, g_4, g_5 \in S$. This means that it must possible to define $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5\}}$, and so there at least five $H_{\{g_i\}}$.

By Lemma 2.1.2 it must be that for each $H_{\{g_i\}}$, either $H_{\{g_i\}} = \Omega_3(q)$ or $H_{\{g_i\}}$ is a subspace stabiliser. Suppose that some $H_{\{g_i\}} = \Omega_3(q)$. Now suppose that $H_{\{g_j\}} = \Omega_3(q)$ for some $j \neq i$. But then $g_i \in H_{\{g_j\}} = H_{\{g_i\}}$, which contradicts the independence of S. So for each $i \geq 2$, $H_{\{g_i\}}$ is a subspace stabiliser. This implies that $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5\}}$ are subspace stabilisers. Since $\Omega_3(q)$ does not stabilise a subspace, it cannot be that $\langle S \rangle$ stabilises a subspace. By Corollary 2.1.1 then, we have that $g_5 \in \bigcap_{i=2}^{4} H_{\{g_i\}} = \{1\}$, which cannot be. So no $H_{\{g_i\}} = \Omega_3(q)$ if $|S| \geq 5$.

Therefore $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ are subspace stabilisers. Now $g_5 \in \bigcap_{i=1}^{4} H_{\{g_i\}}$, so it cannot be that $\bigcap_{i=1}^{4} H_{\{g_i\}} = \{1\}$. By Corollary 2.1.1 then, $\langle S \rangle$ is a subspace stabiliser. This establishes the proposition. □

This completes the study of the case when q is an odd prime. We must now investigate what happens when $SO_3(q)$ is defined over a field of prime-power order.

2.2 Independent sets in $SO_3(q)$ for $q = p^r$, p an odd prime

In this section we deal with the case that $\langle S \rangle$ lies inside $SO_3(q)$ where $q = p^r$ is a power of an odd prime. We will find it helpful to suppose that q is the smallest power of p such that $\langle S \rangle \leq SO_3(q)$. Given the nature of the bound on $|S|$ that we obtain, this assumption is allowable. The main result will still hold true for $SO_3(q^a) \supseteq S$ for any overgroup $SO_3(q^a) \geq SO_3(q)$.

First, we establish some results about the subfield subgroups of $SO_3(q)$. These will be useful in various places.

2.2.1 The subgroups of $SO_3(q)$

We aim to describe the subgroups of $SO_3(q)$. Our first step towards this goal is this:

Proposition 2.2.1. *Suppose that $g \in GO_3(q)$ normalises $\Omega_3(q_0) \leq GO_3(q)$. Then $g \in GO_3(q_0)$.*

Proof. If q_0 is prime, then the proposition is easily established. In this case, the only non-trivial outer automorphism of $\Omega_3(q_0)$ is the diagonal automorphism ([8]). If $g \in GO_3(q)$ is a linear automorphism of $\Omega_3(q_0)$ in this case, then it must act on $\Omega_3(q_0)$ in the same manner as some $k \in GO_3(q_0)$. Then gk^{-1} commutes with $\Omega_3(q_0)$. Now, let $H \leq \Omega_3(q_0)$ be the full stabiliser of a 1-dimensional subspace U. Then for any $h \in H$,

$$(U^{gk^{-1}})^h = U^{h(gk^{-1})} = U^{gk^{-1}}.$$

Hence H stabilises $U^{gk^{-1}}$, a 1-dimensional space. But given that H is the full stabiliser in $\Omega_3(q_0)$ of U, it cannot stabilise two distinct 1-dimensional spaces. So it must be that gk^{-1} fixes U. But this reasoning holds for any 1-dimensional subspace $U \leq V$. Hence gk^{-1} fixes each subspace of V. Therefore gk^{-1} is scalar. Hence, given that the only scalar transformations in $GO_3(q)$ are $\mathbf{I}$ and $-\mathbf{I}$, we have that $g = k$ or $-k \in GO_3(q_0)$.

Suppose now that q_0 is not a prime. Then $\Omega_3(q_0)$ contains some subfield subgroups isomorphic to $\Omega_3(q_1)$ where q_1 is a prime and $q_0 = q_1^e$ for some e. Let $H \cong \Omega_3(q_1)$ be one such subgroup. Given that $\Omega_3(q_0) \cong L_2(q_0)$ and $SO_3(q_0) \cong PGL_2(q_0)$ [13, p. 142], we may assume that all subgroups of $\Omega_3(q_0)$ isomorphic to H are conjugate under the action of $GO_3(q_0)$. Let $g \in GO_3(q)$ normalise $\Omega_3(q_0)$. If g normalises H as well, then the reasoning of the previous paragraph implies that $g \in GO_3(q_0)$. So suppose not. Now, given that all subgroups of $\Omega_3(q_0)$ isomorphic to H are conjugate under the action of $GO_3(q_0)$, there must be some $k \in GO_3(q_0)$ that conjugates H^g to H. Hence $H^{gk} = H$. Therefore gk normalises H. But now the reasoning of the previous paragraph implies that $gk \in GO_3(q_0)$. Given that $k \in GO_3(q_0)$, we conclude that $g \in GO_3(q_0)$. □

We make one observation regarding dihedral subgroups of $SO_3(q)$: Any cyclic subgroup $\langle g \rangle \leq SO_3(q)$ must stabilise any subspace U fixed by g. Since any dihedral group has a cyclic group of index 2, by Lemma 2.1.1 it must be that any dihedral subgroup of $SO_3(q)$ is a subspace stabiliser. We now begin begin our study of the subgroups of $SO_3(q)$.

Proposition 2.2.2. *If $H \leq SO_3(q)$ then either H stabilises a subspace, $H = \Omega_3(q_0)$ for some $q_0|q$, $H = SO_3(q_0)$ for some $q_0|q$ or $\mu'(H) \leq 4$.*

Proof. Suppose that $SO_3(q_1) \leq SO_3(q)$ is the smallest such $SO_3(q_1)$ to contain H. If $H = SO_3(q_1)$ or $\Omega_3(q_1)$ then we are done, so suppose not. Let $K := \Omega_3(q_1) \cap H$. Note that $|H : K| \leq 2$. If K is a subspace stabiliser then so is H, by Lemma 2.1.1.

If $K \leq 2^2 : S_3 \cong S_4$ then $\mu'(K) \leq 3$ by Theorem 1.1.2. Then $\mu'(H) \leq' (K) + 1 \leq 3$.

If $K \leq A_5$ then by Corollary 1.1.2

$$\mu'(H) \leq \mu'(K.2) \leq \mu'(K) + \mu'(2) \leq 3 + 1 = 4.$$

The only possibility left is that K lies in some subfield subgroup $\Omega_3(q_0).a$ for some $a \leq 2$. Suppose $K = \Omega_3(q_0)$. Then H normalises $\Omega_3(q_0)$. By Proposition 2.2.1 we know that $H \leq GO_3(q_0)$. Therefore $H \leq SO_3(q_0) \lneq SO_3(q_1)$, which contradicts the minimality of $SO_3(q_1)$.

Suppose $K = \Omega_3(q_0).2$. By Proposition 2.2.1 we have that $K \leq GO_3(q_0)$, which in turn means that $K = SO_3(q_0)$. Then $\Omega_3(q_0)$ is characteristic in K. Hence any $\Omega_3(q_0) \trianglelefteq H$. So $H \leq GO_3(q_0)$ once again. Thus $H = SO_3(q_0)$, which does not happen.

So suppose that $K \lneq \Omega_3(q_0)$. But we may repeat all of the previous arguments in this proof for this smaller case. Eventually this process must be exhausted and the proposition established. □

2.2.2 Intersections of subfield subgroups

We will use a proposition of Saxl and Whiston, taken from [12]. Their reasoning regarded the intersection of subfield subgroups of $L_2(q) \cong \Omega_3(q)$. We state the result for the current

context.

Proposition 2.2.3 (Saxl, Whiston)**.** *If K_1, K_2 are subfield subgroups of $\Omega_3(q)$ with $K_1 \cap K_2$ containing A_5, S_4 or subfield subgroup $\Omega_3(q_0)$, then K_1, K_2 have no isomorphic overgroups other than $\Omega_3(q)$.*

Corollary 2.2.1. *Suppose J_1, J_2 are subfield subgroups of $SO_3(q)$ with $J_1 \cap J_2$ containing $\Omega_3(q_0)$ or $SO_3(q_0)$, then J_1, J_2 have no isomorphic overgroups other than $SO_3(q)$.*

Proof. Let L_1, $L_2 \cong SO_3(q_1)$ be isomorphic subfield subgroups of $SO_3(q)$ such that $J_1 \leq L_1$, $J_2 \leq L_2$. Let $K_1 := L_1 \cap \Omega_3(q)$ and $K_2 := L_2 \cap \Omega_3(q)$. Observe that $\Omega_3(q_0) \leq K_1 \cap K_2$. $L_1 \cong L_2$, so there must be some $g \in GO_3(q)$ such that $g^{-1}L_1 g = L_2$. g must fix $\Omega_3(q)$, so $g^{-1}(L_1 \cap \Omega_3(q))g = L_2 \cap \Omega_3(q)$. Therefore, $K_1 \cong K_2$. Then it must be that $K_1 = K_2 = \Omega_3(q)$, by Proposition 2.2.3. Therefore $L_1 = L_2 = SO_3(q)$, and the corollary is established. □

2.2.3 Independent sets in $SO_3(q)$

Corollary 2.2.1 allows us to prove the next result, the main one of this section. Its proof closely follows a line of reasoning by Saxl and Whiston. The function $\pi(r)$ is defined to be the number of distinct prime divisors of r.

Proposition 2.2.4. *Suppose that $S = \{g_1, \ldots, g_n\} \subseteq SO_3(q)$ is an independent set, where $q = p^r$ is a power of a prime. Then either $|S| \leq \max\{6, \pi(r) + 3\}$ or $\langle S \rangle$ is a subspace stabiliser.*

Proof. Let $S = \{g_1, \ldots, g_n\}$ be an independent set inside $SO_3(q)$ and, for each $i \leq n$, define $H_{\{g_i\}}$ as before. We suppose that q is minimal in that $SO_3(q)$ is the smallest $SO_3(q)$ to contain S.

Let non-empty $T \subseteq S$ such that $|T| \leq 2$. By Proposition 2.2.2, it must be that either H_T is a subspace stabiliser, $H_T = \Omega_3(q)$, H_T lies in a subfield subgroup or $\mu'(H_T) \leq 4$. If $\mu'(H_T) \leq 4$ then $|S| \leq 4 + |T| \leq 6$. So suppose this does not happen. Therefore for any

$H_{\{g_i\}}$, we have that $H_{\{g_i\}}$ is a subspace stabiliser, lies in a subfield subgroup, or is $\Omega_3(q)$. For similar reasons any $H_{\{g_i,g_j\}}$ is a subspace stabiliser, lies in a subfield subgroup, or is $\Omega_3(q)$.

Suppose there are two $H_{\{g_i\}}$, $H_{\{g_j\}}$ such that $H_{\{g_i\}} = H_{\{g_j\}} = \Omega_3(q)$. Then $g_i \in H_{\{g_j\}} = H_{\{g_i\}}$, which contradicts the independence of S. So at most one of the $H_{\{g_i\}} = \Omega_3(q)$. The other $H_{\{g_j\}}$ must be subspace stabilisers or lie in subfield subgroups.

We now narrow down the possibilities for the groups $H_{\{g_i,g_j\}}$. By Proposition 2.2.2, for any i, j either $H_{\{g_i,g_j\}}$ stabilises a subspace, $H_{\{g_i,g_j\}} = \Omega_3(q)$, $\mu'(H_{\{g_i,g_j\}}) \leq 4$ or $H_{\{g_i,g_j\}}$ is some subfield subgroup $SO_3(q_1)$, $\Omega_3(q_1)$. We have supposed that $\mu'(H_{\{g_i,g_j\}}) \geq 5$, so we ignore the case that $\mu'(H_{\{g_i,g_j\}}) \leq 4$. Suppose $H_{\{g_i,g_j\}} = \Omega_3(q)$. Then the fact that $\Omega_3(q)$ is maximal in $SO_3(q)$ and that $H_{\{g_i\}}$, $H_{\{g_j\}}$ both lie in maximal subgroups of $SO_3(q)$ imply that $H_{\{g_i\}} = H_{\{g_j\}} = \Omega_3(q)$. We have already dealt with this case. If $H_{\{g_i,g_j\}}$ is a subfield subgroup, then $H_{\{g_i\}}$, $H_{\{g_j\}}$ must lie in maximal subfield subgroups J_1, J_2 respectively. By Corollary 2.2.1 it must be that $J_1 \ncong J_2$, otherwise S lies inside a smaller $SO_3(q_0)$. So the remaining possibility is that $H_{\{g_i,g_j\}}$ stabilises a subspace. Hence we suppose that each $H_{\{g_i,g_j\}}$ either stabilises a subspace or is a subfield subgroup.

We consider each of the genuinely different possibilities for the $H_{\{g_i\}}$.

Case: Three of the $H_{\{g_i\}}$ are subspace stabilisers

Now suppose that three of the $H_{\{g_i\}}$ are subspace stabilisers. Without loss of generality, we suppose that $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are subspace stabilisers. Then we may apply Lemma 2.1.3 to conclude that either $\langle S \rangle$ is a subspace stabiliser or $\bigcap_{i=1}^{3} H_{\{g_i\}} = \{1\}$. If $\langle S \rangle$ is not a subspace stabiliser then $\bigcap_{i=1}^{3} H_{\{g_i\}} = \{1\}$. Then $g_4, \ldots, g_n \in \bigcap_{i=1}^{3} H_{\{g_i\}} = \{1\}$, which cannot happen. So there are no such $g_4, \ldots, g_n$. Hence if $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are subspace stabilisers then either $\langle S \rangle$ is a subspace stabiliser or $|S| \leq 3$. So we suppose that this does not happen either. Hence there are at most 2 subspace stabilisers amongst the $H_{\{g_i\}}$.

Case: Precisely two of the $H_{\{g_i\}}$ are subspace stabilisers

Suppose, without loss of generality, that $H_{\{g_1\}}$, $H_{\{g_2\}}$ are the only subspace stabilisers amongst the $H_{\{g_i\}}$. So $H_{\{g_3\}}, \ldots, H_{\{g_n\}}$ are all subfield subgroups, except for at most one

$H_{\{g_i\}} = \Omega_3(q)$ amongst them. If no two of $H_{\{g_3\}}, \ldots, H_{\{g_n\}}$ lie inside isomorphic subfield subgroups $L_1 \cong L_2 \cong \Omega_3(q_1).a_1$ then $n = |S| \leq \pi(r) + 3$. So suppose without loss of generality that $H_{\{g_3\}}, H_{\{g_4\}}$ lie in isomorphic subfield subgroups L_1, L_2. By Corollary 2.2.1 it must be that $H_{\{g_3,g_4\}}$ is a subspace stabiliser. So we have that $H_{\{g_1\}}, H_{\{g_2\}}$ and $H_{\{g_3,g_4\}}$ are subspace stabilisers. Observe that the sets $\{g_1\}, \{g_2\}, \{g_3, g_4\}$ are mutually disjoint, so by Lemma 2.1.3 it must be that either $\langle S \rangle$ is subspace stabiliser or $H_{\{g_1\}} \cap H_{\{g_2\}} \cap H_{\{g_3,g_4\}} = \{1\}$. In the latter case, if $n \geq 5$ then $g_5 \in H_{\{g_1\}} \cap H_{\{g_2\}} \cap H_{\{g_3,g_4\}} = \{1\}$, which is absurd. So either $\langle S \rangle$ is a subspace stabiliser or $|S| \leq 5$.

Case: There is precisely one subspace stabiliser amongst the $H_{\{g_i\}}$

Now we suppose that only $H_{\{g_1\}}$ amongst the $H_{\{g_i\}}$ stabilises a subspace. Therefore $H_{\{g_2\}}, \ldots, H_{\{g_n\}}$ are all subfield subgroups, except for at most one $H_{\{g_i\}} = \Omega_q(3)$ amongst them. Suppose amongst $H_{\{g_2\}}, \ldots, H_{\{g_n\}}$ there is at most one pair $H_{\{g_i\}}, H_{\{g_j\}}$ such that $H_{\{g_i\}}, H_{\{g_j\}}$ lie in isomorphic subfield subgroups. Then $n = |S| \leq \pi(r) + 3$. So suppose there is more than one such pair. Indeed, suppose that $H_{\{g_2\}}, H_{\{g_3\}}$ lie in isomorphic subfield subgroups. Suppose also that $H_{\{g_4\}}, H_{\{g_i\}}$ lie in isomorphic subfield subgroups, where either $i = 2, 3$ or $i \geq 5$. By Corollary 2.2.1 we have that $H_{\{g_2,g_3\}}$ and $H_{\{g_4,g_i\}}$ are subspace stabilisers. We consider the possible cases for i.

Suppose $i \geq 5$. Without loss of generality, we suppose that $i = 5$. So $H_{\{g_4,g_5\}}$ is a subspace stabiliser. So in this case $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_4,g_5\}}$ are subspace stabilisers as well. But now the sets $\{g_1\}, \{g_2, g_3\}, \{g_4, g_5\}$ are mutually disjoint. By Lemma 2.1.3 then, it must be that either $\langle S \rangle$ is a subspace stabiliser or $H_{\{g_1\}} \cap H_{\{g_2,g_3\}} \cap H_{\{g_4,g_5\}} = \{1\}$. In the latter case, if $n \geq 6$ then $g_6 \in H_{\{g_1\}} \cap H_{\{g_2,g_3\}} \cap H_{\{g_4,g_5\}} = \{1\}$, which cannot be. So either $\langle S \rangle$ is a subspace stabiliser or $|S| \leq 6$.

So now suppose that $i = 2$ or 3. Without loss of generality, we suppose that $i = 2$. So $H_{\{g_2,g_4\}}$ is a subspace stabiliser. So in this case $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$ are subspace stabilisers. Let $S^* := S \setminus \{g_2\}$. Let $H^*_{\{g_i\}} := \langle S^* \setminus \{g_i\} \rangle$ for all $i \neq 2$. Observe that $H_{\{g_i,g_2\}} = H^*_{\{g_i\}}$ for all $i \neq 2$. Now consider the sets $\{g_1\}, \{g_3\}, \{g_4\}$, considered as subsets of S^*. They are mutually disjoint, so by Lemma 2.1.3 we conclude that $H_{\{g_2\}} = \langle S^* \rangle$ is a

subspace stabiliser or

$$H^*_{\{g_1\}} \cap H^*_{\{g_3\}} \cap H^*_{\{g_4\}} = H_{\{g_1,g_2\}} \cap H_{\{g_2,g_3\}} \cap H_{\{g_2,g_4\}} = \{1\}.$$

But $H_{\{g_2\}}$ does not stabilise a subspace, so we conclude that $H_{\{g_1,g_2\}} \cap H_{\{g_2,g_3\}} \cap H_{\{g_2,g_4\}} = \{1\}$. If $n \geq 5$ then $g_5 \in H_{\{g_1,g_2\}} \cap H_{\{g_2,g_3\}} \cap H_{\{g_2,g_4\}} = \{1\}$, which cannot be. Therefore $|S| \leq 4$. The case for $i = 3$ is similar, only we consider $H_{\{g_1,g_3\}}$ instead of $H_{\{g_1,g_2\}}$ and look to generate $H_{\{g_3\}}$ rather than $H_{\{g_2\}}$.

Case: No $H_{\{g_i\}}$ stabilises a subspace

So each $H_{\{g_i\}}$ is a subfield subgroup with the possible exception of one $H_{\{g_i\}} = \Omega_3(q)$. Take the set of all type $\mathcal{C}_5$ maximal subgroups of $SO_3(q)$ and partition it into isomorphism classes. We will get $\pi(r)$ such classes $A_1, \ldots, A_{\pi(r)}$. For each $H_{\{g_i\}}$, there must be a maximal subfield subgroup $L_i \leq SO_3(q)$ of smallest size such that $H_{\{g_i\}} \leq L_i$. L_i must be an element of some A_j. Associate $H_{\{g_i\}}$ with A_j. So if each A_j has at most one $H_{\{g_i\}}$ associated with it, then $|S| \leq \pi(r) + 1$.

Suppose two $H_{\{g_i\}}$ are associated to the same A_j. Without loss of generality, we suppose that $H_{\{g_1\}}, H_{\{g_2\}}$ are both associated with A_j. Then there is $L_1, L_2 \in A_j$ such that $H_{\{g_1\}} \leq L_1$ and $H_{\{g_2\}} \leq L_2$. By assumption, either $L_1 \cap L_2$ contains some $\Omega_3(q_0)$ or it stabilises a subspace. Suppose there is some $\Omega_3(q_0) \leq L_1 \cap L_2$. $L_1 \cong L_2$, so by Corollary 2.2.1 it must be that $L_1 = L_2$. Thus, $H_{\{g_1\}}, H_{\{g_2\}} \leq SO_3(q_0)$ for some subfield subgroup $SO_3(q_0) \leq SO_3(q)$. Therefore $\langle S \rangle = \langle H_{\{g_1\}}, H_{\{g_2\}} \rangle \leq SO_3(q_0)$, which contradicts the minimality of $SO_3(q)$. Hence $H_{\{g_1,g_2\}} \leq L_1 \cap L_2$ must stabilise a subspace if both $H_{\{g_1\}}, H_{\{g_2\}}$ are associated with the same A_j.

Now, suppose that there are three A_i that have at least two $H_{\{g_j\}}$ associated with them. So $|S| \geq 6$. Without loss of generality, we suppose that $H_{\{g_1\}}, H_{\{g_2\}}$ are associated with A_1, whilst $H_{\{g_3\}}, H_{\{g_4\}}$ are associated with A_2 and $H_{\{g_5\}}, H_{\{g_6\}}$ are associated with A_3. Consider $H_{\{g_1,g_2\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_5,g_6\}}$. The sets $\{g_1, g_2\}$, $\{g_3, g_4\}$, $\{g_5, g_6\}$ are mutually disjoint, so by Lemma 2.1.3, it must be that either $\langle S \rangle$ is a subspace stabiliser, or $H_{\{g_1,g_2\}} \cap$

$H_{\{g_3,g_4\}} \cap H_{\{g_5,g_6\}} = \{1\}$. If $\langle S \rangle$ is a subspace stabiliser, then so is $H_{\{g_1\}}$. But this is not the case, by assumption. So $H_{\{g_1,g_2\}} \cap H_{\{g_3,g_4\}} \cap H_{\{g_5,g_6\}} = \{1\}$. If $n \geq 7$ then $g_7 \in H_{\{g_1,g_2\}} \cap H_{\{g_3,g_4\}} \cap H_{\{g_5,g_6\}} = \{1\}$, which cannot be. So $|S| \leq 6$.

Suppose that precisely two of the A_i each have at least two $H_{\{g_j\}}$ associated with them. Without loss of generality, suppose that A_1, A_2 each have at least two $H_{\{g_j\}}$ associated with them. If A_1, A_2 each have precisely two $H_{\{g_j\}}$ associated with them then $|S| \leq \pi(r) + 3$. So suppose that $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are associated with A_1 whilst $H_{\{g_4\}}$, $H_{\{g_5\}}$ are associated with A_2. So $H_{\{g_i,g_j\}}$ is a subspace stabiliser for $i, j \leq 3$. Also $H_{\{g_4,g_5\}}$ is a subspace stabiliser. Now consider the subspace stabilisers $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4,g_5\}}$. Now consider the sets $\{g_2\}$, $\{g_3\}$, $\{g_4, g_5\}$ as subsets of $S \setminus \{g_1\}$ They are all mutually disjoint. By Lemma 2.1.3 then, $H_{\{g_1\}}$ must be a subspace stabiliser or $H_{\{g_1,g_2\}} \cap H_{\{g_1,g_3\}} \cap H_{\{g_1,g_4,g_5\}} = \{1\}$. By assumption, $H_{\{g_1\}}$ is not a subspace stabiliser so $H_{\{g_1,g_2\}} \cap H_{\{g_1,g_3\}} \cap H_{\{g_1,g_4,g_5\}} = \{1\}$. But then there can be no $g_6 \in S$ otherwise $g_6 \in H_{\{g_1,g_2\}} \cap H_{\{g_1,g_3\}} \cap H_{\{g_1,g_4,g_5\}} = \{1\}$. So $|S| \leq 5$.

So now suppose that there is only one A_i that has more than one $H_{\{g_j\}}$ associated with it. Without loss of generality, we say that A_1 is this A_i. If A_1 has at most three $H_{\{g_j\}}$ associated with it then $|S| \leq \pi(r)+3$, so suppose that $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ are associated with A_1. So $H_{\{g_i,g_j\}}$ are subspace stabilisers for all $i, j \leq 4$. Consider $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$. Each is a subspace stabiliser. Also, $\{g_2\}$, $\{g_3\}$, $\{g_4\}$ are mutually disjoint subsets of $S \setminus \{g_1\}$. By Lemma 2.1.3 then, $H_{\{g_1\}}$ is a subspace stabiliser or $H_{\{g_1,g_2\}} \cap H_{\{g_1,g_3\}} \cap H_{\{g_1,g_4\}} = \{1\}$. $H_{\{g_1\}}$ does not stabilise a subspace, so $H_{\{g_1,g_2\}} \cap H_{\{g_1,g_3\}} \cap H_{\{g_1,g_4\}} = \{1\}$. But then $|S| \leq 5$ in this case. □

2.3 Conclusion

Altogether then, we have shown

Theorem 2.3.1. *Let $S \subseteq SO_3(q)$ be an independent set in $SO_3(q)$. Then either $\langle S \rangle$ is a subspace stabiliser, or*

1. $|S| \leq 4$ *if* q *is prime, or*

2. $|S| \leq \max\{6, \pi(r) + 3\}$ *where* $q = p^r$, p *is a prime.*

An immediate corollary is

Corollary 2.3.1. *If* q *is a prime then* $\mu(SO_3(q)) \leq 4$. *If* $q = p^r$ *for a prime* p *then* $\mu(SO_3(q)) \leq \max\{6, \pi(r) + 3\}$.

This is because an independent generating set S for $SO_3(q)$ cannot generate a subspace stabiliser. Hence $|S|$ must have the bounds given in Theorem 2.3.1.

CHAPTER 3

INDEPENDENT SETS IN 3-DIMENSIONAL SPECIAL UNITARY GROUPS OVER FIELDS OF ODD CHARACTERISTIC

In this chapter, we wish to show that if S is an independent set in $SU_3(q)$, q odd, then either $|S|$ is bounded or the nature $\langle S \rangle$ is limited. This will not only be an interesting result in its own right, but it will be useful in a later chapter.

We continue with the strategy that we used in the last chapter. Once again, we let $S = \{g_1, \ldots, g_n\}$ be the an independent set, this time within $SU_3(q)$. For any non-empty $T \subsetneqq S$, we let $H_T := \langle S \setminus T \rangle$ lie in a maximal subgroup of $SU_3(q)$. In the case of $SU_3(q)$ we may quote the possible maximal subgroups of this group. They are listed in Table 3.1. The information in this table is drawn from [8].

With a view to continuing with the strategy, we consider the maximal subgroups of $SU_3(q)$ on a case-by-case basis. Without loss of generality, we consider the possible maximal subgroups M that H_T could lie in. We begin with the case that q is an odd prime.

3.1 Independent sets in $SU_3(q)$ for odd prime q

Lemma 2.1.3 of the previous chapter already covers the case of when three subspace stabilisers H_T intersect. We therefore begin by examining the case when H_T lies in some

Class	Isomorphism Types	Conditions
$\mathcal{C}_1$	$E_q^{1+2} : (q^2-1)$ $GU_2(q)$	
$\mathcal{C}_2$	$(q+1)^2 : S_3$	$q \neq 5$
$\mathcal{C}_3$	$(q^2-q+1) : 3$	$q \neq 3, 5$
$\mathcal{C}_5$	$SU_3(q_0).\left(\frac{q+1}{q_0+1}, 3\right)$ $(q+1,3) \times SO_3(q)$	$q = q_0^r$, r an odd prime $q \geq 7$, q odd
$\mathcal{C}_6$	$3^{1+2} : Q_8.\frac{(q+1,9)}{3}$	$q = p \equiv 2 \bmod 3$, $q \geq 11$
$\mathcal{S}_1$	$(q+1,3) \times L_2(7)$ $3A_6$ $3A_6.2$ $3A_7$	$q = p \equiv 3, 5, 6 \bmod 7$, $q \neq 5$ $q = p \equiv 11, 14 \bmod 15$ $q = 5$ $q = 5$

Table 3.1: The Maximal Subgroups of $SU_3(q)$

$\mathcal{C}_2$ subgroup.

