LOW RANK TRANSITIVE REPRESENTATIONS, PRIMITIVE EXTENSIONS, AND THE COLLISION PROBLEM IN $PSL(2,q)$

by

Krishna B. Thapa Magar

A Dissertation Submitted to the Faculty of

The Charles E. Schmidt College of Science

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Florida Atlantic University

Boca Raton, FL

August 2015

LOW RANK TRANSITIVE REPRESENTATIONS, PRIMITIVE EXTENSIONS, AND THE COLLISION PROBLEM IN $PSL(2,q)$

by

Krishna B. Thapa Magar

This dissertation was prepared under the direction of the candidate's dissertation advisor, Dr. Spyros S. Magliveras, Department of Mathematical Sciences, and has been approved by the members of his supervisory committee. It was submitted to the faculty of the Charles E. Schmidt College of Science and was accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

SUPERVISORY COMMITTEE:

Spyros S. Magliveras, Ph.D.
Dissertation Advisor

Lee Klingler, Ph.D.

Rainer Steinwandt, Ph.D.
Chair, Department of Mathematical Sciences

Stephen Locke, Ph.D.

Aaron Meyerowitz, Ph.D.

Janet Blanks, Ph.D.
Interim Dean, The Charles E. Schmidt College of Science

Deborah L. Floyd, Ed.D.
Dean, Graduate College

7/6/2015
Date

ACKNOWLEDGEMENTS

At first, I would like to thank my advisor Dr. Spyros S. Magliveras who continually supported and advised me during my graduate studies at Florida Atlantic University. I was impressed with his teaching and research enthusiasm when I first took his Group Theory course in Fall 2010. Thus, I started to work under his supervision. He guided me from scratch, and taught me how to walk the path to research. His strong knowledge of the field and his persistency contributed to my understanding of the research materials. He is not only the best professor, he is one of the best human being I have ever met. I am proud to be an academic son of Dr. Spyros S. Magliveras.

I would like to thank Dr. Lee Klingler, Dr. Stephen Locke, and Dr. Aaron Meyerowitz for agreeing to be in my PhD committee. I would also like to thank Dr. Tomas Schonbek, Dr. Fred Richman, Dr. William Kalies, Dr. Thomas Eisenbarth, Dr. Rainer Steinwandt, Dr. Lee Klingler, Dr. Ronald Mullin, Dr. Stephen Locke, Dr. Hongwei Long, and Dr. Lianfen Qian who taught me graduate courses. I am grateful to other Faculty members of Department of Mathematical Sciences and to the department's administrative staff members Emily Cimillo, Beth Broer, and Helen Randall who, directly or indirectly, helped me with my studies while in the program.

I would like to remember many individuals, especially Cheban Acharya, Kashi Neupane, Nikhil and Nidhi Singhi, Nicola Pace, Shanaz Tiwari, Emre Kolotoğlu, Parshuram Budhathoki, Madhav Sharma, Bal Kumar Khadka, Chenchu Gottipati, and the Nepalese community in Boca Raton and West Palm Beach. They always helped and supported me.

I am always thankful to my parents for their unconditional love and unflagging

support. Last but the most important, I would like to thank my wife Juni Magar who felt my joy and sorrow in her bones for the last ten years, helping me row this academic boat towards my PhD completion.

ABSTRACT

Author:	Krishna B. Thapa Magar
Title:	Low rank transitive representations, primitive extensions, and the collision problem in $PSL(2,q)$
Institution:	Florida Atlantic University
Dissertation Advisor:	Dr. Spyros S. Magliveras
Degree:	Doctor of Philosophy
Year:	2015

Every transitive permutation representation of a finite group is the representation of the group in its action on the cosets of a particular subgroup of the group. The group has a certain *rank* for each of these representations. We first find almost all rank-3 and rank-4 transitive representations of the projective special linear group $PSL(2,q)$ where $q = p^m$ and p is an odd prime. We also determine the rank of $PSL(2,p)$ in terms of p on the cosets of particular given subgroups. We then investigate the construction of rank-3 transitive and primitive *extensions* of a simple group, such that the extension group formed is also simple. In the latter context we present a new, group theoretic construction of the famous Hoffman-Singleton graph as a rank-3 graph.

The study of group theoretic, Cayley hash functions, is of considerable interest in cryptography. We describe a collision-finding algorithm for two generator Cayley hash functions in $PSL(2,p)$, provide some computational results on *earliest* and *shortest* collisions, and present a conjecture about the existence of *good* generating pairs for such hash functions.

Dedicated to my parents and my wife.

LOW RANK TRANSITIVE REPRESENTATIONS, PRIMITIVE EXTENSIONS, AND THE COLLISION PROBLEM IN $PSL(2,q)$

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The 1960's and 1970's saw an explosion of activity in several areas of mathematics and computer science. Two of the most important such activities were in Group Theory and Computational Algebra. In particular the 1960s saw a powerful surge of work towards the classification of finite simple groups. The result was completed in the mid 1970s with the publication of the famous "*classification theorem of finite simple groups*". The original proof of the theorem consumed some 50,000 journal pages, which were later reduced to "only" about 10,000 pages. For the most part, the theorem was based on classifying simple groups by the isomorphism types of their centralizers of involutions. At the same time, several new, sporadic simple groups were discovered by a strongly geometric/combinatorial approach. This included understanding and classifying doubly transitive groups, and the work of D. G. Higman, J. McLaughlin, J. H. Conway, D. Livingstone, J. McKay, M. Hall Jr., Z. Janko, and many others in understanding and constructing low-rank primitive extensions of groups. The work of this period resulted in the discovery of several new sporadic simple groups, such as the Higman-Sims group [13], the McLaughlin group[24], the Janko groups, the Suzuki's group[32], the Conway groups[2], the Monster and Baby-Monster, the Rudvalis group[31], and several other groups. In particular, the theory of rank-3 primitive extensions is beautiful, simple and fruitful. Further work of D. G. Higman in *coherent configurations* and *intersection matrices* resulted in generalizations of the rank-3 case relating groups to association schemes and the Bose-Mesner algebra [4].

If we assume the correctness of the classification theorem of finite simple groups,

then we see that every finite simple group has a primitive permutation representation of rank at most 8. So, it made sense to ask the question: could a proof of the classification theorem of finite simple groups be based on the theory of primitive extensions of smaller simple groups? using perhaps a giant induction machinery. To know how to extend a particular permutation group G, one needs to know all the transitive representations of the group as well as the theory of the rank-ρ transitive extensions.

Since, with the exceptions of the Suzuki groups $Sz(2^p)$, and $PSL(3,3)$, all minimal simple groups are $PSL(2,q)$, in this thesis we attempt to understand the low rank transitive representations of the groups $PSL(2,q)$. This is a first step towards understanding a classification theory of finite simple groups, based on transitive extensions of smaller simple groups. Next, the dissertation explains some ideas about rank-3 transitive (primitive) extensions, the simplest pathway to learning about rank-ρ transitive (primitive) extensions. The dissertation also presents some applications of rank-3 primitive extensions for constructing some simple groups by the geometric/combinatorial approach.

Computation is a great approach to discovering a new theory. In the last 50 years, the development of computer science is leapfrogging every year. In particular, completely new ideas in cryptography have been introduced at a remarkable rate. In the 70's, public key cryptography was introduced, with the Diffie-Hellman key exchange, discovered by W. Diffie and M. Hellman [6], and the RSA public key cryptosystem introduced by R. Rivest, A. Shamir, and A. Adleman[29]. Later, the use of elliptic curves in cryptography was suggested independently by N. Koblitz [17] and V. S. Miller[25]. People also started to use non-abelian groups in cryptography. S. Magliveras pioneered a kind of non-abelian group theoretic cryptography [22] based on certain type of group factorizations known as *logarithmic signatures*. With his colleagues he published symmetric cryptosystem PGM[21] and public key cryptosystem

series MST1[23], MST2[20], and MST3[16].

This thesis also includes a computational approach to the study of security of Cayley hash functions based on $PSL(2, q)$.

Chapter 2 includes group theoretic basics, properties of the groups $PSL(2, q)$ which are of central interest in this thesis, graph constructions from group orbitals, properties of cryptographic hash functions, and the definition of a Cayley hash function.

Chapter 3 is about the low rank transitive representations of $PSL(2, q)$. There always exists a doubly transitive representation of $PSL(2, q)$ on $q + 1$ points. So, the attention is restricted to rank-3 and rank-4. It also includes the ranks of $PSL(2, p)$ in transitive representations on the cosets of some given subgroups.

Chapter 4 is about rank-3 extensions. The chapter includes properties and examples of rank-3 graphs. It also includes an idea of construction of a rank-3 extension and why the new groups constructed are usually simple. A completely new construction of the well known Hoffman-Singleton graph as a rank-3 graph is also included in this chapter.

Finally, chapter 5 includes an investigation on the strength of Cayley hash functions based on $PSL(2, p)$, over all possible classes of generating pairs (a, b), where the orders of a and b are $\frac{p-1}{2}$. We conclude with a conjecture that for each prime p there will always exist strong generating pairs. In spite of considerable effort, we have not been able to characterize mathematically such strong pairs.

CHAPTER 2

PRELIMINARIES

2.1 GROUP THEORY

We use familiar standard notation of basic group theory as for example in [9, 30]. In particular, if G is a group, we write $H \leq G$ to denote that H is a subgroup of G, $N \trianglelefteq G$ that N is a normal subgroup of G, and $N \overset{\chi}{\trianglelefteq} G$ when N is a characteristic subgroup of G. For $g \in G$, the order of g is denoted by $|g|$ and for a set A, the cardinality of A is denoted by $|A|$. For more complete information on these topics please see [10, 15, 19].

2.1.1 Group Actions

A *group action* is a triple (X, G, exp), where, X is a set, G is a group and $exp : X \times G \to X$ a mapping, which we denote as exponentiation, $((x, g) \mapsto x^g)$, such that

1. $x^1 = x$, for any $x \in X$, where 1 is the identity of G, and
2. $(x^g)^h = x^{(gh)}$, for any $x \in X$, and any $g, h \in G$.

Although we can define actions when either G or X or both are infinite, we assume here that G and X are finite. We simplify the notation (X, G, exp) to $G|X$ for a group action. We also say that G *acts on* X. If $G|X$ is a group action, then $|X|$ is called the *degree* of $G|X$.

2.1.2 Orbits, Stabilizers

A group action $G|X$ induces an equivalence relation on the set X as follows. If $x, y \in X$ we say that x is G-related to y, denoted here by $x \sim y$, if $x^g = y$ for some

$g \in G$. It is easy to check that $\sim$ is indeed an equivalence relation on X. The $\sim$-equivalence classes are called the *G-orbits* (or just *orbits*) of X. Thus, if $G|X$ is a group action, X is naturally partitioned as the disjoint union of orbits:

$$X = X_1 + X_2 + \cdots + X_r$$

where "+" here means the disjoint union of sets. Let $G|X$ be a group action, $A \subset X$ and $Q \subset G$. By A^Q we mean the subset $\{a^q : a \in A, q \in Q\}$ of X. If A is a singleton set $A = \{a\}$, we write a^Q for $\{a\}^Q$. Similarly if $Q = \{q\}$ is a singleton set, we write A^q for $A^{\{q\}}$. If $G|X$ is a group action, and $x \in X$, then the G-orbit containing x is just x^G.

