Base size of finite primitive solvable permutation groups

Ayan Maiti

Under the supervision of Prof. Pal Hegedus

A thesis presented for the partial fulfilment towards the degree of
Masters of Science in Mathematics

Mathematics and its Application
Central European University
Hungary

Declaration of Authorship

I, Ayan Maiti, declare that this thesis titled, ”Base size of finite primitive solvable permutation groups” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a masters degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: Ayan Maiti

Date: 20th May, 2016

Abstract

The content of this thesis report is based on the bounds of the base size of affine type primitive permutation groups, the bound was conjectured by Pyber and later was proved by Akos Seress. The the primary focus of this thesis is to understand the basic idea and the proof given by Akos Seress.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisor Prof. Pal Hegedus for the continuous support of my M.S. study, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of understanding the topic and writing of this thesis. Secondly, I would also want to thank my fellow classmate for the stimulating discussions regarding the related topic discussed in the thesis.

Contents

Chapter 1

Introduction

Overview

The study of Permutation groups plays a significant role in the field of mathematics and science, as they help us to understand the different types of symmetry around us. These concepts can be understood in an efficient way using a very prominent characterization of groups called bases.

In this thesis report I will focus on studying the bounds of the base size of primitive solvable permutation groups. Let G be a transitive permutation group which is acting on a set Ω, it is called primitive if its action can only have the trivial G-invariant partitions of Ω,(formal definition given later on). Subsequently it means that the action of G cannot be disintegrated into smaller portions. Now throughout this thesis report I will denote $b(G)$ as the minimal base size of the group G. However the imprimitive groups have more information stored in their actions than the primitive groups. This makes the study of primitive permutation groups more crucial to solve any problem in permutation group theory. So it is sensible to talk about the base size of these groups and it makes sense to minimize the size as well. There are some extensive research works have been done on bounding the base size of a primitive permutation group [6]. I am going to discuss here a prominent one.

Most of the research on the bounding the bases of primitive permutation groups has been on proving a well known conjecture made by Pyber [10], which states that there exists an absolute constant c for which the base size of a primitive permutation group G of degree n (i.e. the set on which G is acting on has size n) is at most $c \log |G| / \log n$(the formal statement and the discussion given later). Since the base size of G is bounded below by $\log |G| / \log n$, this conjecture, if true, would imply that we can have the necessary control on the base size of a primitive permutation group even when the size of G is infinity. However for the finite primitive groups we have a very powerful theorem which categorizes these groups namely The O'Nan-Scott Theorem [9]. It classifies the finite primitive group into five categories, namely diagonal type, twisted wreath type, product type, affine type and almost simple type.

Cameron [7] conjectured and later which was proved [8] that for almost simple type primitive permutation group $b(G) \leq 7$ unless the group action is standard.(G has a standard action if G is either S_n or A_n acting on the set of k-subsets of $\{1, ..., n\}$) Now apart from the almost simple type groups some research has been done to find the bounds of the base size of affine type primitive permutation groups, which is dealt by Akos Seress [5] and understanding this is the primary goal of my thesis report.

There are some recent developments [11] happened about the base sizes of finite primitive groups of product types and twisted types which satisfies the Pyber's conjecture. For the case of finite primitive groups of diagonal types considerable advancement has been done by Joanna B. Fawcett [17]. This thesis report is structured as follows. In the second chapter I will discuss about some basic definitions, examples and theorems about base, primitive group action, solvable groups, finite group representation theory, and a very important algorithm (namely sim-schreier algorithm) of how to compute base and strong generating set (namely BSGS) of a group. In the third chapter, I will present the proof of the theorem that state that all the primitive solvable permutation groups has base size at most 4 (the proof is due to Akos seress [5], who proved the pyber's conjecture about the base size of a group).

Chapter 2

Basic Concepts

Definition and examples

Definitions

- Let G be a group acting on a set Ω, Now let $\alpha \in \Omega$. Then orbit of $\alpha \in \Omega$ under the action of group is defined as follows :
$$\{\alpha^G = \{\alpha^g, g \in G\}\}.$$
- Let G be a group acting on a set Ω, Now let $\alpha \in \Omega$. Now we will define the stabilizer of α as:
$$G_\alpha = \{g \in G, \alpha^g = \alpha\}.$$
- Let G be a group acting on a set Δ. Now the group blocks are defined as follows : either g preserves Δ, i.e.,
$$g\Delta = \Delta,$$
or g translates everything in Δ out of Δ, i.e.,
$$g\Delta \cap \Delta = \phi.$$
- Let G be a permutation group acting on a finite set Ω of size n. A primitive group action is transitive and it has no nontrivial group blocks.
- An action of a group on a non-empty set is called semiregular if for any two (Possibly equal) elements in the underlying set there is at-most one element in the group taking the first element to the second.
- An action of a group is called regular if it is transitive and semiregular.

- A group G is called solvable if it has a solvable(or normal) series, i.e. if there are subgroups,
$$\{1\} = G_0 \subset G_1 \subset G_2 \subset ... \subset G_k = G,$$
such that G_{t-1} is normal in G_t and G_t/G_{t-1} is abelian.

- A group action of a group G on a set Ω is said to be doubly transitive if given any (a, b) and (a_1, b_1) with $a \neq a_1, b \neq b_1$, elements in Ω there exists a $g \in G$ such that $g(a) = a_1$ and $g(b) = b_1$.

Examples

- The general linear group $GL(2, \mathbb{R})$ acts on the plain $\mathbb{R}^2 - \{0, 0\}$. Now the straight lines $\{at, bt\}$ in the above mentioned plain are the blocks of imprimitivity of the group $GL(2, \mathbb{R})$. As the matrices in the group will either map the straight line into another one or into the same line. In general if two blocks intersect then their intersection is also a block.

- An example of a solvable group is any abelian group(even if the order is infinity). Another example would be S_4. The solvable series of S_4 is :
$$\{1\} \subset K \subset A_4 \subset S_4,$$
Where the the quotients are clearly abelian groups. Here K: the Klein 4- groups,
$$K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$
.

Theorems and lemmas:

Theorem 2.0.1. *If $N \lhd G$ and both N and G/N are solvable then G is solvable.*

Proof. Let $\phi : G \to G/N$ be a cannonical homomorphism. Then solvable series of G can be given as:

$$G = \phi^{-1}(M_0) \geq \phi^{-1}(M_1) \geq \ \geq \phi^{-1}(M_n) = N = N_0 \geq N_1 \geq \ \geq N_k = 1.$$

The first part of the chain involving ϕ coming from the fact that G/N is solvable and the second part is true because N is solvable.

□

Corollary 2.0.2. *If G and H are solvable then $G \times H$ is also solvable.*

Theorem 2.0.3. *Every finite p-group is solvable.*

Proof. Order of any p-group is p^n. We will prove the claim by doing induction on n. If $n = 1$, then the underlying group is cyclic group of order p. Then we have nothing to prove. Now, suppose for $n \leq k - 1$ the statement is true.