3.1.1 Case: $H_T \leq M \in \mathcal{C}_2$

In this case H_T lies in a decomposition space stabiliser, stabilising $U_1 \oplus U_2 \oplus U_3$. In this section, we do not consider any H_T so much as the full $M \in \mathcal{C}_2$ that they lie in. We establish three main results in this section. First, we consider the possibilities when $M_1 \in \mathcal{C}_2$ and $M_2 \in \mathcal{C}_1$. After that, we consider the possible intersections between two decomposition space stabilisers.

The first result is as follows:

Proposition 3.1.1. *Suppose $M_1 \leq SU_3(q)$ stabilises a decomposition $U_1 \oplus U_2 \oplus U_3$ whilst $M_2 \leq SU_3(q)$ stabilises a subspace W. Then either $\mu'(M_1 \cap M_2) \leq 3$ or $M_1 \cap M_2$ stabilises one of the U_i.*

Proof. We suppose that W is 1-dimensional.

If $W = U_i$ for some i then $M_1 \cap M_2$ stabilises $U_i = W$. So suppose not.

Suppose $W \leq U_i \oplus U_j$ for some i, j. Without loss of generality, suppose $W \leq U_1 \oplus U_2$. So $W = \langle \alpha \mathbf{u}_1 + \beta \mathbf{u}_2 \rangle$ for some basis $\{\mathbf{u}_1, \mathbf{u}_2\}$ drawn from U_1, U_2 and some $\alpha, \beta \neq 0$. But now $M_1 \cap M_2$ cannot move U_1 or U_2 to U_3 without moving W. Hence $M_1 \cap M_2$ stabilises

$U_1 \oplus U_2$ and so stabilises U_3. So suppose $W \not\leq U_i \oplus U_j$ for all i, j.

Let $T \leq M_1$ be all the elements of $M_1 \cap M_2$ that fix each U_i in the decomposition $U_1 \oplus U_2 \oplus U_3$. So $M_1 \cap M_2 \leq T.S_3$, considered as a subgroup of M_1. Note that each $t \in T$ fixes W as well, so is a scalar transformation. Hence $H_1 \cap H_2 \leq Z(SU_3(q)).S_3$. Therefore, using Corollary 1.1.2,

$$\mu'(M_1 \cap M_2) \leq \mu'(Z(SU_3(q)).S_3) \leq \mu'(Z(SU_3(q))) + \mu'(S_3) = 1 + 2 = 3.$$

□

The next result regards intersections between decomposition space stabilisers. For this proposition, we work in the wider group $SL_3(q)$, $q = p^r$ for some prime p. This is because the results obtained here will prove useful in the next chapter as well.

Proposition 3.1.2. *Suppose that $M_1, M_2 \leq SL_3(q)$ are decomposition space stabilisers, stabilising $U_1 \oplus U_2 \oplus U_3, W_1 \oplus W_2 \oplus W_3$ respectively. Then either $\langle M_1, M_2 \rangle$ is a decomposition space stabiliser, $\mu'(M_1 \cap M_2) \leq 3$ or $M_1 \cap M_2$ stabilises one of the U_i.*

Proof. If $U_1 \oplus U_2 \oplus U_3 = W_1 \oplus W_2 \oplus W_3$ then $\langle M_1, M_2 \rangle$ stabilises $U_1 \oplus U_2 \oplus U_3 = W_1 \oplus W_2 \oplus W_3$. So suppose that the two decompositions are distinct.

Suppose that $U_i \neq W_j$ for all i, j. We argue that $\mu'(M_1 \cap M_2) \leq 3$. Let $T \leq M_1 \cap M_2$ be the group of all elements of $M_1 \cap M_2$ that fix each U_i. Note T is normal in $M_1 \cap M_2$. Let $K \leq T$ be the subgroup of T that stabilises each W_i. We argue that $K \leq Z(SL_3(q))$. Suppose that there is some W_i such that $W_i \not\leq U_j \oplus U_k$ for all j, k. Then each $k \in K$, in fixing W_i, U_1, U_2, U_3, must be scalar. So suppose there is no such W_i. So each $W_i \leq U_j \oplus U_k$ for some j, k. But not all the W_i can lie in the same $U_j \oplus U_k$. So there are two $U_j \oplus U_k$ that contain some of the W_i. Without loss of generality, we say that $W_1 \leq U_1 \oplus U_2$, $W_2 \leq U_2 \oplus U_3$. But now each $k \in K$ must fix the three distinct points W_1, U_1, U_2 within $U_1 \oplus U_2$, as well as the three distinct points W_2, U_2, U_3 within $U_2 \oplus U_3$. Hence k must be scalar on $U_1 \oplus U_2$ and $U_2 \oplus U_3$. Hence k must be scalar. This shows that K is scalar. So $|K| = 1$ or 3.

Now, let M_2^* be the full stabiliser of $W_1 \oplus W_2 \oplus W_2$. Consider the embedding

$$T/K \to \frac{M_2^*}{(q+1)^2} \cong S_3.$$

T/K is abelian, so T/K cannot be all of S_3. Hence $T = K$, $K.2$ or $K.3$. If $T = K$ then $\mu'(T) = \mu'(K) = 1$. Hence, by Corollary 1.1.2,

$$\mu'(M_1 \cap M_2) \leq \mu'(T.S_3) \leq \mu'(T) + \mu'(S_3) = 1 + 2 = 3$$

in this case.

If $T = K.2$ then either $|T| = 2$ or $|T| = 6$. If $|T| = 2$ then $\mu'(T) = 1$ again, and we have what we want. If $|T| = 6$ then the fact that T is abelian implies that T is cyclic of order 6. Then $|Out(T)| = 2$. Now take any $h \in M_1 \cap M_2$ that permutes all the U_i. h normalises T, and so has an image in $Out(T)$. If this image is non-trivial then $h^2 \in Inn(T)$, and so commutes with T. This can only happen if $T \leq Z(SL_3(q))$. If the image of h in $Out(T)$is trivial, then h must commute with T, and once again $T \leq Z(SL_3(q))$. So there are no such h, and

$$\mu'(M_1 \cap M_2) \leq \mu'(T.2) \leq \mu'(T) + \mu'(2) = 2 + 1 = 3.$$

If $T = K.3$ then either $|T| = 3$ or 9. Now, if C is a cycle of prime-power then $\mu'(C) = 1$. So if T is cyclic in this case then $\mu'(T) = 1$ and we have what we wanted. So suppose $T = 3^2$. We check each possible case. If $\frac{M_1 \cap M_2}{T} \lneq S_3$ then $\frac{M_1 \cap M_2}{T} = \{1\}, 2$ or 3. But then $\mu'(M_1 \cap M_2) \leq \mu'(T) + \mu'\left(\frac{M_1 \cap M_2}{T}\right) \leq 2 + 1 = 3$. So suppose $\frac{M_1 \cap M_2}{T} = S_3$. Let $A := \{h_1, \ldots, h_r\}$ be an independent generating set for $M_1 \cap M_2$ such that $|A| \geq 3$. Now, we can suppose that h_1, h_2 produce the action of S_3 on T in $M_1 \cap M_2$. Now for each $i \geq 3$ there must be $\omega_i \in \langle h_1, h_2 \rangle$ such that $h_i\omega_i \in T$. Suppose that each such $h_i\omega_i \in K \leq Z(SL_3(q))$. As $K \trianglelefteq M_1 \cap M_2$, we have that

$$K.S_3 = \langle h_1, h_2, h_3\omega_3, \ldots, h_r\omega_r \rangle = \langle h_1, \ldots, h_r \rangle = T.S_3,$$

which is absurd. Hence there is some $h_i\omega_i$ that is non-scalar. But then $\langle h_1, h_2, h_i\rangle = \langle h_1, h_2, h_i\omega_i\rangle = M_1 \cap M_2$, which implies that $A = \{h_1, h_2, h_i\}$. Thus, $|A| \leq 3$. Therefore

$$\mu'(M_1 \cap M_2) \leq \mu'(T.S_3) \leq 3$$

here. This completes the case that $U_i \neq W_j$ for all i, j.

Suppose $U_i = W_j$ for some i, j. If $M_1 \cap M_2$ stabilises $U_i = W_j$ then we are done, so suppose not. We may suppose, without loss of generality, that $U_1 = U_i = W_j = W_1$. If there exists some $h \in M_1 \cap M_2$ that permutes all the U_i then $W_1^{h^j} = U_1^{h^j}$ for all j, and so the two decompositions are not distinct. So suppose that there is no such h. But then each $g \in M_1 \cap M_2$ must fix some U_i. Furthermore, there must be some U_i that each $g \in M_1 \cap M_2$ fixes. To see this, suppose there is no such U_i. In that case there must be g_1, $g_2 \in M_1 \cap M_2$ that do not fix each U_i, but permute different U_i. Without loss of generality, suppose g_1 permutes U_1, U_2 while g_2 permutes U_2, U_3. Then the product $g_1 g_2$ permutes all the U_i, which we assumed does not happen. Hence $M_1 \cap M_2$ stabilises some U_i. This establishes the proposition.

□

This completes our study of this case. For the next section, we return to the group $SU_3(q)$ with q prime.

3.1.2 Case: $H_T \leq M \in \mathcal{C}_3$

In this case, H_T stabilises a field extension. That is, H_T embeds into the automorphism group of the field of order q^6. Informally speaking, the aim of this section will be to argue that the intersection of H_T with any other $\mathcal{C}_1, \mathcal{C}_2$ or $\mathcal{C}_3$ group will be small. This will enable us to place limits on the size of $|S|$ if there is a field extension stabiliser amongst the H_T. With this aim in mind, we prove a lemma that will be useful throughout this section.

Lemma 3.1.1. *For all a, b, c, we have hcf$(3(q^2-q+1), (q-1)^a q^b (q+1)^c) = 3^d$ for some d.*

Proof. Let p be a prime dividing both q^2-q+1 and $(q-1)^a q^b (q+1)^c$. So p divides $q-1, q$ or $q+1$.

If $p|q-1$ then $p|(q^2-q+1)-q(q-1) = 1$, which is absurd. If $p|q$ then again $p|(q^2-q+1)-(q-1)q = 1$, which is absurd. So $p|q+1$. Now p must divide the difference $(q^2-q+1)-(q-2)(q+1) = 3$. So $p|3$.

Therefore if p is a prime such that $p|\text{hcf}(3(q^2-q+1), (q-1)^a q^b (q+1)^c)$ then $p = 3$. This establishes the lemma. □

Lemma 3.1.2. *Suppose $M \in \mathcal{C}_3$ is a field extension stabiliser, and $K \leq M$ with $|K| = 3^d$ for some d. Then $\mu'(K) \leq 2$.*

Proof. Let F be the cycle of order q^2-q+1 in M. So $M = F:3$. Consider the image of K in $M/F \cong 3$. If the image of K is 1 then $K \leq F$. But in this case K is a cyclic group of prime-power order, and so $\mu'(K) = 1$. If the image of K in M/F is 3 then $K = (F \cap K):3$. But now $F \cap K$ is a cyclic group of prime-power order. Hence $\mu'(F \cap K) = 1$. Therefore $\mu'(K) \leq \mu'(F \cap K) + \mu'(3) = 1+1 = 2$, using Corollary 1.1.2. □

We now use the fact $|M_1 \cap M_2|$ must divide the orders of both M_1, M_2 to argue that $M_1 \cap M_2$ is of limited size. Observe that $M_1 \in \mathcal{C}_3$ is a subgroup of a group of order $3(q^2-q+1)$.

Proposition 3.1.3. *If $M_1 \in \mathcal{C}_3$ is a field extension stabiliser and $M_2 \in \mathcal{C}_1$ is a subspace stabiliser then $\mu'(M_1 \cap M_2) \leq 2$.*

Proof. Since M_2 is a subspace stabiliser then $M_2 \cong E_q^{1+2} : (q^2-1)$ or $GU_2(q)$. Then $|M_2| = (q-1)q^3(q+1)$ or $(q-1)q(q+1)^2$ respectively.

Now $|M_1 \cap M_2|$ divides $\text{hcf}(|M_1|, |M_2|) = \text{hcf}(3(q^2-q+1), |M_2|)$. Lemma 3.1.1 tells us that $|M_1 \cap M_2| = 3^d$ for some d. By Lemma 3.1.2 we now have that $\mu'(M_1 \cap M_2) \leq 2$. □

Proposition 3.1.4. *If $M_1 \in \mathcal{C}_3$ is a field extension stabiliser whilst $M_2 \in \mathcal{C}_2$ is a decomposition space stabiliser then $\mu'(M_1 \cap M_2) \leq 2$.*

Proof. Now $|M_2| = 6(q+1)^2$. So $|M_1 \cap M_2|$ divides

$$\text{hcf}(|M_1|, |M_2|) = \text{hcf}(3(q^2 - q + 1, 6(q+1)^2).$$

Now, clearly $q^2 - q + 1$ is odd. Thus, $2 \not| 3(q^2 - q + 1)$. Hence

$$\text{hcf}(3(q^2 - q + 1), 6(q+1)^2) = \text{hcf}(3(q^2 - q + 1), 3(q+1)^2).$$

Now, suppose p is a prime that divides both $3(q^2-q+1)$, $3(q+1)^2$. With regard to $3(q+1)^2$, either $p|3$ or $p|(q+1)^2$. If $p|3$ then $p = 3$. If $p|(q+1)^2$ then $p|\text{hcf}(3(q^2-q+1), (q+1)^2) = 3^d$ for some d, by Lemma 3.1.1. Hence $p = 3$ once again. Hence $|M_1 \cap M_2| = 3^e$ for some e. By Lemma 3.1.2 then, $\mu'(M_1 \cap M_2) \leq 2$. □

Proposition 3.1.5. *If $M_1, M_2 \in \mathcal{C}_3$ are distinct field extension stabilisers then $\mu'(M_1 \cap M_2) \leq 3$.*

Proof. Let $F_1 \leq M_1$ be the cycle of order $q^2 - q + 1$ in M_1 and $F_2 \leq M_2$ be the cycle of order $q^2 - q + 1$ in M_2. Since F_1, F_2 are cyclic, $F_1 \cap F_2$ must be the unique cycle of order $|F_1 \cap F_2|$ in F_1 and the unique cycle of order $|F_1 \cap F_2|$ in F_2. So the Frobenius automorphisms of M_1 and M_2 must fix $F_1 \cap F_2$ in both F_1, F_2. Also, $F_1 \cap F_2$ must be normalised by both F_1, F_2 as F_1, F_2 are abelian. Therefore $F_1 \cap F_2$ is normalised by both M_1 and M_2. Hence $F_1 \cap F_2 \trianglelefteq \langle M_1, M_2 \rangle = SU_3(q)$. But the only proper, normal subgroup of $SU_3(q)$ is $Z(SU_3(q))$, if this is non-trivial. So $|F_1 \cap F_2| = 1$ or 3.

Now $F_1 \cap M_2 = F_1 \cap (F_2 : 3) \leq (F_1 \cap F_2) : 3$. So

$$\mu'(F_1 \cap M_2) = \mu'((F_1 \cap F_2) : 3) \leq 1 + 1 = 2$$

by Corollary 1.1.2. So

$$\mu'(M_1 \cap M_2) \leq \mu'((F_1 \cap M_2 : 3) \leq \mu'(F_1 \cap M_2) + \mu'(3) \leq 2 + 1 = 3.$$

□

We now draw two conclusions from all our previous conclusions.

Proposition 3.1.6. *If M_1 is a field extension stabiliser whilst M_2 is a subspace stabiliser, decomposition space stabiliser or field extension stabiliser, then $\langle M_1, M_2 \rangle$ is a field extension stabiliser or $\mu(M_1 \cap M_2) \leq 3$*

Proof. If M_2 is a subspace stabiliser or decomposition space stabiliser then we may appeal to Propositions 3.1.3 and 3.1.4 to conclude that $\mu'(M_1 \cap M_2) \leq 2$.

If M_2 is a field extension stabiliser, then either $M_2 = M_1$, in which case $\langle M_1, M_2 \rangle = M_1$ is a field extension stabiliser, or $M_2 \neq M_1$, in which case $\mu'(M_1 \cap M_2) \leq 3$ by Proposition 3.1.5. □

Therefore, if there is a field extension stabiliser and a subgroup of a $\mathcal{C}_1, \mathcal{C}_2$ or $\mathcal{C}_3$ group amongst the H_i, then $|S| \leq 5$. We are now able to combine all of our results regarding $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$ groups for the final proposition of this section.

Proposition 3.1.7. *Let $T_1, T_2, T_3, T_4 \subsetneqq S$ be non-empty such that $T_i \cap T_j = \varnothing$ for all distinct i, j. Suppose that for each of $H_{T_1}, H_{T_2}, H_{T_3}, H_{T_4}$ either H_{T_i} lies in a $\mathcal{C}_1, \mathcal{C}_2$ or $\mathcal{C}_3$ group. Then either*

1. *$\langle S \rangle$ is a subspace stabiliser, a decomposition space stabiliser, a field extension stabiliser; or*

2. *$H_{T_i} \cap H_{T_j} \cap H_{T_k} \leq Z(SU_3(q))$ for some distinct i, j, k; or*

3. *$\mu'(H_{T_i} \cap H_{T_j}) \leq 3$ for some distinct i, j.*

Proof. If any of the H_{T_i} lies in a $\mathcal{C}_3$ subgroup then we have what we want by Proposition 3.1.6. So we suppose that each H_{T_i} lies inside a $\mathcal{C}_1$ or $\mathcal{C}_2$ subgroup.

If each H_{T_i} is a subspace stabiliser, then we are done by Lemma 2.1.3. In this case either $\langle S \rangle$ is a subspace stabiliser or $H_{T_i} \cap H_{T_j} \cap H_{T_k} \leq Z(SU_3(q))$ for some distinct i, j, k.

So suppose that there is at least one decomposition space stabiliser amongst H_{T_1}, H_{T_2}, H_{T_3}, H_{T_4} that does not stabilise a subspace. Without loss of generality, suppose that H_{T_1} is a decomposition space stabiliser, stabilising $U_1 \oplus U_2 \oplus U_3$. We may suppose that H_{T_1} does not stabilise any of U_1, U_2, U_3 else it would be a subspace stabiliser.

Now consider each H_{T_j} for $j \geq 2$. If $\mu'(H_{T_1} \cap H_{T_j}) \leq 3$ for any j then we are done, so suppose not. If H_{T_j} is a decomposition space stabiliser then by Proposition 3.1.2 it must be that either $\langle H_{T_1}, H_{T_j} \rangle = \langle S \rangle$ is a decomposition space stabiliser or $H_{T_1} \cap H_{T_j}$ stabilises one of the U_i. So we suppose that if H_{T_j} is a decomposition space stabiliser then $H_{T_1} \cap H_{T_j}$ stabilises one of the U_i.

If H_{T_j} is a subspace stabiliser then by Proposition 3.1.1 we have that $\mu'(H_{T_1} \cap H_{T_j}) \leq 3$ or $H_{T_1} \cap H_{T_j}$ stabilises one of the U_i. If $\mu'(H_{T_1} \cap H_{T_j}) \leq 3$ then we are satisfied, so suppose $H_{T_1} \cap H_{T_j}$ stabilises one of the U_i.

Suppose $H_{T_1} \cap H_{T_j}$, $H_{T_1} \cap H_{T_k}$ stabilise the same U_i. Then $H_{T_1} = \langle H_{T_1} \cap H_{T_j}, H_{T_1} \cap H_{T_k} \rangle$ stabilises U_i, which does not happen. So each $H_{T_1} \cap H_{T_j}$ stabilises a distinct U_i. We argue that this case is impossible.

Suppose, without loss of generality, that $H_{T_1} \cap H_{T_2}$ stabilises U_1, $H_{T_1} \cap H_{T_3}$ stabilises U_2 and $H_{T_1} \cap H_{T_4}$ stabilises U_3. Then $H_{T_1} \cap H_{T_2} \cap H_{T_3}$ stabilises $U_1 \oplus U_2$. However, notice that $H_{T_1} \cap H_{T_2} \cap H_{T_3}$ stabilises $U_1 \oplus U_2 \oplus U_3$ as well, so it must be that $H_{T_1} \cap H_{T_2} \cap H_{T_3}$ stabilises U_3. Recall that $H_{T_1} \cap H_{T_4}$ stabilises U_3. Take any $g_i \in S \setminus T_1$. If $g_i \notin T_2 \cup T_3$ then $g_i \in H_{T_1} \cap H_{T_2} \cap H_{T_3}$. Suppose then that $g_i \in T_2 \cup T_3$. Then $g_i \notin T_4$ since the T_j are mutually disjoint. Therefore $g_i \in H_{T_1} \cap H_{T_4}$. So each $g_i \in S \setminus T_i$ lies in at least one of $H_{T_1} \cap H_{T_2} \cap H_{T_3}$, $H_{T_1} \cap H_{T_4}$. Therefore $H_{T_1} = \langle H_{T_1} \cap H_{T_2} \cap H_{T_3}, H_{T_1} \cap H_{T_4} \rangle$ must stabilise U_3, which we assumed did not happen. So, having considered all possible cases

we conclude that the proposition is established. □

3.1.3 Case: $H_T \leq M \in \mathcal{C}_6$

In this case, we have that $H_T \leq 3^{1+2} : Q_8.\frac{(q+1,9)}{3}$. The discussion in this section will be set in the context of the special linear group, as the results established here will be useful in the next chapter as well as this one. In this section, we work towards a single result about independent sets inside $3^{1+2} : Q_8.\frac{(q+1,9)}{3}$.

This next proposition will enable us to establish the main result for this case. We treat this as a standard result and do not prove it. This characterisation of 3^{1+2} as a matrix group is drawn from [10, pp. 149–151].

Proposition 3.1.8. *Suppose the order of the underlying field permits the existence of a primitive cube root of 1, namely ω. Then $K \leq SL_3(q)$ such that $K \cong 3^{1+2}$ if and only if*

$$K = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\rangle,$$

where both matrices are written with respect to some basis $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \boldsymbol{u}_3\}$ of V.

Let $K \leq SL_3(q)$ be as in the statement of Proposition 3.1.8. It is easy to verify by hand that each non-scalar $k \in K$ can be written as

$$k = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

with respect to some basis of V. So we offer no proof of this fact here.

The next lemma will be used on a couple of occasions during the proof of the main result of this section.

Lemma 3.1.3. *Suppose* $3^{1+2} \cong K \leq SL_3(q)$ *and the underlying field permits the existence of primitive cube roots of unity. If* $N \leq K$ *is a non-central, proper subgroup of* K *and* $\langle T \rangle \leq SL_3(q)$ *normalises* N*, then* $\langle T \rangle$ *is a decomposition space stabiliser.*

Proof. Given the assumption on N, there must be $g \in Z(K)$ and $k \notin Z(K)$ such that $N = \langle k \rangle$ or $N = \langle g, k \rangle$. It is a consequence of Proposition 3.1.8 that g must be a scalar transformation. It has been observed that

$$k = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

for some basis of V. But then V can be decomposed into eigenspaces of k, namely $E_1 \oplus E_2 \oplus E_3$. Notice that, given both g, k fix each E_i, N must stabilise each E_i. Observe that for each $g \in N \setminus Z(3^{1+2})$, each E_i has a distinct eigenvalue, since each such g is a power of k multiplied by a scalar transformation. Hence each such g has no 2-dimensional eigenspaces.

But now $\langle T \rangle$ normalises N. So for each $t \in T$ and for each $g \in N \setminus Z(3^{1+2})$ there is some $g' \in N \setminus Z(3^{1+2})$ such that $tgt^{-1} = g'$. For any E_i then, $(E_i^t)^g = E_i^{tg(t^{-1}t)} = E_i^{g't} = \lambda E_i^t$ where λ is the eigenvalue of E_i for g'. So then E_i^t is an eigenspace for g. But g has only E_1, E_2, E_3 as distinct eigenspaces, so $E_i^t = E_1, E_2$ or E_3. Therefore each $t \in T$ fixes $E_1 \oplus E_2 \oplus E_3$, which establishes the claim. □

We will also use the following fact. It is easy to verify, and once again we offer no proof for it.

Proposition 3.1.9. $\mu'(Q_8) = 2$.

We now prove the main result of this section.

Proposition 3.1.10. *Any independent set* $T := \{h_1, \ldots, h_m\}$ *in* $M = 3^{1+2} : Q_8.\frac{(q+1,9)}{3}$ *has size at most 4, or* $\langle T \rangle$ *is a decomposition space stabiliser.*

Proof. Consider the image $T' = \{h'_1, \ldots, h'_m\}$ of T in $M/Z(M) \cong 3^2 : Q_8.\frac{(q+1,9)}{3}$, with each h'_i the image of h_i. Suppose that T' is not independent. Then, re-labelling the elements of T' if necessary, we can assume $h'_m = h'_{i_1}h'_{i_2}\ldots h'_{i_s}$ where no $i_j = m$. But, turning our attention to the pre-images of the h'_i, it cannot be that $h_m = h_{i_1}h_{i_2}\ldots h_{i_s}$ since T is independent. So there must be some $k \in Z(M)$ such that $h_m = h_{i_1}h_{i_2}\ldots h_{i_s}k$.

But now consider $A := T \setminus \{h_m\}$ and let $N := \langle A\rangle \cap 3^{1+2}$. It cannot be that $k \in N$ else $h_m \in \langle k, A\rangle = \langle A\rangle$, which cannot be. So $|N| = 1$ or 3 since N is a subgroup of 3^{1+2} that has trivial intersection with $Z(3^{1+2})$. Suppose $|N| = 1$. Then $\langle A\rangle \cap 3^{1+2} = \{1\}$, and $\langle A\rangle$ is isomorphic to its image in $M/3^{1+2} = Q_8.\frac{(q+1,9)}{3}$. So we may assume $A \subseteq Q_8.\frac{(q+1,9)}{3}$. But A is an independent set, so we use Corollary 1.1.2 in order to say

$$|T| - 1 = |A| \leq \mu'\left(Q_8.\frac{(q+1,9)}{3}\right) \leq \mu'(Q_8) + \mu'\left(\frac{(q+1,9)}{3}\right) \leq 2 + 1.$$

Therefore $|T| \leq 4$.

So suppose $|N| = 3$. Then N is a non-central, proper subgroup of 3^{1+2}. $\langle A\rangle$ normalises N and $k \in Z(3^{1+2})$ normalises N, trivially. So $\langle T\rangle \leq \langle A, k\rangle$ normalises N. But then T is a decomposition space stabiliser, by Lemma 3.1.3. This completes the case that T' is not independent in $M/Z(M)$.

Now suppose that T' is independent in $M/Z(M) \cong 3^2 : Q_8.\frac{(q+1,9)}{3}$. Consider the image $T'' = \{h''_1, \ldots, h''_m\}$ of T' in $\frac{M/Z(M)}{3^2} \cong Q_8.\frac{(q+1,9)}{3}$, where each h''_i is the image of h'_i. If T'' is independent in $Q_8.\frac{(q+1,9)}{3}$ then

$$|T| = |T'| = |T''| \leq \mu'\left(Q_8.\frac{(q+1,9)}{3}\right) \leq 3.$$

Let T'' not be independent in $Q_8.\frac{(q+1,9)}{3}$, then. Re-labelling the elements of T'' if necessary, we get that $h''_m = h''_{i_1}h''_{i_2}\ldots h''_{i_s}$ where each $i_j \neq m$. It cannot be that $h'_m = h'_{i_1}\ldots h'_{i_s}$ given the independence of T', so there is some $k \in 3^2$ such that $h'_m = h'_{i_1}\ldots h'_{i_s}k$.

Let $A := T' \setminus \{h'_m\}$ and let $N := \langle A\rangle \cap 3^2$. $N \neq 3^2$ else $k \in \langle A\rangle$ and thus $h'_m \in \langle A\rangle$. So N is a proper subgroup of 3^2. So $|N| = 1$ or 3. If $|N| = 1$ then $\langle A\rangle$ is isomorphic to

its image in $Q_8.\frac{(q+1,9)}{3}$. This means that

$$|T| - 1 = |A| \leq \mu' \left(Q_8.\frac{(q+1,9)}{3} \right) \leq 3.$$

Hence $|T| \leq 4$ if $|N| = 1$.

So suppose $|N| = 3$. Consider any pre-image N^* of N in 3^{1+2}. N^* must be a proper, non-central subgroup of 3^{1+2}. Since A normalises N, any pre-image of A must normalise N^*. Similarly, since k normalises N, any pre-image of k must normalise N^*. Hence $\langle T \rangle$ must normalise N^*, and so be a decomposition space stabiliser, by Lemma 3.1.3. □

So we get that if $H_T \in \mathcal{C}_6$ then H_T is either a decomposition space stabiliser, or $|S| \leq 5$. We now move on with the other cases.

3.1.4 The remaining cases, with broader assumptions

In this section we assume again that q is either an odd prime or a power of an odd prime, and so allow for fields of arbitrary order. This allows us to state a result that will be useful for later sections as well. Also, again we work the larger group $SL_3(q)$, as the conclusions here will prove useful for the next chapter as well. We begin by stating and proving a lemma that will be useful in this case and in some later cases.