Let $G|X$ be a group action and let $g \in G$. The set of all elements of X fixed by g, i.e. $\{x \in X : x^g = x\}$ is denoted by *Fix(g)*. The cardinality of *Fix(g)* is called the *character* of g, denoted by $\chi_{G|X}(g)$ or simply $\chi(g)$, and the mapping $\chi : g \to \chi(g)$ is called the *character* of the group action.

Let $G|X$ be a group action and let $x \in X$. The collection of all group elements fixing x is called the *stabilizer* of x in G and is denoted by G_x. Thus, $G_x = \{g \in G : x^g = x\}$. G_x is a subgroup of G. For $x \in X$ and for $g, h \in G$, $x^g = x^h$ if and only if g and h are in the same right coset of G_x. Hence, $|x^G| = [G : G_x]$. So that the size of each orbit in a group action $G|X$ divides the order of G. Consider the decomposition of G as the union of distinct right cosets of G_x:

$$G = G_x x_1 + G_x x_2 + \cdots + G_x x_r \ .$$

Then, the complete orbit x^G is in fact equal to $\{x^{x_1}, x^{x_2}, \ldots, x^{x_r}\}$.

A particular group action $G|X$, where $X = G$ is important, known as *conjugation*. Here, for $a, g \in G$, a^g is defined by: $a^g = g^{-1}ag$. In a group G two elements a, b are said to be *conjugate* in G if and only if $b = a^g = g^{-1}ag$ for some $g \in G$. Thus, two elements are conjugate if and only if they are in the same G-orbit in the action $G|G$ by conjugation. The G-orbits of G in the action $G|G$ by conjugation are called the

conjugacy classes of G. G is the disjoint union of its conjugacy classes:

$$G = K_1 + K_2 + \cdots + K_c$$

and c is called the *class number* of G. It follows that the size of each class K_i divides $|G|$.

If G is a group, $A \subseteq G$, and $g \in G$, we denote by A^g the set $\{a^g : a \in A\}$, where $a^g = g^{-1}ag$ as above, i.e. conjugation of a by g. It is easy to show that in fact G acts on the power set $\mathcal{P}(G)$ of G by conjugation, moreover the collection $\Lambda(G)$ of all subgroups of G is the union of orbits of $G|\mathcal{P}(G)$. Thus G also acts on $\Lambda(G)$ by conjugation. Two subgroups H and K of G are said to be *conjugate* if they lie in the same G-orbit of $\Lambda(G)$, i.e. if $H^g = K$ for some element $g \in G$.

Lemma 2.1.1. *Suppose that $G|X$ is a group action, $x \in X$ and $g, h \in G$, then*

i) $Fix(g^h) = (Fix(g))^h$.

ii) $\chi(g) = \chi(g^h)$.

iii) $G_{x^g} = (G_x)^g$.

Proof. i) Let $a \in Fix(g^h)$, then $a^{(g^h)} = a$, therefore $a^{(h^{-1}gh)} = a$, which implies that $a^{h^{-1}g} = a^{h^{-1}}$. Let $b = a^{h^{-1}}$, then $a = b^h$ and $b^g = b$, i.e., $b \in Fix(g)$. Therefore, $a = b^h \in (Fix(g))^h$. The other direction follows similarly.

ii) By definition, and using the result above, we get,

$$\chi(g) = |Fix(g)| = |(Fix(g))^h| = |Fix(g^h)| = \chi(g^h).$$

iii) Let $x \in X$. If $k \in G_{(x^g)}$, then $(x^g)^k = x^g$. So that, $(x^{gk})^{g^{-1}} = x$, which implies $gkg^{-1} \in G_x$ and hence, $k \in g^{-1}G_xg = (G_x)^g$. The other direction follows similarly.

□

Notice that "exponentiation" has two different meanings in the statements above. Thus, if $x, y \in X$ are two elements of the same G-orbit in a group action $G|X$, the stabilizers G_x and G_y are conjugate subgroups of G, hence in fact isomorphic groups.

The *kernel* of a group action $G|X$ denoted by $ker(G|X)$, is defined to be the set $\{g \in G : Fix(g) = X\}$. Since $ker(G|X) = \bigcap_{x \in G} G_x$, $ker(G|X)$ is a normal subgroup of G. $G|X$ is called *faithful* if and only if $ker(G|X) = 1$. The mapping $\pi : G \to \mathbb{S}_X$ from G into the symmetric group on X, defined by:

$$\pi : g \mapsto \begin{pmatrix} x \\ x^g \end{pmatrix}$$

is a representation (homomorphism) of G into $\mathbb{S}_X$ with kernel $ker(G|X)$. Thus a group action can be viewed as a permutation representation of a given group. The converse is also true.

We now state the *Cauchy-Frobenius lemma* without proof. Erroneously, this well known lemma is also called *Burnside's* lemma.

Lemma 2.1.2. *(Cauchy-Frobenius Lemma) Let $G|X$ be a group action, and let $X = X_1 + X_2 + \cdots + X_\rho$ be the decomposition of X into G-orbits, then:*

$$\rho = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

In actual applications it is much more convenient to use the above lemma in the following form:

Lemma 2.1.3. *Let $G|X$ be a group action, and let $G = K_1 + K_2 + \cdots + K_c$ be the decomposition of G as the union of its disjoint conjugacy classes. Let ρ be as above. Then,*

$$\rho = \sum_{i=1}^{c} \frac{\chi(g_i)}{|C(g_i)|}, \text{ where } g_i \in K_i.$$

Here, $C(a) = \{g \in G : ag = ga\}$, is the *centralizer* of a in G, the stabilizer of a in the action $G|G$ by conjugation.

Definition 2.1.1. *Suppose that $G|X$ and $Q|Y$ are two group actions with $\eta : X \times G \to X$ and $\theta : Y \times Q \to Y$ the corresponding action mappings. We say that the two actions are isomorphic if and only if*

1. *There exists a group isomorphism $\phi : G \to Q$, and*
2. *There exists a bijection $\lambda : X \to Y$, so that the following diagram of mappings commutes:*

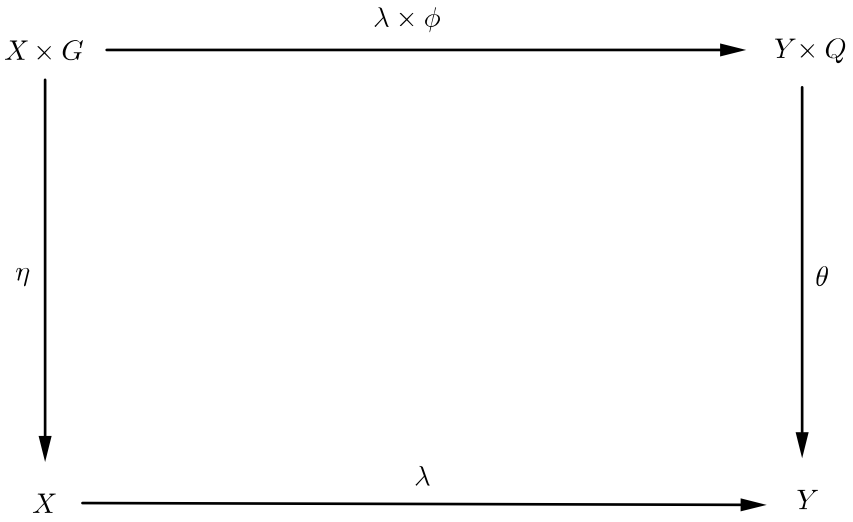

Figure 2.1: Commuting diagram

Definition 2.1.2. *A group action $G|X$ is said to be* transitive *if and only if X is a single G-orbit. Thus, $G|X$ is transitive if and only if for any two elements $x, y \in X$ there exists a group element $g \in G$ such that $x = y^g$.*

Definition 2.1.3. *An action $G|X$ is called* semiregular *if and only if $G_x = 1$ for each $x \in X$. Thus in a semiregular action, the stabilizer of any point of X is the identity in G. It follows that in a semiregular group action, all orbits have the same length, namely $|G|$. A semiregular group action $G|X$ is also called* $\frac{1}{2}$-transitive.

Definition 2.1.4. *An action $G|X$ is called* regular *if and only if it is both transitive and semiregular. Thus, in a regular group action X is a single G-orbit, and $|X| = |G|$.*

2.1.3 Induced Actions

If $G|X$ is a group action, there are numerous other actions that are related to $G|X$. We describe some of these here.

Restriction of an action

Suppose that $G|X$ is a group action and H be a subgroup of G. Then, by restricting $exp : X \times G \to X$ to $X \times H$, we obtain the action $H|X$, described also by $(x, h) \mapsto x^h$.

Suppose next that $G|X$ is a group action and that Y is the union of one or more G-orbits of X. Then we obtain an action $G|Y$, by restricting the action of G to Y only as follows: $(y, g) \mapsto y^g$ for any $y \in Y$, $g \in G$.

The induced action on ordered pairs

Let G be a group, X and Y two sets, and suppose that $G|X$ and $G|Y$ are two actions of G on X and Y respectively. A new action $G|(X \times Y)$ can be defined in the obvious way: For $(x, y) \in X \times Y$ and $g \in G$, $(x, y)^g = (x^g, y^g)$. In the special case where $X = Y$, above, the group action $G|X$ induces an action $G|(X \times X)$ as follows: $(x, y)^g = (x^g, y^g)$ for $x, y \in X, g \in G$. If $|X| \geq 2$, then there will be at least two G-orbits in $X \times X$. This is true even when $G|X$ is a transitive action. The G-orbits on $X \times X$ are called *orbitals* .

If the induced action $G|(X \times X)$ has exactly two orbitals, then $G|X$ must be transitive, and

$$X \times X = I + \Delta$$

where I is the *identity* or *diagonal* orbital $(x, x)^g$, and Δ the orbital $(x, y)^g$, where $x \neq y \in X$.

Definition 2.1.5. *$G|X$ is called a* doubly transitive *action if $G|(X \times X)$ has exactly 2 orbitals. This is equivalent to saying that for any (x_1, y_1) and (x_2, y_2), for which $x_1 \neq y_1$, and $x_2 \neq y_2$, there exists $g \in G$ such that $(x_1, y_1)^g = (x_2, y_2)$.*

Induced action on ordered k-sets, k-transitivity

If $G|X$ is a group action and $Y = \{(x_1, x_2, \ldots, x_k) : x_i \in X, x_i \neq x_j \text{ for } i \neq j\}$, then $G|X$ induces an action $G|Y$ by: $(x_1, x_2, \ldots, x_k)^g = (x_1^g, x_2^g, \ldots, x_k^g)$.