Therefore if $n = k$ then then by class equation, center of the group namely $Z(G)$ is non-trivial. And it's order is a power of p. Hence $Z(G)$ is solvable. Now $G/Z(G)$ is a p-group with order p^t where $t \leq k - 2$. Therefore $G/Z(G)$ is also solvable. So according to the theorem (theorem 2.0.1) discussed above we can conclude that G is solvable.

So every p-group is solvable. □

A subgroup H of a group G is called characteristic subgroup if $\phi(H) = H$ for all automorphisms ϕ of G.

Examples of characteristic subgroup:

- $Z(G)$ is a characteristic subgroup of G.
- the commutator subgroup G' is a characteristic subgroup of G.
- The frattini subgroup [Intersection of all maximal subgroup of G] $\Phi(G)$ of G is a characteristic subgroup of G.
- A_n is a characteristic subgroup of S_n. This is because A_n is generated by all elements of order 3 in S_n, since automorphisms take elements of order 3 to elements of order 3.

Theorem 2.0.4. *For any homomorphism $f : G \to H$ we have $f(G') = f(G)' \leq H'$. In particular, $\phi(G') = G'$ for any automorphism ϕ of G.*

Proof. f maps the generators of G' to the generators of $f(G)'$,since $f([a, b]) = f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a), f(b)]$ □

Theorem 2.0.5. *Every subgroup of a solvable group is solvable.*

Proof. We know by the definition of commutator subgroup that, $H' \leq G'$ if $H \leq G$. Then $H^{(n)} \leq G^{(n)} \leq 1$.Where $G' = G^1$, $G'' = G^2$,... etc. □

Theorem 2.0.6. *Any minimal normal subgroup of a solvable group is elementary abelian.*

Proof. Let N be a normal subgroup of G. We have to first realize that N is abelian. First of all, N is solvable by the previous theorem. Now let's look at the first commutator subgroup of N viz. N'. So N', by definition is a characteristic subgroup of N, hence a normal subgroup of G. Therefore looking at the assumption we can say that $N' = 1$. ($N' = N$, this option can not happen as N is solvable, otherwise the solvable series will not stop)

Let $p||N|$, then N has a p-Sylow subgroup P. Since N is normal in G and P is characteristic in N (because it's the unique Sylow subgroup since N is abelian) we must have that P is normal in G, by assumption this implies that $P = N$ so that $|N| = p^n$ for some n.
Now we have to prove that N is elementary abelian. We will those elements $n \in N$, which have order p(by Cauchy's theorem), this will generate a subgroup(say M) of N which is

characteristic, so M will be normal in G, but by minimality of N means M will be same as N. Hence N is elementary abelian.

□

Now we have described some useful theorems and lemmas about solvable groups, we would turn our attention towards primitive groups. The results and lemmas which are presented here are mostly taken from the book on matrix groups written by D.Suprunenko.[15]

In this section we will assume that G is a group and Ω is the set on which it is acting on.

Let G be a transitive permutation group acting on Ω, then we will define a partition of

$$\Omega = \bigcup X_\alpha,$$

where $\alpha \in I$. If the conditions are as follows:

- $|I| > 1$.
- There exists an α such that $|X_\alpha| > 1$.
- For an $\alpha \in I$ and any $g \in G$,there exist a β such that $g(X_\alpha) \subset X_\beta$.

Then we call the partition of Ω as a system of Imprimitivity for a group G. If there are no partition of Ω, then we call the group G primitive.

Lemma 2.0.7. *If we consider the partition of Ω as described above for a imprimitive group G, then all the sets X_α have same cardinality. Moreover for any $\alpha \in I$ and $g \in G$ there exists a $\beta \in I$ such that:*

$g(X_\alpha) = X_\beta$

Proof. Now by the third condition given in the above, we can say that $g(X_\alpha) \subset X_\beta$, where $\beta \in I$.

Therefore we can say that $g^{-1}(X_\beta) \supset X_\alpha$. If $x \in g(X_\alpha)$ then $g^{-1}(x) \in (X_\alpha)$, so in turn we can conclude that $g^{-1}(X_\beta) \subset X_\alpha$. This proved the second statement of the lemma.

As the underlying group G is transitive, for $a, b \in I$ there exist $h \in G$ such that $h(X_a) = X_b$. So the cardinality of the sets are the same. □

Corollary 2.0.8. *A transitive permutation group acting on a set whose cardinality is prime (Group of prime degree) is primitive.*

Theorem 2.0.9. *A doubly transitive group is is primitive.*

Proof. Let for contradiction G is a doubly transitive group which is imprimitive. Then by the above we can have a partition of Ω based on the imprimitivity of G.

So for any two elements $a, a' \in X_\alpha$ and $b \in X_\beta$ where $a \neq a'$ and $\alpha \neq \beta$, by the doubly transitivity of G there exist $g \in G$ such that g will send (a, a') to (a, b) i.e. $g(a) = a$ and $g(a') = b$. But $g(a) = a$ means $X_\alpha = X_\beta$ which is contradictory to our assumption. □

Now the theorem below will tell us about the primitivity criterion of a transitive permutation group.

Theorem 2.0.10. *A transitive permutation group is primitive if and only if any stabilizer of an element in its permutation domain is maximal.*

Proof. Suppose G is transitive group acting on a set Ω. Let $a \in \Omega$ and G_a is stabilizer subgroup of G fixing a.

Suppose on contrary G_a is not a maximal subgroup of G, so there exist another subgroup H such that $G_a \subset H \subset G$. We will try to show that this strict inclusion makes G imprimitive. Now we partition G into left cosets of H.

So

$$G = \bigcup_{\alpha \in I} g_\alpha H,$$

now define

$$g_\alpha H := H_\alpha$$

where $\alpha \in I$.

Now denote $X_\alpha := H_\alpha(a)$ where ,

$$\Omega = \bigcup X_\alpha$$

.

We will show that this partition defines the partition of imprimitivity of G. So we have to show that $X_\alpha \cap X_\beta = \emptyset$ if $\alpha \neq \beta$. Let $x(a) = y(a)$ for $x \in H_\alpha$ and $y \in H_\beta$. Therefore $x^{-1}y(a) = a$, it implies that $x^{-1}y \in G_a$. Hence $y \in xG_a \subset H_\alpha$. This proves contradiction to the partition of G. Therefore

$$\Omega = \bigcup X_\alpha$$

really represents the partition of imprimitivity of G.

Now the converse.

Suppose first that G has a nontrivial system of imprimitivity and B is a block of imprimitivity that contains a. Then we will show that $G_a < G_B < G$ and therefore that G_a is not maximal. If $g \in G_a$,then $B \cap B^g$ is nonempty (for it contains a) and hence $B = B^g$. Thus $G_a \leq G_B$.

Now to show that the inclusion is proper we find an element in G_B that is not in G_a. Let $b \neq a$ be another element of B. Since G is transitive it contains an element h such that $h(a) = b$. But then $B = B^h$, yet $h \notin G_a$, and hence $G_a < G_B$. □

Corollary 2.0.11. *A regular permutation group is either imprimitive or of prime order.*

Corollary 2.0.12. *A transitive permutation group whose all subgroups are normal is a imprimitive group except when order of the group and the degree is same prime number.*

Corollary 2.0.13. *Any stabilizer of a symmetric group is maximal.*

Now we will talk about normal subgroups of Transitive groups.