Lemma 3.1.4. *Suppose that $T := \{h_1, \ldots, h_m\}$ is an independent set inside $SL_3(q)$. Let $T' = \{h'_1, \ldots, h'_m\}$ be the image of T in $L_3(q)$ under the natural homomorphism. If T' is not an independent set then the following consequences hold:*

1. *There is some $A \subseteq T$ such that $|A| = |T| - 1$ and $\langle A \rangle \cap Z(SL_3(q)) = 1$.*

2. *$\langle T \rangle = \langle Z(SL_3(q)), A \rangle$.*

Proof. Suppose that T' is not an independent set inside $L_3(q)$. Then, re-labelling elements if necessary, we can assume that $h'_1 = h'_{i_1} \ldots h'_{i_r}$ where no $i_j = 1$. But this means that $h_1 = z h_{i_1} \ldots h_{i_r}$ for some central element z, otherwise T is not independent. Now let

$A := \{h_2, \ldots, h_m\}$. Obviously $|A| = m-1 = |T|-1$. Suppose that $\langle A\rangle \cap Z(SL_3(q)) \neq \{1\}$. Then $Z(SL_3(q)) \leq \langle A\rangle$. But then $h_1 = zh_{i_1} \ldots h_{i_r} \in \langle A\rangle$ can be written as a word in elements of $A = T \setminus \{h_1\}$. But this contradicts the independence of S. So we have the A we want.

Note that if we set $\alpha := h_{i_1} \ldots h_{i_r} \in \langle A\rangle$ then $h_1 \in T \setminus A$ can be written as $z\alpha$ for some $z \in Z(SL_3(q))$. But then $\langle T\rangle = \langle h_1, \ldots, h_m\rangle = \langle z, h_2, \ldots, h_m\rangle = \langle Z(SL_3(q)), A\rangle$.

□

We use this lemma to draw conclusions about independent sets T that lie in various subgroups of $SL_3(q)$ and $SU_3(q)$.

Proposition 3.1.11. *If q is prime then let $l := 4$. If $q = p^r$ is a power of an odd prime then let $l := \max\{6, \pi(r) + 3\}$, where $\pi(r)$ is the number of distinct prime divisors of r. Let $T := \{h_1, \ldots, h_m\} \leq Z \times SO_3(q)$, where $|Z| = 1$ or 3, and Z is a group of scalar transformations. If T is an independent set then one of the following holds:*

1. *$\langle T\rangle$ is a subspace stabiliser, or*

2. *$|T| \leq l + 1$.*

Proof. Suppose that $\langle T\rangle \cap Z = \{1\}$. Let M be the projection of $\langle T\rangle$ into $SO_3(q)$. Then the image of $\langle T\rangle$ in $L_3(q)$ is isomorphic to M. Thus, the image of T in $L_3(q)$ is an independent set in $SO_3(q)$. From the previous chapter (Theorem 2.3.1), we know that:

1. M is a subspace stabiliser, or

2. $|T| \leq 4$ if q is an odd prime, or

3. $|T| \leq \max\{6, \pi(r) + 3\}$ if q is a power of an odd prime.

Suppose M is a subspace stabiliser. Then $\langle T\rangle$, as a pre-image of M in $SO_3(q)$, must be a subspace stabiliser. So the result holds in this case.

Suppose that $\langle T\rangle \cap Z \neq \{1\}$. If the image of T is independent in $SO_3(q)$ then we have that:

1. the image of $\langle T \rangle$ is a subspace stabiliser, or

2. $|T| \leq 4$ if q is an odd prime, or

3. $|T| \leq \max\{6, \pi(r)+3\}$ if q is a power of an odd prime.

If the image of $\langle T \rangle$ is a subspace stabiliser then its pre-image $\langle T \rangle$ must be a subspace stabiliser in $Z \times SO_3(q)$. Suppose that the image of T in $L_3(q)$ is not independent, then.

By Lemma 3.1.4, there must be an $A \subseteq T$ such that $|A| = |T| - 1$ and $\langle A \rangle \cap Z = \{1\}$. Also $\langle T \rangle = \langle Z, A \rangle$. Since $\langle A \rangle \cap Z = \{1\}$ it must be that $\langle A \rangle$ is isomorphic to its image in $L_3(q)$. From the previous chapter we have that either

1. the image of $\langle A \rangle$ is a subspace stabiliser, or

2. $|A| \leq 4$ if q is an odd prime, or

3. $|A| \leq \max\{6, \pi(r)+3\}$ if q is a power of an odd prime.

If the image of $\langle A \rangle$ is a subspace stabiliser then $\langle T \rangle = \langle Z, A \rangle$ is a subspace stabiliser. In the other cases $|T| = |A| + 1 \leq l + 1$.

This establishes the proposition. □

We now deal with the possibility that T lies in an $\mathcal{S}_1$ subgroup. We begin by dealing with the $\mathcal{S}_1$ subgroups $Z \times L_2(7)$, $|Z| = 1$ or 3, and $3\dot{A}_6$. It is easy to show the following proposition.

Proposition 3.1.12. *If $T = \{h_1, \ldots, h_m\} \subseteq 3\dot{A}_6$ is independent then $|T| \leq 4$.*

Proof. Let Z be the normal subgroup of order 3 extended by A_6 in $3\dot{A}_6$. Suppose that $\langle T \rangle \cap Z = \{1\}$. Then $\langle T \rangle$ isomorphic to its image in $\frac{3\dot{A}_6}{Z} \cong A_6$. Hence the image of T is independent in A_6. If the image of $\langle T \rangle$ is isomorphic to A_6, then $\langle T \rangle$ itself is isomorphic to A_6. But then $3\dot{A}_6 = \langle Z, T \rangle = 3 \times A_6$ is a split extension, which is absurd. So $\langle T \rangle$ is isomorphic to a subgroup of A_6. Now, the maximal subgroups of A_6 are isomorphic to S_4, A_5 or $3^2.4$. Note that $\mu'(3^2.4) \leq 3 = \mu'(S_4) = \mu'(A_5)$. So if T lies in any of these groups then $|T| \leq 3$.

Suppose that $\langle T\rangle \cap Z \neq \{1\}$. If the image of T is independent in A_6, then $|T| \leq \mu'(A_6) = 4$. So suppose that the image of T in A_6 is not independent. Lemma 3.1.4 tells us that there is an $A \subseteq T$ such that $|A| = |T|-1$ and $\langle A\rangle \cap Z = \{1\}$. So $\langle A\rangle$ is isomorphic to its image in A_6. If $\langle A\rangle \cong A_6$ then the fact that $\langle A\rangle \cap Z = \{1\}$ means that

$$3\dot{A}_6 \geq \langle Z, A\rangle \geq Z : A_6.$$

So $3\dot{A}_6$ is a split extension $3 : A_6$. But this is absurd. So $\langle A\rangle$ is a proper subgroup of A_6. But we have just seen that any such group cannot contain an independent set of size 4. Hence $|A| \leq 3$. Thus, $|T| = |A| + 1 \leq 4$.

This establishes the proposition. □

So we deal with the case that $T \subseteq Z \times L_2(7)$, $|Z| = 1$ or 3.

Proposition 3.1.13. *If $T = \{h_1, \ldots, l_m\} \subseteq Z \times L_2(7)$, $|Z| = 1$ or 3, is independent then $|T| \leq 5$.*

Proof. We begin the proof by determining $\mu'(L_2(7))$. To this end, let S' be an independent set inside $L_2(7)$. If $\langle S'\rangle = L_2(7)$ then $|S'| \leq 4$ by Theorem 1.1.3. So suppose $\langle S'\rangle$ is a proper subgroup of $L_2(7)$. But then $\langle S'\rangle$ lies within a maximal subgroup of size $6, 8, 21, 24$ or 60. If $\langle S'\rangle$ lies in a group of order 6 or 8 then clearly $|S'| \leq 3$. So suppose S' lies in a maximal subgroup M of order 21. Now, Sylow's Theorem implies that M must contain a normal subgroup of order 7 and index 3. Hence if $S' \subseteq M$ then $|S'| \leq \mu'(M) \leq \mu'(M) + \mu'(M/7) = \mu'(7) + \mu'(3) = 2$ here. If $\langle S'\rangle$ lies in a group of order 24, then it lies within a decomposition stabiliser of isomorphism type $2^2.S_3$. $|S'| \leq 4$ here. Finally, if $\langle S'\rangle$ lies in a group of order 60, then $\langle S'\rangle$ lies in an A_5 group. $|S'| \leq 3$ in this case. Therefore $\mu'(L_2(7)) \leq 4$.

Therefore $|T| \leq \mu'(Z \times L_2(7)) \leq \mu'(Z) + \mu'(L_2(7)) \leq 1 + 4 = 5$, using Corollary 1.1.2.

□

Finally, if $G = SU_3(5)$ then we also have the extra $\mathcal{S}_1$ subgroups $3\dot{A}_6.2$ and $3\dot{A}_7$. To deal with these cases, we use Lemma 3.1.4 once again.

Proposition 3.1.14. *If $T := \{h_1, \ldots, h_m\} \subseteq 3A_6.2$ or $3A_7$ is an independent set, then $|T| \leq 5$.*

Proof. Let Z be the normal subgroup of order 3 extended by $A_6.2$ in $3A_6.2$, or by A_7 in $3A_7$. Suppose that $\langle T \rangle \cap Z = \{1\}$. Then $\langle T \rangle$ is isomorphic to its image in $\frac{3A_6.2}{Z} \cong A_6.2$ or $\frac{3A_7}{Z} \cong A_7$. Suppose that $T \subseteq 3A_6.2$ and that the image of $\langle T \rangle$ in $A_6.2$ is the full $A_6.2$ group. Then $\langle T \rangle \cong A_6.2$. But $\langle T \rangle \cap Z = \{1\}$, so $3A_6.2 = \langle Z, T \rangle = 3 : A_6.2$, which is absurd. So $\langle T \rangle$ is isomorphic to a proper subgroup of $A_6.2$. By similar reasoning, we get that if $T \subseteq 3A_7$ then $\langle T \rangle$ is isomorphic to a proper subgroup of A_7.

The maximal subgroups of A_7 are isomorphic to one of the following: A_6, $L_2(7)$, S_5, $(A_4 \times 3) : 2$. But each of these groups contain independent sets of size at most 4. The maximal subgroups of $A_6.2$ are isomorphic to one of the following: $D_8.2$, $D_{10}.2$, 9.4.2, A_6. Now $D_8.2$, $D_{10}.2$, A_6 cannot contain independent sets of size more than 4. With regard to 9.4.2, neither 9 nor 4 can contain independent sets of size 2, so 9.4.2 contains independent sets of size at most 3. Hence each of the maximal subgroups of $A_6.2$ contains independent sets of size at most 4.

Since $\langle T \rangle$ is isomorphic to a proper subgroup of $A_6.2$ or A_7, $\langle T \rangle$ must lie in a maximal subgroup of $A_6.2$ or A_7. Therefore $|T| \leq 4$ in this case.

So suppose that $\langle T \rangle \cap Z \neq \{1\}$. If the image of T is independent in $A_6.2$ or A_7 then $|T| \leq \mu'(A_6.2), \mu'(A_7) \leq 5$. So suppose that the image of T in $A_6.2$ or A_7 is not independent. By Lemma 3.1.4 there must be some $A \subseteq T$ such that $|A| = |T| - 1$ and $\langle A \rangle \cap Z = \{1\}$. So $\langle A \rangle$ must be isomorphic its image in $A_6.2$ or A_7. Suppose that $T \subseteq 3A_6.2$ and that the image of $\langle A \rangle$ in $A_6.2$ is the full $A_6.2$ group. But then $\langle A \rangle \cong A_6.2$. So $3A_6.2 = \langle Z, A \rangle = 3 : A_6.2$, which is absurd. So $\langle A \rangle$ is isomorphic to a proper subgroup of $A_6.2$. By similar reasoning we have that if $T \subseteq A_7$ then $\langle A \rangle$ is isomorphic to a proper subgroup of A_7. Therefore $|A| \leq 4$. Thus, $|T| \leq |A| + 1 \leq 5$. □

3.1.5 Independent Sets in $SU_3(q)$ when q is a Prime

We may draw all the previous results together to prove:

Proposition 3.1.15. *If q is a prime and $S \subseteq SU_3(q)$ is an independent set then either $|S| \leq 6$ or $\langle S \rangle$ lies in a subspace stabiliser, decomposition space stabiliser or field extension stabiliser.*

Proof. If any $H_{\{g_i\}}$ lies in a $\mathcal{C}_6, \mathcal{S}$ or $Z \times SO_3(q)$ subgroup then by Propositions 3.1.10, 3.1.11, 3.1.12, 3.1.13 and 3.1.14 we have that $|S \setminus \{g_i\}| \leq 5$. Therefore $|S| \leq 6$. So suppose that each $H_{\{g_i\}}$ lies in a $\mathcal{C}_1, \mathcal{C}_2$ or $\mathcal{C}_3$ subgroup.

Suppose that $|S| \geq 7$. Given that any $H_{\{g_i\}} \cap H_{\{g_j\}} \cap H_{\{g_k\}}$ must contain at least two $g_l \in S$, it cannot be that $H_{\{g_i\}} \cap H_{\{g_j\}} \cap H_{\{g_k\}} \leq Z(SU_3(q))$. Also, each $H_{\{g_i\}} \cap H_{\{g_j\}}$ contains at least four g_k, so it cannot be that $\mu'(H_{\{g_i\}} \cap H_{\{g_j\}}) \leq 3$ for any distinct i, j. By Proposition 3.1.7 then, it must be that $\langle S \rangle$ is a subspace stabiliser, decomposition space stabiliser or field extension stabiliser. □

3.2 q is not a Prime

We suppose that $S \subseteq SU_3(q)$ is an independent set. In this section, we will follow closely the line of argument taken by Saxl and Whiston when dealing with $L_2(q)$ for q not a prime. Previous reasoning about intersections of subspace stabilises, decomposition space stabilisers and field extensions still hold.

However, we now have the possibility that some H_T lies in a subfield subgroup. Given subfield subgroups H_{T_1}, H_{T_2} we wish to place limits on how they intersect. To do this, we want to describe their possible intersections. To this end, we state the possible subgroups of subfield subgroups.

3.2.1 Subgroups of $SU_3(q)$

In a paper of 1911, Howard Mitchell established a result about the subgroups of $U_3(q)$ for q a power of an odd prime [11][9]. We state it here.

Theorem 3.2.1 (Mitchell)**.** *Suppose $H \leq U_3(q)$. If H is not the image of a subspace stabiliser, decomposition space stabiliser or field extension stabiliser in $U_3(q)$ then H is isomorphic to one of the following:*

1. *the stabiliser of a conic, of order $q_0(q_0^2 - 1)$ where $q_0|q$*
2. *$U_3(q_0).a$ where $a = 1$ or 3, and $q_0|q$*
3. *the Hessian groups of orders 216 (if $9|q+1$), 72 and 36 (if $3|q+1$)*
4. *groups of order 168, 360, 720 or 2520*

So the image of any $H \leq SU_3(q)$ in $U_3(q)$ must be described by Mitchell's theorem. In case 1, a stabiliser of a conic is a stabiliser of a quadratic form[1]. So if the image of H in $U_3(q)$ is such a group then H is $z \times SO_3(q_0)$ for some z where $|z| = 1$ or 3. In case 2, these subgroups are images of subfield subgroups in $SU_3(q)$. So if any $H \leq SU_3(q)$ has such an image then $H \cong SU_3(q_0).a$, $a = 1$ or 3; or $H \cong z \times U_3(q_0).a$, where $a, z \in \{1, 3\}$ and $U_3(q_0) \cong SU_3(q_0)$. In case 3, these subgroups are images of subgroups that lie in $\mathcal{C}_6$ groups. So if $H \leq SU_3(q)$ has such an image then either $\mu'(H) \leq 4$ or H is a decomposition space stabiliser, by Proposition 3.1.10. For case 4, if $H \leq SU_3(q)$ has such an image, then H lies in an $\mathcal{S}_1$ subgroup. From Propositions 3.1.12, 3.1.13 and 3.1.14 we have that $\mu'(H) \leq 5$ in this case.

[1]Mitchell seems to ignore the possibility that $\Omega_3(q_0) \leq U_3(q)$. This creates no great problems for us, as we wish to use Mitchell's theorem in the context of intersections of full subfield subgroups. If some $\Omega_3(q_0)$ is contained in a full subfield subgroup, then that subfield subgroup will contain $SO_3(q_0)$ as well. Hence we can assume that $SO_3(q_0)$ lies in the intersection of two full subfield subgroups if $\Omega_3(q_0)$ does.

3.2.2 Intersections of Subfield Subgroups

We wish to establish some results about the intersections of maximal subgroups of isomorphism type $SU_3(q_0).\left(\frac{q+1}{q_0+1}, 3\right)$. Once again, we attempt to prove a result of a similar sort to Saxl and Whiston's proposition regarding intersection of subfield subgroups of $L_2(q)$ (Proposition 2.2.3). We argue that for any subfield subgroups J_1, J_2 of this type, $J_1 \cap J_2$ is a subspace, decomposition or field extension stabiliser; or $J_1 \cap J_2$ contains small independent sets; or $J_1 = J_2$. The proof runs along similar lines to the proof for the comparable result in Saxl and Whiston's work.

We work in $G = GU_3(q)$ and with J_i that have the image of $U_3(q_i).a_i$, $a_i = 1$ or 3; or $SO_3(q_i)$ in $U_3(q)$. If $J_1 \cong J_2$ contains some $SU_3(q_0)$ or $SO_3(q_0)$ then by Theorem 3.2.1 we have that the image of $J_1 \cap J_2$ in $U_3(q)$ contains $U_3(q_0)$ or $SO_3(q_0)$. But the only subgroups of $U_3(q)$ that contain such subgroups are images of subfield subgroups of $SU_3(q)$. Hence $J_1 \cap J_2 \cong SU_3(q_1).a$, $J_1 \cap J_2 \cong z \times U_3(q_1).a \cong z \times SU_3(q_1).a$ or $J_1 \cap J_2 \cong z \times SO_3(q_1)$ where $a, z \in \{1, 3\}$.

We use the following fact.

Proposition 3.2.1. *Let $H \leq SU_3(q)$ where q is odd, and suppose $H \cong SU_3(q_1).a$, $z \times U_3(q_1).a$ or $z \times SO_3(q_1)$ where $a, z \in \{1, 3\}$. Then H is conjugate in $GU_3(q)$ to any subgroup K of $SU_3(q)$ that is isomorphic to H.*

Proof. This proposition is easily derived from observations in [11]. Let H be a subgroup of $SU_3(q)$ that fulfills the hypothesis of the proposition. Now suppose that there is a $K \leq SU_3(q)$ such that $K \cong H$ but H, K are not conjugate in $SU_3(q)$. Now, Mitchell ([11]) observes that in this case $N_{GU_3(q)}(H)$ is $N_{SU_3(q)}(H)$ extended by scalar transformations. So if $\overline{H}$ is the image of H in $PGU_3(q)$, it must be that $|N_{PGU_3(q)}(\overline{H})| = |N_{U_3(q)}(\overline{H})|$. He also observes, regarding the present case, that the set of subgroups of $SU_3(q)$ isomorphic to H must form three orbits under the action of $SU_3(q)$.

However in this case we also have $|PGU_3(q)| = 3|U_3(q)|$ (from [13]) as well as

$$|N_{PGU_3(q)}(\overline{H})| = |N_{U_3(q)}(\overline{H})|.$$

An easy application of the Orbit-Stabiliser Theorem then implies that the subgroups of $SU_3(q)$ isomorphic to H form a single conjugacy class under $GU_3(q)$. □

Proposition 3.2.2. *Suppose J_1, J_2 are distinct maximal subfield subgroups of $SU_3(q)$ such that $J_1 \cap J_2$ contains some $SU_3(q_0)$ or $SO_3(q_0)$. Then J_1 is not isomorphic to J_2.*

Proof. Suppose J_1, J_2 are isomorphic. By Proposition 3.2.1, we may take $a \in GU_3(q)$ such that $a^{-1}J_1a = J_2$. Observe that $J_1 \cap J_2$, $a^{-1}(J_1 \cap J_2)a$ are both isomorphic subgroups of J_2. $J_1 \cap J_2$, $a^{-1}(J_1 \cap J_2)a$ are both conjugate in $N_{GU_3(q)}(J_2)$, so take $b \in N_{GU_3(q)}(J_2)$ such that $b^{-1}a^{-1}(J_1 \cap J_2)ab = J_1 \cap J_2$. Then $ab \in N_{GU_3}(J_1 \cap J_2) \leq N_{GU_3(q)}(J_2)$. But $b \in N_{GU_3(q)}(J_2)$, so $a = (ab)(b^{-1}) \in N_{GU_3(q)}(J_2)$. Therefore $J_1 = J_2$, a contradiction. So J_1 is not isomorphic to J_2. □

Proposition 3.2.3. *Suppose that J_1, J_2 are isomorphic subfield subgroups of $SU_3(q)$ with $J_1 \cap J_2$ containing some $SU_3(q_0)$ or $SO_3(q_0)$. Then $J_1 = J_2$.*

Proof. Suppose that $J_1 \neq J_2$. Since $J_1 \neq J_2$, we can find $L_1 \geq J_1$ and $L_2 \geq J_2$ that meets the following conditions: The L_i are the largest, distinct isomorphic subfield subgroups of G such that J_i is contained in L_i. Let $H \leq G$ be a subfield subgroup of G such that L_1, $L_2 \leq H$, and H is the smallest subfield subgroup of G to contain the L_i. We consider the two possibilities for H.

Suppose $H \cong z_1 \times SO_3(q_1)$. Then L_1, $L_2 \leq H$ must be isomorphic to some $z_2 \times SO_3(q_2)$. For each $i \leq 2$ let K_i be the $SO_3(q_2)$ subgroup of L_i. So K_1, K_2 are distinct, isomorphic subfield subgroups of $SO_3(q_1)$ and $K_1 \cap K_2$ is a subfield subgroup of $SO_3(q_1)$. But notice that in this case $J_1 \cap J_2 = z \times SO_3(q_0)$, and that $SO_3(q_0) \leq K_1 \cap K_2$. By Corollary 2.2.1 of the previous chapter, we have that $K_1 = K_2$. Then $L_1 = L_2$, a contradiction. So $J_1 = J_2$ in this case.

Suppose H has the image $U_3(q_1).a_1$ in $U_3(q)$, then. Suppose J_1, $J_2 \cong SU_3(q_2).3$, $3 \times SU_3(q_2).3$ or $3 \times SO_3(q_2)$. Then the $SU_3(q_0)$ or $SO_3(q_0)$ subgroup that lies in $J_1 \cap J_2$ must lie in the $SU_3(q_2)$ or $SO_3(q_2)$ subgroups of the J_i. If this fact means that the $SU_3(q_2)$ or $SO_3(q_2)$ subgroups of the J_i are identical, then we can conclude that $J_1 = J_2$. So if J_1,

$J_2 \cong SU_3(q_2).3$, $3 \times SU_3(q_2).3$ or $3 \times SO_3(q_2)$ then it is enough to investigate the nature of their $SU_3(q_2)$ or $SO_3(q_2)$ subgroups. Hence we may suppose that J_1, $J_2 \cong SU_3(q_2)$ or $SO_3(q_2)$ respectively. Similar considerations for L_1, L_2 mean that if L_1, $L_2 \cong SU_3(q_3).3$, $3 \times SU_3(q_3).3$ or $3 \times SO_3(q_3)$ then we can suppose that L_1, $L_2 \cong SU_3(q_3)$ or $SO_3(q_3)$. If we can replace H with a smaller subfield subgroup that contains the L_i, then now do so. Re-labelling if necessary, we say that $H \cong SU_3(q_1)$.

Now, L_1 and L_2 must be isomorphic, maximal subfield subgroups of H, otherwise we could find larger, isomorphic subfield subgroups M_1, $M_2 \leq H$ such that $J_i \leq M_i$ for each i. But now $L_1 \cap L_2$ contains $SU_3(q_0)$ or $SO_3(q_0)$, so by Proposition 3.2.2 we have that L_1, L_2 are not distinct. But this is a contradiction. So $J_1 = J_2$.

□

Proposition 3.2.4. *Let H_1, H_2 be subfield subgroups of $SU_3(q)$ that do not lie in the same maximal subfield subgroup. If $H_1 \cap H_2$ contains an $SU_3(q_0)$ or $SO_3(q_0)$ then H_1, H_2 have no isomorphic overgroups other than $SU_3(q)$.*

Proof. Suppose that J_1, J_2 are isomorphic subfield subgroups of $SU_3(q)$ such that $H_1 \leq J_1, H_2 \leq J_2$. Then $J_1 \cap J_2$ contains an $SU_3(q_0).a$ or $z \times SO_3(q_0)$. Therefore $J_1 = J_2$ by Proposition 3.2.3, which contradicts the assumption on H_1, H_2. Hence the result. □

3.2.3 Independent Sets Inside $SU_3(q)$ for $q = p^r$ a Power of a Prime

We are now in a position to prove the main proposition. As in the previous chapter, $\pi(r)$ is set to be the number of distinct prime divisors of r.

Theorem 3.2.2. *Suppose that $S = \{g_1, \ldots, g_n\} \subseteq SU_3(q)$ is an independent set, and that $q = p^r$. Suppose further that no smaller $SU_3(q_1) \leq SU_3(q)$ contains S. Then either*

1. $|S| \leq \max\{8, \pi(r) + 5\}$, *or*

2. $\langle S \rangle$ *stabilises a subspace, decomposition space or a field extension, or*

3. $\langle S \rangle$ lies in a subfield subgroup of $SU_3(q)$.

Proof. For each non-empty $T \subseteq S$ we define $H_T := \langle S \setminus T \rangle$ in the standard way. By Theorem 3.2.1 and the discussion following its statement, we know that for each H_T, one of the following holds:

1. H_T stabilises a subspace, decomposition space or field extension (throughout this proof, such subgroups will described as "geometric").
2. $H_T = SU_3(q_0).a$ or $z \times SO_3(q_0)$ is a subfield subgroup.
3. $\mu'(H_T) \leq 5$.

For any non-empty $T \subseteq S$ where $|T| \leq 2$, if $\mu'(H_T) \leq 5$ then $|S| \leq 7$, so suppose this does not happen. Also, if $H_{\{g_i\}} \leq z \times SO_3(q)$ then by Theorem 2.3.1 either $H_{\{g_i\}}$ is geometric, or $|S \setminus \{g_i\}| \leq \max\{7, \pi(r)+4\}$. In the latter case $|S| \leq \max\{8, \pi(r)+5\}$. So we suppose that each $H_{\{g_i\}}$ is either geometric or equal to some $SU_3(q_0).a$. We also suppose that each $H_{\{g_1,g_2\}}$ is either geometric, or equal to some $SU_3(q_0).a$ or $z \times SO_3(q_0)$. Also, we suppose that $|S| \geq 8$.

If any four of the $H_{\{g_i\}}$ are geometric then by Proposition 3.1.7 either $\langle S \rangle$ is geometric, the intersection of three of the $H_{\{g_i\}}$ lie in $Z(SU_3(q))$, or the intersection of two of the $H_{\{g_i\}}$ contain independent sets of size at most 3. If $\langle S \rangle$ is geometric then we have what we want. So suppose that the intersection of three of the $H_{\{g_i\}}$ is central. Without loss of generality, suppose that $\bigcap_{i=1}^{3} H_{\{g_i\}} \leq Z(SU_3(q))$. Now for any $j \geq 4$, $g_j \in \bigcap_{i=1}^{3} H_{\{g_i\}} \leq Z(SU_3(q))$. But $Z(SU_3(q))$ cannot contain an independent set of size 2, so there can be at most one such g_j. Hence $|S| \leq 4$. So suppose that there are $H_{\{g_i\}}$, $H_{\{g_j\}}$ whose intersection contains independent sets of size at most 3. But $S \setminus \{g_i, g_j\}$ is an independent set in $H_{\{g_i\}} \cap H_{\{g_j\}}$. Hence $|S| = |S \setminus \{g_i, g_j\}| + 2 \leq 3 + 2 = 5$.

So suppose there are at most three geometric $H_{\{g_i\}}$ with the rest lying in $\mathcal{C}_5$ subgroups. If any two $H_{\{g_i\}}$, $H_{\{g_j\}}$ lie in the same $\mathcal{C}_5$ subgroup M, then $\langle S \rangle = \langle H_{\{g_i\}}, H_{\{g_j\}} \rangle \leq M$, so suppose not.