Definition 2.1.6. *A group action $G|X$ is said to be* k-transitive *if and only if the action on ordered k-tuples (described above) is transitive. Thus, $G|X$ is k-transitive if and only if for any two ordered k-tuples $(x_1, x_2, \ldots, x_k)$, $(y_1, y_2, \ldots, y_k)$ of elements of X, with the x_i distinct, and the y_i distinct, there exists an element $g \in G$ such that*

$$(x_1, x_2, \ldots, x_k)^g = (y_1, y_2, \ldots, y_k).$$

For $k \geq 2$, it is easy to prove that if $G|X$ is k-transitive, then it is also $(k-1)$-transitive. Moreover, $G|X$ is k-transitive if and only if $G_x|(X \setminus \{x\})$ is $(k-1)$-transitive.

Induced Action on unordered k-sets, k-homogeneity

Let $G|X$ be a group action, and $Y = \binom{X}{k}$ be the collection of all (unordered) k-subsets of X, thus, $|Y| = \binom{|X|}{k}$. The action $G|X$ induces an action $G|Y$ by: $(A, g) \mapsto A^g$, for $A \in Y$, $g \in G$.

Definition 2.1.7. *Let $k \geq 2$. A group action $G|X$ is called* k-homogeneous*, or* k^*-transitive*, if the induced action of G on $\binom{X}{k}$ is transitive.*

It is clear that if $G|X$ is k-transitive then it is also k^*-transitive. Consider the following result proved around 1965.

Theorem 2.1.1. *(Livingstone & Wagner) Let $G|X$ be a group action, and suppose that $2 < k \leq \frac{|X|}{2}$. Then [The number of orbits of G on unordered k-sets] $\geq$ [The number of orbits of G on ordered (k-1)-sets].*

In particular, if G is k^*-transitive, then it must be $(k-1)$-transitive. The following result however is rather surprising:

Theorem 2.1.2. *(Livingstone & Wagner) If $G|X$ is k^*-transitive and $k \geq 5$, then $G|X$ is also k-transitive.*

Thus, for $k \geq 5$ the notions of k-transitivity and k-homogeneity coincide.

Definition 2.1.8. *$G|X$ is said to be of type k^* if and only if it is k^*-transitive but not k-transitive.*

Group actions of type k^* exists only for $k = 2, 3, 4$. [35]

Theorem 2.1.3. *(Kantor W., 1968) If $G|X$ is of type 4^*, then $G \cong PSL_2(5)$, $PGL_2(5)$, $PSL_2(8)$, $P\Gamma L_2(8)$, or $P\Gamma L_2(32)$ in their canonical permutation representations.(errata:above is valid only if $|G_x|$ is odd.)*

2.1.4 Primitivity

Let $G|X$ be a transitive group action. A subset Δ of X is called a *block of imprimitivity* (b.i) if for any $g \in G$, $\Delta \cap \Delta^g = \Delta$ or $\emptyset$. The subsets $\emptyset, X$ and the singleton sets $\{x\}, x \in X$ are always blocks of imprimitivity for $G|X$, the *trivial* blocks. If the only blocks of imprimitivity for $G|X$ are trivial, then $G|X$ is called a *primitive* action.

If Δ is a non-trivial b.i. for a transitive action $G|X$, let $x \in \Delta$ and $y \notin \Delta$. Since $G|X$ is transitive, there exists $g \in G$ such that $x^g = y$, but then $\Delta \cap \Delta^g = \emptyset$, while of course, $|\Delta^g| = |\Delta|$. Moreover, Δ^g is also a b.i. By letting y range over $X \backslash \Delta$ we can cover X with sets Δ^g that is, we get a regular partition of X as the disjoint union of b.i.'s. The collection of distinct b.i.'s obtainable this way from a single one is called a *system of imprimitivity*. A consequence of the fact that X is the disjoint union of sets of size $|\Delta|$, is that the size of any b.i. divides $|X|$.

Let $G|X$ be a transitive action, and Δ a non-trivial b.i. The set $H = \{g \in G : \Delta^g = \Delta\}$ is easily seen to be a subgroup of G, and if $x \in \Delta$, then $G_x \lneqq H \lneqq G$. Conversely, if $G|X$ is a transitive group action, and H is an intermediate subgroup containing G_x, for some $x \in X$, say $G_x \lneqq H \lneqq G$, then the set $\Delta = x^H$ is easily seen to be a b.i. for $G|X$. Thus, we have the following lemma:

Lemma 2.1.4. *A transitive action $G|X$ is primitive if and only if G_x is a maximal subgroup of G. Also, a 2-transitive action $G|X$ must be primitive.*

2.1.5 Basic theorem for transitive permutation representations

Let H be a subgroup of a group G. By a right(left) transversal of H in G, we mean a complete set $T = \{x_i\}$ of distinct right(left) coset representatives of H. The following theorem characterizes the transitive actions of a group G, and investigates the corresponding character of such a group action.

Let G be a group, H a subgroup of G and let X be the collection of all distinct right cosets of H in G. Consider the group action $G|X$ defined by $(Hx, g) \mapsto Hxg$. For a discussion of induced representations, induced characters, and proofs or the various parts of the theorem that follows, see [7, 9].

Theorem 2.1.4. *(a) The action $G|X$ defined above is transitive, with kernel the* core *N of H, that is, $N = core(H) := \bigcap_{x \in G} H^x$.*

(b) The character θ of the above action is the induced *character $\theta = [1]_H \uparrow^G$ of the* principal *character of H, $[1]_H$, to G.*

(c) If we let $g = |G|$, $h = |H|$, $x \in G$, $K_x = x^G$ the conjugacy class of $x \in G$, $g_x = |K_x|$ and $h_x = |K_x \cap H|$, then

$$\theta(x) = \frac{g \cdot h_x}{h \cdot g_x}.$$

(d) Any transitive action $G|\Omega$ is equivalent to a group action $G|X$ as above, where H can be chosen to be the stabilizer G_x for any given $x \in \Omega$.

(e) Two transitive actions $G|X$ and $G|Y$ of a group are equivalent if and only if, for $x \in X$, and $y \in Y$ the stabilizers G_x and G_y are conjugate in G.

2.1.6 Special linear group and projective special linear group

Given a finite field $\mathbb{F}_q = GF(q)$, of q elements, and a fixed natural number$n$, the group of all $n \times n$ non-singular matrices with respect to the operation of matrix

multiplication is known as the *general linear group* of degree n over $\mathbb{F}_q$, and is denoted by $GL(n,q)$. The order of the group is $|GL(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i)$. The set of all matrices in $GL(n,q)$ of determinant 1 forms a subgroup of $GL(n,q)$, the *special linear group*, denoted by $SL(n,q)$. $SL(n,q)$ is the kernel of the *determinant* homomorphism $det : GL(n,q) \to \mathbb{F}_q^*$, and therefore $|SL(n,q)| = \frac{|GL(n,q)|}{q-1}$. The center $Z(GL(n,q))$, of $GL(n,q)$, consists of all scalar matrices $\{\lambda I : \lambda \in \mathbb{F}_q^*\}$, thus the center of $SL(n,q)$ consists of all matrices $\{\lambda I : \lambda^n = 1\}$. The *projective special linear group* of degree n over $\mathbb{F}_q$, is the quotient group $PSL(n,q) = SL(n,q)/Z(SL(n,q))$. Here, we deal with the case $n = 2$, where q is odd, hence $|SL(2,q)| = q(q^2-1)$ and $|PSL(n,q)| = \frac{q(q^2-1)}{2}$.

For the group $PSL(n,q)$ it is also common to use the following notation: $PSL_n(q)$, $PSL_n(\mathbb{F}_q)$ or $PSL(n,\mathbb{F}_q)$, and similarly for the group $SL(n,q)$ to use the notation: $SL_n(q), SL_n(\mathbb{F}_q)$ or $SL(n,\mathbb{F}_q)$. $PSL(n,q)$ is also called the *linear fractional* group over $\mathbb{F}_q$ and is also denoted by $LF_n(q)$. The latter terminology is rather old, and comes from the classical linear fractional transformations of the Complex plane $\mathbb{C}$.

In what follows we state without proof some of the properties of the groups $PSL(2,q)$ as they are central in my research. The properties discussed below are well known and can be found in [3].

For $q \geq 4$ the groups $PSL(2,q)$ are simple. For q an odd prime power, let $\mathbb{F}_q$ be Galois field of q elements and V the 2-dimensional vector space over $\mathbb{F}_q$. Two non-zero vectors $\mathbf{u},\mathbf{v} \in V$ are defined to be *projectively equivalent* if $\mathbf{u} = s\mathbf{v}$ for some $s \in \mathbb{F}_q^*$. The $q+1$ equivalence classes constitute the *projective line* $\mathcal{L}$, and $G = PSL(2,q)$ acts doubly transitively on $\mathcal{L}$ by left multiplication of V by the elements of G, modulo non-zero scalar multiples from $\mathbb{F}_q$, that is

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\right) \to \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix}\right) \to \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} \to \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

As can be seen from the above line, a convenient way of viewing projectively the elements of $\mathcal{L}$ is to think of $\binom{x}{y}$ as the quotient $\frac{x}{y} \in \mathbb{F} \cup \{\infty\}$, where we assign ∞ to quotients $\frac{x}{0}$ when $x \neq 0$, and the element $\frac{x}{y} \in \mathbb{F}$ otherwise.

It is also the case that there are exactly $q+1$ Sylow-p subgroups of G on which G acts doubly-transitively by conjugation. The latter representation of G is equivalent to the doubly transitive representation of G mentioned earlier. A Sylow-p subgroup Q of G is isomorphic to the additive group of $\mathbb{F}_q$, hence it is elementary abelian of order $q = p^m$. The normalizer in G of Q is of order $\frac{q(q-1)}{2}$ and is a split extension of Q by cyclic group of order $\frac{q-1}{2}$. When $q \equiv 3 \pmod 4$, G acts as a 3-homogeneous group on the projective line $\mathcal{L}$. G is 2-transitive on $\mathcal{L}$ but fails to be 3-homogeneous when $q \equiv 1 \pmod 4$.

We gain further understanding of the structure of the groups $PSL(2,q)$ when we examine the following:

Proposition 2.1.1. *For $q = p^m$, p an odd prime, consider the group $G = PSL(2,q)$ in its doubly transitive representation on the $q+1$ points of $\mathcal{L}$, and suppose that $g \in G$. Then g is semi-regular on the points of $\mathcal{L}$ not fixed by g, i.e. excluding the fixed points, all cycles of g have the same length. Moreover, exactly one of the following holds:*

i) *g fixes 0 points, and belongs to a cyclic subgroup of order $\frac{q+1}{2}$ or,*

ii) *g fixes exactly 1 point and is of order p, or,*

iii) *g fixes exactly two points and belongs to a cyclic subgroup of order $\frac{q-1}{2}$.*

We will need some additional well known facts about the groups $PSL(2,q)$, $q = p^m$, p an odd prime, which we state below without proof, as a proposition. In what follows ϕ stands for the Euler ϕ function.