Theorem 2.0.14. *Let G be a transitive permutation group acting on Ω. And N be a normal intransitive subgroup of G. Then partition of Ω into orbits of N defines a system of imprimitivity of G.*

Proof. Let

$$\Omega = \bigcup X_\alpha,$$

where $\alpha \in I$ defines the partition of Ω into orbits of N.

Now as N is intransitive, $|I| > 1$ and as N is non-trivial, there exist an $\alpha \in I$ such that $|X_\alpha| > 1$.

Now we have to show that $h(X_\alpha) \subset (X_\beta)$ for $h \in G$ and $\alpha, \beta \in I$.

Let $x, y \in h(X_\alpha)$, therefore we can say that $x = h(x_1)$ and $y = h(y_1)$ with $x_1, y_1 \in X_\alpha$. Now as the partition was made by the orbits of N, there exists $n \in N$ such that $n(x_1) = y_1$.

N being a normal subgroup we can say that $n_1 = hnh^{-1} \in N$. Consequently $n_1(x) = y$. Hence $x, y \in X_\beta$. So the partition of Ω defines the imprimitivity of G. □

Corollary 2.0.15. *Any non trivial normal subgroup of a primitive group is transitive.*

Corollary 2.0.16. *A non-trivial abelian normal subgroup of a primitive group contains no non-trivial characteristic subgroup.*

Proof. Let, otherwise H be a characteristic subgroup of N. By the previous corollary we can say that H is a transitive abelian subgroup, which is maximal abelian subgroups of symmetric groups. So H can not be a proper subgroup of N, which will lead to the contradiction of the statement assumed before. □

Corollary 2.0.17. *The additive group of a division ring is characteristically simple.*

Proof. Let D be a division ring. And G be the subgroup of the symmetric group acting on D, consisting of elements defined as below :

$\phi \in G$,such that $\phi(x) = ax + b$,where $x, a, b \in D$ and $a \neq 0$.

We can clearly say that G is doubly transitive which by above theorem is primitive. Now the maps $f \in G$ defined as $f(x) = x + c$ where $c \in D$ form a normal subgroup of G. Which is a additive group of the division ring.

□

Theorem 2.0.18. *A transitive permutation group G acting on Ω with non-trivial center is imprimitive except the $|G| = |\Omega| = p$ where p is a prime number.*

Proof. Let G be a primitive group and $Z(G)$ denotes it's center. By the above corollary $Z(G)$ is a transitive subgroup. Now as $Z(G)$ is abelian, $Z(G)$ defines the regular action on Ω. Therefore $|Z(G)| = |\Omega|$. Now $(g)Z(G)$ is also transitive abelian where (g) is a cyclic group generated by an element $g \in G$. Now any transitive abelian group is maximal among the abelian subgroups. $(g)Z(G) = Z(G)$. So $G = Z(G)$. Now any regular permutation group is either imprimitive or of prime order. Hence $|G| = |\Omega| = p$. □

Theorem 2.0.19. *Clifford's Theorem:*
Let G be an irreducible subgroup of $GL(V)$, and let H be a normal subgroup of G. Then H is completely reducible.

Proof. Let S_1 be a H-irreducible subspace of V, such that $S_1^H = S_1$. If $S_1 = V$, then we are done.
So suppose $S_1 \neq V$, then there exist $g_1 \in G$ such that $g_1(S_1) \neq S_1$. As H is normal the subspace $g_1(S_1)$ is H-irreducible and H-invariant. Therefore $S_1 + g_1(S_1)$ is a direct sum.
Now as V is finite dimensional we can have finitely many elements $g_1, g_2, ..., g_k \in G$ such that the sum

$$S = S_1 + g_1(S_1) + g_2(S_1) + ... + g_k(S_1)$$

is a direct sum but for any other element $t \in G$, $S + t(S)$ is not a direct sum. So by the construction of S and H-irreducibility of $t(S)$ we can conclude that $t(S) = S$. As G is irreducible, $S = V$. So the decomposition of S shows the complete reducibility of H. □

Now we will describe the concept of imprimitive linear group. The notion of an imprimitive group of permutations can be defined similarly for the groups of linear transformations of vector spaces. Namely, a linear representation ρ of a group is called imprimitive if there exists a decomposition of the vector space V of the representation ρ into a direct sum of proper subspaces $V_1, V_2, ..., V_k$ with the following property: For any $g \in G$ and any $\alpha = 1(1)k$ there exists a $\beta = 1(1)k$, such that:

$$\rho(g)(V_\alpha) = V_\beta,$$

Here $V_1, V_2, ..., V_k$ are the systems of imprimitivity of G. And the group G is called primitive linear group if there is no decomposition of V.

Let V be a linear space over some field F and we can decompose V as

$$V = \sum_{i \in I} L_i,$$

according to the systems of imprimitivity of G .Then each element of G induces a permutation of the set $\{L_i, i \in I\}$.Therefore we can define a epimorphism:

$$\phi : G \to H, g \mapsto h,$$

where $h : L_i \mapsto h(L_i)$. So clearly H is a subgroup of the symmetric group $S(T)$, where $T = \{L_i, i \in I\}$. Now fix a index $\alpha \in I$, and let H_{L_α} be the stabilizer of L_α. Now we define a subgroup H_α of G as

$$H_\alpha = \phi^{-1}(H_{L_\alpha})$$

.

Theorem 2.0.20. *Let G be an irreducible imprimitive subgroup of $GL(V)$ and*

$$V = \sum_{i \in I} L_i.$$

where this decomposition explains the system of imprimitivity of G. Let H be the subgroup of the symmetric group $S(T)$, where $T = \{L_i, i \in I\}$ and $H_i = \{g \in G | g(L_i) = L_i\}$ Then followings are true:

1. *The subgroup H is transitive.*

2. *The set of all distinct subgroups H_α's are the conjugate subgroups of G.*

3. *The subgroup $H_\alpha | L_\alpha$ is an irreducible subgroup of $GL(L_\alpha)$.*

Proof. Let O be the orbit of H. Then the sum of all the subspaces (say W) of all the L_i's that lies inside the aforementioned orbit is G-invariant. Now as G is irreducible we can conclude that $W = V$. So H is transitive.
As H is transitive, the set of stabilizers namely H_α will constitute a class of conjugate subgroups.

□

Now we will focus on the imprimitivity criterion of groups. We will assume that V is a vector space over some field F of dimension n.