Now, recall that we assumed for any $H_{\{g_i\}}$, $H_{\{g_j\}}$ that $H_{\{g_i,g_j\}}$ is geometric or a subfield subgroup. If $H_{\{g_i\}}$, $H_{\{g_j\}}$ lie in isomorphic subfield subgroups and $H_{\{g_i,g_j\}}$ is a subfield subgroup then $H_{\{g_i\}}$, $H_{\{g_j\}}$ both lie in some subfield subgroup by Proposition 3.2.4. But this case has already been covered. Hence, if $H_{\{g_i\}}$, $H_{\{g_j\}}$ lie in distinct, isomorphic subfield subgroups then we may suppose that $H_{\{g_i,g_j\}}$ is geometric.

So we have that at most three of the $H_{\{g_i\}}$ are geometric with the rest subfield subgroups. We deal with three cases.

Case: Precisely three of the $H_{\{g_i\}}$ are geometric:

Without loss of generality, we suppose that $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are geometric with $H_{\{g_i\}}$ a subfield subgroup for $i \geq 4$. Suppose that $H_{\{g_4,g_5\}}$ is geometric. Now $\{g_1\}$, $\{g_2\}$, $\{g_3\}$, $\{g_4, g_5\}$ are mutually disjoint, so by Proposition 3.1.7 we have that either $\langle S\rangle$ stabilises a subspace, decomposition space or field extension; the intersection of three of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4,g_5\}}$ is central; or the intersection of two of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4,g_5\}}$ contains independent sets of size at most 3. In the latter case we may suppose, without loss of generality, that $\mu'(H_{\{g_1\}} \cap H_{\{g_2\}}) \leq 3$ or $\mu'(H_{\{g_1\}} \cap H_{\{g_4,g_5\}}) \leq 3$. If $\mu'(H_{\{g_1\}} \cap H_{\{g_2\}}) \leq 3$ then $|S| \leq 5$. If $\mu'(H_{\{g_1\}} \cap H_{\{g_4,g_5\}}) \leq 3$ then $|S| \leq 6$.

So suppose the intersection of three of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4,g_5\}}$ is central. Then there cannot be two $g_i \in S$ the intersection, so $|S| \leq 5$. Hence if $H_{\{g_4,g_5\}}$ is geometric then either $|S| \leq 6$ or $\langle S\rangle$ is a subspace stabiliser, decomposition space stabiliser or field extension stabiliser.

So suppose $H_{\{g_i,g_j\}}$ is not geometric for all $i, j \geq 4$. Then the $H_{\{g_i\}}$ lie in distinct, maximal, non-isomorphic subfield subgroups of $SU_3(q)$ for $i \geq 4$. Thus, $|S| \leq \pi(r) + 3$.

Case: Precisely two of the $H_{\{g_i\}}$ are geometric:

Suppose, without loss of generality, that $H_{\{g_1\}}$, $H_{\{g_2\}}$ are geometric, and that the other $H_{\{g_3\}}$, ..., $H_{\{g_n\}}$ are subfield subgroups. If no two of $H_{\{g_3\}}, \ldots, H_{\{g_n\}}$ lie in isomorphic subfield subgroups then $|S| \leq \pi(r) + 2$. So suppose that $H_{\{g_3\}}$, $H_{\{g_4\}}$ lie in isomorphic subfield subgroups. Hence $H_{\{g_3,g_4\}}$ is geometric. We consider the possibilities for $H_{\{g_5\}}$.

If $H_{\{g_5\}}$, $H_{\{g_6\}}$ lie in isomorphic subfield subgroups then $H_{\{g_5,g_6\}}$ is geometric. By

Proposition 3.1.7 either $\langle S\rangle$ stabilises a subspace, decomposition space or field extension; or the intersection of three of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_5,g_6\}}$ is central; or two of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_5,g_6\}}$ have an intersection that contains independent sets of size at most 3. If the latter case happens then we have that $|S| \leq 7$. If the intersection of three of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_5,g_6\}}$ is central then there cannot be more than one $g_i \in S$ in the intersection, so $|S| \leq 7$. So if $H_{\{g_3,g_4\}}$, $H_{\{g_5,g_6\}}$ are geometric then either $\langle S\rangle$ is geometric or $|S| \leq 7$.

If $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5\}}$ lie in isomorphic subfield subgroups then $H_{\{g_4,g_5\}}$, $H_{\{g_3,g_5\}}$ are geometric. Now, observe that $H_{\{g_1,g_5\}}$, $H_{\{g_2,g_5\}}$ are geometric by the assumption on $H_{\{g_1\}}$, $H_{\{g_2\}}$. Also, if $S' := S \setminus \{g_5\}$ observe that $H_{\{g_i,g_5\}} = \langle S' \setminus \{g_i\}\rangle$ for all $i \leq 4$. Now, observe that $\{g_1\}$, $\{g_2\}$, $\{g_3\}$, $\{g_4\}$ are disjoint subsets of S'. By Proposition 3.1.7, it must be that either $\langle S'\rangle = H_{\{g_5\}}$ is geometric, $\bigcap_{i\leq 4}\langle S' \setminus \{g_i\}\rangle = \bigcap_{i\leq 4} H_{\{g_i,g_5\}} \leq Z(SU_3(q))$, or some $\langle S'\setminus\{g_i\}\rangle \cap \langle S'\setminus\{g_j\}\rangle = H_{\{g_i,g_5\}} \cap H_{\{g_j,g_5\}}$ contains independent sets of size at most 3. Now $H_{\{g_5\}}$ is not geometric by assumption. So either the intersection of the $H_{\{g_i,g_5\}}$ is central, or there are two $H_{\{g_i,g_5\}}$ whose intersection contains independent sets of size at most 3. If the intersection $\bigcap_{i\leq 4} H_{\{g_i,g_5\}} \leq Z(SU_3(q))$ then $|S| \leq 6$. If $\mu'(H_{\{g_i,g_5\}} \cap H_{\{g_j,g_5\}}) \leq 3$ then $|S| \leq 6$. In any event, we have a desired result.

The only other genuine possibility is that $H_{\{g_3\}}$, $H_{\{g_4\}}$ are the only $H_{\{g_i\}}$, $i \geq 3$, that lie in isomorphic subfield subgroups. But in that case $|S| \leq \pi(r) + 3$.

Case: Precisely one of the $H_{\{g_i\}}$ is geometric

Suppose, without loss of generality, that only $H_{\{g_1\}}$ is geometric, and that $H_{\{g_2\}}, \ldots, H_{\{g_n\}}$ lie in subfield subgroups. If $|S| \leq \pi(r) + 3$ then we have what we want. Suppose not, then. Then by the pigeonhole principle there are at least three subgroups $H_{\{g_i\}}$, where each $H_{\{g_i\}}$ can be paired with some $H_{\{g_j\}}$ such that $H_{\{g_i\}}$, $H_{\{g_j\}}$ lie in isomorphic subfield subgroups. The following list exhausts all the genuinely distinct possibilities here:

1. $H_{\{g_i\}}$, $H_{\{g_{i+1}\}}$ lie isomorphic subfield subgroups for $i = 2$, 4, 6.

2. $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ lie in isomorphic subfield subgroups whilst $H_{\{g_5\}}$, $H_{\{g_6\}}$ also lie in isomorphic subfield subgroups.

3. $H_{\{g_i\}}$ lie in isomorphic subfield subgroups for $2 \leq i \leq 5$.

We consider each case in turn. In the first case $H_{\{g_i,g_{i+1}\}}$ is geometric for $i = 2, 4, 6$. By Proposition 3.1.7 then, it must be either that $\langle S \rangle$ is geometric; the intersection of three of $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ is central; or there are two of $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ whose intersection contains independent sets of size at most 3. If $\langle S \rangle$ is geometric then we are satisfied. So suppose the intersection of three of $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ is central. Then $|S| \leq 7$. So suppose that there are two of $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ whose intersection contains independent sets of size at most 3. $|S| \leq 7$ here as well.

In the second case we have that $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_5,g_6\}}$ are geometric. Notice that $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_5,g_6\}}$ are geometric as well. Now, $\{g_1\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5, g_6\}$ are disjoint subsets of $S \setminus \{g_2\}$. By Proposition 3.1.7 then, either $\langle S \setminus \{g_2\} \rangle = H_{\{g_2\}}$ is geometric; the intersection of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5,g_6\}}$ is central, or there are two of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5,g_6\}}$ whose intersection contains independent sets of size at most 3. $H_{\{g_2\}}$ is not geometric by assumption, so the first possibility does not occur. If the intersection of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5,g_6\}}$ is central then $|S| \leq 7$. If two of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5,g_6\}}$ have an intersection containing independent sets of size at most 3 then $|S| \leq 7$ here.

Finally, in the third case we have that $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$ are geometric. Now, $H_{\{g_1,g_2\}}$ must be geometric as well. Observe that $\{g_1\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5\}$ are disjoint subsets of $S \setminus \{g_2\}$. By Proposition 3.1.7 then, either $H_{\{g_2\}}$ is geometric (which is not the case); the intersection of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$ is central; or two of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$ have an intersection containing independent sets of size at most 3. If the intersection of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$ is central then $|S| \leq 6$. If two of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$ have an intersection containing independent sets of size at most 3 then $|S| \leq 6$ once again.

Case: Each $H_{\{g_i\}}$ lies in a subfield subgroup

So now suppose that each $H_{\{g_i\}}$ lies in a subfield subgroup and is not geometric. Partition

the maximal subfield subgroups of $SU_3(q)$ that do not stabilise a quadratic form into isomorphism classes $A_1, \ldots, A_{\pi(r)}$. For each $H_{\{g_i\}}$ there must be a smallest maximal subfield subgroup $J_i \cong SU_3(q_1).a$ for some q_1, a such that J_i contains $H_{\{g_i\}}$. If A_j contains J_i then associate $H_{\{g_i\}}$ with A_j. Suppose $H_{\{g_i\}}, H_{\{g_j\}}$ are associated with the same A_k, and there is some $J_i \in A_k$ such that $H_{\{g_i\}}, H_{\{g_j\}} \leq J_i$. Then $\langle S \rangle = \langle H_{\{g_i\}}, H_{\{g_j\}} \rangle$ lies in a subfield subgroup of $SU_3(q)$. So suppose that this does not happen. Thus, if $H_{\{g_i\}}, H_{\{g_j\}}$ are associated with A_k, then $H_{\{g_i,g_j\}}$ is geometric.

We now consider each genuinely distinct case. These are listed here:

1. $H_{\{g_i\}}$, $H_{\{g_{i+1}\}}$ are both associated with some A_j for $i = 1, 3, 5, 7$.

2. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are associated with A_1; $H_{\{g_4\}}$, $H_{\{g_5\}}$ are associated with A_2 and $H_{\{g_6\}}$, $H_{\{g_7\}}$ are associated with A_3.

3. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are associated with A_1 while $H_{\{g_4\}}$, $H_{\{g_5\}}$, $H_{\{g_6\}}$ are associated with A_2.

4. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ are associated with A_1 whilst $H_{\{g_5\}}$, $H_{\{g_6\}}$ are associated with A_2.

5. Each $H_{\{g_i\}}$ is associated with A_1 for $i \leq 5$.

6. Each A_i has at most two $H_{\{g_j\}}$ associated with it, and at most three A_i have more than one $H_{\{g_j\}}$ associated with it.

For the first case, $H_{\{g_i,g_{i+1}\}}$, $i = 1, 3, 5, 7$, is geometric. But by using Proposition 3.1.7 again, we get that either $\langle S \rangle$ is geometric, the intersection of three of these $H_{\{g_i,g_{i+1}\}}$ is central, or there are two of them whose intersection contains independent sets of size at most 3. If $\langle S \rangle$ is geometric then we are satisfied. Suppose the intersection of three of the $H_{\{g_i,g_{i+1}\}}$ is central. Without loss of generality, suppose that $H_{\{g_1,g_2\}} \cap H_{\{g_3,g_4\}} \cap H_{\{g_5,g_6\}} \leq Z(SU_3(q))$. Then $|S| \leq 7$. So suppose that two of the $H_{\{g_i,g_{i+1}\}}$ have an intersection containing independent sets of size at most 3. But then $|S| \leq 7$ again.

For the second case, $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_4,g_5\}}$ and $H_{\{g_6,g_7\}}$ are geometric. Therefore $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4,g_5\}}$ and $H_{\{g_1,g_6,g_7\}}$ are geometric. Observe that $\{g_2\}$, $\{g_3\}$, $\{g_4,g_5\}$, $\{g_6,g_7\}$ are mutually disjoint subsets of $S\setminus\{g_1\}$, the generating set of $H_{\{g_1\}}$. By Proposition 3.1.7 either $H_{\{g_1\}}$ is geometric; the intersection of three of $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_6,g_7\}}$ is central; or the intersection of two of them contains independent sets of size at most 3. $H_{\{g_1\}}$ is not geometric by assumption, so one of the other two possibilities holds. But in either case $|S|\leq 8$.

For the third case $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_4,g_6\}}$ and $H_{\{g_5,g_6\}}$ are geometric. Observe that $\{g_2\}$, $\{g_3\}$, $\{g_5\}$, $\{g_6\}$ are mutually disjoint subsets of $S\setminus\{g_1,g_4\}$. By Proposition 3.1.7 applied to the geometric subgroups $H_{\{g_1,g_2,g_4\}}$, $H_{\{g_1,g_3,g_4\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_4,g_6\}}\leq H_{\{g_1,g_4\}}$, it must be that either $H_{\{g_1,g_4\}}$ is geometric; the intersection of three of $H_{\{g_1,g_2,g_4\}}$, $H_{\{g_1,g_3,g_4\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_4,g_6\}}$ is central; or the intersection of two of them contains independent sets of size at most 3. For either of the final two possibilities $|S|\leq 7$, so suppose that $H_{\{g_1,g_4\}}$ is geometric. So now $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5,g_6\}}$ are geometric. Note that these subgroups generate $H_{\{g_1\}}$, which is not geometric. Also, $\{g_2\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5,g_6\}$ are disjoint subsets of $S\setminus\{g_1\}$. By Proposition 3.1.7 then, it must be that either the intersection of three of $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5,g_6\}}$ is central, or the intersection of two of them contains independents sets of size at most 3. In either case $|S|\leq 7$.

For the fourth case, $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$ and $H_{\{g_1,g_5,g_6\}}\leq H_{\{g_5,g_6\}}$ are geometric. But we have already dealt with this case.

For the fifth case, $H_{\{g_1,g_i\}}$ is geometric for $2\leq i\leq 5$. Note that these groups generate $H_{\{g_1\}}$ and that $H_{\{g_1\}}$ is not geometric. Also, note that $\{g_2\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5\}$ are disjoint subsets of $S\setminus\{g_1\}$. By Proposition 3.1.7 then, either $\bigcap_{i=2}^{5}H_{\{g_1,g_i\}}$ is central or $\mu'(H_{\{g_1,g_i\}}\cap H_{\{g_1,g_j\}})\leq 3$ for some i,j. In either case, $|S|\leq 6$.

For the final case, we have that $|S|\leq\pi(r)+3$. This establishes the proposition.

□

3.3 Conclusion

Altogether, then we have shown in this chapter:

Theorem 3.3.1. *Let q be a power of an odd prime. Suppose $S \subseteq SU_3(q)$ is independent. Then one of the following holds:*

1. *$\langle S \rangle$ is a subspace stabiliser, decomposition space stabiliser or field extension stabiliser.*

2. *$\langle S \rangle$ lies in a subfield subgroup.*

3. *q is prime and $|S| \leq 6$.*

4. *$q = p^r$ for some odd prime p and $|S| \leq \max\{8, \pi(r) + 3\}$.*

CHAPTER 4

MINIMAX SETS IN 3-DIMENSIONAL SPECIAL LINEAR GROUPS OVER FIELDS OF ODD CHARACTERISTIC

We can use what we have established in the previous two chapters to help us with various cases in this chapter. In this chapter, we seek to place limits on the size of a minimax set $S := \{g_1, \ldots, g_n\}$ in $SL_3(q)$. However, for most of the argument we will simply assume that S is an independent set in $SL_3(q)$ rather than a minimax set.

With this end in mind, we define $H_T := \langle S \setminus T \rangle$ for each non-empty $T \subsetneqq S$, as is familiar from previous chapters. Each such H_T lies in one of the groups listed in Table 4.1. Once again, the information in this table is drawn from [8].

So we deal with each case in turn.

4.1 Case: $H_T \leq M \in \mathcal{C}_1$

Here H_T is a subspace stabiliser, stabilising either a 1-dimensional subspace or a 2-dimensional subspace. Let U_1 be the subspace stabilised by H_T. We have only one result to establish in this section.

Proposition 4.1.1. *Let S be an independent set in $SL_3(q)$. Let non-empty T_1, T_2, T_3, T_4, $T_5 \subseteq S$ such that $T_i \cap T_j = \varnothing$. Suppose further that H_{T_1}, H_{T_2}, H_{T_3}, H_{T_4}, H_{T_5} stabilise subspaces U_1, U_2, U_3, U_4, U_5 respectively. Then either $\langle S \rangle$ is a subspace stabiliser or*

Class	Isomorphism Types	Conditions
$\mathcal{C}_1$	$E_q^2 : GL_2(q)$ $E_q^{1+2} : (q-1)^2$	
$\mathcal{C}_2$	$(q-1)^2 : S_3$	$q \geq 5$
$\mathcal{C}_3$	$(q^2+q+1) : 3$	$q \geq 4$
$\mathcal{C}_5$	$SL_3(q_0).(r, q-1, 3)$	$q = q_0^r$, r prime
$\mathcal{C}_6$	$3^{1+2} : Q_8 : \frac{(q+1,9)}{3}$	$q = p \equiv 1 \bmod 3$
$\mathcal{C}_8$	$(q+1, 3) \times SO_3(q)$ $SU_3(q_0)$	q odd $q = q_0^2$
$\mathcal{S}_1$	$(q+1, 3) \times L_2(7)$ $3 \cdot A_6$	$q = p \equiv 1, 2, 4 \mod 7$, $p \neq 2$ $q = p \equiv 1, 4 \mod 15$ $q = p^2$, $p \equiv 2, 3 \bmod 5$, $p \neq 3$

Table 4.1: The maximal subgroups of $SL_3(q)$

$\bigcap_{i=1}^{5} H_{T_i} \leq Z(SL_3(q))$.

Proof. Suppose $U_i = U_j$ for some i, j. Since $T_i \cap T_j = \varnothing$ each $g_k \in S$ lies in at least one of $S \setminus T_i$, $S \setminus T_j$. Therefore each $g_k \in S$ lies in one of H_{T_i}, H_{T_j} and so fixes $U_i = U_j$. Therefore $\langle S \rangle$ stabilises U_i. So we suppose the U_i are distinct.

Consider the dimensions of the U_i. Now, it must be that either three of them are of dimension 1 or three of them are of dimension 2. We consider each case in turn. Also, for the rest of the proof, we work in the projective space PV, and replace each U_i with its image $\overline{U_i}$ in PV. Thus, if U_i is 1-dimensional then $\overline{U_i}$ will be a point in PV, and if U_i is 2-dimensional then $\overline{U_i}$ will be a line in PV. If $\overline{U_i}$, $\overline{U_j}$ are distinct points in PV then we denote by $\overline{U_i} \oplus \overline{U_j}$ the unique line in PV that is incident with both $\overline{U_i}$, $\overline{U_j}$. We allow $\langle S \rangle$ to act on PV. This action is induced from the action of $\langle S \rangle$ on V.

Case: $\overline{U_i}$ is a point for at least three $\overline{U_i}$

We suppose, without loss of generality, that $\overline{U_1}$, $\overline{U_2}$, $\overline{U_3}$ are all points in PV. Given what has been established already, we may suppose that they are mutually distinct, Suppose $\overline{U_1} \oplus \overline{U_2} = \overline{U_1} \oplus \overline{U_3} = \overline{U_2} \oplus \overline{U_3}$. Take any $g_i \in S$. Suppose $g_i \in T_a$ for some $a \leq 3$. Then $g_i \notin T_b, T_c$ for the other $b, c \leq 3$. Hence $g_i \in H_{T_b \cup T_b} \leq H_{T_b} \cap H_{T_c}$ and so g_i must fix $\overline{U_b} \oplus \overline{U_c} = \overline{U_1} \oplus \overline{U_2}$. This is because fixing two points incident with a line is sufficient to fix the line itself. Suppose $g_i \notin T_a$ for all $a \leq 3$. Then $g_i \notin T_1 \cup T_2$. Thus,

$g_i \in H_{T_1 \cup T_2} \leq H_{T_1} \cap H_{T_2}$, and so fixes $\overline{U_1} \oplus \overline{U_2}$. Since each $g_i \in S$ must fix $\overline{U_1} \oplus \overline{U_2}$, $\langle S \rangle$ stabilises $\overline{U_1} \oplus \overline{U_2}$. So now suppose that $\overline{U_1} \oplus \overline{U_2} \neq \overline{U_2} \oplus \overline{U_3}$ or $\overline{U_1} \oplus \overline{U_2} \neq \overline{U_1} \oplus \overline{U_3}$. So the points $\overline{U_1}$, $\overline{U_2}$, $\overline{U_3}$ are not collinear.

Consider $\overline{U_4}$, $\overline{U_5}$ in PV. Suppose that $\overline{U_4}$ is a point. If $\overline{U_4}$ is incident with any $\overline{U_i} \oplus \overline{U_j}$ for any $i, j \leq 3$ then $\overline{U_i} \oplus \overline{U_j} = \overline{U_i} \oplus \overline{U_4} = \overline{U_j} \oplus \overline{U_4}$. But we have just seen that $\langle S \rangle$ is a line stabiliser in this case. So we suppose that $\overline{U_4}$ is not incident with the line $\overline{U_i} \oplus \overline{U_j}$ for any $i, j \leq 3$. In that case, each $g \in \bigcap_{i=1}^{4} H_{T_i}$ fixes each of $\overline{U_1}$, $\overline{U_2}$, $\overline{U_3}$, $\overline{U_4}$. Since no three of $\overline{U_1}$, $\overline{U_2}$, $\overline{U_3}$, $\overline{U_4}$ are collinear, g must fix all points in PV. Hence g is scalar.

So suppose that both $\overline{U_4}$, $\overline{U_5}$ are lines in PV. Since they are distinct, there must be a unique point W that is incident with both $\overline{U_4}$, $\overline{U_5}$. Now suppose that $W = \overline{U_i}$ for some $i \leq 3$. Any $g_j \in T_i$ cannot lie in $T_4 \cup T_5$. Therefore any $g_j \in T_i$ lies in $H_{T_4 \cup T_5} \leq H_{T_4} \cap H_{T_5}$, and so fixes $W = \overline{U_i}$. Hence, $\langle S \rangle = \langle S \setminus T_i, T_i \rangle$ stabilises $\overline{U_i}$. So suppose $W \neq \overline{U_i}$ for all $i \leq 3$.

Now suppose that W is incident with $\overline{U_1} \oplus \overline{U_2}$. So $\overline{U_1} \oplus \overline{U_2} = \overline{U_1} \oplus W = \overline{U_2} \oplus W$. Take any $g_i \in S$. If $g_i \in T_1$ then $g_i \notin T_2 \cup T_4 \cup T_5$. So if $g_i \in T_1$ then $g_i \in H_{T_2 \cup T_4 \cup T_5} \leq H_{T_2} \cap H_{T_4} \cap H_{T_5}$, which stabilises $\overline{U_2} \oplus W = \overline{U_1} \oplus \overline{U_2}$. Similarly, if $g_i \in T_2$ then $g_i \notin T_1 \cup T_4 \cup T_5$, and so fixes $\overline{U_1} \oplus W = \overline{U_1} \oplus \overline{U_2}$. If $g_i \notin T_1 \cup T_2$ then $g_i \in H_{T_1 \cup T_2}$, and so must fix $\overline{U_1} \oplus \overline{U_2}$. Hence $\langle S \rangle$ stabilises the line $\overline{U_1} \oplus \overline{U_2}$. So suppose that W is not incident with the line $\overline{U_i} \oplus \overline{U_j}$ for all $i, j \leq 3$. Then any $g \in \bigcap_{i=1}^{5} H_{T_i}$ must fix $\overline{U_1}$, $\overline{U_2}$, $\overline{U_3}$, W and so be scalar.

This completes the study of this case.

Case: $\overline{U_i}$ are lines for at least three $\overline{U_i}$

Suppose, without loss of generality, that $\overline{U_1}$, $\overline{U_2}$, $\overline{U_3}$ are lines in PV. We work in the dual space PV^*. So we regard the points of PV as lines in PV^*, and the lines of PV as points in PV^*. The action of $\langle S \rangle$ on PV^* is induced by its action on PV.

Now, $\overline{U_1}$, $\overline{U_2}$, $\overline{U_3}$ are points in PV^*, and we are in the previous case. By the previous case then, $\langle S \rangle$ must be scalar.

This establishes the proposition.

□

This completes the section.

4.2 $H_T \leq M \in \mathcal{C}_2$

The case where two H_T subgroups each lie in a $\mathcal{C}_2$ subgroup is covered by Proposition 3.1.2 of the previous chapter. So in this section we deal only with the case that one H_T stabilises a decomposition while another stabilises a subspace.

Proposition 4.2.1. *Let S be an independent set in $SL_3(q)$. Let $T_1, T_2 \subseteq S$ such that $T_1 \cap T_2 = \varnothing$. Suppose also that H_{T_1} stabilises a decomposition space $U_1 \oplus U_2 \oplus U_3$ whilst H_{T_2} stabilises a subspace W. Then either $H_{T_1} \cap H_{T_2}$ stabilises one of the U_i or $\mu'(H_{T_1} \cap H_{T_2}) \leq 3$*

Proof. $dim(W) = 1$ or 2. We divide the proof into the two cases.

Case: $dim(W) = 1$

If $W = U_i$ for some i then clearly $H_{T_1} \cap H_{T_2}$ stabilises $U_i = W$, so suppose $W \neq U_i$ for all i. Suppose further that $W \leq U_i \oplus U_j$ for some i, j. Without loss of generality, suppose $W \leq U_1 \oplus U_2$. If $H_{T_1} \cap H_{T_2}$ does not stabilise $U_1 \oplus U_2$, then there must be some $U_i \oplus U_j$ such that $(U_1 \oplus U_2)^g = U_i \oplus U_j$ for some $g \in H_{T_1} \cap H_{T_2}$. But $H_{T_1} \cap H_{T_2}$ stabilises W, so $W \leq (U_1 \oplus U_2) \cap (U_i \oplus U_j) = U_1$ or U_2. Hence $W = U_1$ or U_2. So we may suppose that $H_{T_1} \cap H_{T_2}$ stabilises $U_1 \oplus U_2$. In so doing, it must stabilise U_3.

So suppose $W \not\leq U_i \oplus U_j$ for all i, j. Then any $g \in H_{T_1} \cap H_{T_2}$ that fixes each U_i must fix W as well, and hence be scalar. Then $H_{T_1} \cap H_{T_2} \leq 3.S_3$. So here

$$\mu'(H_{T_1} \cap H_{T_2}) \leq \mu'(3.S_3) \leq \mu'(3) + \mu'(S_3) \leq 3$$

by Corollary 1.1.2.

Case: $dim(W) = 2$

If $W = U_i \oplus U_j$ for some i, j then $H_{T_1} \cap H_{T_2}$ must stabilise the remaining U_k. So suppose $W \neq U_i \oplus U_j$ for all i, j. Suppose $U_i \leq W$ for some i. Without loss of generality, suppose

$U_1 \leq W$. If $H_{T_1} \cap H_{T_2}$ stabilises U_1 then we have what we want, so suppose $H_{T_1} \cap H_{T_2}$ does not stabilise U_1. So there is some $g \in H_{T_1} \cap H_{T_2}$ such that $U_1^g = U_2$ or U_3. But $H_{T_1} \cap H_{T_2}$ stabilises W, so $U_1, U_1^g \leq W$. Therefore $W = U_1 \oplus U_1^g = U_1 \oplus U_2$ or $U_1 \oplus U_3$. This cannot be, so $U_i \not\leq W$ for all i. Therefore $W \cap (U_i \cap U_j)$ is a point distinct from both U_i, U_j in $U_i \oplus U_j$.

But now consider any $g \in H_{T_1} \cap H_{T_2}$ that fixes each U_i. g will fix W as well. Therefore, g will fix three points U_i, U_j, $W \cap (U_i \oplus U_j)$ in each $U_i \oplus U_j$. This means that g must be scalar. Therefore $H_{T_1} \cap H_{T_2} \leq 3.S_3$ in this case. Therefore $\mu'(H_{T_1} \cap H_{T_2}) \leq \mu'(3.S_3) \leq 3$. □

We have achieved all we have wished to achieve in this section.

4.3 $H_T \leq M \in \mathcal{C}_3$

In this case H_T must stabilise a field extension. We begin with two lemmas.

Lemma 4.3.1. *For all a, b, c, hcf$(3(q^2+q+1), (q-1)^a q^b (q+1)^c) = 3^d$ for some d.*

Proof. Let p be a prime that divides both q^2+q+1 and $(q-1)^a q^b (q+1)^b$. So p divides $q-1$, q or $q+1$.