Proposition 2.1.2. *Suppose that $G = PSL(2,q)$, $q = p^m$, p an odd prime. Then,*

i) *The Sylow-p subgroup of G is elementary abelian of order q.*

ii) *If $g \in G$ is of order d, then d divides $\frac{q-1}{2}$, or $d = p$, or d divides $\frac{q+1}{2}$.*

iii) *There is a single conjugacy class of cyclic subgroups of order $\frac{q-1}{2}$. Similarly, there is a single conjugacy class of cyclic subgroup of order $\frac{q+1}{2}$.*

iv) *If $g \in G$ is of order $d \neq 2$ dividing $\frac{q\pm1}{2}$, then g belongs to one and only one cyclic subgroup of G of order $\frac{q\pm1}{2}$.*

v) *If $d \neq 2$ divides $\frac{q\pm1}{2}$, there are $\frac{\phi(d)}{2}$ conjugacy classes of elements of order d in G. If $g \in G$ is an element of order d, then g is conjugate to g^{-1}.*

vi) *If $g \in G$ is of order $d|\frac{q\pm1}{2}$, $d \neq 2$. then the centralizer $C_G(g)$ is $\langle g \rangle$, while the normalizer $N_G(\langle g \rangle)$is dihedral of order $q \pm 1$.*

vii) *The centralizer of an element of order 2 has order $q-1$ if $q \equiv 1$ (mod 4) and $q+1$ if $q \equiv 3$ (mod 4).*

2.2 GROUPS AND THEIR GRAPHS

Let G be a transitive permutation group acting on a finite set X, and consider the action of G on $X \times X$. Recall that G-orbit in $X \times X$ are called orbitals. Clearly, $I = \{(x, x) : x \in X\}$ is always an orbital of G. If Δ is an orbital, then for $x \in X$ set $\Delta(x) = \{y \in X : (x, y) \in \Delta\}$. Let G_x be the subgroup of G which fixes x, and observe that $\Delta(x)$ is an orbit of G_x on X as the following demonstrates. If $y \in \Delta(x)$ and $g \in G_x$, then $(x, y) \in \Delta$ implies $(x^g, y^g) = (x, y^g) \in \Delta$, and thus $y^g \in \Delta(x)$. Conversely, if y_1 and y are in the same G_x-orbit of X, then there exists a permutation $g \in G_x$ such that $y_1 = y^g$, so $(x, y) \in \Delta$ implies $(x^g, y^g) = (x, y_1) \in \Delta$, so $y_1 \in \Delta(x)$. Hence $\Delta(x)$ is a G_x-orbit of X. Let Y be any G_x-orbit of X. If $x \in Y$, then $Y = \{x\}$. If $y \in Y$, $y \neq x$, then (x, y) is in some orbital $\Delta \neq I$ of $X \times X$, so $\Delta(x)$ is a G_x-orbit and $y \in \Delta(x)$, therefore $Y = \Delta(x)$. For fixed x, this establishes a one-to-one correspondence between G-orbitals and G_x-orbits. The *rank* of G is the number of orbitals of G, or equivalently the number of orbits of G_x for any $x \in X$

If Δ is an orbital, then $\Delta(x)^g = \Delta(x^g)$ for all $g \in G$. Moreover, the *converse* $\Delta^C = \{(y, x) : (x, y) \in \Delta\}$ of Δ is again orbital, so that $\Delta \mapsto \Delta^C$ is a pairing of the set of orbitals.

Lemma 2.2.1. *An orbital Δ is either symmetric ($\Delta = \Delta^C$) or asymmetric ($\Delta \cap \Delta^C = \emptyset$).*

Proof. To see this, suppose Δ is not asymmetric and $\Delta \neq I$ (clearly I is symmetric). Then there must be two ordered pairs $(x_1, y_1), (y_1, x_1) \in \Delta$, with $x_1 \neq y_1$. Now let (x, y) be any other ordered pair in Δ. Since Δ is an orbital, there exist $g_1, g_2 \in G$ such that $(x_1, y_1) = (x, y)^{g_1}$ and $(y_1, x_1) = (x_1, y_1)^{g_2}$. Then, $(x, y)^{g_1 g_2 g_1^{-1}} = (y_1, x_1)^{g_1^{-1}} = (y_1^{g_1^{-1}}, x_1^{g_1^{-1}}) = (y, x)$, so Δ is symmetric. □

The classical condition for the existence of a symmetric orbital is now stated. For the proof, see Wielandt [34], p.45.

Theorem 2.2.1. *A transitive permutation group G has a symmetric orbital other than I if and only if G has even order.*

Since an orbital $\Delta \neq I$ is a **relation** on X, we can form a digraph (which when symmetric is a graph) $\mathcal{G}_\Delta = (X, \Delta)$ having vertex set X and edge set (strictly speaking, directed edge set) Δ. Every orbital $\Delta \neq I$ is irreflexive, hence $\mathcal{G}_\Delta$ has no loops and is either an ordinary graph (if symmetric) or an oriented graph (if asymmetric).

Using the 1-1 correspondence between orbitals of G and G_x- orbits, we now obtain an alternate description of the graph we have just constructed. Let x be a fixed element of X and let $\Delta(x)$ be an orbit of G_x on X corresponding to an orbital Δ. It is then obvious that $\Delta(x)$ consists of precisely the vertices of $\mathcal{G}_\Delta$ that are adjacent to x. Since G is transitive, for all $y \in X$, there is a $g \in G$ such that $y = x^g$. But earlier we observed that $\Delta(x^g) = \Delta(x)^g$; hence the vertices adjacent to $y = x^g$ are the images under g of the vertices adjacent to x. This means that G is a subgroup of the automorphism group of $\mathcal{G}_\Delta$ which is transitive on the edges of $\mathcal{G}_\Delta$ as well as vertices. It follows that $\mathcal{G}_\Delta$ could have been constructed by joining a vertex x to a vertex y in the orbit $\Delta(x)$ of G_x; all other edges in $\mathcal{G}_\Delta$ are images of this edge under elements of G.

An easy example: We illustrate the rank of a group using the cyclic group of order 4. Let $X = \{1, 2, 3, 4\}$ and let $G = \langle (1\ 2\ 3\ 4) \rangle$. Let Δ be the orbital containing (1 2).

Then $\Delta = \{(1\ 2), (2\ 3), (3\ 4), (4\ 1)\}$ and $\mathcal{G}_\Delta$ is an oriented graph consisting of the directed 4-circuit.

Let Γ be the orbital containing (1 3). Then $\Gamma = \{(1\ 3), (2\ 4), (3\ 1), (4\ 2)\}$ and so $\mathcal{G}_\Gamma$ is the (undirected) graph.

Let Φ be the orbital containing (1 4). Then $\Phi = \{(1\ 4), (2\ 1), (3\ 2), (4\ 3)\}$ and $\mathcal{G}_\Phi$ is the oriented graph which is the converse of $\mathcal{G}_\Delta$.

The four orbitals Δ, Γ, Φ and I exhaust $X \times X$; hence this group G has rank 4.

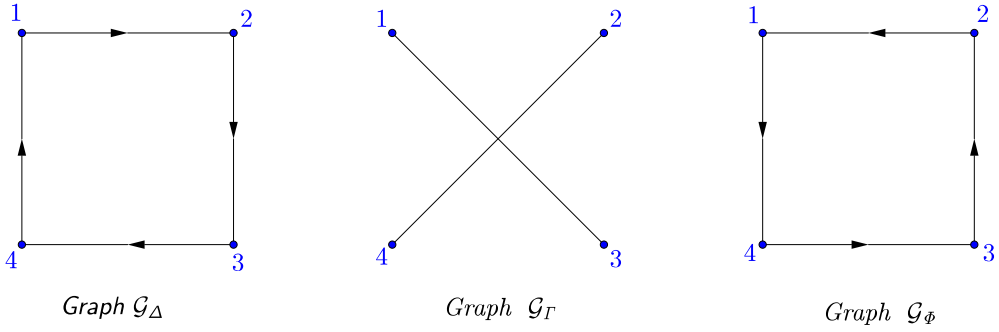

Figure 2.2: Graphs

2.3 MINIMAL NORMAL SUBGROUPS

Recall that a subgroup N of a group G is *normal*, denoted by $N \trianglelefteq G$, if it is invariant under all *inner automorphisms* of G. If a given subgroup H of G is invariant under *all automorphisms* in $Aut(G)$ then H is said to be *characteristic* in G, denoted by $H \overset{\chi}{\trianglelefteq} G$.

Results concerning characteristic subgroups are:

1. Characteristic subgroups are normal.

2. If H is a unique subgroup of G of a given order, then H is characteristic in G.

3. Recall that if $H \trianglelefteq K$ and $K \trianglelefteq G$, it does not necessarily follow that $H \trianglelefteq G$. However if $K \overset{\chi}{\trianglelefteq} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$.

Thus we may think of characteristic subgroups as "strongly normal" subgroups. For example, every subgroup of a cyclic group is characteristic.

A group G is said to be *simple* if it has no proper, non-trivial normal subgroups. G is said to be *characteristically simple* if it has no proper, non-trivial characteristic subgroups. We state an important theorem about the structure of characteristically simple groups.

Theorem 2.3.1. *If G is a finite characteristically simple group, then $G \cong H \times H \times \cdots \times H$ where H is simple.*

Corollary 2.3.1. *If G is characteristically simple, then either*

1. *$G = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, or*

2. *$G = A \times A \times \cdots \times A$, where A is non-solvable simple.*

For any group G, a *minimal normal subgroup* is a normal subgroup M of G such that the only normal subgroups of G which are contained in M are 1 and M. Every minimal normal subgroup of a group is characteristically simple. In particular, every minimal normal subgroup of a finite solvable group is an elementary abelian p-group for some prime p.

Proofs of above results can be found in group theory books, for example [1, 30]

2.4 CRYPTOGRAPHIC HASH FUNCTIONS

A *hash function* is any function that can be used to map digital data of arbitrary size to digital data of much smaller, fixed size. Denote by h such a hash function. For message bit string x, the value $y = h(x)$ is called the hash value, message digest, digital fingerprint, or simply the hash of x. A *cryptographic hash function* is a hash function which is considered practically infeasible to invert, that is, to recreate any

preimages from the hash value alone. Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication.

2.4.1 Properties of cryptographic hash functions

To be considered secure, a hash function h has to satisfy the following three properties:

i) Pre-image resistance: Given a hash value y, it should be difficult to find any message x such that $y = h(x)$. This concept is related to that of one-way function. Functions that lack this property are vulnerable to *pre-image attacks*.

ii) Second pre-image resistance: Given an input x_1 it should be difficult to find another input x_2 such that $x_1 \neq x_2$ and $h(x_1) = h(x_2)$. Functions that lack this property are considered vulnerable to *second pre-image attacks*.

iii) Collision resistance: It should be difficult to find two different messages x_1 and x_2 such that $h(x_1) = h(x_2)$. Such a pair is called a cryptographic hash collision. This property is sometimes referred to as *strong collision resistance*. It requires a hash value at least twice as long as that required for pre-image resistance; otherwise collisions may be found by what is known a *birthday* attack.