Theorem 2.0.21. *Let $G \leq GL(V)$ is a irreducible subgroup. Then G is imprimitive if and only if there exist a subspace S of V such that $F : S = m$, where $m|n$, and the index of $H = \{g | g \in G, g(S) = S\}$ is n/m.*

Proof. G is a irreducible imprimitive subgroup of $GL(V)$. Set

$$V = \sum_{i \in I} L_i$$

as the systems of imprimitivity of G. Then we define S as L_i and H as H_i(as mentioned in theorem 2.0.20). So according to the previous discussion, dimension of S over F is m, such that $m|n$. And the index of H is n/m.
Now the we will show the converse. Let G be irreducible and S be the subspace of V that satisfies the statement. Suppose $a = n/m$ and t_i's are the left transversal to H in G, where $t_1 = 1$. Consider the subspace defined as follows:

$$Q = t_1(S) + t_2(S) + ... + t_a(S).$$

Let $g \in G$, then $g(t_\alpha(S)) = (t_\beta(h(S))) = t_\beta(S)$, where $h \in H$.
Therefore $g(Q) = Q$. But as G is irreducible we can conclude that $Q = V$. So the dimension of Q over F is n only if the sum presented above is a direct sum. And as $g(t_\alpha(S)) = t_\beta(S)$, we proved that the sum defines the imprimitivity of G. □

The wreath product of a linear group and a permutation group is an important concept. It will help us to prove the conjecture on bounds of the base size of the primitive group. It can be defined as follows:
Let Q be a linear space over the field F, and G be the subgroup of $GL(Q)$. Suppose T is a subgroup of the symmetric group S_k, $k > 1$. Now let us define the cartesian product Q^k as U, where U can be regarded as the linear space over F. Take any vector $u \in U$, then we can write u as $(q_1, q_2, ..., q_k)$, where $q_i \in Q$. For any $\phi_1, \phi_2, ..., \phi_k \in G$ and $t \in T$ we define a mapping

$$\phi : U \to U$$

as

$$\phi = (\phi_1, \phi_2, ..., \phi_k, t).$$

Where $\phi(u) = \phi(u_1, u_2, ..., u_k) = \bar{u} \in U$. Where the $t(\alpha)$th component of $\bar{u}$ is $\phi_\alpha(u_\alpha)$, $\alpha = 1(1)k$.
Now, obviously ϕ is an automorphism of U. Let Φ be the set of all such ϕ's. Let $f \in \Phi$ be another element defined by $f = (f_1, f_2, ..., f_k, s)$. Then we can define the product $f\phi$ as $(f_{t(1)}\phi_1, ..., f_{t(k)}\phi_k, st) \in \Phi$.
It follows that, Φ is a subgroup of $GL(U)$. This group F is called the wreath product of the linear group G and the permutation group T and denoted as $G \wr T$.

Now we will talk about the strong generating set of a primitive permutation group. The concept of strong generating set was introduced by Charles Sim. Afterwards we will discuss about the algorithm that were presented by Schreier and Sim to get the strong generating set of a permutation group. The main motivation of this algorithm was to do group membership test (if a permutation is given, whether it is contained in a group).

Let G be a permutation group acting on a finite set Ω of size n. A subset of Ω is said to be a base for G if its pointwise stabilizer in G is trivial. The minimal size of a base for G is denoted by $b(G)$. Bases have been studied since the early years of permutation group theory, particularly in connection with orders of primitive groups and, more recently, with computational group theory.

With the notation we can say that a subset of Ω defined as $\alpha_1, \alpha_2, ..., \alpha_k$ where $\alpha_i \in \Omega, 1 \leq i \leq k$ will be called as a base of G if $G_{\alpha_1, \alpha_2, ..., \alpha_k} = 1$. That means only element of G which fixes the underlying set is identity.

Now we can define a series as follows:

$$G^i = G_{\alpha_1, \alpha_2, ..., \alpha_{i-1}}$$

where $1 \leq i \leq k + 1$.

so we will have a series of stabilizers:

$$G = G^1 \geq G^2 \geq G^3 \geq ... \geq G^{k+1} = 1.$$

Now let us define the strong generating set with notations.

The strong generating set(SG) of a group with respect to its base is the set of elements of a group which together with G^i generate G^i, i.e.

$< SG \cap G^i >= G^i$. We will denote $< SG \cap G^i >$ as SG^i, These are the elements of SG which will fix $\{\alpha_1, \alpha_2, ..., \alpha_{i-1}\}$.

We begin with a number of examples of bases and strong generating sets.

- The base of S_n is $\{1, 2, 3, ..., n-1\}$, and the alternating group A_n has the base $\{1, 2, 3, ..., n-2\}$ .therefore $b(S_n) = n-1$ and $b(A_n) = n-2$.
- The dihedral group acting on n points has base $\{1, 2\}$.
- Let $G = S_k$ acting on the set Ω of pairs in {1, . . . k}. Write $k = 3l+r$ with $0 \leq r \leq 2$, and define B to be the subset of consisting of the pairs {1, 2}, {2, 3}, {4, 5}, {5, 6}, . . . , {3l - 2, 3l - 1 }, {3l - 1, 3l} (adding also {3l, 3l + 1} if $r = 2$). It is easy to see that B is a base so that $b(G) \leq \frac{2}{3}k + 1$ in this example.
- If $G = PGL_d(q)$ acting on the set Ω of 1-spaces in the underlying vector space $V_d(q)$, then $b(G) = d+1$, a minimal base being $\{< v_1 >, ..., < v_d >, < v_1 + ... + v_d >\}$,where $v_1, ..., v_d$ is a basis for $V_d(q)$.Let G be the affine group $AGL_d(q)$ acting on $V_d(q)$, of degree q^d. Then $b(G) = d+1$
- The strong generating set of S_n is $\{(12), (23), ..., (n-1\ \ n)\}$.
- the strong generating set of A_n is $\{(123), (234), ..., (n-2\ \ n-1\ \ n)$.

Lemma 2.0.22. *(Schreier Lemma)Let $G =< X >$ be a finite group, $H \leq G$ and T set of representatives of the left cosets of H in G such that T contains 1. Denote by $\bar{g}$ the representative of gH for $g \in G$ such that $gH = tH$ for a unique $t \in T$.*

Then $H =< X_H >=< \{(\bar{xt})^{-1}xt | t \in T, x \in X\} >$.

Proof. We have to prove that H is generated by $X_H \cap X_H^{-1}$. Let $h \in H$. Then it also lies in G, so $h = x_1x_2x_3...x_k$ for some sequence of generators x_i in X. Let $t_i = \overline{x_{i+1}...x_k}$, the coset representative of $x_{i+1}...x_k$. Note that $t_k = e$ by definition, and $t_0 = \overline{x_1..x_k} = \overline{h} = 1$.
So we can rewrite h as $h = (t_0^{-1}x_1t_1)(t_1^{-1}x_2t_2)...(t_{k-1}^{-1}x_kt_k)$.
We can also see that $(x_it_i)H = x_i(t_iH) = x_i(x_{i+1}..x_kH) = (x_ix_{i+1}..x_k)H = \overline{x_ix_{i+1}..x_k} = t_{i-1}$ so $\overline{x_it_i} = t_{i-1}$.
We use this to rewrite h once again, to get $h = (\overline{x_1t_1}^{-1}x_1t_1)(\overline{x_2t_2}^{-1}x_2t_2)...(\overline{x_kt_k}^{-1}x_kt_k)$.
Any element h in H is a product of such factors, so it follows that the set $\{\overline{xt}^{-1}(xt) | t \in T, x \in X\}$ will generate H. □

Sims idea was to represent an element of G in terms of coset representatives of the stabilizer subgroups of G. An element $g \in G^{i-1}$ will be in a coset of G^i. Suppose we have that $g = ab$ with $a \in G^i$ and b a coset representative for G^i in G^{i-1}.