If $p|q-1$ then $p|q^2+q+1-(q+2)(q-1) = 3$. So $p = 3$.

If $p|q$ then $p|q^2+q+1-(q+1)q = 1$, which is absurd.

If $p|q+1$ then $p|q^2+q+1-q(q+1) = 1$, which cannot be.

So if p is a prime that divides both $(q-1)^a q^b (q+1)^c$ and $3(q^2+q+1)$ then either $p|3$, in which case $p = 3$, or $p|(q^2+q+1)$, in which case $p = 3$. Hence hcf$(3(q^2+q+1), (q-1)^a q^b (q+1)^c)$ is a power of 3. □

Lemma 4.3.2. *Suppose $M \in \mathcal{C}_3$ is a field extension stabiliser, and $K \leq M$ with $|K| = 3^d$ for some d. Then $\mu'(K) \leq 2$.*

Proof. Let F be the cycle of order q^2+q+1 in M. So $M = F : 3$. If $K \leq F$ then K is a cycle of prime-power order, and so $\mu'(K) = 1$. If $K \not\leq F$ then $K = (K \cap F) : 3$.

But $K \cap F$ must be a cycle of prime-power order,so $\mu'(K \cap F) = 1$. Hence we may use Corollary 1.1.2 to say

$$\mu'(K) = \mu'((K \cap F) : 3) \leq \mu'(K \cap F) + \mu'(3) = 1 + 1 = 2.$$

□

We will assume throughout the next few propositions that $M_1 \in \mathcal{C}_3$ is a field extension stabiliser. In this case, $|M_1| = 3(q^2 + q + 1)$.

Proposition 4.3.1. *Suppose $M_1 \in \mathcal{C}_3$ is a field extension stabiliser whilst $M_2 \in \mathcal{C}_1$ is a subspace stabiliser. Then $\mu'(M_1 \cap M_2) \leq 2$.*

Proof. Given that $M_2 \in \mathcal{C}_1$, it must be that $M_2 \cong E_{q^2} : GL_2(q), E_q^{1+2} : (q-1)^2$ or $GL_2(q)$. Then $|M_2| = (q-1)^2q^3(q+1), (q-1)^2q^3$ or $(q-1)^2q(q+1)$ respectively.

Now $|M_1 \cap M_2|$ must divide $\text{hcf}(|M_1|, |M_2|) = \text{hcf}(3(q^2 + q + 1), |M_2|)$. Given Lemma 4.3.1, it must be that $|M_1 \cap M_2| = 3^d$ for some d. By Lemma 4.3.2, we must have $\mu'(M_1 \cap M_2) \leq 2$. □

Proposition 4.3.2. *Suppose $M_1 \in \mathcal{C}_3$ is a field extension stabiliser whilst $M_2 \in \mathcal{C}_2$ is a decomposition space stabiliser. Then $\mu'(M_1 \cap M_2) \leq 2$.*

Proof. $|M_2| = 6(q-1)^2$. So $|M_1 \cap M_2|$ divides $\text{hcf}(3(q^2 + q + 1), 6(q-1)^2)$. It must be that $q^2 + q + 1$ is odd. Thus $3(q^2 + q + 1)$ is odd and $2 \not| 3(q^2 + q + 1)$. So we have $\text{hcf}(3(q^2 + q + 1), 6(q-1)^2) = \text{hcf}(3(q^2 + q + 1), 3(q-1)^2)$. Suppose p is a prime that divides both $3(q^2 + q + 1)$ and $3(q-1)^2$. Then $p|3$ or $p|(q-1)^2$. If $p|3$ then $p = 3$. If $p|(q-1)^2$ then $p = 3$ by Lemma 4.3.1. Therefore $\text{hcf}(3(q^2 + q + 1), 3(q-1)^2) = 3^d$ for some d. So $|M_1 \cap M_2|$ divides 3^d. By Lemma 4.3.2 then, $\mu'(M_1 \cap M_2) \leq 2$. □

Proposition 4.3.3. *Suppose $M_1, M_2 \in \mathcal{C}_3$ are distinct field extension stabilisers. Then $\mu'(M_1 \cap M_2) \leq 3$.*

Proof. Let $F_1 \leq M_1$ be the cycle of order $q^2 + q + 1$ in M_1 and $F_2 \leq M_2$ be the cycle of order $q^2 + q + 1$ in M_2. Since F_1, F_2 are cyclic, $F_1 \cap F_2$ must be the unique cycle of

order $|F_1 \cap F_2|$ in F_1 and the unique cycle of order $|F_1 \cap F_2|$ in F_2. So the Frobenius automorphisms of M_1 and M_2 must fix $F_1 \cap F_2$ in both F_1, F_2. Also, $F_1 \cap F_2$ must be normalised by both F_1, F_2 as F_1, F_2 are abelian. Therefore $F_1 \cap F_2$ is normalised by both M_1 and M_2. Hence $F_1 \cap F_2 \trianglelefteq \langle M_1, M_2 \rangle = SL_3(q)$. But the only proper, normal subgroup of $SL_3(q)$ is $Z(SL_3(q))$, if this is non-trivial. So $|F_1 \cap F_2| = 1$ or 3.

But now $M_1 \cap M_2 \leq (F_1 \cap M_2) : 3$. Now $F_1 \cap M_2 \leq (F_1 \cap F_2) : 3 \leq 3 : 3$, so $\mu'(F_1 \cap M_2) \leq 2$. Hence

$$\mu'(M_1 \cap M_2) \leq \mu'((F_1 \cap M_2) : 3) \leq \mu'(F_1 \cap M_2) + \mu'(3) \leq 2 + 1 = 3$$

by Corollary 1.1.2. □

We may now draw some conclusions from everything established so far.

Proposition 4.3.4. *Let S be an independent set in $SL_3(q)$. Suppose non-empty T_1, T_2, T_3, T_4, $T_5 \subseteq S$ such that $T_i \cap T_j = \varnothing$ for all i, j. If each H_{T_i} lies in a $\mathcal{C}_1$, $\mathcal{C}_2$ or $\mathcal{C}_3$ group then either*

1. *$\langle S \rangle$ stabilises a subspace, decomposition space or field extension;*
2. *$\mu'(H_{t_i} \cap H_{T_j}) \leq 3$ for some i, j; or*
3. *the intersection of five of the H_{T_i} lies in $Z(SL_3(q))$.*

Proof. Suppose one of the H_{T_i} lies in a $\mathcal{C}_3$ group. Then either $\mu'(H_{T_i} \cap H_{T_j}) \leq 3$ for any $j \neq i$, or $\langle S \rangle$ stabilises a field extension, by Propositions 4.3.1, 4.3.2 and 4.3.3. So we suppose that each H_{T_i} lies in a $\mathcal{C}_1$ or $\mathcal{C}_2$ group.

Suppose $|S| \geq 6$. Suppose each H_{T_i} is a subspace stabiliser for $i \leq 6$. If $\langle S \rangle$ is not a subspace stabiliser then by Proposition 4.1.1 it must be that five of $H_{T_1}, \ldots, H_{T_6}$ have an intersection that lies in $Z(SL_3(q))$. So suppose that H_{T_1} stabilises $U_1 \oplus U_2 \oplus U_3$ without stabilising any U_i.

Take any $i \geq 2$. Suppose that H_{T_i} lies in a $\mathcal{C}_1$ group. By Proposition 4.2.1 we know that either $\mu'(H_{T_1} \cap H_{T_i}) \leq 3$ or $H_{T_1} \cap H_{T_i}$ stabilises one of the U_j. If $\mu'(H_{T_1} \cap H_{T_i}) \leq 3$ then we have what we wanted, so suppose that $H_{T_1} \cap H_{T_i}$ stabilises one of the U_i.

Suppose that H_{T_i} lies in a $\mathcal{C}_2$ subgroup. By Proposition 3.1.2, we know that either $\langle H_{T_1}, H_{T_i} \rangle$ stabilises a decomposition, $\mu'(H_{T_1} \cap H_{T_i}) \leq 3$ or $H_{T_1} \cap H_{T_i}$ stabilises one of the U_j. If $\mu'(H_{T_1} \cap H_{T_j}) \leq 3$ then we are done. If $\langle H_{T_1}, H_{T_i} \rangle$ stabilises a decomposition, then we note that each $g_k \in S$ lies in at least one of H_{T_1}, H_{T_i} since $T_1 \cap T_i = \varnothing$. But then $\langle S \rangle = \langle H_{T_1}, H_{T_i} \rangle$ stabilises a decomposition. So we can assume that $H_{T_1} \cap H_{T_i}$ stabilises one of the U_j.

Therefore each $H_{T_1} \cap H_{T_i}$ stabilises one of the U_k. Suppose, without loss of generality, that $H_{T_1} \cap H_{T_2}$, $H_{T_1} \cap H_{T_3}$ both stabilise U_1. Take any $g_i \in S \setminus T_1$. It cannot be that g_i lies in both T_2, T_3 as $T_2 \cap T_3 = \varnothing$. So g_i lies in at least one of $H_{T_1} \cap H_{T_2}$, $H_{T_1} \cap H_{T_3}$. Therefore $H_{T_1} = \langle S \setminus T_1 \rangle \leq \langle H_{T_1} \cap H_{T_2}, H_{T_1} \cap H_{T_3} \rangle$ stabilises U_1, which we assumed does not happen. Therefore each $H_{T_1} \cap H_{T_i}$ stabilises a distinct U_j.

So without loss of generality, we suppose that $H_{T_1} \cap H_{T_2}$ stabilises U_1 while $H_{T_1} \cap H_{T_3}$ stabilises U_2. Then $\bigcap_{i=1}^{3} H_{T_i} \leq (H_{T_1} \cap H_{T_2}) \cap (H_{T_1} \cap H_{T_3})$ stabilises both U_1, U_2, and so must stabilise U_3 as well. Now $H_{T_1} \cap H_{T_4}$ must stabilise one of the U_i. We know that we have what we want if $H_{T_1} \cap H_{T_4}$ stabilises U_1 or U_2, as $H_{T_1} \cap H_{T_2}$, $H_{T_1} \cap H_{T_3}$ already stabilise these. So suppose $H_{T_1} \cap H_{T_4}$ stabilises U_3. Now each $g_i \in T_4$ lies in $H_{T_1} \cap H_{T_2} \cap H_{T_3}$, and so fixes U_3. Thus, $H_{T_1} \leq \langle H_{T_1} \cap H_{T_4}, T_4 \rangle$ must stabilise U_3, which we assumed did not happen. This completes the study of all the possible cases, and so completes the proposition. □

4.3.1 Independent Generating Sets for $SL_3(q)$, q an Odd Prime

We are now able to prove an upper bound for $\mu(SL_3(q))$ where q is an odd prime.

Theorem 4.3.1. $\mu(SL_3(q)) \leq 6$ *where* q *is an odd prime.*

Proof. Let $S = \{g_1, \ldots, g_n\}$ be a minimax set for $SL_3(q)$. For each $g_i \in S$, define

$H_{\{g_i\}} := \langle S \setminus \{g_i\} \rangle$. Each $H_{\{g_i\}}$ must lie in a maximal subgroup of $SL_3(q)$. We can read the possible maximal subgroups for prime q from Table 4.1.

Suppose some $H_{\{g_i\}}$ lies in an $\mathcal{S}_1$ subgroup. Propositions 3.1.12 and 3.1.13 inform us that in this case $\mu'(H_{\{g_i\}}) \leq 5$. Hence $|S| \leq 6$.

Suppose some $H_{\{g_i\}}$ lies in a $\mathcal{C}_8$ subgroup. Then given that q is prime, it must be that $H_{\{g_i\}} \leq (q-1,3) \times SO_3(q)$. Proposition 3.1.11 tells us that either $H_{\{g_i\}}$ is a subspace stabiliser, or $|S \setminus \{g_i\}| \leq 5$. Hence either $|S| \leq 6$, or we can assume that $H_{\{g_i\}}$ is a subspace stabiliser.

Suppose some $H_{\{g_i\}}$ lies in a $\mathcal{C}_6$ subgroup. Proposition 3.1.10 tells us that either $|S \setminus \{g_i\}| \leq 4$, or $H_{\{g_i\}}$ is a decomposition space stabiliser. Hence either $|S| \leq 5$ or we can assume that $H_{\{g_i\}}$ is a decomposition space stabiliser.

So now suppose that none of these cases hold. Then each $H_{\{g_i\}}$ must lie in a $\mathcal{C}_1$, $\mathcal{C}_2$ or $\mathcal{C}_3$ subgroup. Now, $\langle S \rangle = SL_3(q)$ does not stabilise a subspace, decomposition space or field extension, so by Proposition 4.3.4 it must be that either $\mu'(H_{\{g_i\}} \cap H_{\{g_j\}}) \leq 3$ for some i, j; or the intersection of five of the $H_{\{g_i\}}$ is central. If $\mu'(H_{\{g_i\}} \cap H_{\{g_j\}}) \leq 3$ for some i, j then $|S| \leq 5$ and we are satisfied. So suppose that the intersection of five of the $H_{\{g_i\}}$ is central and that $|S| \geq 6$. Without loss of generality, suppose $\bigcap_{i=1}^{5} H_{\{g_i\}} \leq Z(SL_3(q))$. Then for each $i \geq 6$, $g_i \in Z(SL_3(q))$. Now $\langle g_1, \ldots, g_5 \rangle$ must lie in some maximal subgroup M of $SL_3(q)$, otherwise this contradicts the independence of S. But $Z(SL_3(q)) \leq M$ as well, so $\langle S \rangle \leq M \lneqq SL_3(q) = \langle S \rangle$, which is absurd. So $|S| \leq 5$ once again.

This establishes the proposition. □

Note that, in general, no minimax $S \subseteq SL_3(q)$ can contain a g that lies in $Z(SL_3(q))$. There must be some maximal $M \leq SL_3(q)$ such that $\langle S \setminus \{g\} \rangle \leq M$. But $g \in M$ as well, since $g \in Z(SL_3(q))$. Then $\langle S \rangle \leq M$, which is absurd.

4.4 $q = p^r$ is a Power of a Prime

In this section, we seek good bounds on $\mu(SL_3(q))$. To do this, we some preliminary results.

4.4.1 Subgroups of $SL_3(q)$

Howard Mitchell managed to describe the subgroups of $L_3(q)$ [11][9].

Theorem 4.4.1 (Mitchell)**.** *Let $H \leq L_3(q)$. If H is not the image of a subspace stabiliser, decomposition space stabiliser or field extension stabiliser in $SL_3(q)$, then H is isomorphic to one of the following:*

1. *the stabiliser of conic of order $q_0(q_0^2 - 1)$*
2. *$L_3(q_0).a$ where $a = 1$ or 3*
3. *$U_3(q_0).a$ where $a = 1$ or 3*
4. *the Hessian groups of order 216 (if $9|q-1$), 72 and 36 (if $3|q-1$)*
5. *groups of order 168, 360 720 and 2520*

So the image of any $H \leq SL_3(q)$ in $L_3(q)$ must be described by one of cases in Theorem 4.4.1. In case 1, the stabiliser of a conic is a stabiliser of a quadratic form, as for Theorem 3.2.1. Its pre-image in $SL_3(q)$ will be a subgroup of $z \times SO_3(q)$, where $z = 1$ or 3. In case 2, the pre-image of this group in $SL_3(q)$ will be $SL_3(q_0).a$ or $z \times L_3(q_0).a \cong z \times SL_3(q_0).a$ where $a, z \in \{1, 3\}$. The pre-image in $SL_3(q)$ of the group in Case 3 will be $SU_3(q_0).a$ or $z \times U_3(q_0).a \cong z \times SU_3(q_0).a$ where $a, z \in \{1, 3\}$. In Case 4, the pre-image H in $SL_3(q)$ of any one of these groups lies in a normaliser of a group of symplectic type. We know from Proposition 3.1.10 that either $\mu'(H) \leq 4$ or H stabilises a decomposition space. For cases 5, these groups are isomorphic to one of $L_2(7)$, A_6, $A_6.2$ A_7. The pre-image H of any one of these groups will be an $\mathcal{S}_1$ group in some subfield subgroup of $SL_3(q)$. Propositions 3.1.12, 3.1.13 and 3.1.14 imply that $\mu'(H) \leq 5$ in these cases.

4.4.2 Intersections of Subfield Subgroups

In this section we aim to produce a comparable result to Proposition 2.2.3. We work in $GL_3(q)$ and with J_i that have the image $L_3(q_i).a_i$, $a_i = 1$ or 3, in $L_3(q)$. If the image of $J_1 \cap J_2$ in $L_3(q)$ contains an $L_3(q_0).a_0$, $U_3(q_0).a_0$ or $SO_3(q_0)$ group, then we can see from Theorem 4.4.1 that the image of $J_1 \cap J_2$ in $L_3(q)$ must itself be an $L_3(q_1).a_1$, $U_3(q_1).a_1$ or $SO_3(q_1)$ group. We then take it as given in that case that $J_1 \cap J_2$ is conjugate in $GU_3(q)$ to any group isomorphic to it.

Proposition 4.4.1. *Suppose J_1, J_2 are distinct maximal subfield subgroups of $SL_3(q)$ such that $J_1 \cap J_2$ contains $SL_3(q_0)$, $SO_3(q_0)$ or $SU_3(q_0)$ for some $q_0|q$. Then J_1 is not isomorphic to J_2.*

Proof. Suppose that $J_1 \cong J_2$. Then there is some $a \in GL_3(q)$ such that $J_2 = a^{-1}J_1a$. Observe that both $J_1 \cap J_2$, $a^{-1}(J_1 \cap J_2)a$ are isomorphic subgroups of J_2. So there must be some $b \in N_{GL_3(q)}(J_2)$ such that $b^{-1}a^{-1}(J_1 \cap J_2)ab = J_1 \cap J_2$. So $ab \in N_{GL_3(q_0)}(J_1 \cap J_2) \leq \langle Z(GU_3(q)), GL_3(q_0)\rangle$. But b lies in this group. So ab lies in this group. However, $\langle Z(GL_3(q)), GL_3(q_0)\rangle$ normalises J_2, so ab normalises J_2, a contradiction. Hence the result. □

Proposition 4.4.2. *Suppose that J_1, J_2 are isomorphic subfield subgroups of $SL_3(q)$ such that $J_1 \cap J_2$ contains some $SL_3(q_0)$, $SO_3(q_0)$ or $SU_3(q_0)$. Then $J_1 = J_2$.*

Proof. Suppose $J_1 \neq J_2$. If J_1, $J_2 \cong 3 \times SL_3(q_1).a_1$, $a_1 = 1$ or 3, then $J_1 = J_2$ if their $SL_3(q_1)$ groups are the same. So we may suppose that J_1, $J_2 \cong SL_3(q_1)$ for some $q_1|q$. Since J_1, J_2 are distinct, there must be distinct isomorphic L_1, $L_2 \leq SL_3(q)$ such that each L_i is a subfield subgroup, and $J_i \leq L_i$. Note that if the L_i are isomorphic to $3 \times SL_3(q_2).a_2$, $a_2 = 1$ or 3, then $L_1 = L_2$ if their $SL_3(q_2)$ subgroups agree. Hence we may suppose that L_1, $L_2 \cong SL_3(q_2)$ for some $q_2|q$. Let H be the smallest subfield subgroup of G to contain both L_1, L_2. So $H \cong SL_3(q_3).a_3$ for some $q_1|q$. So L_1, $L_2 \leq SL_3(q_3)$.

Now, L_1 and L_2 must be isomorphic, maximal subfield subgroups of $SL_3(q_3)$, otherwise we could find larger, isomorphic subfield subgroups M_1, $M_2 \leq SL_3(q_3)$ such that $J_i \leq M_i$

for each i. But now $L_1 \cap L_2$ contains $SL_3(q_0)$, $SU_3(q_0)$ or $SO_3(q_0)$, so by Proposition 4.4.1 we have that L_1, L_2 are not distinct. But this is a contradiction. So $J_1 = J_2$. □

Proposition 4.4.3. *Suppose J_1, J_2 are subfield subgroups of $SL_3(q)$ such that $J_1 \cap J_2$ contains some $SL_3(q_0)$, $SO_3(q_0)$ or $SU_3(q_0)$. Then J_1, J_2 have no isomorphic overgroups other than $SL_3(q)$.*

Proof. Suppose that L_1, L_2 are isomorphic overgroups of J_1, J_2 respectively. Then

$$L_1 \cap L_2 \geq J_1 \cap J_2 \geq SL_3(q_0), SO_3(q_0) \text{ or } SU_3(q_0).$$

Proposition 4.4.2 implies that $L_1 = L_2$. □

We are now in a position to prove the main result of this section. $\pi(r)$ is taken to be the number of distinct prime divisors of r.

Theorem 4.4.2. *If $q = p^r$ for some odd prime p then $\mu(SL_3(q)) \leq \max\{10, \pi(r) + 6\}$.*

Proof. Let $S := \{g_1, \ldots, g_n\}$ be a minimax set for G. For any non-empty $T \subseteq S$, let $H_T := \langle S \setminus T \rangle$ as previously. If any H_T lies in a $\mathcal{C}_1$, $\mathcal{C}_2$ or $\mathcal{C}_3$ subgroup then call such a group "geometric".

Let non-empty $T \subseteq S$ such that $|T| \leq 2$. If H_T lies in an $\mathcal{S}_1$ subgroup then $|S \setminus T| \leq 5$ by Propositions 3.1.13 and 3.1.12. So $|S| \leq 7$. If H_T lies in a $\mathcal{C}_8$ subgroup then either H_T is geometric, or $|S \setminus \{g_i\}| \leq \max\{8, \pi(r) + 5\}$ by Theorems 2.3.1 and 3.3.1. So H_T is geometric or $|S| \leq \max\{9, \pi(r) + 6\}$. If H_T lies in a $\mathcal{C}_6$ subgroup then either H_T is geometric or $|S \setminus T| \leq 4$ by Proposition 3.1.10. Therefore either H_T is geometric or $|S| \leq 5$. So either $|S|$ has a bound we want, or H_T is geometric and so covered by another case. Hence we suppose that none of these cases happen. So any such H_T is either geometric, or lies in a subfield subgroup. Also, we suppose that $|S| \geq 11$.

Suppose H_{g_i}, H_{g_j} lie in subfield subgroups. If they lie in isomorphic subfield subgroups then by Proposition 4.4.3 it must be that $H_{\{g_i, g_j\}} \leq H_{\{g_i\}} \cap H_{\{g_j\}}$ is geometric.

We now turn our attention to the subgroups $H_{\{g_i\}}$ and deal with the genuinely distinct cases.

Case: Five of the $H_{\{g_i\}}$ are geometric

Suppose $H_{\{g_i\}}$ is geometric for $i \leq 5$. By Proposition 4.3.4, either $\langle S \rangle$ is geometric, or $\bigcap_{i=1}^{5} H_{\{g_i\}} \leq Z(SL_3(q))$, or two of the $H_{\{g_i\}}$ have an intersection that contains independent sets of size at most 3. $\langle S \rangle$ cannot be geometric, so one of the other two possibilities holds. If the intersection of $H_{\{g_i\}}$, $H_{\{g_j\}}$ contains independent sets of size at most 3 then $|S \setminus \{g_i, g_j\}| \leq 3$. So $|S| \leq 5$. If $\bigcap_{i=1}^{5} H_{\{g_i\}} \leq Z(SL_3(q))$ then any $g_j \in S$, $j \geq 6$ lies in $Z(SL_3(q))$, which cannot be. So $|S| \leq 5$ again. This completes the study of this case

Case: Precisely four of the $H_{\{g_i\}}$ are geometric

Suppose $H_{\{g_i\}}$ is geometric for $i \leq 4$ with the other $H_{\{g_j\}}$ lying in subfield subgroups. If the $H_{\{g_j\}}$, $j \geq 5$ lie in non-isomorphic, maximal, subfield subgroups of $SL_3(q)$ then $|S| \leq \pi(r) + 4$. So suppose that $H_{\{g_5\}}$, $H_{\{g_6\}}$ lie in isomorphic subfield subgroups. Then $H_{\{g_5,g_6\}}$ is geometric. $\{g_1\}$, $\{g_2\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5, g_6\}$ are mutually disjoint subsets of S, so by Proposition 4.3.4 either $\langle S \rangle$ is geometric (which is not the case); two of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5,g_6\}}$ have an intersection with independent sets of size at most 3; or the intersection of all the $H_{\{g_i\}}$, $i \leq 4$ with $H_{\{g_5,g_6\}}$ is central. If two of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5,g_6\}}$ have an intersection containing independent sets of size at most 3, then $|S| \leq 6$. So suppose the intersection of all $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5,g_6\}}$ is central. But then there can be no $g_7 \in S$, as it would lie in this intersection. Hence $|S| \leq 6$ here. So we have what we wanted.

Case: Precisely three of the $H_{\{g_i\}}$ are geometric

Suppose $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are geometric, with the other $H_{\{g_j\}}$ lying in subfield subgroups. Suppose that $H_{\{g_4\}}$, $H_{\{g_5\}}$ lie in isomorphic subfield subgroups and $H_{\{g_6\}}$, $H_{\{g_7\}}$ lie in isomorphic subfield subgroups. Then $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ are geometric. Using the fact that $\{g_1\}$, $\{g_2\}$, $\{g_3\}$, $\{g_4, g_5\}$, $\{g_6, g_7\}$ are disjoint subsets of S, and the fact that $\langle S \rangle$ is not geometric, Proposition 4.3.4 implies that either two of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ have an intersection that contains independent sets of size at most 3; or that the

intersection of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ is central. If the final possibility holds then there can be no $g_8 \in S$ as then $g_8 \in Z(SL_3(q))$. So suppose that two of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4,g_5\}}$, $H_{\{g_6,g_7\}}$ have an intersection containing independent sets of size at most 3. Then $|S| \leq 7$ here.

Now suppose that $H_{\{g_4\}}$, $H_{\{g_5\}}$, $H_{\{g_6\}}$ all lie in isomorphic subfield subgroups. Then $H_{\{g_4,g_6\}}$, $H_{\{g_5,g_6\}}$ are geometric. Notice also that $H_{\{g_i,g_6\}}$ is geometric for $i \leq 3$, since $H_{\{g_i\}}$ is geometric. Let $S' := S \setminus \{g_6\}$. Note that $H_{\{g_6\}} = \langle S' \rangle$ and that $H_{\{g_i,g_6\}} = \langle S' \setminus \{g_i\} \rangle$ for any $i \leq 5$. Since $H_{\{g_6\}}$ is not geometric by assumption, and since $\{g_1\}$, $\{g_2\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5\}$ are disjoint subsets of S', we may use Proposition 4.3.4 to conclude that either $\bigcap_{i=1}^{5} H_{\{g_i,g_6\}} \leq Z(SL_3(q))$ or that $\mu'(H_{\{g_i,g_6\}} \cap H_{\{g_j,g_6\}}) \leq 3$ for some distinct $i, j \leq 5$. If $\bigcap_{i=1}^{5} H_{\{g_i,g_6\}} \leq Z(SL_3(q))$ then there can be no $g_7 \in S$, as then $g_7 \in Z(SL_3(q))$. So $|S| \leq 7$ here. So suppose that $\mu'(H_{\{g_i,g_6\}} \cap H_{\{g_j,g_6\}}) \leq 3$ for some $i, j \leq 5$. Then $|S| \leq 6$.

The only other genuine possibility is that there are at most two $H_{\{g_i\}}$, $i \geq 4$ that lie in isomorphic subfield subgroups. But then $|S| \leq \pi(r) + 4$, and we have what we wanted.

Case: Precisely two of the $H_{\{g_i\}}$ are geometric

Suppose $H_{\{g_1\}}$, $H_{\{g_2\}}$ are geometric with the other $H_{\{g_j\}}$ lying in subfield subgroups. If $|S| \leq \pi(r) + 4$ then we are satisfied. Suppose then that $|S| \geq \pi(r) + 5$. Since, up to isomorphism, there are only $\pi(r)$ maximal subfield subgroups, we can assume that one of the following holds:

1. $H_{\{g_i\}}$, $H_{\{g_{i+1}\}}$ lie in isomorphic subfield subgroups for $i = 3, 5, 7$.

2. $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5\}}$ lie in isomorphic subfield subgroups, as do $H_{\{g_6\}}$, $H_{\{g_7\}}$.

3. $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5\}}$, $H_{\{g_6\}}$ all lie in isomorphic subfield subgroups.

Suppose the first case holds. Since $\{g_1\}$, $\{g_2\}$, $\{g_3, g_4\}$, $\{g_5, g_6\}$, $\{g_7, g_8\}$ are mutually disjoint, by Proposition 4.3.4 it must be that either two of $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_5,g_6\}}$, $H_{\{g_7,g_8\}}$ have an intersection containing independent sets of size at most 3; or the intersection of all $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_5,g_6\}}$, $H_{\{g_7,g_8\}}$ is central. If the first possibility

occurs then $|S| \leq 7$. If the second possibility occurs then there can be no $g_9 \in S$,as then $g_9 \in Z(SL_3(q))$. Hence $|S| \leq 8$.