2.4.2 A construction based on Cayley Graphs

Given a (multiplicative) group G and a generating set $S = \{s_1, \dots s_k\}$ of G, the corresponding *Cayley graph* is a $k-$regular graph that has vertex set G and there is an edge between two vertices u and v if and only if $v = us_i$ for some $s_i \in S$. We can build a hash function from this graph as follows. The message m is first written as a string $m = m_1 \dots m_N$ where $m_i \in \{1, \dots, k\}$. Then the group product

$$h = s_{m_1} s_{m_2} \cdots s_{m_N}$$

is computed and mapped onto a bitstring. A hash function constructed in this way is called a *Cayley hash function.*

Several Cayley hash functions are proposed in the literature that use the matrix group $SL(2,\mathbb{F})$ or $PSL(2,\mathbb{F})$, where $\mathbb{F}$ is either $\mathbb{F}_p$ or $\mathbb{F}_{2^p}$ [5, 33]. At CRYPTO'94, Jean-Pierre Tillich and Gilles Zémor, [33] introduced a new family of Cayley functions defined as follows:

Consider a finite field of order 2^n given by $\mathbb{F}_{2^n} := \mathbb{F}[x]/\langle q(x)\rangle$ where $q(x)$ is a given irreducible polynomial of degree n. Let α be a root of $q(x)$ and denote by G the group $SL_2(\mathbb{F}_{2^n})$ of 2×2 matrices of determinant 1 over $\mathbb{F}_{2^n}$. Define the matrices s_0 and s_1 of group G by:

$$s_0 := \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix}, \; s_1 := \begin{pmatrix} \alpha & \alpha+1 \\ 1 & 1 \end{pmatrix}$$

According to the Tillich-Zémor proposal, a binary bitstring $v = b_1 \dots b_m \in \{0,1\}^*$ is hashed by applying the function $h : \{0,1\}^* \to G$:

$$h(b_1 \dots b_m) := s_{b_1} \dots s_{b_m} \in G.$$

One big advantage of Cayley hash functions over classical hash functions is that their computation can be very easily parallelized. Large messages can be cut into various pieces and distributed to different computing units, and the associativity of group ensures that the final result can be recovered from all partial products.

CHAPTER 3

LOW RANK TRANSITIVE REPRESENTATIONS OF $PSL(2, q)$

Let $G|X$ be a transitive action of a group G on a set X. Then, by the rank ρ of the action, we mean the number of orbits of G on $X \times X$, or equivalently, the number of orbits of G_x on X for $x \in X$. Rank 2 means doubly transitive. It is well known that every $PSL(2, q)$, where q is a prime power, has a doubly transitive representation on the $q + 1$ points of the projective line. So, for odd q, there always exists a rank-2 representation of $PSL(2, q)$ on the cosets of a subgroup of order $\frac{q(q-1)}{2}$. We will choose q to be an odd prime power and will discuss rank-3 and rank-4 representations of $PSL(2, q)$. We will use the notation $(n_1, n_2, \ldots, n_\rho)$ to denote the orbits sizes of G_x on X, and call $(n_1, n_2, \ldots, n_\rho)$ the *subdegrees* of $G|X$.

Let $G|X$ be a rank$-\rho$ transitive permutation group of order g and let h be the order of the subgroup G_x fixing a point x. One orbit of G_x is {x} of length 1. The maximum length of each of the other $\rho - 1$ G_x-orbits is h. So that, $1 + (\rho - 1)h \geq |X|$. Thus, using the transitivity of G on X and $[G : G_x] = |x^G|$, we get $\frac{g}{h} = |X| \leq 1 + (\rho - 1)h$ and therefore, $h(1 + (\rho - 1)h) \geq g$. Hence, we have:

$$\begin{aligned} &h(1 + 2h) \geq g \text{ for } \rho = 3, \text{ and} \\ &h(1 + 3h) \geq g \text{ for } \rho = 4 \end{aligned} \tag{3.1}$$

3.1 LOW RANK TRANSITIVE REPRESENTATION OF $PSL(2, p)$

To illustrate the use of above inequalities, we will first find all rank-3 and rank-4 representations of the groups $PSL(2, p)$ for an odd prime p. In chapter 20 of [1], all subgroups $H \leq PSL(2, p)$ are determined and if $h = |H|$, it is shown that $h \leq p - 1$

or h is p, $p+1$, pd_- (where $d_-|\frac{p-1}{2}$), 12, 24 or 60. In Theorem 2.4 of [15], all the subgroups of $PSL(2,q)$ are listed. Below is that particular theorem, where $q=p^m$, p an odd prime, $G=PSL(2,q)$, $M(q)=\frac{q(q^2-1)}{2}$, $d_\mp$ is any divisor of $\frac{q\mp1}{2}$, $d_\mp \neq 1$, $r_\mp=\frac{(q\mp1)/2}{d_\mp}$ and G_d denotes a subgroup of order d.

Theorem 3.1.1. *[I. Ilić [15]] Using the notation mentioned above, G has*

1. *$q+1$ conjugate elementary abelian groups of order q,*
2. *$\frac{q(q\pm1)}{2}$ conjugate cyclic groups $G_{d_\mp}$ of order $d_\mp$,*
3. *$\frac{M(q)}{2d_\mp}$ conjugate dihedral groups of order $2d_\mp$ for $r_\mp$ odd,*
4. *Two systems each of $\frac{M(q)}{4d_\mp}$ conjugate dihedrals $G_{2d_\mp}$ for $r_\mp$ even, $d_\mp>2$,*
5. *For $q\equiv\pm3$ (mod 8), one set of $\frac{M(q)}{12}$ conjugate Klein 4-groups,*
6. *For $q\equiv\pm1$ (mod 8), two sets each of $\frac{M(q)}{24}$ conjugate Klein 4-groups,*
7. *$\frac{(p^m-1)(p^m-p)\cdots(p^m-p^{m-1})}{(p^t-1)(p^t-p)\cdots(p^t-p^{t-1})}$ sets each of $\frac{p^{2m}-1}{(2,1)(p^k-1)}$ conjugate abelian groups of order p^t, for each $t\leq m$, where (2,1) is read 2 or 1 depending as $\frac{m}{k}$ is an even or odd integer. Here, k is a divisor of t depending on the particular G_{p^t},*
8. *Certain sets of $\frac{(p^{2m}-1)p^{m-t}}{(2,1)(p^k-1)}$ conjugate $G_{p^td_-}$, where k and d_- depend on t, where $t|m$,*
9. *(2,1) sets each of $\frac{M(q)}{(2,1)M(p^k)}$ conjugate $G_{M(p^k)}\cong PSL(2,p^k)$, where $k|m$,*
10. *Two systems each of $\frac{M(q)}{2M(p^k)}$ conjugate groups $G_{2M(p^k)}\cong PGL(2,p^k)$ where $\frac{m}{k}$ is an even integer,*
11. *For $q\equiv\pm1$(mod 8), two sets of $\frac{M(q)}{24}$ symmetric groups $\mathbb{S}_4$,*
12. *For $q\equiv\pm1$(mod 8), two sets of $\frac{M(q)}{24}$ alternating groups $\mathbb{A}_4$,*
13. *For $q\equiv\pm3$(mod 8), or $q=2^m$, m even, $\frac{M(q)}{12}$ conjugate alternating groups $\mathbb{A}_4$,*

14. For $q \equiv \pm 1 (mod\ 10)$, two sets of $\frac{M(q)}{60}$ conjugate alternating groups $\mathbb{A}_5$.

We will take all possible cases of subgroups of $G = PSL(2,p)$ as G_x and find out possible values of odd prime p, using (3.1). It is sufficient to use the second inequality $h(1+3h) \geq g$ of (3.1) to find the possible values of p for both rank-3 and rank-4. After we obtain the values of possible primes, we use computation in APL to check the rank of $PSL(2,p)$ on the cosets of given subgroups.

1. If we represent $PSL(2,p)$ as a permutation group on the cosets of a subgroup of order $\leq p-1$, then we must have $(p-1)(1+3(p-1)) \geq \frac{1}{2}p(p^2-1)$, which implies $p^2 - 5p + 4 \leq 0$. So, $p = 3$ is the only possible odd prime. $PSL(2,3) \cong \mathbb{A}_4$ has a rank-4 representation with subdegrees (1,1,2,2) on the cosets of a subgroup of order 2. Since all subgroups of order 2 are conjugate in $\mathbb{A}_4$, the above rank-4 representation is unique up to equivalence.

2. If we represent the group on the cosets of a subgroup of order p, then we get $p^2 - 6p - 3 \leq 0$. So, the possible values of p are $p = 3, 5$. $PSL(2,3) \cong \mathbb{A}_4$ has a doubly transitive representation with subdegrees (1,3) on the cosets of a subgroup of order 3. Since all Sylow-3 subgroups are conjugate in $\mathbb{A}_4$ we get a single such representation. If we represent $PSL(2,5) \cong \mathbb{A}_5$ on the cosets of a sylow 5 subgroup, we obtain a rank-4 representation with subdegrees (1,1,5,5). Again this representation is unique up to equivalence.

3. In the case of a subgroup of order $p+1$, we will get $p^2 - 7p - 8 \leq 0$. So, p must be 3, 5 or 7. For $p = 3$, the group is $PSL(2,3) \cong \mathbb{A}_4$, which does not have a cyclic subgroup of order 4. So, the subgroup of order 4 must be a Klein 4-group. There is exactly one Klein 4-group inside $PSL(2,3)$. There is a unique, doubly transitive, non-faithful representation of $\mathbb{A}_4$ up to equivalence with subdegrees (1,2). For $p = 5$, the group is $PSL(2,5) \cong \mathbb{A}_5$. Since there can not be a cyclic subgroup of order 6 in an $\mathbb{A}_5$, the subgroup has to be D_6, a dihedral group of

order 6. There is a single conjugacy class of D_6's in $PSL(2,5)$. If we represent $PSL(2,5)$ on the cosets of a dihedral subgroup of order 6 we obtain a rank-3 representation with subdegrees (1,3,6). This representation is also unique up to equivalence. In case of $p = 7$, we have $PSL(2,7)$, where a subgroup of order 8 is a sylow-2 subgroup. Since all sylow-2 subgroups are conjugate, there is exactly one conjugacy class of D_8's, dihedral subgroups of order 8. In this case, we obtain a unique rank-6 representation of $PSL(2,7)$ up to equivalence with subdegrees (1,2,2,4,4,8) on the cosets of dihedral subgroups of order 8.

4. If $PSL(2,p)$ is represented on the cosets of a subgroup of order 12, we will have $444 \geq \frac{1}{2}p(p^2-1)$. So, p must be 3, 5 or 7. If $p = 5$, then $PSL(2,5) \cong \mathbb{A}_5$ and a subgroup of order 12 inside an $\mathbb{A}_5$ must be an $\mathbb{A}_4$. There is a single conjugacy class of $\mathbb{A}_4$'s in $PSL(2,5)$. The representation will be doubly transitive with subdegrees (1,4). Again, this representation is unique up to equivalence. For $p = 7$, the group is $PSL(2,7)$, where the subgroups of order 12 are $\mathbb{A}_4$'s. There are two conjugacy classes of $\mathbb{A}_4$'s in $PSL(2,7)$. Both give similar rank-3 representations with subdegrees type (1,1,12). The reason is because automorphism group of $PSL(2,7)$ is $PGL(2,7)$ and these two conjugacy classes fuse together in $PGL(2,7)$. So, there are two inequivalent rank-3 representations of $PSL(2,7)$ on the cosets of subgroups of order 12.