So by the above lemma(Schreier)if we define U_i a set of representatives for the cosets of G^{i-1} in G^i, then any element $g \in G$ can be written as product of elements from the the sets of U_i. So $g = u_t u_{t-1} ... u_1$. Where each u_i correspond to the orbit of β_i under the action of G^{i-1}.

Baiscs of group representation

Take $F = \mathbb{C}$, V is a $\mathbb{C}$ vector space, G finite and let $\rho : G \to GL(V)$ be a group homomorphism. Then representation of G defines by the vector space V together with the homomorphism ρ. For $v \in V$ and $g \in G$ denote gv as $\rho(g)v$. Therefore the homomorphism means we will have $(gh)v = g(hv)$,where $g, h \in G$, $v \in V$, $ev = v$, where e is the identity element of G. And $g(\alpha v_1 + \beta v_2) = \alpha g(v_1) + \beta g(v_2)$, where $\alpha, \beta \in \mathbb{C}$, $v_1, v_2 \in V$. So we can have a bijective correspondence between the group homomorphisms and the $\mathbb{C}G$ modules. Now we will state a important lemma concerning irreducible subspaces. The lemma is called Schur's lemma.

Theorem 2.0.23. *Schur's Lemma*

1. *A non-zero homomorphism between two irreducible representation of a group G is an isomorphism.*
2. *Let $\rho : G \to GL(V)$ be a finite dimensional irreducible representation over $\mathbb{C}$. Then any G equivariant linear map between V is $\alpha\, \mathrm{id}_V$, where $\alpha \in \mathbb{C}$.*

Proof. To prove this I will state the same version of this lemma for the modules.

Lemma 2.0.24. *Schur's Lemma for modules If M_1 and M_2 are simple R-modules, where R is any ring, then any non-zero R-module homomorphism $\phi : M_1 \to N_1$ is an isomorphism.*

Proof. Here $\phi \neq 0$ is a homomorphism between M_1 and M_2. So by definition of homomorphism, $ker(\phi)$ and $Im(\phi)$ are the submodule of M_1 and M_2 respectively. Now as they both are simple modules, the above mentioned homomorphism is surjective as well as injective. □

So, to prove the first part of the theorem, we can use the similar configuration as discussed above.

To prove the second part, let $T : V \to V$ be a linear map and $T\rho(g) = \rho(g)T$ for all $g \in G$ by the definition G-equivariant map. Take an eigenvalue α of T in $\mathbb{C}$. Now we can see that $T - \alpha\, \mathrm{id}_V$ is also a G-module homomorphism. However, $Ker(T - \alpha\, \mathrm{id}_V) = \{0\}$. So by the first part we can deduce that $T - \alpha\, \mathrm{id}_V = 0$. It means that $T = \alpha\, \mathrm{id}_V$.

□

The character $\chi = \chi_V = \chi$ is defined as $\chi(g) = tr\rho(g)$. Where $\rho(g)$ is a matrix and the degree of the character is the dimension of V.

Now I will state a basic theorem concerning the bounds of minimal base size of a finite group.

Theorem 2.0.25. *For a group G we have $2^{b(G)} \leq |G| \leq n^{b(G)}$.*

Proof. By the discussion above we can say that there exist a chain of stabilizers defined as:

$$G = G^1 < G^2 < G^3 < ... < G^{k+1} = 1$$

.

now we can easily get the inequality:

$$2 \leq [G^i : G^{i+1}] \leq n$$

.

We can say that $[G : 1] = [G^1 : G^2][G^2 : G^3]...[G^k : G^{k+1}]$, where $G^{k+1} = 1$.
So multiplying the left hand side and right hand side of the inequality separately we will get the statement.

□

At the first sight the Proposition seems elementary, however it defines a significant connection between the order of G and the value of $b(G)$, leading to a number of important results and conjectures. The minimal base size for G is the minimal number $b(G)$ such that a base of size $b(G)$ exists. Since any element of G is determined by the images of the base elements, it follows that $|G| \leq |\Omega|^{b(G)}$.

Taking logarithm, one get the lower bound $b(G) \geq \frac{\log |G|}{\log |\Omega|}$. On the other hand, a conjecture of L. Pyber asserts that for a primitive permutation group G acting on Ω the upper bound $b(G) \leq c\frac{\log |G|}{\log |\Omega|}$ holds with some universal constant $c \geq 1$.

Results and conjectures:

Theorem 1:

(Bochert [18]) If G is a primitive permutation group of degree n not containing A_n, then $b(G) \leq n/2$

Theorem 2:

(Babai [19, 20]) Let G a primitive permutation group of degree n not containing A_n.

1. If G is not 2-transitive then $b(G) < 4n^{1/2}\log n$.
2. If G is 2-transitive then $b(G) < c(\log n)^{n/2}$, where c is an absolute constant.

Theorem 3 :

(Pyber [21])If G is a 2-transitive group of degree n not containing A_n, then $b(G) \leq c\log^2 n$, where c is an absolute constant.

The above results were proved using combinatorial methods, in particular not using the classification of finite simple groups.And the above examples shows that these bounds are not far off from the best possibles.

Chapter 3

Main Theorem

statement of the theorem

Akos seress answered Pyber's question in the first non-trivial case, for primitive solvable groups.
The statement of the theorem he proved is as follows:

Theorem 3.0.1. *All primitive solvable permutation groups have a base of size at most four.*

The method he used to prove the theorem is mostly combinatorial. It is well known (I will prove it later) that if $G \leq S_n$ is primitive solvable, then $n = p^d$ for some prime p, and the point-stabilizer M is isomorphic to an irreducible subgroup of $GL(d, p)$. First, he used an extension of a counting method due to Gluck and Manz to handle the case of primitive (as a linear group) G. Gluck and Manz [12] showed that if a certain parameter e(I will define it later), has value at least 132, then G has one orbit on which it acts regularly and so the minimal base size is 1. For most smaller values, this argument helps us to show that G has a minimal base of size at most 3. When this counting argument fizzles out, then he used some group theory (mostly, information about maximal solvable subgroups in certain low dimensional symplectic groups).

Definition 1. *Socle of a finite group is The subgroup generated by the minimal normal subgroups of that group.For solvable case the socle is product of elementary abelian groups.*

Now assume that $G \leq S_n$ is primitive and solvable. Then there exists a unique conjugacy class of a maximal subgroups M namely the point-stabilizer ; the index of M in G is called the degree of G ($|G : G_a| = |\Omega|$). Moreover, M complements the socle N of G. Therefore, the index of M in G is a prime power, p^n.
While handling the case where M is imprimitive, he proved the following theorem:

Theorem 3.0.2. *Let $G \leq Sym(\Omega)$ be an arbitrary solvable permutation group. Then there is a partition P of Ω into at most five parts such that only the identity element of G fixes P.*

This bound is best possible. For example, $S_4 \wr C_2$ acts on 8 points imprimitively. Then the partition requires five parts, since if the first four points lies into one partition, then an element of $S_4 \times 1$ will fix the partition. Similarly, the second four points must fall into different parts. However, if there are only four parts then we can have some element of $S4 \wr C2$, that will fix the partition.