Suppose the second case holds. Then $H_{\{g_3,g_4\}}$, $H_{\{g_3,g_5\}}$, $H_{\{g_6,g_7\}}$ are geometric. Observe that $\{g_1\}$, $\{g_2\}$, $\{g_4\}$, $\{g_5\}$, $\{g_6, g_7\}$ are mutually disjoint subsets of $S \setminus \{g_3\}$. By Proposition 4.3.4 then, either $H_{\{g_3\}}$ is geometric; two of $H_{\{g_1,g_3\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_3,g_5\}}$, $H_{\{g_3,g_6,g_7\}}$ have an intersection that contains independent sets of size at most 3, or $\bigcap_{i\leq 7, i\neq 3} H_{\{g_3,g_i\}} \leq Z(SL_3(q))$. $H_{\{g_3\}}$ is not geometric by assumption. If two of $H_{\{g_1,g_3\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_3,g_5\}}$, $H_{\{g_3,g_6,g_7\}}$ have an intersection that contains independent sets of size at most 3 then $|S| \leq 7$. If the intersection of all $H_{\{g_1,g_3\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_3,g_5\}}$, $H_{\{g_3,g_6,g_7\}}$ is central then there is no $g_8 \in S$. Hence $|S| \leq 7$.

Suppose the third case holds, then. Then $H_{\{g_3,g_i\}}$ is geometric for $i = 4, 5, 6$. But then $\{g_1\}$, $\{g_2\}$, $\{g_4\}$, $\{g_5\}$, $\{g_6\}$ are disjoints subsets of $S \setminus \{g_3\}$. $H_{\{g_3\}}$ is not geometric, so by Proposition 4.3.4 either two of $H_{\{g_1,g_3\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_3,g_4\}}$, $H_{\{g_3,g_5\}}$, $H_{\{g_3,g_6\}}$ have an intersection that contains independent sets of size at most 3, or $\bigcap_{i\leq 6, i\neq 3} H_{\{g_i,g_3\}} \leq Z(SL_3(q))$. If the first possibility holds then $|S| \leq 6$. If the second possibility holds then there is no $g_7 \in S$, and so $|S| \leq 6$ again.

Case: Precisely one of the $H_{\{g_i\}}$ is geometric

Suppose $H_{\{g_1\}}$ is geometric with the other $H_{\{g_j\}}$ lying in subfield subgroups. If $|S| \leq \pi(r) + 4$ then we are satisfied, so suppose that $|S| \geq \pi(r) + 5$. Then we can assume one of the following holds:

1. $H_{\{g_i\}}$, $H_{\{g_{i+1}\}}$ lie in isomorphic subfield subgroups for $i = 2, 4, 6, 8$.
2. $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ lie in isomorphic subfield subgroups, as do $H_{\{g_5\}}$, $H_{\{g_6\}}$ and $H_{\{g_7\}}$, $H_{\{g_8\}}$.
3. $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ lie in isomorphic subfield subgroups, as do $H_{\{g_5\}}$, $H_{\{g_6\}}$, $H_{\{g_7\}}$.
4. $H_{\{g_2\}}$, ..., $H_{\{g_5\}}$ lie in isomorphic subfield subgroups, as do $H_{\{g_6\}}$, $H_{\{g_7\}}$.
5. $H_{\{g_i\}}$ lie in isomorphic subfield subgroups for $2 \leq i \leq 6$.

In the first case we have that $H_{\{g_i,g_{i+1}\}}$ is geometric for $i = 2, 4, 6, 8$. Observe that $\{g_1\}$, $\{g_2, g_3\}, \ldots, \{g_8, g_9\}$ are mutually disjoint subsets of S. Then by Proposition 4.3.4 either two of $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}, \ldots, H_{\{g_8,g_9\}}$ have an intersection containing independent sets of size at most 3, or the intersection of all $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}, \ldots, H_{\{g_8,g_9\}}$ is central. If two of $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}, \ldots, H_{\{g_8,g_9\}}$ have an intersection containing independent sets of size at most 3 then $|S| \leq 7$. If the intersection of all $H_{\{g_1\}}$, $H_{\{g_2,g_3\}}, \ldots, H_{\{g_8,g_9\}}$ is central, then there is no $g_{10} \in S$, and so $|S| \leq 9$.

In the second case, we observe that $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5,g_6\}}$, $H_{\{g_2,g_7,g_8\}}$ are geometric. Note that $\{g_1\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5, g_6\}$, $\{g_7, g_8\}$ are mutually disjoint subsets of $S \setminus \{g_2\}$. $H_{\{g_2\}}$ is nor geometric, by assumption. So by Proposition 4.3.4 we conclude that either two of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5,g_6\}}$, $H_{\{g_2,g_7,g_8\}}$ have an intersection containing independent sets of size at most 3; or the intersection of all $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5,g_6\}}$, $H_{\{g_2,g_7,g_8\}}$ is central. If the first possibility holds, then $|S| \leq 8$. If the second possibility holds then $|S| \leq 8$ again.

In the third case, we observe that $H_{\{g_1,g_2,g_5\}}$, $H_{\{g_2,g_3,g_5\}}$, $H_{\{g_2,g_4,g_5\}}$, $H_{\{g_2,g_5,g_6\}}$, $H_{\{g_2,g_5,g_7\}}$ are geometric. Now $\{g_1\}$, $\{g_3\}$, $\{g_4\}$, $\{g_6\}$,$\{g_7\}$ are mutually disjoint subsets of $S \setminus \{g_2, g_5\}$. So by Proposition 4.3.4 we have either that $H_{\{g_2,g_5\}}$ is geometric; two of $H_{\{g_1,g_2,g_5\}}$, $H_{\{g_2,g_3,g_5\}}$, $H_{\{g_2,g_4,g_5\}}$, $H_{\{g_2,g_5,g_6\}}$, $H_{\{g_2,g_5,g_7\}}$ have an intersection that contains independent sets of size at most 3; or the intersection of all $H_{\{g_1,g_2,g_5\}}$, $H_{\{g_2,g_3,g_5\}}$, $H_{\{g_2,g_4,g_5\}}$, $H_{\{g_2,g_5,g_6\}}$, $H_{\{g_2,g_5,g_7\}}$ is central. For either of the second or third possibilities, $|S| \leq 8$. So we suppose that $H_{\{g_2,g_5\}}$ is geometric. Hence $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$, $H_{\{g_2,g_6,g_7\}}$ are geometric. But now we observe that $\{g_1\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5\}$, $\{g_6, g_7\}$ are mutually disjoint subsets of $S \setminus \{g_2\}$. $H_{\{g_2\}}$ is not geometric, so by Proposition 4.3.4 either two of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$, $H_{\{g_2,g_6,g_7\}}$ have an intersection containing independent sets of size at most 3, or the intersection of all $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$, $H_{\{g_2,g_6,g_7\}}$ is central. If the first possibility holds then $|S| \leq 7$. If the second possibility holds then $|S| \leq 8$.

So suppose that the fourth case holds. Then $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$,

$H_{\{g_2,g_6,g_7\}}$ are geometric. We observe that $\{g_1\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5\}$, $\{g_6, g_7\}$ are mutually disjoint subsets of $S \setminus \{g_2\}$. $H_{\{g_2\}}$ is not geometric, so by Proposition 4.3.4it must be that either two of $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$, $H_{\{g_2,g_6,g_7\}}$ have an intersection containing independent sets of size at most 3; or the intersection of all $H_{\{g_1,g_2\}}$, $H_{\{g_2,g_3\}}$, $H_{\{g_2,g_4\}}$, $H_{\{g_2,g_5\}}$, $H_{\{g_2,g_6,g_7\}}$ is central. If the first possibility holds then $|S| \leq 7$. If the second possibility holds then $|S| \leq 7$ as well.

For the fifth case, we observe that $H_{\{g_i,g_6\}}$ is geometric for $i \leq 5$, and that $\{g_1\}$, $\{g_2\}, \ldots, \{g_6\}$ are mutually disjoint sets of $S \setminus \{g_6\}$. $H_{\{g_6\}}$ is not geometric, so by Proposition 4.3.4 it must that either $\mu'(H_{\{g_i,g_6\}} \cap H_{\{g_j,g_6\}}) \leq 3$ or $\bigcap_{i=1}^{5} H_{\{g_i,g_6\}} \leq Z(SL_3(q))$. In either case $|S| \leq 6$. This completes the study of the case that precisely one $H_{\{g_i\}}$ is geometric.

Case: No $H_{\{g_i\}}$ is geometric

Thus, each $H_{\{g_i\}}$ lies in a subfield subgroup. As in the proof of Theorem 3.2.2, let $A_1, \ldots, A_{\pi(r)}$ be the isomorphism classes of the maximal subfield subgroups of $SL_3(q)$. For each $H_{\{g_i\}}$ let L_i be the smallest maximal subfield subgroup that contains $H_{\{g_i\}}$, and associate $H_{\{g_i\}}$ with the A_j that contains L_i. So if $H_{\{g_i\}}$, $H_{\{g_j\}}$ are associated with the same A_k, then $H_{\{g_i,g_j\}}$ is geometric.

If $|S| \leq \pi(r) + 4$ then we are satisfied, so suppose that $|S| \geq \pi(r) + 5$. Then all the genuinely distinct possibilities for memberships of the A_i are listed here:

1. $H_{\{g_i\}}$, $H_{\{g_{i+1}\}}$ are associated with some A_j for $i = 1, 3, 5, 7, 9$.

2. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are associated with A_1, whilst $H_{\{g_i\}}$, $H_{\{g_{i+1}\}}$ are associated with some $A_j \neq A_1$ for $i = 4, 6, 8$.

3. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$ are associated with A_1; $H_{\{g_4\}}$, $H_{\{g_5\}}$, $H_{\{g_6\}}$ are associated with A_2, and $H_{\{g_7\}}$, $H_{\{g_8\}}$ are associated with A_3.

4. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ are associated with A_1; $H_{\{g_5\}}$, $H_{\{g_6\}}$ are associated with A_2 and $H_{\{g_7\}}$, $H_{\{g_8\}}$ are associated with A_3.

5. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$ are associated with A_1 and $H_{\{g_5\}}$, $H_{\{g_6\}}$, $H_{\{g_7\}}$ are associated with A_2.

6. $H_{\{g_1\}}$, $H_{\{g_2\}}$, $H_{\{g_3\}}$, $H_{\{g_4\}}$, $H_{\{g_5\}}$ are associated with A_1 and $H_{\{g_6\}}$, $H_{\{g_7\}}$ are associated with A_2.

7. $H_{\{g_i\}}$ is associated with A_1 for $i \leq 6$.

In the first case, $H_{\{g_i,g_{i+1}\}}$ is geometric for $i = 1, 3, 5, 7, 9$. Notice that the subsets $\{g_i, g_{i+1}\} \subseteq S$ for $i = 1, 3, 5, 7, 9$ are mutually disjoint, so by Proposition 4.3.4 either $\mu'(H_{\{g_i,g_{i+1}\}} \cap H_{\{g_j,g_{j+1}\}}) \leq 3$ for some i, j; or $\bigcap_{i=1,3,5,7,9} H_{\{g_i,g_{i+1}\}} \leq Z(SL_3(q))$. If the first possibility holds then $|S| \leq 7$, If the second possibility holds the there can be no $g_{11} \in S$, as this will then lie in $Z(SL_3(q))$. So $|S| \leq 10$ here.

In the second case, $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_6,g_7\}}$, $H_{\{g_1,g_8,g_9\}}$ are geometric. Observe that the subsets $\{g_2\}$, $\{g_3\}$ and $\{g_i, g_{i+1}\}$ for $i = 4, 6, 8$ are mutually disjoint subsets of $S \setminus \{g_1\}$. $H_{\{g_1\}}$ is not geometric, so by Proposition 4.3.4 either two of $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_6,g_7\}}$, $H_{\{g_1,g_8,g_9\}}$ have an intersection containing independent sets of size at most 3, or the intersection of all $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_6,g_7\}}$, $H_{\{g_1,g_8,g_9\}}$ is central. The first possibility implies that $|S| \leq 8$. The second possibility implies that $|S| \leq 9$.

In the third case $H_{\{g_1,g_2,g_4\}}$, $H_{\{g_1,g_3,g_4\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_4,g_6\}}$, $H_{\{g_1,g_4,g_7,g_8\}}$ are geometric. Note that $\{g_2\}$, $\{g_3\}$, $\{g_5\}$, $\{g_6\}$, $\{g_7, g_8\}$ are mutually disjoint subsets of $S \setminus \{g_1, g_4\}$. By Proposition 4.3.4 then , either $H_{\{g_1,g_4\}}$ is geometric; or two of $H_{\{g_1,g_2,g_4\}}$, $H_{\{g_1,g_3,g_4\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_4,g_6\}}$, $H_{\{g_1,g_4,g_7,g_8\}}$ have an intersection containing independent sets of size at most 3; or the intersection of all $H_{\{g_1,g_2,g_4\}}$, $H_{\{g_1,g_3,g_4\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_4,g_6\}}$, $H_{\{g_1,g_4,g_7,g_8\}}$ is central. If the second possibility holds then $|S| \leq 8$. If the third possibility holds then $|S| \leq 8$ as well. So suppose that $H_{\{g_1,g_4\}}$ is geometric. Note that now $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5,g_6\}}$, $H_{\{g_1,g_7,g_8\}}$ are geometric. We use the fact that $\{g_2\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5, g_6\}$, $\{g_7, g_8\}$ are mutually disjoint subsets of $S \setminus \{g_1\}$. $H_{\{g_1\}}$ is not geometric so by Proposition 4.3.4 it must be that either two of $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5,g_6\}}$, $H_{\{g_1,g_7,g_8\}}$ have

an intersection containing independent sets of size at most 3; or the intersection of all $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5,g_6\}}$, $H_{\{g_1,g_7,g_8\}}$ is central. If the first possibility holds then $|S| \leq 8$. If the second possibility holds then $|S| \leq 8$ again.

In the fourth case, $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5,g_6\}}$, $H_{\{g_1,g_7,g_8\}}$ are geometric, and generate $H_{\{g_1\}}$. But we have already covered this case.

In the fifth case, we have that $H_{\{g_1,g_2,g_5\}}$, $H_{\{g_1,g_3,g_5\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_5,g_6\}}$, $H_{\{g_1,g_5,g_7\}}$ are geometric. Now, $\{g_2\}$, $\{g_3\}$, $\{g_4\}$, $\{g_6\}$, $\{g_7\}$ are mutually disjoint subsets of $S \setminus \{g_1, g_5\}$. By Proposition 4.3.4 then, either $H_{\{g_1,g_5\}}$ is geometric; two of $H_{\{g_1,g_2,g_5\}}$, $H_{\{g_1,g_3,g_5\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_5,g_6\}}$, $H_{\{g_1,g_5,g_7\}}$ have an intersection containing independent sets of size at most 3; or the intersection of all $H_{\{g_1,g_2,g_5\}}$, $H_{\{g_1,g_3,g_5\}}$, $H_{\{g_1,g_4,g_5\}}$, $H_{\{g_1,g_5,g_6\}}$, $H_{\{g_1,g_5,g_7\}}$ is central. If the second possibility holds then $|S| \leq 7$. If the second possibility holds then $|S| \leq 7$ as well. So suppose that $H_{\{g_1,g_5\}}$ is geometric. Then $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5\}}$, $H_{\{g_1,g_7,g_8\}}$ are all geometric. Recall that $H_{\{g_1\}}$ is not geometric. We use the fact that $\{g_2\}$, $\{g_3\}$, $\{g_4\}$, $\{g_5\}$, $\{g_6, g_7\}$ are mutually disjoint subsets of $S \setminus \{g_1\}$ to conclude, by Proposition 4.3.4, that either two of $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5\}}$, $H_{\{g_1,g_7,g_8\}}$ have an intersection containing independent sets of size at most 3; or the intersection of all $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5\}}$, $H_{\{g_1,g_7,g_8\}}$ is central. If the first possibility holds then $|S| \leq 7$. If the second possibility holds then $|S| \leq 8$.

In the sixth case, we have that $H_{\{g_1,g_2\}}$, $H_{\{g_1,g_3\}}$, $H_{\{g_1,g_4\}}$, $H_{\{g_1,g_5\}}$, $H_{\{g_1,g_7,g_8\}}$ are geometric and generate $H_{\{g_1\}}$. But we have covered this case.

In the seventh case, we have that $H_{\{g_i,g_6\}}$ is geometric for $i \leq 5$. Now the subsets $\{g_i\}$, $2 \leq i \leq 6$ are mutually disjoint subsets of $S \setminus \{g_6\}$. $H_{\{g_6\}}$ is not geometric, so we may apply Proposition 4.3.4 to this situation to get that either $\mu'(H_{\{g_i,g_6\}} \cap H_{\{g_j,g_6\}}) \leq 3$ for some i, j; or $\bigcap_{i \leq 5} H_{\{g_i,g_6\}} \leq Z(SL_3(q))$. If the first possibility holds then $|S| \leq 6$. If the second possibility holds then $|S| \leq 6$ again.

This completes the proof. □

4.5 Conclusion

In this chapter, we have shown

Theorem 4.5.1. *Let q be the power of an odd prime. Then*

1. $\mu(SL_3(q)) \leq 6$ *if q is a prime.*

2. $\mu(SL_3(q)) \leq \max\{10, \pi(r) + 6\}$ *if $q = p^r$ for an odd prime p.*

We remark here that we do not know if the bounds given are tight. More work would be required to check, for instance, whether there is a minimax set of size $\pi(r) + 6$ in $SL_3(p^r)$, where $\pi(r) + 5$ of these generators lie in $SU_3(p^r)$.

CHAPTER 5

MINIMAX SETS IN GROUPS WITH NORMAL, ABELIAN SUBGROUPS

Cameron and Cara in [3] gave a short proof giving an upper bound for $\mu(G)$ when G contained a normal, abelian subgroup. Given a group A acting on another group G, they defined $\mu'_A(G)$ to be the size of a largest subset S of G such that no $g \in S$ lay in the group generated by the A-images of $S \setminus \{g\}$. The result they proved was this:

Lemma 5.0.1 (Cameron, Cara)**.** *Suppose G is a finite group with $N \trianglelefteq G$ an abelian subgroup of G. Then $\mu(G) \leq \mu(G/N) + \mu'_G(N)$.*

We wish to strengthen Cameron and Cara's result: Given a normal, abelian subgroup N of G, we wish to prove a precise statement for $\mu(G)$ in terms of $\mu(G/N)$ and the action of G on N. This is the main goal of this chapter.

5.1 Abelian Normal Subgroups

Let G be a finite group. Let $K \leq N \leq G$ such that $K, N \trianglelefteq G$.

We have that a subgroup $M \leq N/K$ is normal in G/K if and only if the full pre-image $M^* \leq N$ of M is normal in G. So given any $M \leq N/K$ that is normal in G/K, it makes sense to talk of M as being G-*invariant*, even though it is not a subgroup of G.

Definition 5.1.1. Let $N \trianglelefteq G$ and suppose that there is some $K \lneqq N$ such that $K \trianglelefteq G$

and $G/K = N/K : H$ for some non-trivial $H \leq G/K$. Then N is said to be *loosely entangled in* G and K is said to be a *releasing group for* N.

Observe that if N is abelian then N decomposes into a direct product $N_1 \times N_2 \times \ldots \times N_a$ where each N_i is G-invariant and no longer decomposition into G-invariant subgroups is possible. Note that it could be that $a = 1$. Any factor group N/K also has a longest such decomposition. Given a factor group N/K, let $a(N/K)$ be the number of factors in a longest decomposition of N/K into G-invariant subgroups.

Definition 5.1.2. Suppose $N \trianglelefteq G$ is abelian. If N is loosely entangled in G then let

$$R(G, N) := \max\{a(N/K) | K \text{ is a releasing group for } N\},$$

otherwise let $R(G, N) := 0$.

There are three lemmas and one proposition that will prove useful for proving the main proposition. We treat the first lemma as a standard result, and so do not prove it.

Lemma 5.1.1. *Suppose that* $N = \langle N_1, \ldots, N_r \rangle$ *for subgroups* $N_1, \ldots, N_r \leq N$ *where* $r \geq 2$. *Then* $N = N_1 \times \ldots \times N_r \Leftrightarrow N = N_i \times \langle N_j | j \neq i \rangle$ *for all* i.

Lemma 5.1.2. *Suppose* $G = (N_1 \times N_2 \times \ldots \times N_r) : H$ *where each* N_i *is abelian and* G*-invariant. Suppose further that there is some* $K \leq N_1$ *such that* $K \trianglelefteq G$. *Then* $G/K = (N_1/K \times N_2 \times \ldots \times N_r) : H$.

Proof. Let $N := N_1 \times \ldots \times N_r$. So $G = N : H$ and $N \cap H = \{1\}$. We begin by arguing that $G/K \cong (N/K) : H$. Since $K \leq N_1$, it must be that $K \leq N$. However, since $N \cap H = \{1\}$ we have that $K \cap H = \{1\}$. Hence H is isomorphic to its image in G/K. The image of H in G/K must normalise N/K. Also, the image of H in G/K has a trivial intersection with the image of H. Hence $G/K \cong N/K : H$. So if we show that $N/K \cong N_1/K \times N_2 \times \ldots \times N_r$ then we are done.

Let $N_{2\ldots r} := N_2 \times \ldots \times N_r$. So $N = N_1 \times N_{2\ldots r}$ and $N_1 \cap N_{2\ldots r} = \{1\}$. Now $K \leq N_1$ so $K \cap N_{2\ldots r} = \{1\}$. Therefore $N_{2\ldots r}$ is isomorphic to its image in N/K. Observe that since

$K \leq N_1$, the image of N_1 in N/K is isomorphic to N_1/K. Now, the image of $N_{2\ldots r}$ in N/K must commute with the image of N_1. Also, the image of $N_{2\ldots r}$ must have a trivial intersection with the image of N_1. Hence $N/K \cong N_1/K \times N_2 \times \ldots \times N_r$, which is what we wanted. □

Lemma 5.1.3. *Let G be a finite group containing an $N \trianglelefteq G$ such that $N \lneqq G$. If G/N contains an independent generating set S' then G contains an independent generating set S such that $|S| \geq |S'|$.*

Proof. Let $S' =: \{g'_1, \ldots, g'_m\}$ be an independent generating set for G/N. For each i, let $Ng_i \subseteq G$ be the coset of N that is mapped to $g'_i \in G/N$. So Ng_i is the full pre-image of g'_i under the natural map $\phi : G \to G/N$. Let $T := \bigcup_{i=1}^{m} Ng_i$. Since T contains the full pre-images of all $g'_i \in S'$, and since S' generates G/N, it must be that the elements of T generate all cosets of N in G. But then T generates every element of G, and so T is a a generating set for G. Therefore, T must contain an independent generating set S for G. We seek a lower bound for $|S|$.

Suppose $|S| \leq |S'| - 1$. Note that for each $t \in T$, $\phi(t) \in S'$. Since $S \subseteq T$, it must be that $\phi(S) \subseteq S'$. As $|S| < |S'|$, the image of S in S' must be a proper subset of S'. $\langle S \rangle = G$, so we have that the image of S in G/N generates G/N. Hence a proper subset of S' generates G/N, which contradicts the independence of S'. Therefore, $|S| \geq |S'|$. □

Proposition 5.1.1. *Suppose that $N \lneqq G$ such that $N \trianglelefteq G$ and N is abelian. Then N is loosely entangled in G if and only if $N \leq \Phi(G)$.*

Proof. Suppose $N \leq \Phi(G)$. We wish to argue that N is not loosely entangled in G. So suppose that N has a releasing subgroup K and that $G/K = N/K : H$ for some $H \leq G/K$. Let H' be the full pre-image of H in G. H is a proper subgroup of G/K, so H' is a proper subgroup of G. Therefore there must be some maximal subgroup $M \leq G$ such that $H' \leq M$. Now, $N \leq \Phi(G) \leq M$, so both N/K and H lie in the image of M in G/K. Therefore, the image of M is $N/K : H = G/K$. Take any $g \in G \setminus M$. The image of g in G/K must lie in the image of M, so there is some $m \in M$ and $k \in K$ such that

$g = km$. But $k \in K \leq N \leq M$, so $g = km \in M$, a contradiction. So N is not loosely entangled in G.

Suppose $N \not\leq \Phi(G)$. We argue that N is loosely entangled in G. Since $N \not\leq \Phi(G)$, there must be some maximal $M \leq G$ such that $N \not\leq M$. Note that $G = \langle M, N \rangle$. Let $K := N \cap M$. We wish to show that K is a releasing group for N, which immediately implies that N is loosely entangled in G. Observe that $K \trianglelefteq M$ since $N \trianglelefteq G$. Also, $K \trianglelefteq N$ since N is abelian. Hence $K \trianglelefteq \langle M, N \rangle = G$. Now, if $K = N$ then $N = K \leq M$, which is not the case. So $K \neq N$. Now, as $K \lneqq N$, N/K is non-trivial in G/K. Also, if $M = K$ then $M = K \leq N$, which implies that $M = N$. So $K \neq M$. As $K \lneqq M$, M/K is non-trivial in G/K.

Let $g' \in N/K \cap M/K$ and take any pre-image g of g' in G. Then $g \in N \cap M = K$. So $g' = 1$ and $N/K \cap M/K = \{1\}$. Given that N, M generate G, their images $N/K, M/K$ must generate G/K. Since $N \trianglelefteq G$, we have $N/K \trianglelefteq G/K$. So we have that $G/K = N/K : M/K$ and N is loosely entangled in G. □

We may now state and prove the main proposition of this section.

Proposition 5.1.2. *If $N \lneqq G$ with $N \trianglelefteq G$ and N abelian, then $\mu(G) = \mu(G/N) + R(G, N)$.*

Proof. We deal with two cases: when N is loosely entangled in G, and when N is not loosely entangled in G.

Case 1: N is not loosely entangled in G.

In this case $R(G, N) = 0$ and we have to establish that $\mu(G) = \mu(G/N) + R(G, N) = \mu(G/N)$. By Proposition 5.1.1 we know that $N \leq \Phi(G)$. Hence $\mu(G) = \mu(G/N)$ by Proposition 1.1.1.

Case 2: N is loosely entangled in G.

In this case $R(G, N) > 0$, and we have to establish that $\mu(G) = \mu(G/N) + R(G, N)$. We begin by establishing that $\mu(G) \leq \mu(G/N) + R(G, N)$. Let $S = \{g_1, \ldots, g_n\}$ be a minimax set for G. Let $S' = \{g_1, \ldots, g_n\}$ be the multiset of images of the elements of S

in G/N. Suppose that S' is independent in G/N. Then

$$\mu(G) = |S| = |S'| \leq \mu(G/N) \leq \mu(G/N) + R(G, N).$$

So suppose that S' is not independent. Since $N \lneqq G$, and S is a minimax set for G, there must be at least one $g_i \in S$ that has non-trivial image in G/N. We may suppose that there is some $r \geq 1$ such that $B = \{g_{r+1}, \ldots, g_n\} \subseteq S$ and the image of B in G/N is an independent generating set for G/N. So the elements of B generate the action of G/N on N, and $|B| \leq \mu(G/N)$. We now seek to produce a releasing subgroup K for N such that $N/K = N_1 \times \ldots \times N_r$ is a decomposition of N/K into G-invariant subspaces. We begin by producing a suitable K, and then continue by producing candidate subgroups of N whose images in N/K will be $N_1, \ldots, N_r$.

A candidate subgroup K for a releasing group for N:
Recall that r was such that $B = \{g_{r+1}, \ldots, g_n\}$. Let

$$K = \left(\bigcap_{i \leq r} \langle S \setminus \{g_i\} \rangle \right) \cap N.$$

We show that $K \lneqq N$ and $K \trianglelefteq G$. To see that $K \lneqq N$, suppose that $K = N$. Since B generates the action of G/N on N, there must be some $\omega_1 \in \langle B \rangle$ such that $g_1\omega_1 \in N$. Then $g_1\omega_1 \in N = K \leq \langle S \setminus \{g_1\} \rangle$. So there is some $k \in \langle S \setminus \{g_1\} \rangle$ such that $g_1\omega_1 = k$. But $\omega_1 \in \langle B \rangle \leq \langle S \setminus \{g_1\} \rangle$ as well, so $g_1 = k\omega_1^{-1} \in \langle S \setminus \{g_1\} \rangle$, which contradicts the independence of S. So $K \lneqq N$.