5. If $PSL(2,p)$ is represented on the cosets of a subgroup of order 24, we will get $1752 \geq \frac{1}{2}p(p^2-1)$ and p must be congruent to ± 1 mod 8. So, $p = 7$ is the only possibility. A subgroup of order 24 in $G \cong PSL(2,7)$ is isomorphic to $\mathbb{S}_4$, the symmetric group on 4 letters. Moreover, there are two conjugacy classes of $\mathbb{S}_4$'s in $PSL(2,7)$. Hence, there are two inequivalent, representations of $PSL(2,7)$ on the cosets of subgroups of order 24. In each case the subdegrees are (1,6), hence both are doubly transitive.

6. When we consider a subgroup of order 60, we know that $p \equiv \pm 1 \bmod 10$ and also $10860 \geq \frac{1}{2}p(p^2-1)$ and hence $p = 11$ or 19. In the case of $p = 11$, a subgroup of $PSL(2,11)$ of order 60 is an $\mathbb{A}_5$. There are two conjugacy classes of $\mathbb{A}_5$'s in $PSL(2,11)$. We know that $PSL(2,11)$ has a doubly transitive representation on 11 points and we have $[PSL(2,11) : \mathbb{A}_5] = 11$. Hence, we obtain two inequivalent doubly transitive representations of $PSL(2,11)$ on the cosets of subgroups of order 60 with subdegrees (1,10). When $p = 19$, a subgroup of order 60 in $PSL(2,19)$ is an $\mathbb{A}_5$. There are two conjugacy classes of $\mathbb{A}_5$'s in $PSL(2,19)$. In this case, we obtain two inequivalent rank-4 representations with the same subdegree structure (1,6,20,30).

   The case of subgroup of order pd_-, where $d_-|\frac{p-1}{2}$, is addressed below. We have to make a serious note at this point. This work is motivated by [28] where the author missed this case.

Lemma 3.1.1. *Let G be a finite transitive permutation group represented on a set X. Let G_x be the subgroup fixing the letter x. Let $r = [N_G(G_x) : G_x]$. Then, there are r orbits of length 1 for the group G_x.*

Proof. Let $G = G_x + G_xx_2 + \cdots + G_xx_{|X|}$ be a coset decomposition of G where $N_G(G_x) = G_x + G_xx_2 + \cdots + G_xx_r$. It is well known that there is a permutation isomorphism between G acting on the cosets of G_x and G acting on points of X. We will show that every element of G_x fixes $G_x, G_xx_2, \cdots, G_xx_r$. So, let $a \in G_x$ and $2 \leq i \leq r$, then $x_iax_i^{-1} \in G_x$. Hence, $G_xx_ia = G_x(x_iax_i^{-1})x_i = G_xx_i$. If $j > r$, then $x_j \notin N_G(G_x)$ and so there exists a $b \in G_x$ such that $x_jbx_j^{-1} \notin G_x$ and hence $G_xx_jb = G_xx_jbx_j^{-1}x_j \neq G_xx_j$, otherwise equality would imply $x_jbx_j^{-1} \in G_x$. Thus $G_xx, G_xx_2, \cdots, G_xx_r$ are exactly the elements fixed by all elements of G_x. □

Theorem 3.1.2. *If $H \leq G \cong PSL(2,p)$ with $|H| = pd_-$ where $d_-|\frac{p-1}{2}$, then the representation of G on the cosets of H has rank $2r$, where $r = \frac{(p-1)/2}{d_-}$. Moreover,*

there are r H-orbits of length 1 and r H-orbits of length p.

Proof. The normalizer of H in G is of order $\frac{p(p-1)}{2}$. So, $[N_G(H) : H] = r$ and $[G : N_G(H)] = p + 1$. Let us assume $N_G(H) = H + Ha_2 + \cdots + Ha_r$ and $G = N_G(H) + N_G(H)b_2 + \cdots N_G(H)b_{p+1}$. So that, $G = H + Ha_2 + \cdots + Ha_r + Hb_2 + Ha_2b_2 + \cdots Ha_rb_2 + \cdots + Hb_{p+1} + Ha_2b_{p+1} + \cdots + Ha_rb_{p+1}$. If we assume

$$X = \{H, Ha_2, \ldots, Ha_r, Hb_2, Ha_2b_2, \cdots, Ha_rb_2, \cdots, Hb_{p+1}, Ha_2b_{p+1}, \cdots, Ha_rb_{p+1}\},$$

then $|X| = (p + 1)r$. And in the action $G|X$, we have $G_H \cong H$. By lemma 3.1.1, there are r $H-$orbits of length 1 and they are precisely $\{H\}, \{Ha_2\}, \ldots$ and $\{Ha_r\}$.

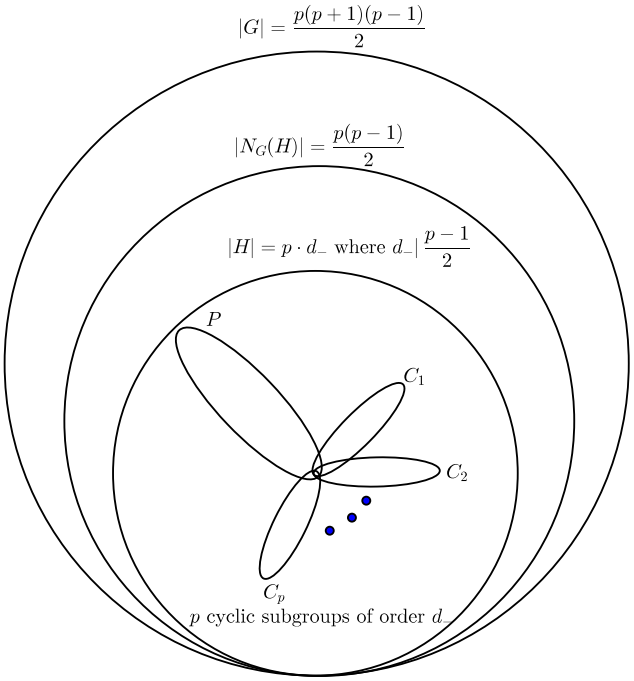

Figure 3.1: Structure of H in G

We then want to prove that there are r H-orbits of length p. So, we first prove that $|(Ha_lb_k)^H| = p$ for $2 \leq k \leq p + 1$ and $1 \leq l \leq r$, where $a_1 = 1$. The subgroup H has a cyclic subgroup of order p, and p cyclic subgroups of order d_-. There is a single conjugacy class of H in G. Since the number of conjugates of H in G is equal to $[G : N_G(H)] = p + 1$ and there is a single conjugacy class of size $p + 1$ of

cyclic subgroups of order p [theorem 3.1.1], the cyclic subgroups of order p in the conjugates of H are all distinct. Let $P = \langle p_1 \rangle \leq H$ be the subgroup of order p. Let $2 \leq k \leq p+1$ and $1 \leq l \leq r$, where $a_1 = 1$. Then, for $1 \leq i, j \leq p$, $i \neq j$, if $Ha_l b_k p_1^i = Ha_l b_k p_1^j$, then $Ha_l b_k p_1^{i-j} b_k^{-1} a_l^{-1} = H$ that means, $a_l b_k p_1^{i-j} b_k^{-1} a_l^{-1} \in H$. So that, $b_k p_1^{i-j} b_k^{-1} \in a_l^{-1} H a_l = H$ and hence, $p_1^{i-j} \in b_k^{-1} H b_k$, which is a contradiction because H and $b_k^{-1} H b_k$ are distinct conjugate subgroups. So, $Ha_l b_k p_1^i$ for $1 \leq i \leq p$ are all distinct which proves that for given k and l as above, we have $|(Ha_l b_k)^H| \geq p$.

We then want to prove that $|(Ha_l b_k)^H| \leq p$. Using the formula $|(Ha_l b_k)^H| = [H : H_{(Ha_l b_k)}]$, we only need to show that $|H_{(Ha_l b_k)}| \geq d_-$. Let $C_i = \langle c_i \rangle$ for $1 \leq i \leq p$, be p cyclic subgroups of H of order d_-. We would be done if we could show that $Ha_l b_k c_i = Ha_l b_k$ for some i, $1 \leq i \leq p$, because if $Ha_l b_k c_i = Ha_l b_k$ for some i, then $Ha_l b_k c_i^j = Ha_l b_k$ for $1 \leq j \leq d_-$ and so, $|H_{|Ha_l b_l|}| \geq d_-$. So, let $Ha_l b_k c_i \neq Ha_l b_k$ for all i, $1 \leq i \leq p$, then $c_i \notin b_k^{-1} H b_k$ for all i, $1 \leq i \leq p$. This result forces the total number of elements of order d_- to be $\phi(d_-)p(p+1)$, because the number of elements of order d_- in a cyclic group of order d_- is $\phi(d_-)$, there are p cyclic subgroups of order d_- in H, and the number of conjugates of H in G is $p+1$. On the other hand, by theorem 3.1.1 there is a single conjugacy class of size $\frac{p(p+1)}{2}$ of cyclic subgroups of order d_-. So that the total number of elements of order d_- is $\phi(d_-)\frac{p(p+1)}{2}$, which is a contradiction to the above result. This contradiction guarantees that there exists some i, $1 \leq i \leq p$ such that $Ha_l b_k c_i = Ha_l b_k$ which implies $|H_{(Ha_l b_k)}| \geq d_-$ and hence $|(Ha_l b_k)^H| \leq p$. This proves that $|(Ha_l b_k)^H| = p$. Since k, $2 \leq k \leq p+1$ and l, $2 \leq l \leq r$ were arbitrarily chosen, the length of each orbit is p and number of such H-orbits is $\frac{((p+1)r-r)}{p} = r$. This completes the proof. □

Corollary 3.1.1. *If $d_- = \frac{(p-1)/2}{2}$ in the above theorem, then the representation of G on the cosets of H has rank 4.*

Proof. The proof follows immediately, since $r = \frac{(p-1)/2}{d_-} = 2$. □

Corollary 3.1.2. *If $p \equiv 1$ (mod 4), then there always exists a rank-4 representation of $PSL(2,p)$.*

Proof. The proof is immediate since $d_- = \frac{p-1}{4}$ for $p \equiv 1 \pmod 4$. □

In this way, we found all rank-3 and rank-4 representations of $PSL(2,p)$. We will summarize them in the following theorem.