We can also strengthen the theorem 3.0.1 about the base size in the case of primitive groups of odd order.The theorem is stated as follows:

Theorem 3.0.3. *All primitive permutation groups of odd order have a base of size at most three.*

Palfy [13] proved that if $G \leq S_n$ is primitive of odd order, then $|G| \leq 3^{-1/2}n^c$ with $c = 2.278...$, and equality holds for infinitely many values of n.

Gluck [14] showed a variant of the theorem 3.0.2 concerning the partition of the underlying set on which the group is acting on. The variation is as follows:

Theorem 3.0.4. *There is always a partition of Ω into two parts whose stabilizer in G is the identity with finitely many exceptions.*

Let $G \leq Sym(\Omega)$ be a primitive solvable permutation group. We will define Ω with the vector space $V = GF(p)^n$, where p is a prime, and let G_0, be the stabilizer of the 0 element of V. In order to prove the main Theorem (namely theorem 3.0.1), we have to prove that G_0 has a base of size at most 3. In this section, we will discuss about the case when $G_0 \leq GL(n,p)$ is a primitive linear group.
We say that the bases $A = (\alpha_1, \alpha_2, ..., \alpha_k), B = (\beta_1, \beta_2, ..., \beta_k)$ for G_0 are nonequivalent if there is no $g \in G_0$ satisfying $\alpha_j^g = \beta_j$ for $1 \leq j \leq k$.

Now we can write the following theorem for the case where our underlying group is solvable primitive linear.

Theorem 3.0.5. *Let $G_0 \leq GL(n,p)$ be a primitive solvable linear group, acting on $V = GF(p)^n$. Then G_0 has a base of size at most 3. Moreover, when the minimal base size of G_0 is 3, G_0 has at least five non-equivalent minimal bases.*

It is enough to prove the above theorem in the case when G_0 is a maximal primitive solvable linear group (with respect to inclusion).
The following lemma [15] (section 19-20) describes the most important properties of the maximal primitive solvable linear group.

Lemma 3.0.6. *Let $G_0 \leq GL(n,p)$ be a maximal solvable primitive group. Then G_0 has a unique maximal abelian normal subgroup N. Let $C = C_{G_0}(N)$ and $B = Fit(C)$, the Fitting subgroup of C. Then we have the following:*

1. *N is cyclic of order $p^a - 1$ for some integer a.*
2. *The linear span of N in $M_n(\mathbb{F}_p)$ is the field $GF(p^a)$.*
3. *G_0/C is isomorphic to a subgroup of $Aut(GF(p^a))$.*
4. *$n = ae$ for an integer e.*
5. *$C \leq GL(e, p^a)$.*
6. *Let $e = \prod q_i^{e_i}$be the prime decomposition of e. Then each q_i divides $|A| = p^a - 1$.*
7. *$|B/N| = e^2$ and B/N is the direct product of elementary abelian groups.*
8. *There is a C-invariant non-degenerate symplectic form on each Sylow subgroup of B/N.*
9. *C/B is isomorphic to a completely reducible subgroup of the direct product of symplectic groups $Sp(2e_i, q_i)$.[3]*
10. *For each q_i, the q_i-Sylow subgroup of B can be written in the form $E_{q_i}T_{q_i}$,where E_{q_i} is an extraspecial group of order $q_i^{2e_i+1}$, T_{q_i} is the q_i-Sylow subgroup of N.*
11. *The degree of the irreducible components of E_{q_i} over $GF(p^a)$ is $q_i^{e_i}$.*

Proof. To prove 1 and 2 we will try to construct a maximal solvable primitive group which has a maximal abelian normal subgroup. Let G' is an arbitrary solvable primitive subgroup of $GL(n,p)$ which has N' as its normal abelian subgroup.
By clifford's theorem N' is a completely reducible subgroup of G'. And its irreducible components are pairwise equivalent. Let m be the degree of an irreducible component of N'. So $m|n$. Therefore the set

$$\sum n_i f_j = \Delta,$$

where $n_i \in N'$ and $f_i \in \mathbb{F}_p$ is a field of degree m over $\mathbb{F}_p$.
Let

$$N'_1 = \Delta^*.$$

Therefore N'_1 is a normal abelian subgroup. So $G'_1 = N'_1G'$ will be a solvable group. If it happens that N'_1 is maximal subgroup of G'_1, then we are done. If not then we can take $N'_1 \leq N'_2$ and define $G'_2 = N'_2G'_1$, Where $N'_2 = \Delta_1^*$ and $\Delta_1^* = \sum n'_i f'_j$, $n'_i \in N'_1$ and $f'_j \in \Delta^*$.
So we will have a series of fields

$$\Delta \leq \Delta_1 \leq \Delta_2 \leq ...$$

But as n is finite and the orders of the fields are the divisors of n this chain will stop. So we take the field which is maximum in this chain.Let's call it Σ. So the maximal abelian normal subgroup is $\Sigma^* = N$. Let the degree of N is a. So order of N is $p^a - 1$.
To prove 3 let us define a map

$$\phi : G_0 \to Aut(GF(p^a)), \{n \mapsto f_n\},$$

where $f_n : \Sigma \to \Sigma$,$f_n(a) = nan^{-1}$. Then $Ker(\phi) = C$. So G_0/C is subgroup of $Aut(\Sigma/\mathbb{F}_p)$. The other proofs can be seen in [3] and [15].

□

For any $g \in G_0$, the fixed points of g produces a subspace of $V = GF(p)^n$.
Gluck and Manz [12] observed that this subspace is of size $o(p^n)$. More exactly, the following lemma holds. Let $C_V(g)$ denote the set of fixed points of g, where $g \in G$.

Lemma 3.0.7. *Let $G_0 \leq GL(n, p)$ be a maximal solvable primitive groups, then the following holds:*

1. *if $g \in N$,then$|C_V(g)| = 1$.*
2. *if $g \in B \setminus N$, then $C_V(g) \leq (p^n)^{1/2}$.*
3. *if $g2 \in C \setminus B$, then $C_V(g) \leq (p^n)^{3/4}$.*
4. *if $g \in G \setminus C$, then $C_V(g) \leq (p^n)^{1/2}$.*

Gluck and Manz used this Lemma to show that G_0 has a regular orbit when $e \geq 132$, by proving that the union of the sets $C_V(g)$ cannot cover V. A similar argument shows that for most of the values of e, the minimal base size of G_0 is at most 3.
Now we will collect some lemmas that will help us to prove the theorem 3.0.5. Extensive proofs are given by seress in [5].