We now argue that $K \trianglelefteq G$. For each $i \leq r$, $B \subseteq \langle S \setminus \{g_i\} \rangle$ so B normalises $\left(\bigcap_{i \leq r} \langle S \setminus \{g_i\} \rangle \right) \cap N$. N is abelian, and so must normalise K, since $K \leq N$. But then

$$K = \left(\bigcap_{i \leq r} \langle S \setminus \{g_i\} \rangle \right) \cap N \trianglelefteq \langle N, B \rangle = G.$$

This sets up K as a candidate for a releasing subgroup of N. We now argue that K

is such a subgroup.

K is a releasing subgroup for N:

Here we wish to show that that $G/K = N/K : H$ for some $H \leq G/K$. Consider the image H of $\langle B \rangle$ in G/K. Indeed, suppose that $z' \in (N/K) \cap H$. Let z be a pre-image of z' in G. So z must lie in the pre-image of H and in the pre-image of N/K. So $z \in K\langle B \rangle$ and $z \in N$. So there is some $k \in K$, $g \in \langle B \rangle$ and $h \in N$ such that $z = kg = h$. Now $k \in K \leq N$. So $g = k^{-1}h \in N$ and $g \in \langle B \rangle \leq \bigcap_{i \leq r} \langle S \setminus \{g_i\} \rangle$. Therefore $g \in \left(\bigcap_{i \leq r} \langle S \setminus \{g_i\} \rangle\right) \cap N = K$. Therefore $z = kg \in K$. So z', the image of z in G/K, is trivial. Therefore $H \cap (N/K) = \{1\}$. N/K is clearly normal in G/K. Also, $G = \langle N, B \rangle$, so the images of N and $\langle B \rangle$ in G/K generate G/K. Altogether then, $G/K = N/K : H$. Thus, K is a releasing group for N. We now find r subgroups of N whose images in N/K provide a suitable decomposition of N/K.

Candidate subgroups of N that provide $N_1, \ldots, N_r \leq N/K$:

For each $i \leq r$, define

$$M_i := \langle g_i, B \rangle \cap N.$$

These will eventually provide the N_1, ..., $N_r \leq N/K$. We establish some properties of the M_i - namely we establish that each M_i is non-trivial, that each $M_i \trianglelefteq G$ and that the M_i generate N. Since B generates the action of G on N, there must be some $\omega_i \in \langle B \rangle \leq \langle g_i, B \rangle$ such that $g_i\omega_i \in N$. Take

$$z_i := g_i\omega_i \in \langle g_i, B \rangle \cap N = M_i.$$

Note that if any $z_i = 1$ then $g_i = \omega_i^{-1} \in \langle B \rangle \leq \langle S \setminus \{g_i\} \rangle$, which contradicts the independence of S. So each z_i (and hence each M_i) is non-trivial.

The elements of B must normalise each M_i, since each $M_i = \langle g_i, B \rangle \cap N$ is normal in $\langle g_i, B \rangle$. Also, N is abelian so N must normalise each $M_i \leq N$. Therefore each

$M_i \trianglelefteq \langle N, B\rangle = G$. This means that the images of the M_i in any factor group N/K will be G-invariant.

We now wish to argue that the M_i generate N. Observe that

$$\begin{aligned}\langle\langle M_1, \ldots, M_r\rangle, \langle B\rangle\rangle &\geq \langle z_1, \ldots, z_r, B\rangle \\ &= \langle g_1\omega_1, \ldots, g_r\omega_r, B\rangle \\ &= \langle g_1, \ldots, g_n\rangle = G.\end{aligned}$$

Thus, G is generated by $\langle M_1, \ldots, M_r\rangle$ and $\langle B\rangle$. Furthermore, since each $M_i \trianglelefteq G$, it must be that $\langle M_1, \ldots, M_r\rangle \trianglelefteq G$. So for each $g \in G$ there is $\xi \in \langle M_1, \ldots, M_r\rangle$ and $\rho \in \langle B\rangle$ such that $g = \xi\rho$. Now, suppose $g \in N$. Then $g = \xi\rho$ for some $\xi \in \langle M_1, \ldots, M_r\rangle$, $\rho \in \langle B\rangle$. But $\xi \in N$ as well, so $\rho = \xi^{-1}g \in N$. Therefore $\rho \in \langle B\rangle \cap N \leq M_i$ for all i. So $g \in \langle M_1, \ldots, M_r\rangle$ and the M_i generate N. Therefore we have established the three desired properties for the M_i. So we now have r subgroups of N such that their images in N/K are G-invariant and generate N/K. We now examine the images of the M_i in N/K. We must show that the images are non-trivial and that N/K decomposes into a direct product of these images.

The images of the M_i in N/K:

Since B generates the action of G/N on N, for each $i \leq r$ there is some $\omega_i \in \langle B\rangle$ such that $g_i\omega_i \in N$. For each $i \leq r$, $g_i\omega_i \in \langle g_i, B\rangle \cap N = M_i$. If we show that each $g_i\omega_i \notin K$ then we will have shown that each M_i has a non-trivial image in N/K. So suppose that some $g_i\omega_i \in K$. Then for some $k \in K$, $g_i\omega_i = k \in K \leq \langle S \setminus \{g_i\}\rangle$. But $\omega_i \in \langle B\rangle \leq \langle S \setminus \{g_i\}\rangle$ so $g_i = k\omega_i^{-1} \in \langle S \setminus \{g_i\}\rangle$, which contradicts the independence of S. Therefore no $g_i\omega_i \in K$ and we have what we want.

Let $N_i \leq N/K$ be the image of M_i in N/K. To see that $N/K = N_1 \times \ldots \times N_r$ it is sufficient, using Lemma 5.1.1, to show that $N/K = N_i \times \langle N_1, \ldots, N_{i-1}, N_{i+1}, \ldots, N_r\rangle$ for each i. But since N/K is abelian, if we show that $N_i \cap \langle N_1, \ldots, N_{i-1}, N_{i+1}, \ldots, N_r\rangle = \{1\}$

for any $i \leq r$ then we will have what we want.

To this end, we show that the pre-image of $N_i \cap \langle N_1, \ldots, N_{i-1}, N_{i+1}, \ldots, N_r \rangle$ lies in K. That is, we show that $KM_i \cap (K\langle M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_r \rangle) \leq K$. If we show that any $h \in KM_i \cap (K\langle M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_r \rangle)$ lies in K then this is sufficient. Since h must lie in N, it suffices to show that $h \in \langle S \setminus \{g_j\} \rangle$ for all $j \leq r$.

Suppose that $j \leq r$ and that $j \neq i$ (Recall that i is the index that picks out KM_i in $KM_i \cap (K\langle M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_r \rangle)$). Then we regard h as an element of KM_i. $K \leq \langle S \setminus \{g_j\} \rangle$ by construction. But also, since each element of $\{g_i\} \cup B$ lies in $S \setminus \{g_j\}$, we have that $M_i = \langle g_i, B \rangle \cap N \leq \langle S \setminus \{g_j\} \rangle$ by construction. So h, as an element of KM_i, must lie in $\langle S \setminus \{g_j\} \rangle$.

Now suppose that $j = i$. Then we use the fact that $h \in K\langle M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_r \rangle$. Once again, $K \leq \langle S \setminus \{g_j\} \rangle$ by construction. Also, for all $k \neq j$, we have $\{g_k\} \cup B \subseteq S \setminus \{g_j\}$. Therefore $M_k \leq \langle S \setminus \{g_k\} \rangle$ for each $k \leq r$, $k \neq j$. But this in turn implies that $h \in K\langle M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_r \rangle \leq \langle S \setminus \{g_j\} \rangle$. Altogether then, for any $j \leq r$ we have that $h \in \langle S \setminus \{g_j\} \rangle$, which gives the desired result. Hence $N_i \cap \langle N_1, \ldots, N_{i-1}, N_{i+1}, \ldots, N_r \rangle = \{1\}$ and N/K is a direct product of the N_i by Lemma 5.1.1.

Thus, we have produced a releasing group K for N such that N/K decomposes into a direct product of r subgroups, each G-invariant. Altogether then, we have shown that $r \leq R(G, N)$. This means that

$$\mu(G) = |S| = |B| + r \leq \mu(G/N) + R(G, N).$$

We now have to establish that $\mu(G) \geq \mu(G/N) + R(G, N)$. N is loosely entangled in G, so there must be a releasing subgroup K for N that provides $R(G, N)$. That is, $G/K = (N_1 \times \ldots \times N_r) : H$ where $N/K = N_1 \times \ldots \times N_r$ is a decomposition into G-invariant subgroups of N/K and $r = R(G, N)$. Since $H \cap (N/K) = \{1\}$, H is isomorphic to its image in $\frac{G/K}{N/K} \cong G/N$. In this case, the image of H must be all of G/N, so $H \cong G/N$. Therefore $\mu(H) = \mu(G/N)$. Let $B = \{g_1, \ldots, g_m\}$ be a minimax set for H. We make B

part of a larger independent generating set for G/K. To begin with, we seek to find, for each N_i, a $z_i \in N_i$ such that $\langle z_i, B\rangle \cap N = N_i$.

Generation of the N_i:

It is necessary first step that we show for any $A \subseteq N_i$, $\langle A, B\rangle \cap N \leq N_i$. So take any N_i and let $A = \{a_1, \ldots, a_m\} \subseteq N_i$. $\langle A, B\rangle \cap N \leq \langle N_i, B\rangle \cap N$, so if we show that $\langle N_i, B\rangle \cap N = N_i$ then we are done. Let $z \in \langle N_i, B\rangle \cap N$. N_i is normal in G/K so we have $\xi \in N_i, \rho \in \langle B\rangle$ such that $z = \xi\rho$. $z, \xi \in N/K$ so $\rho = \xi^{-1}z \in N/K$. Hence $\rho \in (N/K) \cap \langle B\rangle = (N/K) \cap H = \{1\}$. Therefore $z = \xi \in N_i$, which proves that $\langle A, B\rangle \cap N \leq \langle N_i, B\rangle \cap N = N_i$.

We now want to prove that for each N_i there is a $z_i \in N_i$ such that $\langle z_i, B\rangle \cap N = N_i$. Suppose not, then. Without loss of generality, suppose that there is no $z \in N_1$ such that $\langle z, B\rangle \cap N = N_1$. Let $A = \{z_1, \ldots, z_m\} \subseteq N_1$ be a smallest subset of N_1 such that $\langle A, B\rangle \cap N = N_1$. By assumption $|A| > 1$ so $\{\{z_1\}, \{z_2, \ldots, z_m\}\}$ is a non-trivial partition of A. Let $M_1 = \langle z_1, B\rangle \cap N$ and $M_2 = \langle z_2, \ldots, z_m, B\rangle \cap N$. Each element of B must normalise both M_1, M_2. N/K is abelian so N/K normalises M_1, $M_2 \leq N/K$. Hence M_1, M_2 are normal in $G/K = \langle N/K, B\rangle$. Suppose $z_1 \in M_2$. Then

$$N_1 = \langle z_1, \ldots, z_m, B\rangle \cap N = \langle z_2, \ldots, z_m, B\rangle \cap N$$

and A has a proper subgroup A' such that $\langle A', B\rangle \cap N = N_1$. But this contradicts the minimality of A. So $z_1 \notin M_2$ and M_2 is a proper subgroup of N_1. Similarly, if any $z_i \in M_1, i \geq 2$ then $N_1 = \langle z_1, \ldots, z_m, B\rangle \cap N = \langle z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_m, B\rangle \cap N$ which contradicts the minimality of A. So no $z_i \in A$ lies in $M_1 \cap M_2$. Therefore we have that $M_1 \not\leq M_2, M_2 \not\leq M_1$ and $M_1 \cap M_2 \lneqq M_1, M_2$.

Let $L := M_1 \cap M_2$. Since M_1, M_2 are normal in G/K it must be that $L = M_1 \cap M_2$ is normal in G/K. Given that $M_1, M_2 \leq N_1$ we have that $L \leq N_1$. Therefore by Lemma 5.1.2 we have that $\frac{G/K}{L} = (N_1/L \times N_2 \times \ldots \times N_r) : H$. We now want to argue that N_1/L

decomposes into a direct product of the images of M_1, M_2. Let N_1^*, N_1^{**} in N_1/L be the images of M_1, M_2 respectively. Since $L = M_1 \cap M_2 \leq M_1$ we have that the full pre-image of N_1^* in N_1 is M_1. Similarly, since $L = M_1 \cap M_2 \leq M_2$, the full pre-image of N_1^{**} in N_1 is M_2. But now suppose that $g \in N_1^* \cap N_1^{**}$. Any pre-image of g must now lie in both M_1, M_2. Hence any pre-image g' of g lies in $M_1 \cap M_2 = L$. But the image of any such g' in N_1/L is 1, so $g = 1$. So $N_1^* \cap N_1^{**} = \{1\}$ and the subgroups N_1^*, N_1^{**} must form a direct product $N_1^* \times N_1^{**}$ within the abelian group N_1/L. We want to show that $N_1^* \times N_1^{**} = N_1/L$. We can do this if we show that $N_1/L = \langle N_1^*, N_1^{**} \rangle$. But given that N_1^*, N_1^{**} are images of M_1, M_2 it is sufficient to show that M_1, M_2 generate N_1.

We now argue that M_1, M_2 generate N_1. By assumption, $N_1 = \langle z_1, \ldots, z_m, B \rangle \cap N$. Let $\gamma \in N_1$ be a word in the alphabet $\{z_1, \ldots, z_m\} \cup B$. We now show that we can rewrite γ as a word in elements of $M_1 \cup M_2$: Take γ as it was initially defined. We can characterise γ as the string $\alpha_1 z_{i_1} \alpha_2 z_{i_2} \alpha_3 \ldots \alpha_s z_{i_s} \alpha_{s+1}$ where each $z_{i_j} \in \{z_1, \ldots, z_m\}$ and each α_j is a (possibly trivial) word in the alphabet B. Now, we do not change the element γ if we insert representations of the identity into this string. For each $j \leq s$, insert the string $\alpha_j^{-1} \alpha_{j-1}^{-1} \ldots \alpha_1^{-1} \alpha_1 \ldots \alpha_{j-1} \alpha_j$ after the z_{i_j} symbol in γ. Then

$$\begin{aligned} \gamma &= \alpha_1 z_{i_1} (\alpha_1^{-1} \alpha_1) \alpha_2 z_{i_2} \ldots (\alpha_{s-1}^{-1} \ldots \alpha_1^{-1} \alpha_1 \ldots \alpha_{s-1}) \alpha_s z_{i_s} (\alpha_s^{-1} \ldots \alpha_1 \alpha_1 \ldots \alpha_s) \alpha_{s+1} \\ &= (\alpha_1 z_{i_1} \alpha_1^{-1}) \ldots (\alpha_1 \ldots \alpha_j z_{i_j} \alpha_j^{-1} \ldots \alpha_1^{-1}) \ldots (\alpha_1 \ldots \alpha_s z_{i_s} \alpha_s^{-1} \ldots \alpha_1^{-1}) (\alpha_1 \ldots \alpha_s \alpha_{s+1}) \end{aligned}$$

after re-bracketing. So we have broken our rewritten γ into strings of the form $\beta_j z_{i_j} \beta_j^{-1}$, where $j \leq s$ and $\beta_j := \alpha_1 \ldots \alpha_j \in \langle B \rangle$, together with a string of the form $\alpha_1 \ldots \alpha_{s+1}$. Now, note that each z_{i_j} must lie in one of M_1, M_2, by definition of the M_i. Also, for each j, since $\beta_j \in \langle B \rangle$ normalises both M_1, M_2, it must be that $\beta_j z_{i_j} \beta_j^{-1}$ lies in one of M_1, M_2. But now consider the final part of our rewritten γ: namely the string $\alpha_1 \ldots \alpha_{s+1}$, which lies in $\langle B \rangle$. Given that $\gamma \in N_1$ and each $\beta_j z_{i_j} \beta^{-1} \in N_1$, we have that

$$\alpha_1 \ldots \alpha_{s+1} = (\beta_s z_{i_s}^{-1} \beta_s^{-1}) \ldots (\beta_1 z_{i_1}^{-1} \beta_1^{-1}) \gamma \in N_1 \leq N/K$$

as well. So $\alpha_1 \ldots \alpha_{s+1} \in \langle B \rangle \cap N/K = \{1\} \leq M_1, M_2$. Therefore we can write γ as a word in elements of $M_1 \cup M_2$. Therefore M_1, M_2 generate N_1.

Hence, the image of N_1 in $\frac{G/K}{L}$ decomposes into a direct product of non-trivial, G-invariant subgroups N_1^*, N_1^{**}. Thus, $\frac{G/K}{L} \cong ((N_1^* \times N_1^{**}) \times N_2 \times \ldots \times N_r) : H$.

The full pre-image $K.L$ of L in G must be a normal subgroup of N. So

$$\frac{G}{K.L} \cong \frac{G/K}{L} \cong ((N_1^* \times N_1^{**}) \times N_2 \times \ldots \times N_r) : H$$

by the Third Isomorphism Theorem. Therefore we have $K.L$ a releasing subgroup of N with $N/(K.L)$ decomposing into at least $r+1$ G-invariant subgroups. But this contradicts the maximality of r. So $A \subseteq N_1$ cannot be the smallest subset such that $N_1 = \langle A, B \rangle \cap N$. Therefore for any N_i there is some $z_i \in N_i$ such that $N_i = \langle z_i, B \rangle \cap N$.

An independent generating set for G/K:

Therefore, we select a set $\{z_1, \ldots, z_r\} \subseteq N/K$ such that each $z_i \in N_i$ and each $N_i = \langle z_i, B \rangle \cap N$. Let $S' = \{z_1, \ldots, z_r\} \cup B$. We now argue that S' is an independent generating set for G/K. By the choice of the z_i, S' must generate each N_i. Therefore S' generates $N/K = N_1 \times \ldots \times N_r$. Since $\langle B \rangle = H$, it must be that $\langle S' \rangle = N/K : H = G/K$. We now argue that S' is independent.

Given any z_i,

$$\begin{aligned} \langle S' \setminus \{z_i\} \rangle &\leq \langle N_1, \ldots, N_{i-1}, N_{i+1}, \ldots, N_r, H \rangle \\ &= (N_1 \times \ldots \times N_{i-1} \times N_{i+1} \times \ldots \times N_r) : H, \end{aligned}$$

which is a proper subgroup of G/K. So take any $g \in B$. Recall that B was a minimax set for H and that H is isomorphic to its image in G/N. In fact $H \cong G/N$. Suppose that $S \setminus \{g\}$ generates G/K. But now each of the remaining elements of B in $S \setminus \{g\}$ have non-trivial image in G/N whilst each z_i is mapped to 1 in G/N. Therefore the images of $B \setminus \{g\}$ in G/N generate G/N. The isomorphism $G/N \cong H$ ensures that $\langle B \setminus \{g\} \rangle = H$,

which contradicts the fact that B is a minimax set. Therefore any proper subset of S' generates a proper subgroup of G/K. This is equivalent to saying that S' is an independent generating set for G/K.

An independent generating set for G:
So we have S' as an independent generating set for G/K of size $|S'| = |B| + r = \mu(G/N) + R(G,N)$. By Lemma 5.1.3 there must be an independent generating set S for G of size at least $|S'|$. So $\mu(G) \geq \mu(G/K) + R(G,N)$.

Therefore, $\mu(G) = \mu(G/N) + R(G,N)$. □

Proposition 5.1.2, taken with Proposition 5.1.1, has a direct corollary:

Corollary 5.1.1. *Suppose that $N \lneqq G$ such that $N \trianglelefteq G$ and N is abelian. Then*

$$\mu(G) = \mu(G/N) \Leftrightarrow N \leq \Phi(G).$$

5.2 The Centre of G

If $N = Z(G)$, then for any decomposition $N = N_1 \times \ldots \times N_r$, each N_i must be G-invariant. This is because G must stabilise each subgroup of N. Observe also that $Z(G)$ will be loosely entangled in G if there is some $K \lneqq Z(G)$ such that $G/K \cong (Z(G)/K) \times H$ for some proper $H \leq G/K$. Any such K will be a releasing group for $Z(G)$.

When $N = Z(G)$, we are able to state Proposition 5.1.2 without defining $R(G,N)$. We do this now, stating the result as a corollary to Proposition 5.1.2.

Corollary 5.2.1. *If $Z(G)$ is loosely entangled in G, then*

$$\mu(G) = \mu(G/Z(G)) + \max\{\mu(Z(G)/K) | K \text{ is a releasing group for } Z(G)\},$$

otherwise $\mu(G) = \mu(G/Z(G))$.

Proof. We begin with the case that $Z(G)$ is loosely entangled in G. Suppose that $N \trianglelefteq G$ is abelian, with $M \lneqq N$ such that $M \trianglelefteq G$. Recall that we defined $a(N/M)$ to be the length of a longest decomposition of N/M into G-invariant subgroups. For $N = Z(G)$ and any $M \lneqq Z(G)$, any subgroup of $Z(G)/M$ will be G-invariant. Hence $a(Z(G)/M)$ is the length of the decomposition of $Z(G)/M$ into cycles of prime-power order. But the this length is precisely $\mu(Z(G)/M)$ [15, p. 8]. Thus, $a(Z(G)/M) = \mu(Z(G)/M)$. Then

$$\begin{aligned} R(G, Z(G)) &= \max\{a(Z(G)/K) | K \text{ is a releasing group for } Z(G)\} \\ &= \max\{\mu(Z(G)/K) | K \text{ is a releasing group for } Z(G)\}. \end{aligned}$$

If $Z(G)$ is not loosely entangled in G then $R(G, Z(G))$ is defined to be 0.

Applying Proposition 5.1.2 in both cases gives us

$$\mu(G) = \mu(G/Z(G)) + R(G, Z(G)),$$

which proves the statement of the corollary. □

Corollary 5.1.1 also has a nice interpretation in the current context:

Corollary 5.2.2. $\mu(G) = \mu(G/Z(G)) \Leftrightarrow Z(G) \leq \Phi(G)$.

CHAPTER 6

MINIMAX SETS IN SOME FINITE COXETER GROUPS

We wish to use the main result of the last chapter to determine $\mu(G)$ for most finite, irreducible Coxeter groups G. A result by Whiston (Theorem 1.1.2) implies that if G is a finite, irreducible Coxeter group of type A_n then $\mu(G) = n$. Also, Whiston showed in his PhD thesis that if G is a dihedral group of order $2n$, then $\mu(G) = 1 + \pi(n)$, where $\pi(n)$ is the number of distinct prime divisors of n [15, pp. 7–8] . Therefore, if we determine $\mu(G)$ for G a finite, irreducible Coxeter group of type B_n or D_n then we will know $\mu(G)$ for all the infinite classes A_n, B_n, D_n, $I_2(n)$ of Coxeter groups. This will be our main task in this chapter. The main result of the last chapter will come in useful as finite Coxeter groups of type B_n or D_n have large, normal, abelian subgroups.

6.1 Finite, Irreducible Coxeter Groups of Type B_n

6.1.1 The Structure of Coxeter Groups of Type B_n

Let G be a finite, irreducible Coxeter group of type B_n. Let

$$\Omega := \{-n, \ldots, -1, 1, \ldots, n\}$$

and let $\Omega^+ := \{1, \ldots, n\}$, $\Omega^- := \{-1, \ldots, -n\}$. So Ω is the disjoint union of Ω^+, Ω^-. Consider all permutations g of Ω such that $x^g = y \Leftrightarrow (-x)^g = -y$ for all x, $y \in \Omega$. The group of all such permutations g is called "the group of signed permutations of Ω". G has a natural interpretation as such a group [2, pp. 245–248].

Let $A := \{(-x, x) | x \in \Omega^+\} \subseteq G$ be the set of all transpositions that take some $i \leq n$ and permute it with its negative. Let $N := \langle A \rangle \leq G$ be a subgroup of G with a distinguished generating set A. It is trivial to check that the elements of A commute with each other, and that A is invariant under the action of G. Hence $N = \langle A \rangle$ is abelian and normal in G. Now, let $S \leq G$ be the full stabiliser in G of the set Ω^+. So $S \cong \mathrm{Sym}(\Omega^+)$. Note that S is the full stabiliser in G of Ω^- as well. It is easy to check that $N \cap S = \{1\}$ and $G = \langle N, S \rangle$. Therefore $G = N : S$.

Now, given any $g \in N$ and $x \in \Omega^+$, an easy argument shows that either g permutes x and $-x$, or g fixes x. If $g \in N$ and g permutes $x, -x$ for $x \in \Omega^+$, we say that g *moves* x.

Definition 6.1.1. Let $E \subseteq N$ be the set of all $g \in N$ such that g moves an even number of $x \in \Omega^+$.

It is easy to check that E forms a normal subgroup of G.

Proposition 6.1.1. *Suppose that g_1, $g_2 \in N$ such that g_1, g_2 move the same number of $x \in \Omega^+$. Then there is some $h \in S$ such that $g_1^h = g_2$.*

Proof. If g_1, g_2 each move m elements of Ω^+ then there are $x_1, x_2, \ldots, x_m \in \Omega^+$ and $y_1, y_2, \ldots, y_m \in \Omega^+$ such that

$$g_1 = (-x_1, x_1)(-x_2, x_2) \ldots (-x_m, x_m) \text{ and } g_2 = (-y_1, y_1)(-y_2, y_2) \ldots (-y_m, y_m).$$

But there must be some $h \in S$ such that

$$h = \begin{pmatrix} -x_m & \ldots & -x_2 & -x_1 & x_1 & x_2 & \ldots & x_m \\ -y_m & \ldots & -y_2 & -y_1 & y_1 & y_2 & \ldots & y_m \end{pmatrix},$$

where h is presented in two-cycle notation. But it is clear that $g_1^h = g_2$. □

Proposition 6.1.2. *Let $H \leq G$ such that $S \leq H$. Also, let $K \leq H \cap N$ such that S normalises K. If there is some $g \in K$ such that g moves precisely two elements of Ω^+ then $E \leq K$.*

Proof. Let $g_1 \in E$ and let m be the number of $x \in \Omega^+$ moved by g_1. So m is even. If we show that $g_1 \in K$ then the proposition is established.

We will use $I := \{i \leq m | i \text{ odd}\} = \{1, 3, \ldots, m-1\}$ as a set of odd indices. Consider the elements $(-i, i)(-(i+1), i+1) \in E$ for $i \in I$. Each moves precisely two elements of Ω^+, precisely the same number of elements of Ω^+ moved by g. So by Proposition 6.1.1, for each $i \in I$ there must be an $h_i \in S$ such that $g^{h_i} = (-i, i)(-(i+1), i+1)$. Since $g \in K$ and S normalises K, it must be that each $g^{h_i} \in K$. But then their product $g_2 := \prod_{i \in I} g^{h_i}$ lies in K.

Note that g_2 moves m elements of Ω^+, as does g_1. So by Proposition 6.1.1 there must be some $h \in S$ such that $g_2^h = g_1$. But $g_2 \in K$, and S normalises K. Therefore $g_1 \in K$. □

It will be useful here if we introduce a distinguished element of N. We set

$$t := (-1, 1)(-2, 2) \ldots (-n, n)$$

to be the product of all elements of A. Note that $|\langle t \rangle| = 2$. Also, observe that t moves every element of Ω^+, and that it is the unique element of N that does this.

Proposition 6.1.3. *If $K \leq N$ such that S normalises K, then*

$$K = \{1\}, \langle t \rangle, E \text{ or } N.$$

Proof. $\{1\}, N \trianglelefteq G$, trivially. So S normalises $\{1\}$, N.

If $h \in S$ and $a \in A$, then it must be the case that $a^h \in A$. This means that $t^h = t$. Therefore $\langle t \rangle$ is normalised by S.

So now suppose that $K \lneq N$ such that S normalises K, and suppose that $K \neq \{1\}, \langle t \rangle$ or N. So there is some $g \in K$ such that $g \neq 1, t$. Therefore g cannot fix every $x \in \Omega^+$, otherwise $g = 1$, and g cannot move every $x \in \Omega^+$, otherwise $g = t$. So there must be some $x, y \in \Omega^+$ such that g fixes x and permutes $-y, y$. But now there must be an element $h := (-x, -y)(x, y) \in S$ that permutes x, y. Clearly g^h fixes y and permutes $-x, x$. Also, it is easy to see that g^h permutes the other $z \in \Omega$ in precisely the same way as g. But g will either fix z, or permute $z, -z$. For any $z \in \Omega^+ \setminus \{x, y\}$, g^h will fix z if g fixes z, and g^h will map $-z$ to z if g maps z to $-z$. Thus, the product gg^h moves both x and y, but will fix all other $z \in \Omega^+$. Since S normalises K it must be that $g^h \in K$, and so $gg^h \in K$. Therefore K contains an element that shifts precisely two elements of Ω^+. Proposition 6.1.2 now implies that $E \leq K$.