Theorem 3.1.3. *[Rank-3 representations] There are precisely three rank-3 representations of $PSL(2,p)$, namely, the unique representation of $PSL(2,5) \cong \mathbb{A}_5|10$ up to equivalence with subdegrees (1,3,6) and two inequivalent representations of $PSL(2,7)|14$ with same subdegree type (1,1,12).*

Theorem 3.1.4. *[Rank-4 representations] For $p \equiv 1$ (mod 4), the representations of $PSL(2,p)|(2p+2)$ has rank 4 with subdegrees $(1,1,p,p)$. Also, the representation of $PSL(2,3)|6$ has rank 4 with subdegrees (1,1,2,2), and the representation of $PSL(2,19)|57$ has rank 4. More precisely, there are two inequivalent rank-4 representations of $PSL(2,19)|57$ with same subdegree type (1,6,20,30).*

3.2 LOW RANK REPRESENTATION OF $PSL(2,q)$

The idea of finding rank-3 and rank-4 representations of $PSL(2,q)$, where $q = p^m$, p an odd prime, is very similar to the case of $PSL(2,p)$ in section 3.1. The difference is that we replace p by q and we deal with two more cases (10) and (11) of theorem 3.1.1. Let us take the cases as in section 3.1. The case when $m = 1$ in $q = p^m$ is already addressed in section 3.1, so, we assume that $m > 1$.

1. If we represent $PSL(2,q)$ as a permutation group on the cosets of a subgroup of order $\leq q-1$, then we must have $(q-1)(1+3(q-1)) \geq \frac{1}{2}q(q^2-1)$ which implies $q^2 - 5q + 4 \leq 0$. There is no q satisfying this inequality.

2. If we represent the group on the cosets of a subgroup of order q, then we get $q^2 - 6q - 3 \leq 0$. Again, there is no q satisfying this inequality.

3. In the case of a subgroup of order $q + 1$, we will get $q^2 - 7q - 8 \leq 0$. No q satisfies this inequality either.

4. If $PSL(2, q)$ is represented on the cosets of a subgroup of order 12, we will get $444 \geq \frac{1}{2}q(q^2 - 1)$. Only $q = 9$ satisfies this inequality. A subgroup of order 12 in $PSL(2, 9) \cong \mathbb{A}_6$ is an $\mathbb{A}_4$. The normalizer of an $\mathbb{A}_4$ in $PSL(2, 9)$ is $\mathbb{S}_4$, so $[N_G(\mathbb{A}_4) : \mathbb{A}_4] = 2$, which implies that there are two H-orbits of length 1. But, $\frac{g}{h} = \frac{360}{12} = 30$. Thus, rank-4 and hence rank-3 representations are not possible, because the sum of maximum possible subdegrees is $1 + 1 + 12 + 12 < 30$.

5. If we represent $PSL(2, q)$ on the cosets of a subgroup of order 24, we get $1752 \geq \frac{1}{2}q(q^2 - 1)$ and q must be congruent to ± 1 mod 8. So, $q = 9$ is the only possibility. A subgroup of order 24 in $PSL(2, 9) \cong \mathbb{A}_6$ is an $\mathbb{S}_4$. There are two conjugacy classes of $\mathbb{S}_4$'s in $PSL(2, 9)$. Hence, we obtain two inequivalent rank-3 representations of $PSL(2, 9)$ on the cosets of subgroups of order 24 with subdegrees (1,6,8).

6. When we consider a subgroup of order 60, we know that $q \equiv \pm 1$ mod 10 and also $10860 \geq \frac{1}{2}q(q^2 - 1)$ and hence $q = 9$. A subgroup of order 60 in $PSL(2, 9) \cong \mathbb{A}_6$ is an $\mathbb{A}_5$. And, there are two conjugacy classes of $\mathbb{A}_5$'s in $PSL(2, 9)$. In this case, we obtain two inequivalent doubly transitive representations of $PSL(2, 9)$ on the cosets of subgroups of order 60 with subdegrees (1,5).

   We will now consider the cases (10) and (11) of theorem 3.1.1.

7. When we consider a subgroup $PSL(2, p^k)$, where $k|m$, let $m = kt$ for some positive integer $t > 1$. Then,

$$h(1+3h) \geq g$$

i.e., $$\frac{p^k(p^k+1)(p^k-1)}{2}(1+3\frac{p^k(p^k+1)(p^k-1)}{2}) \geq \frac{p^m(p^m+1)(p^m-1)}{2}$$

i.e., $$\frac{2+3p^k(p^{2k}-1)}{2} \geq p^{kt-k}\frac{(p^{2tk}-1)}{(p^{2k}-1)}$$

and hence, $2+3p^k(p^{2k}-1) \geq 2p^{k(t-1)}(p^{2k(t-1)}+p^{2k(t-2)}+\cdots+p^{2k}+1)$

(3.2)

For $t=3$, we get

$$2+3p^k(p^{2k}-1) \geq 2p^{2k}(p^{4k}+p^{2k}+1)$$

$$\text{i.e., } 2p^{6k}+2p^{4k}-3p^{3k}+2p^{2k}+3p^k-2 \leq 0 \tag{3.3}$$

which is impossible for any value of prime p and $k > 1$. This result is also sufficient to say that the inequality (3.2) is impossible for any $t > 3$. So, the only case remaining is for $t = 2$.

For $t=2$, we get

$$2+3p^k(p^{2k}-1) \geq 2p^k(p^{2k}+1)$$

$$\text{i.e., } p^{3k}-5p^k+2 \geq 0 \tag{3.4}$$

which is not impossible.

However, for $H = PSL(2,p^k)$ and $a \in X$,

$$|X| = |a^G| = [G:G_a] = \frac{g}{h} = \frac{p^{2k}(p^{4k}-1)}{p^k(p^{2k}-1)} = p^k(p^{2k}+1) = p^{3k}+p^k.$$

Rank 3 is not possible because, one H-orbit is of length 1 ($|\{a\}| = 1$), and the maximum possible length of each of the other H-orbits is $h = \frac{p^k(p^{2k}-1)}{2}$, and so,

$$1+\frac{p^k(p^{2k}-1)}{2}+\frac{p^k(p^{2k}-1)}{2} = 1+p^{3k}-p^k < p^{3k}+p^k = |X|.$$

Again, for $\frac{m}{k}$ even, $N_G(PSL(2,p^k)) \cong PGL(2,p^k)$, so, $k = [N_G(PSL(2,p^k)) : PSL(2,p^k)] = 2$, which means that by lemma 3.1.1, there are two H-orbits of length 1. This helps us to prove that rank 4 is also impossible because

$$1+1+\frac{p^k(p^{2k}-1)}{2}+\frac{p^k(p^{2k}-1)}{2} = 2+p^{3k}-p^k < p^{3k}+p^k = |X|.$$

8. When we consider a subgroup $H = PGL(2, p^k)$, where $\frac{m}{k}$ is even, we will analyze with the same approach as above. Let $m = kt$ for some even positive integer t. Then,

$$h(1 + 3h) \geq g$$

$$\text{i.e.,} \quad p^k(p^{2k} - 1)(1 + 3p^k(p^{2k} - 1)) \geq \frac{p^m(p^{2m} - 1)}{2}$$

$$\text{hence,} \ 2 + 6p^k(p^{2k} - 1) \geq p^{k(t-1)}(p^{2k(t-1)} + p^{2k(t-2)} + \cdots + p^{2k} + 1) \tag{3.5}$$

For $t = 4$,

$$2 + 6p^k(p^{2k} - 1) \geq p^{3k}(p^{6k} + p^{4k} + p^{2k} + 1)$$

$$\text{i.e.,} \ \ p^{9k} + p^{7k} + p^{5k} - 5p^{3k} + 6p^k - 2 \leq 0 \tag{3.6}$$

which is impossible for any value of prime p and $k > 1$. As before, this result is also sufficient to say that the inequality is impossible for any even integer $t > 4$. So, the only case left to consider is $t = 2$, because $t = 3$ is odd which is not possible. For $t = 2$, we get

$$2 + 6p^k(p^{2k} - 1) \geq p^k(p^{2k} + 1)$$

$$\text{i.e.,} \ \ 5p^{3k} - 7p^k + 2 \geq 0 \tag{3.7}$$

which is not impossible.

The approach as in 7, does not work to show the non-existence of rank-3 and rank-4 representations. Hence, we haven't ruled out this case.

In conclusion, we find another lower rank transitive representation, namely two inequivalent rank-3 representations of $PSL(2, 9)$ on the cosets of two conjugacy classes of $\mathbb{S}_4$'s.

3.3 RANK OF $PSL(2, p)$ ON COSETS OF PARTICULAR SUBGROUPS

In this section, we will find the rank of $PSL(2, p)$ on the cosets of some given subgroups.

On the cosets of subgroup of order p

Theorem 3.3.1. *Let $H \leq G = PSL(2,p)$ where H is a subgroup of order p. Then the representation of G on the cosets of H has rank $p-1$. Moreover, there are $\frac{p-1}{2}$ $H-$orbits of length 1 and $\frac{p-1}{2}$ $H-$orbits of length p.*

Proof. By Sylow's theorem, there is a single conjugacy class of subgroups of order p. Let $H \leq G$ with $|H| = p$. The normalizer of H is of order $\frac{p(p-1)}{2}$. Then, $r = [N_G(H) : H] = \frac{p-1}{2}$. We can assume that $G = H + Ha_2 + \cdots + Ha_r + Ha_{r+1} + \cdots + Ha_n$ where $N_G(H) = H + Ha_2 + \cdots + Ha_r$ and $n = \frac{p^2-1}{2}$. If we assume $X = \{H, Ha_2, \cdots, Ha_r, Ha_{r+1}, \cdots, Ha_n\}$, then in the action $G|X$, we have $G_H \cong H$. By lemma 3.1.1, there are $r = \frac{p-1}{2}$ H-orbits of length 1 and these are precisely $\{H\}, \{Ha_2\}, \ldots$ and $\{Ha_r\}$.

For $a \notin N_G(H)$, we must have $|(Ha)^H| > 1$, because, if $Hax = Ha \ \forall x \in H$, then, $Haxa^{-1} = H$ and $axa^{-1} \in H$ which is a contradiction to $a \notin N_G(H)$. Using $|(Ha)^H| = [H : H_{(Ha)}]$, we get $|(Ha)^H| = p$. So, the number of H-orbits of length p is

$$\frac{1}{p}\Big[\frac{p^2-1}{2} - \frac{p-1}{2}\Big] = \frac{p-1}{2}.$$

Hence, the total number of H-orbits is

$$\frac{p-1}{2} + \frac{p-1}{2} = p-1.$$

□

On the cosets of a cyclic subgroup of order $d_\pm$ where $d_\pm | \frac{p\pm1}{2}$

Theorem 3.3.2. *Let $H \leq G = PSL(2,p)$ where H is a subgroup of order $d\pm$ where $d \pm | \frac{p\pm1}{2}$. Then the representation of G on the cosets of H has rank $\frac{(p\pm1)(p^2\mp p+2d_\pm-2)}{2d_\pm^2}$. Moreover, there are $\frac{p-1}{d_\pm}$ $H-$orbits of length 1 and $\frac{(p\pm1)^2(p\mp2)}{2d_\pm^2}$ $H-$orbits of length $d_\pm$.*

Proof. By theorem 2.4 of [15], there is a single conjugacy class of cyclic subgroups of order $d_\pm$ for $d_\pm | \frac{p\pm1}{2}$. Let $H \leq G$, $|H| = d_\pm$. The normalizer of H in G is a

dihedral group $D_{p\pm1}$. Let us take $d_-|\frac{p-1}{2}$. Then $r = [N_G(H) : H] = \frac{p-1}{d_-}$. So, we can assume that $G = H + Ha_2 + \cdots + Ha_r + Ha_{r+1} + \cdots + Ha_n$ where $n = \frac{|G|}{d_-}$ and $N_G(H) = H + Ha_2 + \cdot + Ha_r$. If we assume $X = \{H, Ha_2, \ldots, Ha_r, Ha_{r+1}, \ldots, Ha_n\}$, then in the action $G|X$, we have $G_H \cong H$. Again, by lemma 3.1.1, there are $r = \frac{p-1}{r}$ H-orbits of length 1 and they are precisely $\{H\}, \{Ha_2\}, \ldots$ and $\{Ha_r\}$.