Lemma 3.0.8. *Let $G_0 \leq GL(n, p)$ be a maximal solvable primitive group, $n = ae$, and suppose that $e \geq 3$. Then B has a regular orbit unless the pair (p^a, e) is one of $(4, 3), (3, 4)$ and $(5, 4)$.*

Lemma 3.0.9. *Let $G_0 \leq GL(n, p)$ be a maximal solvable primitive group, $n = ae$,$e \geq 3$,and (p^a) is one of $(4, 3), (3, 4)$ and $(5, 4)$. Then if we have this following inequality:*

$$\left\lfloor \frac{|C/B|}{p^{a\lfloor \frac{e}{4} \rfloor}} \right\rfloor (p^{a\lfloor \frac{3e}{4} \rfloor} + (a-1)p^{\lfloor \frac{ae}{2} \rfloor} + 4a) < p^{ae},$$

then G_0 satisfies the theorem 3.0.5.

Lemma 3.0.10. *Let $G_0 \leq GL(n,p)$ be a maximal solvable primitive group, and $n = ae$. If $e \geq 16$, then G_0 satisfies the conclusion of the Theorem* 3.0.5 *unless $p^a = 3$ and $e = 16$.*

Lemma 3.0.11. *Let $G_0 \leq GL(n,p)$ be a maximal solvable primitive group, and $n = ae$. If $3 \leq e \leq 7$ or $10 \leq e \leq 15$, then G_0 satisfies the conclusion of the above mentioned theorem* 3.0.5 *unless the pair (p^a, e) is one of $(4,3)$, $(3,4)$, $(5,4)$ and $(1,4)$.*

Lemma 3.0.12. *Let $G_0 \leq GL(e,p)$ (we are assuming here that $a = 1$) be a maximal solvable primitive group,with the conditions that $e \geq 4$, and $(p,e) \neq (3,4),(5,4)$. Moreover, let k denote the number of elements of prime order in G_0/B. If the following inequality holds:*

$$\left\lceil \frac{k}{p^{e/4}} \right\rceil p^{3e/4} < p^e - 4\frac{|G_0|}{|B|},$$

then G_0 will follow the conclusion of theorem 3.0.5*.*

These above mentioned lemmas followed by some other special case scenarios (can be seen in [5]) will finish the proof of theorem 3.0.5.
Given a field automorphism θ of a field F, a function $\phi : V \to W$ between two F vector spaces V and W is semilinear, if for all $a, b \in V$ and $\lambda \in F$ it follows:

- $\phi(a+b) = \phi(a) + \phi(b)$.
- $\phi(\lambda a) = \lambda^\theta \phi(a)$.

Let $\Gamma L(1,p^n)$ be the group of semilinear transformations of $GF(p^n)$. Palfy and Espuelas [16] proved the following analogue of theorem 3.0.5:

Theorem 3.0.13. *Let p be an odd prime, and let $G_0 \leq GL(n,p)$ be primitive linear of odd order. Then G_0 has at least two regular orbits unless $G_0 \leq \Gamma L(1,p^n)$.*

Proof of theorem 3.0.2

A partition of the underlying set Ω, on which G acting on can be considered as a colouring of Ω. For each primitive solvable permutation group G, we define a colouring of the underlying set on which the group is acting on, with the minimal possible number of colours such that only identity will preserve the colouring.

Clearly, it is enough to prove Theorem 3.0.2 in the case when $G \leq Sym(\Omega)$ is transitive, as the partition can be done according to the orbits. So we will assume that G is transitive.

Now let us define a structured tree of the permutation domain of G according to it's partition. Let T be the structure tree, where $T_0, T_1, T_2, ..., T_k$ define the levels of the tree with T_0 and T_k being the root and leaves of the tree respectively. The construction is as follows: $T_0 = \{\Omega\}$, and $T_k = \Omega$ and for the other levels, we partition Ω into certain blocks of imprimitivity of G. Suppose, α is a non-leaf node. Then we will also need the set-wise stabilizer of α to be acting as a primitive group on the children of α.

Let us define a colouring

$$C : T \to \mathbb{F}_5.$$

We will first colour the root T_0 with 0. Now suppose recursively $T_1, T_2, T_3, .., T_i$ are coloured. Let $\alpha \in T_i$, we denote the set-wise stabilizer of α as G_α. It will act on the children of α as a primitive group by the construction of the structure tree. And there is a fixed colouring of G_α with $j \leq 4$ colours(from the conclusion of theorem 3.0.1). So we can colour the children of α with $c(\alpha) + j$ colours.

Now we have to show that only colour preserving permutation of T is the identity. We will use induction on the no. of the levels of the structured tree to prove that. So by induction on $i = 0, 1, 2, 3, .., k$,we can say that the colour preserving permutation on

$$T_0 \cup T_1 \cup T_2 \cup ... \cup T_k$$

will fix this union pointwise.(As the setwise stabilizer of a non-leaf node acts primitively on the children of that node by the construction of the tree). So eventually the colour preserving permutation will fix $T_k = \Omega$.

Also, we claim that the only colour-preserving permutation of G of $T_k = \Omega$ is the identity. We first observe that from the colouring of T_k, it is possible to get back the colouring of the entire tree T. Then, by induction on $i = k, k-1, ..., 0$, it is clear that the colour preserving partition must preserve the colouring of

$$T_i \cup T_{i+1} \cup ... \cup T_m.$$

In particular, g preserves the colouring of T, so g is the identity

Theorem 3.0.14. *Let $G_0 \leq GL(n, p)$ be an irreducible imprimitive solvable linear group, acting on $V = GF(p)^d$. Then G_0 has a base of size at most 3.*

Proof. As G_0 is imprimitive linear group we will have a decomposition (non-refinable) of V into subspaces.Therefore

$$V = \bigoplus_{j=1}^{k} V_j.$$

Let $dimV_j = l$. Let L be the subgroup of S_k induced by G_0 on $V_1, ..., V_k$. As G_0 is irreducible, L is transitive.(Let I be an orbit of $\{1, 2, 3..., k\}$, then $\bigoplus_{t \in I} V_t$ will be a subspace of V,contradictory to the fact that G_0 is irreducible)

Let $T \leq GL(V_1)$ be a primitive linear group which is a subgroup of G_0 which stabilizes V_1 as a set, then $G_0 \leq T \wr L$. It will be enough to prove that base size of $T \wr L$ is at most 3.

By the theorem 3.0.5, we can conclude that the minimal base size of T is at least 3. Also by the previous theorem (namely theorem 3.0.2) $\{1, 2, 3, ..., k\}$ can be partitioned into at most 5 parts, say $P_i, i = 1, 2, 3, 4, 5$, such that only the identity element will fix the partition. We will allow some of the partitions to be empty.