Now, taking $\mathcal{P}(\Omega^+)$ to be the power set of Ω^+, it is easy to satisfy oneself that the function $\phi : N \to \mathcal{P}(\Omega^+)$ defined by

$$\phi(g) = \{x \in \Omega^+ | x^g \neq x\}$$

is a bijection. It is also easy to check that $\phi|_E$ is a bijection between E and all subsets of Ω^+ of even size. Precisely half of the elements of $\mathcal{P}(\Omega^+)$ have even size, so precisely half of the elements of N move an even number of $x \in \Omega^+$. Therefore $|N : E| = 2$. Since $E \leq K$ it must now be the case that $K = N$ or $K = E$. $K \neq N$ by assumption, so $K = E$.

This establishes the proposition. □

Any $K \leq N$ such that $K \trianglelefteq G$ must be normalised by S. So Proposition 6.1.3 has an immediate corollary:

Corollary 6.1.1. *Let G be a finite, irreducible Coxeter group of type B_n, and let $N, S \leq G$*

be as defined at the beginning of this section. If $K \leq N$ such that $K \trianglelefteq G$, then

$$K = \{1\}, \langle t \rangle, E \text{ or } N.$$

6.1.2 Independent Sets in Finite Coxeter Groups of Type B_n

In order to make good use of what has been already established, we will find the next lemma helpful. It is easy to prove, but still useful. We will temporarily drop our assumption that G is a finite, irreducible Coxeter group of type B_n. Instead, we will establish the lemma for finite groups G with normal, abelian subgroups.

Lemma 6.1.1. *Suppose that $N \trianglelefteq G$ is a proper, abelian subgroup of G. If $\mu(G) > \mu(G/N) + 1$ then N has distinct subgroups $K_1, K_2, K_3 \lneq N$ such that each $K_i \trianglelefteq G$, $K_1 \not\leq K_2$, $K_2 \not\leq K_1$ and $K_3 \leq K_1, K_2$.*

Proof. Suppose that $\mu(G) = \mu(G/N) + r > \mu(G/N) + 1$. This happens if and only if N contains a releasing group K such that

$$G/K = (N_1 \times \ldots \times N_r) : G/N,$$

where $N_1 \times \ldots \times N_r \cong N/K$ is a decomposition of N/K into G-invariant subgroups. Let K_1 be the full pre-image of N_1 in N and let K_2 be the full pre-image of N_2 in N. K_1, K_2 must be proper subgroups of N that are normal in G. Also, note that it cannot be that $K_1 \leq K_2$ or $K_2 \leq K_1$, otherwise $N_1 \leq N_2$ or $N_2 \leq N_1$. If we set $K_3 := K$ then we have found K_1, K_2, K_3 that answer the description given. □

We now state and prove the main result for Coxeter groups of type B_n.

Proposition 6.1.4. *If G is a finite, irreducible Coxeter group of type B_n, then*

$$\mu(G) = \begin{cases} n, & \text{if } n \text{ is even;} \\ n+1, & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Since G is a split extension $N : S$ we have that N is loosely entangled in G. Since N is abelian, we may apply Theorem 1.1.2 to conclude that

$$\mu(G) = R(G,N) + \mu(G/N) = R(G,N) + \mu(S) = R(G,N) + (n-1).$$

Observe that $R(G,N) \geq 1$.

Suppose n is even. Then t moves an even number of $x \in \Omega^+$. That is, $t \in E$. We know that $R(G,N) \geq 1$. We wish to argue that $R(G,N) \leq 1$. To this end, suppose that $R(G,N) \geq 2$. By Lemma 6.1.1 N contains distinct subgroups $K_1, K_2, K_3 \lneqq N$ such that each $K_i \trianglelefteq G$, $K_1 \not\leq K_2, K_2 \not\leq K_1$ and $K_3 \leq K_1, K_2$. Corollary 6.1.1 tells us that the only subgroups $K_1, K_2, K_3 \lneqq N$ that are normal in G are $\{1\}, \langle t \rangle, E$. K_3 can only be $\{1\}$ in this case, then. That means we can say $K_1 = \langle t \rangle, K_2 = E$. But $\langle t \rangle \leq E$ and $\langle t \rangle = K_1 \not\leq K_2 = E$, a contradiction. Hence $R(G,N) \leq 1$. Therefore,

$$\mu(G) = R(G,N) + (n-1) = 1 + (n-1) = n.$$

Suppose n is odd. Then t moves an odd number of $x \in \Omega^+$. That is, $t \notin E$. We saw during the proof of Proposition 6.1.3 that $|N : E| = 2$. This implies that

$$N = \langle t, E \rangle = \langle \langle t \rangle, E \rangle.$$

$|\langle t \rangle| = 2$ and $t \notin E$, so $\langle t \rangle \cap E = \{1\}$. Using the fact that N is abelian, we now have that

$$N = \langle t \rangle \times E.$$

Now, given that G is a split extension $N : S$, any $K \lneqq N$ such that $K \trianglelefteq G$ must be a releasing group for N. So, taking $K := \{1\}$ as a releasing group, we have that $N/K \cong \langle t \rangle \times E$ can be decomposed into a direct product of two G-invariant groups. It cannot be further decomposed into smaller G-invariant subgroups as Corollary 6.1.1 assures us that there are no such subgroups. But now consider the other releasing groups of N. By Corollary 6.1.1 we know that the only other releasing groups contained in N are $\langle t \rangle$ and E. But $N/\langle t \rangle \cong E$ and $N/E \cong \langle t \rangle$ cannot be further decomposed into direct products of G-invariant groups. By observation then, $R(G, N) = 2$ in this case. Therefore,

$$\mu(G) = R(G, N) + (n - 1) = 2 + (n - 1) = n + 1.$$

□

6.2 Finite, Irreducible Coxeter Groups of Type D_n

6.2.1 The Structure of Coxeter Groups of type D_n

If H is a finite, irreducible Coxeter group of type D_n then we may regard H as a subgroup of the finite, irreducible Coxeter group G of type B_n. Indeed, suppose that $N, S \leq G$ are as defined in the previous section, and let $E \leq N$ be the group of elements of N that move an even number of $x \in \Omega^+$. Then $H = \langle E, S \rangle$ [2, pp. 252–255]. Let $t \in G$ be as defined in the previous section. Note that $t \in H$ if and only if $t \in E$.

Now, suppose that $K \leq H \cap N = E$ such that $K \trianglelefteq H$. Then we have that S normalises K. We are now able to draw another corollary from Proposition 6.1.3, one relevant to the current situation.

Corollary 6.2.1. *Suppose that $K \leq H \cap N = E$ such that S normalises K. Then*

$$K = \{1\}, \langle t \rangle, \text{ or } E.$$

Proof. From Proposition 6.1.3 we have that $K = \{1\}, \langle t \rangle, E$ or N. But $K \leq E$, so $K = \{1\}, \langle t \rangle$ or E. □

6.2.2 Independent Sets in Coxeter Groups of Type D_n

Here we show

Proposition 6.2.1. *If H is a finite, irreducible Coxeter group of type D_n, then $\mu(H) = n$.*

Proof. Observe that $H = E : S$ is a split extension. So E is loosely entangled in H and any $K \lneqq E$ such that $K \trianglelefteq H$ must be a releasing group for E. So

$$\mu(H) = R(H, E) + \mu(S) = R(H, E) + (n - 1).$$

It is easy to see that $R(H, E) \geq 1$.

Suppose $R(H, E) \geq 2$. By Lemma 6.1.1 we have that there are distinct $K_1, K_2, K_3 \lneqq E$ such that each $K_i \trianglelefteq H$, $K_1 \not\leq K_2, K_2 \not\leq K_1$ and $K_3 \leq K_1, K_2$. But Corollary 6.2.1 assures us that there are only two $K \lneqq E$ such that $K \trianglelefteq H$. Therefore we cannot find three K_1, K_2, K_3 as described. Therefore $R(H, E) \leq 1$.

Thus,

$$\mu(H) = R(H, E) + (n - 1) = 1 + (n - 1) = n.$$

□

6.3 The Infinite Families of Finite, Irreducible Coxeter Groups

As we have already mentioned, Whiston determined $\mu(G)$ for when G is a symmetric group or a dihedral group (p. 89). We may now combine Whiston's results with Propositions

6.1.4 and 6.2.1 to produce a single theorem:

Theorem 6.3.1. *Suppose G is a finite, irreducible Coxeter group of type A_n, B_n, D_n or $I_2(n)$. Then*

1. $\mu(G) = n$ *if G is of type A_n or D_n*
2. $\mu(G) = \begin{cases} n, & \text{if } n \text{ is even;} \\ n+1, & \text{if } n \text{ is odd.} \end{cases}$ *if G is of type B_n*
3. $\mu(G) = 1 + \pi(n)$ *if G is of type $I_2(n)$.*

6.4 The Other Families of Finite Coxeter Groups

Suppose G is a finite, irreducible Coxeter group that is not of type A_n, B_n, D_n or $I_2(n)$. Then, up to isomorphism, G can only be one of six possible groups. We may assume that G is of type E_6, E_7, E_8, F_4, H_3 or H_4. It is natural to ask what $\mu(G)$ will be on these occasions. We offer a partial answer below. More specifically, we determine $\mu(G)$ if G is of type F_4, H_3 or H_4. We do not determine $\mu(G)$ for when G is of type E_6, E_7 or E_8.

6.4.1 The Finite, Irreducible Coxeter Group of Type F_4

If G is a Coxeter group of type F_n, it is usually assumed that $n \geq 4$. Up to isomorphism, there is only a single finite, irreducible Coxeter group of type F_n. It occurs when $n = 4$. Let G be the finite, irreducible Coxeter group of type F_4. Now, $G \cong W : S_3$, where W is an irreducible Coxeter group of type D_4 [7, p. 45]. So immediately we have that $\mu(G) \leq \mu'(W) + \mu(S_3)$, by Corollary 1.1.2. However, this approach is unlikely to lead to a tight bound. Instead we take another approach, which we now describe.

We begin by considering the contribution, if any, of $Z(G)$ to $\mu(G)$. That is, we ask if $\mu(G) > \mu(G/Z(G))$ or not. $|Z(G)| = 2$, so $Z(G)$ can only be loosely entangled in G if $\{1\}$ is a releasing subgroup for $Z(G)$. That is to say, $Z(G)$ can only be loosely entangled

in G if $G = Z(G) \times H$ for some $H \leq G$. Now, for any finite group G, if $K \trianglelefteq G$ and there is some $H \leq G$ such that $H \cap K = \{1\}$ and $G = \langle H, K \rangle$ then H is said to be a *complement* to K in G. With regard to our present case of G being a Coxeter group of type F_4 then, if $Z(G)$ is loosely entangled in G then $Z(G)$ must have a complement H in G. But GAP tells us that there is no such H[1]. Hence $Z(G)$ is not loosely entangled in G, and $\mu(G) = \mu(G/Z(G))$, by Proposition 5.1.2.

Now, GAP also informs us that $G/Z(G)$ has a normal, abelian subgroup N isomorphic to 2^4. It also informs us that this subgroup has a complement isomorphic to $S_3 \times S_3$. Hence $G/Z(G) \cong 2^4 : (S_3 \times S_3)$. Finally, we also learn from GAP that in the factor group $G/Z(G) \cong 2^4 : (S_3 \times S_3)$, the only normal subgroups of $G/Z(G)$ contained in the elementary abelian group N are $\{1\}$ and N itself. So N is obviously loosely entangled, with its only releasing group being $\{1\}$. The only G-invariant subgroups of $N/\{1\}$ are $\{1\}$ and N, otherwise N contains more than two normal subgroups of $G/Z(G)$. Hence $R(G/Z(G), N) = 1$ and

$$\mu(G) = \mu(2^4 : (S_3 \times S_3)) = \mu(S_3 \times S_3) + 1.$$

Now,

$$\mu(S_3 \times S_3) \leq \mu'(S_3) + \mu(S_3) = 2 + 2 = 4.$$

Each of the two S_3 factors in $S_3 \times S_3$ has an independent generating set of size 2. The disjoint union of these generating sets obviously forms an independent generating set of $S_3 \times S_3$ of size 4. Hence $\mu(S_3 \times S_3) = 4$.

We have just shown

Proposition 6.4.1. *If G is a finite, irreducible Coxeter group of type F_4 then $\mu(G) = 5$.*

[1]Details of some of the GAP calculations performed for this section appear in the appendix.

6.4.2 Finite, Irreducible Coxeter Groups of Type H_n

If G is a Coxeter group of type H_n, it is usually assumed that $n \geq 3$. Up to isomorphism, there are only two finite, irreducible Coxeter groups of type H_n. They occur when $n = 3$ and when $n = 4$.

The Finite, Irreducible Coxeter Group of Type H_3

Let G be the finite, irreducible Coxeter group of type H_3. Then $G \cong 2 \times A_5$ [7, p. 46]. It is clear, using Corollary 1.1.2, that

$$\mu(G) = \mu(2 \times A_5) \leq 1 + \mu(A_5) = 1 + 3 = 4.$$

Obviously the cyclic group 2 has an independent generating set of size 1. We may also find an independent generating set of size 3 for the A_5 subgroup. Their disjoint union will obviously give an independent generating set for $2 \times A_5$ of size 4. Therefore we have

Proposition 6.4.2. *If G is a finite, irreducible Coxeter group of type H_3 then $\mu(G) = 4$.*

The Finite, Irreducible Coxeter Group of Type H_4

Let G be the finite, irreducible Coxeter group of type H_4. GAP tells us that $|Z(G)| = 2$. So if $Z(G)$ is loosely entangled in G then $Z(G)$ has a complement in G. From GAP we learn that $Z(G)$ has no complement in G[1]. So $\mu(G) = \mu(G/Z(G))$ by Proposition 5.1.2. GAP also informs us that $G/Z(G) \cong A_5 \wr 2$. Hence $\mu(G) = \mu(A_5 \wr 2)$.

We establish

Proposition 6.4.3. $\mu(A_5 \wr 2) = 5$.

Proof. We begin by proving that $\mu(A_5 \wr 2) \leq 5$.

[1]Details of some of the GAP calculations performed for this section appear in the appendix.

Let $S := \{g_1, \ldots, g_n\}$ be a minimax set in $A_5 \wr 2$. For each i, let $H_i := \langle S \setminus \{g_i\} \rangle$. Clearly, each H_i lies in a maximal subgroup of $A_5 \wr 2$.

GAP informs us that if M is a maximal subgroup of $A_5 \wr 2$ then M is isomorphic to one of the following groups:

1. $A_5 \times A_5$
2. $2 \times A_5$
3. $A_5.2$
4. $S_3 \wr 2$
5. $D_{10} \wr 2$
6. $A_4 \wr 2$

There is only one maximal subgroup of $A_5 \wr 2$ that is isomorphic to $A_5 \times A_5$. So if there are distinct $H_i, H_j \leq A_5 \times A_5$ then

$$\langle S \rangle = \langle H_i, H_j \rangle \leq A_5 \times A_5.$$

This cannot be, so at most one of the H_i lies in $A_5 \times A_5$. Without loss of generality, suppose H_1 does not lie in $A_5 \times A_5$. We deal with the separate cases.

Case: $H_1 \leq 2 \times A_5$ *or* $A_5.2$

If $H_1 \leq 2 \times A_5$ or $A_5.2$ then by Corollary 1.1.2,

$$\mu'(H_1) \leq \mu'(2) + \mu'(A_5) = 1 + 3 = 4.$$

But $S \setminus \{g_1\}$ is an independent set in H_1, so $|S| \leq 5$.

Case: $H_1 \leq S_3 \wr 2$ *or* $D_{10} \wr 2$

Suppose $H_1 \leq M_1 \cong S_3 \wr 2$. Now M_1 contains a normal subgroup $K \cong 3^2$ such that $M_1/K \cong 2 \wr 2$.

It is easy to check that $\mu'(2 \wr 2) = 2$. Thus, by Corollary 1.1.2

$$\mu'(H_1) \leq \mu'(K.(2 \wr 2)) \leq \mu'(3^2) + \mu'(2 \wr 2) = 2 + 2 = 4.$$

But $S \setminus \{g_1\}$ is an independent set in H_1, so $|S| \leq 5$.

Suppose $H_1 \leq M_1 \cong D_{10} \wr 2$. Then M_1 contains a normal subgroup K such that $K \cong 5^2$. Furthermore, $M_1/K \cong 2 \wr 2$. Hence,

$$\mu'(H_1) \leq \mu'(K.(2 \wr 2)) \leq \mu'(5^2) + \mu'(2 \wr 2) = 2 + 2 = 4.$$

Therefore $|S| \leq 5$.

Case: $H_1 \leq A_4 \wr 2$

If $|S| \leq 3$ then we are done, so suppose that $|S| \geq 4$. Then H_1, H_2, H_3, H_4 are defined. At most one of these can lie in $A_5 \times A_5$, so we can suppose that H_1, H_2, H_3 do not lie in $A_5 \times A_5$. Also, given the previous cases, if any of H_1, H_2, H_3 lies in an $A_5.2$, $2 \times A_5$, $S_3 \wr 2$ or $D_{10} \wr 2$ subgroup, then we have that $|S| \leq 5$. So we can suppose that each of H_1, H_2, H_3 lies in an $A_4 \wr 2$ subgroup. It cannot be that two H_i, H_j both lie in some maximal $M \cong A_4 \wr 2$, otherwise $\langle S \rangle = \langle H_i, H_j \rangle \leq M$, which is absurd. So we may suppose that H_1, H_2, H_3 lie in distinct M_1, M_2, M_3 respectively, with each $M_i \cong A_4 \wr 2$. GAP informs us that

$$\bigcap_{i=1}^{3} M_i \cong A_4, 3^2, 3 \text{ or } 2.$$

It must be that $\mu'(M_1 \cap M_2 \cap M_3) \leq 2$. $S \setminus \{g_1, g_2, g_3\}$ is an independent set in $H_1 \cap H_2 \cap H_3 \leq M_1 \cap M_2 \cap M_3$, so it must be that $|S| \leq 5$.

Therefore, $\mu(A_5 \wr 2) \leq 5$.

We now argue that $\mu(A_5 \wr 2) \geq 5$. To see this, observe that the elements

$$\begin{aligned}(3,5,4)(8,9,10),\\ (2,5)(3,4)(7,10)(8,9),\\ (1,2)(3,4)(6,7)(8,9),\\ (3,5,4)(8,10,9),\\ (1,6)(2,7)(3,8)(4,9)(5,10)\end{aligned}$$

form an independent set S in S_{10}, and that $\langle S \rangle \cong A_5 \wr 2$. Hence $\mu(A_5 \wr 2) \geq 5$.

Therefore, $\mu(A_5 \wr 2) = 5$. □

We have now established the main proposition of this section:

Proposition 6.4.4. *If G is a finite, irreducible Coxeter group of type H_4 then $\mu(G) = 5$.*

6.5 Conclusion

We may combine Theorem 6.3.1 with Propositions 6.4.1, 6.4.2 and 6.4.4 to produce a broader theorem:

Theorem 6.5.1. *Suppose G is a finite, irreducible Coxeter group of type A_n, B_n, D_n, $I_2(n)$, F_4, H_3 or H_4. Then*

1. *$\mu(G) = n$ if G is of type A_n or D_n*
2. *$\mu(G) = n + 1$ if G is of type F_4, H_3 or H_4*
3. *$\mu(G) = \begin{cases} n, & \text{if } n \text{ is even;} \\ n+1, & \text{if } n \text{ is odd.} \end{cases}$ if G is of type B_n*
4. *$\mu(G) = 1 + \pi(n)$ if G is of type $I_2(n)$.*

One summary of this theorem could be:

Corollary 6.5.1. *Suppose G is a finite, irreducible Coxeter group with n vertices in its Coxeter diagram, such that G is not of type E_6, E_7 or E_8. If G is not dihedral then $\mu(G) = n$ or $n+1$.*

It is tempting to wonder if the assumption that G is not of type E_6, E_7 or E_8 could be dropped. However, we have not seen anything to suggest that this is the case, other than a trend for the other Coxeter groups. This is a dangerous basis upon which to make a conjecture.

APPENDIX

GAP CALCULATIONS FOR THE FINITE COXETER GROUPS

The Calculations for F_4

We wish to investigate the groups structure of Coxeter groups of type F_4. We begin by creating a copy of F_4.

```
gap> f:=FreeGroup(4);;
gap> r:=[f.1^2,(f.1*f.2)^3,(f.1*f.3)^2,(f.1*f.4)^2,f.2^2];;
gap> r:=Union(r,[(f.2*f.3)^4,(f.2*f.4)^2,f.3^2]);;
gap> r:=Union(r,[(f.3*f.4)^3,f.4^2]);;
gap> g:=f/r;
<fp group on the generators [ f1, f2, f3, f4 ]>
```

So g is our copy of F_4. We want to found out how large $Z(\mathsf{g})$ is, and to investigate how it sits within the group structure of g.

```
gap> Size(Centre(g));
2
gap> Complementclasses(g,Centre(g));
[ ]
```

So $|Z(\mathsf{g})| = 2$, and there is no $H \leq \mathsf{g}$ such that $H \cap Z(\mathsf{g}) = \{1\}$ and $\mathsf{g} = \langle Z(\mathsf{g}), H \rangle$. Given this, and the size of $Z(\mathsf{g})$, we have that $Z(\mathsf{g})$ is not loosely entangled in g. Therefore $\mu(\mathsf{g}) = \mu(\mathsf{g}/Z(\mathsf{g}))$.

But now we find all the normal subgroups of $\mathsf{g}/Z(\mathsf{g})$.

```
gap> N:=NormalSubgroups(g/Centre(g));;
gap> for n in N do
> Print(Size(n),", ",IsElementaryAbelian(n),"\n");od;
1, true
16, true
48, false
96, false
48, false
144, false
288, false
288, false
96, false
288, false
576, false
gap> C:=Complementclasses(g/Centre(g),N[2]);
[ <permutation group with 4 generators> ]
gap> S:=SymmetricGroup(3);;
gap> IsomorphismGroups(DirectProduct(S,S),C[1])<>fail;
true
```

So $\mathtt{g}/Z(\mathtt{g})$ has an elementary abelian group A of order 16. Note that the only normal subgroups of g contained in this subgroup are $\{1\}$ and A. Also A has a complement in $\mathtt{g}/Z(\mathtt{g})$ isomorphic to $S_3 \times S_3$. Hence $\mathtt{g}/Z(\mathtt{g}) \cong 2^4 : (S_3 \times S_3)$. This completes our investigation of the structure of F_4.

The Calculations for H_4

The Structure of H_4

We wish to investigate the group structure of Coxeter groups of type H_4. We begin by creating a copy of H_4.

```
gap> f:=FreeGroup(4);;
gap> r:=[f.1^2,(f.1*f.2)^5,(f.1*f.3)^2,(f.1*f.4)^2,f.2^2];
gap> r:=Union(r,[(f.2*f.3)^3,(f.2*f.4)^2,f.3^2]);;
gap> r:=Union([(f.3*f.4)^3,f.4^2]);;
gap> g:=f/r;
<fp group on the generators [ f1, f2, f3, f4 ]>
```

So g is our copy of H_4. As for F_4, we check $Z(\mathtt{g})$ and its relationship to the rest of g.

```
gap> Size(Centre(g));
2
gap> Complementclasses(g,Centre(g));
[ ]
```

So $Z(\mathtt{g})$ has no complement in g. Given the size of $Z(\mathtt{g})$, $Z(\mathtt{g})$ is not loosely entangled in g. Hence $\mu(\mathtt{g}) = \mu(\mathtt{g}/Z(\mathtt{g}))$. We now describe the group structure of $\mathtt{g}/Z(\mathtt{g})$.

```
gap> W:=WreathProduct(AlternatingGroup(5),CyclicGroup(2));
<group of size 7200 with 3 generators>
gap> IsomorphismGroups(g/Centre(g),W)<>fail;
true
```

Thus, $\mathtt{g}/Z(\mathtt{g}) \cong A_5 \wr 2$. This completes our study of the structure of H_4.

The Maximal Subgroups of $A_5 \wr 2$

The proof of Proposition 6.4.3 requires an exhaustive list of the maximal subgroups of $A_5 \wr 2$. These are most easily provided in GAP if we regard $A_5 \wr 2$ as a subgroup of S_{10}.

```
gap> S:=[(1,2,3),(1,2,3,4,5),(1,6)(2,7)(3,8)(4,9)(5,10)];;
gap> G:=Group(S);;
gap> M:=MaximalSubgroups(G);;
```

We begin our study of these maximal subgroups by finding all the possible isomorphism types for them.

```
gap> T:=[];
gap> for m in M do
> flag:=1;
> for t in T do
> if IsomorphismGroups(t,m)<>fail then flag:=0;fi;od;
> if flag=1 then Append(T,[m]);fi;od;
gap> for t in T do
> Print(Size(t),",");od;Print("\n");
72,120,120,200,288,3600,
gap> D6:=DihedralGroup(6);;D10:=DihedralGroup(10);;
gap> A4:=AlternatingGroup(4);;A5:=AlternatingGroup(5);;
gap> C:=CyclicGroup(2);;
gap> IsomorphismGroups(T[1],WreathProduct(D6,C))<>fail;
true
```

```
gap> IsomorphismGroups(T[4],WreathProduct(D10,C))<>fail;
true
gap> IsomorphismGroups(T[5],WreathProduct(A4,C))<>fail;
true
gap> IsomorphismGroups(T[6],DirectProduct(A5,A5))<>fail;
true
gap> IsomorphismGroups(T[2],DirectProduct(A5,C))<>fail;
true
gap> IsomorphismGroups(T[3],SymmetricGroup(5))<>fail;
true
```

This shows that each maximal subgroup of $A_5 \wr 2$ is isomorphic to one of $D_6 \wr 2$, $D_{10} \wr 2$, $A_4 \wr 2$, $A_5 \times 2$, S_5 and $A_5 \times A_5$.

With regard to the subgroups isomorphic to $A_4 \wr 2$, we wish to find the possible intersections of any three of them, up to isomorphism.

```
gap> a:=[ ];;int:=[ ];;
gap> for m in M do
> if Size(m)=288 then Append(a,[m]);fi;od;
gap> for c in Combinations(a,3) do
> I:=Intersection(c);
> flag:=1;
> for i in int do
> if IsomorphismGroups(i,I)<>fail then flag:=0;fi;od;
> if flag=1 then Append(int,[I]);fi;od;
gap> for i in int do
> Print(i,"\n");od;
Group([ (8,9,10), (7,8)(9,10) ])
Group([ (8,9,10),(3,4,5) ])
Group([ (8,9,10) ])
Group([ (1,6)(2,7)(3,8)(4,9)(5,10) ])
```

By inspection, we see that the possible intersections of any three maximal subgroups of order 288 are, up to isomorphism, A_4, 3^2, 3 or 2.

LIST OF REFERENCES

[1] Michael Aschbacher. On the maximal subgroups of the finite classical groups. *Inventiones Mathematicae*, 76(3):469 – 514, 1984.

[2] Anders Björner and Franceso Brenti. *Combinatorics of Coxeter Groups*, volume 231 of *Graduate Texts in Mathematics*. Springer, New York, 2005.

[3] Peter Cameron and Philippe Cara. Independent generating sets and geometries for symmetric groups. *Journal of Algebra*, 258(2):641 – 650, December 2002.

[4] Persi Diaconis and Laurent Saloff-Coste. Walks on generating sets of groups. *Inventiones Mathematicae*, 134(2):251–299, 1998.

[5] Klaus Doerk and Trevor Hawkes. *Finite Soluble Groups*, volume 4 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter, Berlin, 1992.

[6] David Dummit and Richard Foote. *Abstract Algebra*. John Wiley and Sons, 2003.

[7] James Humphreys. *Reflection Groups and Coxeter Groups*, volume 29 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[8] Derek Holt John Bray and Colva Roney-Dougal. *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*. London Mathematical Society Lecture Note Series. Cambridge Uninversity Press, to appear.

[9] Oliver King. *Survey in Combinatorics*, volume 327 of *London Mathematical Society Lecture Note Series*, chapter The Subgroup Structure of Finite Classical Groups in Terms of Geometric Configurations, pages 29 – 56. Cambridge University Press, Cambridge, 2005.

[10] Peter Kleidman and Martin Liebeck. *The Subgroup Structure of the Finite Classical Groups*, volume 129 of *London mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[11] Howard Mitchell. Determination of the ordinary and modular ternary linear groups. *Transactions of the American Mathematical Society*, 12(2):207 – 242, April 1911.

[12] Jan Saxl and Julius Whiston. On the maximal size of independent generating sets of $\mathrm{PSL}_2(q)$. *Journal of Algebra*, 258(2):651 – 657, December 2002.

[13] Donald Taylor. *The Geometry of the Classical Groups*, volume 9 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, 1992.

[14] Julius Whiston. Maximal independent generating sets of the symmetric group. *Journal of Algebra*, 232(1):255 – 268, September 2000.

[15] Julius Whiston. *The Minimal Generating Sets of Maximal Size of Selected Groups*. PhD thesis, Pembroke College: Univeristy of Cambridge, July 2001.