We will have three cases, let $b(T) = 1$. Let $v_1^1 \in V_1$ be an element from the regular orbit of T. Suppose that $v_1^i \in V_i$ is the image of v_1^i by the action of L in V_i. Let

$$v_1 = \sum_{i \in P_1 \cup P_2 \cup P_3} v_1^i,$$

$$v_2 = \sum_{i \in P_1 \cup P_4} v_1^i$$

and

$$v_3 = \sum_{i \in P_2 \cup P_5} v_1^i.$$

We will prove that (v_1, v_2, v_3) is a base for $T \wr L$. Let $g \in (T \wr L)_{v_1, v_2, v_3}$. We have to show that g is identity. Let $V_k^g = V_j$ where $k \in P_1$. As g fixes v_1 pointwise so $j \in P_1 \cup P_2 \cup P_3$ and as g fixes v_2 pointwise so $J \in P_1 \cup P_4$. Therefore g fixes P_1 and similarly other parts of the partition. So g is identity.
Now if $b(T) = 2$, let (v_1^1, v_2^1) be a base of T, and let (v_1^i, v_2^i) be the L image of those two base vectors in V_i. Let

$$v_1 = \sum_{i \in P_1 \cup P_2 \cup P_3 \cup P_4} v_1^i,$$

$$v_2 = \sum_{i \in P_1 \cup P_2 \cup P_3 \cup P_5} v_2^i,$$

$$v_3 = \sum_{i \in P_1 \cup P_4} v_2^i + \sum_{i \in P_2 \cup P_5} v_1^i.$$

We claim that $(v_1, v_2.v_3)$ will form a base. Let $g \in (T \wr L)_{v_1, v_2, v_3}$. We have to show that g is identity. Let $V_i^g = V_j$, where $i \in P_1$. Now as g fixes v_1, v_2, v_3 , $j \notin P_5$. As g fixes both v_2 and v_3, we can conclude that $j \notin P_3 \cup P_4$. Now from the fact that $v_2^g = v_2$, we can say that ${v_2^i}^g = v_2^j$. Similarly as g fixes v_3 we can say that ${v_2^i}^g = v_1^j$. So we reach a contradiction. So $j \notin P_2$. Therefore g fixes P_1. Similarly it will fix the other parts of the partition. So g is identity.
And for the last case which is $b(T) = 3$,let us assume that $C_1, C_2, ..., C_5$ be the five non-equivalent bases. Let (v_1^i, v_2^i, v_3^i) be the L- image of C_k where $i \in P_k$, $k = 1(1)5$ and $i \in P_k$. Let us assume that:

$$v_1 = \sum_{i=1}^{t} v_1^i$$

,

$$v_2 = \sum_{i=1}^{t} v_2^i$$

,

$$v_3 = \sum_{i=1}^{t} v_3^i$$

.

We claim that v_1, v_2, v_3 are the elements of the base. Suppose g fixes the set $\{v_1, v_2, v_3\}$ point-wise. For $l \leq t$, let $V_l^g = V_m$. Therefore $(v_1^i, v_2^i, v_3^i)^g = (v_1^j, v_2^j, v_3^j)$. But the definition of non-refinable bases means they can not be images of the bases. Therefore g fixes the partition P_k's. So g is identity.

Proof of Theorem 3.0.3

It is enough to show that for a odd order group $G_0 \leq GL(n, p)$, where p is odd, and G_0 is acting irreducibly on the vector space $V = GF(p)^n$ then minimal base size of G_0 is at most 2. If G_0 is primitive linear group then this statement follows from the theorem 3.0.14.
Now if the group G_0 is imprimitive linear then by notation which is described above, $n = kl$, and

$$V = \bigoplus_{j=1}^{k} V_j,$$

and $G \leq T \wr L$, where $T \leq GL(V_1)$ is primitive linear and a transitive group $L \leq S_k$. Gluck [14] showed that there exist a partition P namely $\{1, 2, 3, ..., k\} = P_1 \bigcup P_2$, such that only identity element of L will fix the partition.
We break up T into two possibilities. One is when $T \leq \Gamma L(V)$ and another when it is not a subgroup of the semilinear transformation.
If $T \leq \Gamma L(V)$, let $v_1, v_2 \in V$ be in different regular orbit of T. Suppose that $v_1^i, v_2^i \in V_i$ are the images of v_1, v_2 by the action of L. Then

$$v = \sum_{i \in P_1} v_1^i + \sum_{i \in P_2} v_2^i$$

will be in the regular orbit of $T \wr L$.(By using the method described in the previous proof)
Now if T is not a subgroup of $\Gamma L(1, P^d)$, then we will have two non-equivalent bases of T namely B_1, B_2, both have size 2. Now for $i \in P_k$ we denote $(v_1^i, v_2^i) \in V_i$ as the L-image of B_k. Let us define

$$v_\alpha = \sum_{i=1}^{k} v_1^i$$

and

$$v_\beta = \sum_{i=1}^{k} v_2^i.$$

Now by the similar argument showed above we can conclude that (v_α, v_β) is a base of $T \wr L$.
□

Bibliography

[1] Bailey, Cameron. *Base size, metric dimension and other invariants of groups and graphs*, Bull. Lond. Math. Soc., 43 (2011), 209–242.

[2] Gluck, Magaard. *Base sizes and regular orbits for co-prime affine permutation groups*, J. London Math. Soc. (2) 58 1998 no3 603–618.

[3] Olaf Manz,Thomas R. Wolf. *Representation of Solvable groups.*

[4] MW. Liebeck *Bases of Primitive Permutation Groups*, J. Algebra 252 (2002), no. 1, 95–113. (Reviewer: David Gluck) 20B15.

[5] Seress, Akos *Permutation group algorithms*, Cambridge Tracts in Mathematics,vol. 152, Cambridge University Press, Cambridge, 2003.

[6] Babai, L. *On the order of uniprimitive permutation groups*, Ann. Math. 113 (1981),553568.

[7] Cameron, P. J. *Permutation groups*, Cambridge University Press, Cambridge,1999.

[8] Burness, T. C. *On base sizes for actions of finite classical groups*, J. London Math.Soc. 75 (2007), 545562.

[9] Liebeck, M. W., Praeger, C. E., and Saxl, J. *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. 44 (1988), 389396.

[10] Pyber, L. *Asymptotic results for permutation groups*, DIMACS Ser. Discrete Math. Theoret. Comp. Sci. 11 (1993), 197219.

[11] Burness, T. C., and Seress, A.*On Pybers base size conjecture*, Trans. Amer.Math. Soc. 367(2015),no. 8, 5633-5651.

[12] D. Gluck and O. Manz, *Prime factors of character degrees of solvable groups*, Bull. London Math. Soc. 19(1987)431-437.

[13] P. P. Palfy, *Bounds for linear groups of odd order*, Proc. Second Internat. Group Theory Conf. ,Bressanone/Brixen 1989, Suppl. Rend. Circ. Mat. Palermo 23 (1990) 253-263.

[14] D. Gluck, *Trivial set-stabilizers in finite permutation groups*, Canad. J. Math. 35 (1983) 59-67.

[15] D. A. Suprunenko, *Matrix groups* (Amer. Math. Soc, Providence, RI, 1976)

[16] A. Espuelas, *Large character degrees of groups of odd order*, Illinois J. Math. 35 (1991) 499-505.

[17] J. B. Fawcett, *The base size of a primitive diagonal group*, J. Algebra 375, 302-321 (2013).

[18] A. Bochert, *Uber die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann*, Math. Ann. 33 (1889), 584-590

[19] L. Babai, *the order of uniprimitive permutation groups*, Ann. of Math. 113 (1981),553568.

[20] L. Babai, *On the order of doubly transitive permutation groups*, Invent. Math. 65(1982), 473484

[21] L. Pyber, *On the orders of doubly transitive permutation groups, elementary estimates*, J. Combin. Theory Ser. A 62 (1993), 361366.