For $a \notin N_G(H)$, we must have $|(Ha)^H| > 1$. If d_- is prime, by $|(Ha)^H| = [H : H_{(Ha)}]$, we get $|(Ha)^H| = d_-$. So, the number orbits of length d_- is

$$\frac{1}{d_-}[\frac{1}{d_-}\frac{p(p+1)(p-1)}{2} - \frac{p-1}{d_-}] = \frac{(p-1)^2(p+2)}{2d_-^2}.$$

And hence, the total number of orbits is

$$\frac{(p-1)^2(p+2)}{2d_-^2} + \frac{p-1}{d_-} = \frac{(p-1)(p^2+p+2d_--2)}{2d_-^2}.$$

Suppose that d_- is not a prime. We have to prove that $H_{(Ha)} = \{1\}$, i.e. $Hah \neq Ha$ for all $h \in H, h \neq 1$. If there exists $h \in H$ such that $Hah = Ha$, then, $h \in a^{-1}Ha$. Note that the total number of elements of order s in G where $s|d_-$ is $\frac{\phi(s)}{2}p(p+1)$. Since there is a single conjugacy class of $\frac{p(p+1)}{2}$ cyclic subgroups of order d_-, we must have $|H \cap a^{-1}Ha| = 1$. So that $h = 1$ and hence $H_{(Ha)} = \{1\}$.

Similarly, for $d_+|\frac{p+1}{2}$, the number of H-orbits of length 1 is $\frac{p+1}{2}$, and that of length d_+ is $\frac{(p+1)^2(p-2)}{2d_+^2}$. And hence, the total number of H-orbits is $\frac{(p+1)(p^2-p+2d_+-2)}{2d_+^2}$. □

On the cosets of subgroup of order pd_- where $d_-|\frac{p-1}{2}$

This case is already addressed by theorem 3.1.2.

On the cosets of dihedral subgroups of order p-1 and p+1

Theorem 3.3.3. *The representation of $PSL(2,p)$ on the cosets of D_{p-1}, the dihedral subgroup of order $p-1$ has rank $\frac{3p+7}{4}$ for $p \equiv 3$ (mod 4) and rank $\frac{3(p+3)}{4}$ for $p \equiv 1$ (mod 4). Furthermore, The representation of $PSL(2,p)$ on the cosets of D_{p+1}, the*

dihedral subgroup of order $p+1$ has rank $\frac{3(p+1)}{4}$ for $p \equiv 3$ (mod 4) and rank $\frac{3(p-1)}{4}$ for $p \equiv 1$ (mod 4).

Proof. We will present a proof of the rank of $PSL(2,p)$ on the cosets of D_{p-1} in the case when $p \equiv 3 \pmod 4$ using computation with character theory. Below are character tables of $PSL(2,q)$ for $q \equiv 1 \pmod 4$ and for $q \equiv 3 \pmod 4$.

x:	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ -1 & \lambda \end{bmatrix}$
$\lvert x\rvert$:	1	p	2	All divisors of $\frac{q-1}{2}$	All divisors of $\frac{q+1}{2}$
σ_x:	$\frac{q(q^2-1)}{2}$	q	$q-1$	$\frac{q-1}{2}$	$\frac{q+1}{2}$
# classes ⇒ # irr. chars ⇓	1	2	1	$\frac{q-5}{4}$	$\frac{q-1}{4}$
1	1	1	1	1	1
1	q	0	1	1	-1
$\frac{q-5}{4}$	$q+1$	1	$2\chi(-1)$	$\chi(\lambda)+\chi(\lambda^{-1})$	0
$\frac{q-1}{4}$	$q-1$	-1	0	0	$-(\psi(x)+\psi(x^{-1}))$
2	$\frac{q+1}{2}$	$\frac{1\pm\sqrt{q}}{2}$	$\chi_{-1}(-1)$	$\chi_{-1}(\lambda)$	0

Table 3.1: Character table of $PSL(2,q)$ for $q = p^m \equiv 1 \pmod 4$

x:	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ \beta & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ -1 & \lambda \end{bmatrix}$
$\lvert x\rvert$:	1	p	2	All divisors of $\frac{q-1}{2}$	All divisors of $\frac{q+1}{2}$, $\neq 2$
σ_x:	$\frac{q(q^2-1)}{2}$	q	$q-1$	$\frac{q-1}{2}$	$\frac{q+1}{2}$
# classes ⇒ # irr. chars ⇓	1	2	1	$\frac{q-3}{4}$	$\frac{q-3}{4}$
1	1	1	1	1	1
1	q	0	1	1	-1
$\frac{q-3}{4}$	$q+1$	1	0	$\chi(\lambda)+\chi(\lambda^{-1})$	0
$\frac{q-3}{4}$	$q-1$	-1	$-2\psi(x)$	0	$-(\psi(x)+\psi(x^{-1}))$
2	$\frac{q-1}{2}$	$\frac{-1\pm\sqrt{-q}}{2}$	$-\psi(x)$	0	$-\psi_{-1}(x)$

Table 3.2: Character table of $PSL(2,q)$ for $q = p^m \equiv 3 \pmod 4$

Let $x \in G$ and θ be the character of x. We will use notations and formula $\theta(x) = \frac{g \cdot h_x}{h \cdot g_x}$ of theorem 2.1.4.

x:	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ \beta & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ -1 & \lambda \end{bmatrix}$
$\|x\|$:	1	p	2	d_-	d_+
σ_x:	$\frac{p(p^2-1)}{2}$	p	$p-1$	$\frac{p-1}{2}$	$\frac{p+1}{2}$
g_x	1	$\frac{p^2-1}{2}$	$\frac{p(p11)}{2}$	$p(p+1)$	$p(p-1)$
h_x	1	0	$\frac{p-1}{2}$	$\phi(d_-)$	0
$\theta(x) = \frac{g \cdot h_x}{h \cdot g_x}$	$\frac{p(p+1)}{2}$	0	$\frac{p+1}{2}$	n_{d_-}	0

In the calculation above, n_{d_-} is the total number of divisors of $\frac{p-1}{2}$ except 1, because identity element is already included. We know that the rank of a group is equal to $\langle \theta, \theta \rangle$.

Now,

$$\begin{aligned}
\langle \theta, \theta \rangle =& \frac{1}{|G|} \left[1 \cdot \frac{p^2(p+1)^2}{4} + \frac{p(p-1)}{2} \cdot \frac{(p+1)^2}{4} + p(p+1) \cdot n_{d_-} \right] \\
=& \frac{p(p+1)}{g} \left[\frac{p(p+1)}{4} + \frac{(p+1)(p-1)}{8} + n_{d_-} \right] \\
=& \frac{p(p+1)}{g} \left[\frac{(p+1)(3p-1)}{8} + n_{d_-} \right]. \qquad (3.8)
\end{aligned}$$

For example, for $p = 7$, we have $d_- = 3$. Hence, the rank of $PSL(2,7)$ on the cosets of D_{p-1} is $\frac{7 \cdot 8}{168} \left[\frac{8 \cdot 20}{8} + 1 \right] = 7$.

Similarly, we can prove the remaining cases. □

Remark: The $H-$orbit structures in case of $H \cong D_{p-1}$ are

$$\left(1 \times (1) + \frac{p-1}{2} \times \left(\frac{p-1}{2} \right) + \frac{p+5}{4} \times (p-1) \right) \text{ for } p \equiv 3 \pmod 4$$

$$\left(1 \times (1) + 2 \times \left(\frac{p-1}{4} \right) + \frac{p-5}{2} \times \left(\frac{p-1}{2} \right) + \frac{p+7}{4} \times (p-1) \right) \text{ for } p \equiv 1 \pmod 4$$

Similarly, the $H-$orbit structures in case of $H \cong D_{p+1}$ are

$$\left(1 \times (1) + 2 \times \left(\frac{p+1}{4}\right) + \frac{p-3}{2} \times \left(\frac{p+1}{2}\right) + \frac{p-3}{4} \times (p+1)\right) \text{ for } p \equiv 3 \bmod 4 \ .$$

$$\left(1 \times (1) + \frac{p-3}{2} \times \left(\frac{p+1}{2}\right) + \frac{p-1}{4} \times (p+1)\right) \text{ for } p \equiv 1 \bmod 4 \ .$$

The meaning of $H-$orbit structure $\sum a \times (b)$ is that there are a orbits of length (b).

CHAPTER 4

RANK-3 EXTENSIONS

A *rank-3 transitive (primitive) extension* of a group H is a permutation group G which is transitive (primitive) on a finite set X, such that the stabilizer of a point $x \in X$, G_x is isomorphic to H and there are three orbits of H on X. Or, equivalently, there are three orbitals of G on $X \times X$, which we will denote by I, Δ, and Γ. By the one-to-one correspondence between the orbitals of $G|(X \times X)$ and the orbits of $G_x|X$, the three orbits of $G_x \cong H$ are $I(x) = \{x\}$, $\Delta(x)$ and $\Gamma(x)$. The lengths of these orbits: $1 = |I(x)|$, $k = |\Delta(x)|$, and $\ell = |\Gamma(x)|$ are called the *subdegrees* of G. Notice that $n = 1 + k + \ell = |X|$ is the *degree* of the group G.

4.1 RANK-3 GRAPHS

Assume now that G is a rank-3 group with orbitals I, Δ and Γ. We also suppose that G has even order, so by Wielandt's theorem, [34] Δ and hence Γ are both symmetric. Hence, we can construct graphs $\mathcal{G}_\Delta$ and $\mathcal{G}_\Gamma$ by the method as explained in section 2.2, and they are complementary graphs. We call a graph $\mathcal{G}_\Delta$ obtained this way a *rank-3 graph*.

Let $\mathcal{G} = (X, E)$ be an undirected graph with vertex set X and edge set E. For $x, y \in X$ we denote by $d(x, y)$ the distance from x to y. If r is a non-negative integer, by the sphere of radius r about x we mean the set $S_r(x) = \{y \in X \mid d(x, y) = r\}$. In the notation above, $\Delta(x) = S_1(x)$ and $\Gamma(x) = S_2(x)$.

Definition 4.1.1. *A graph $\mathcal{G}$ is* strongly regular *if*

1. *$|S_1(x)|$ is independent of x, that is, the graph is regular and,*

2. $|S_1(x) \cap S_1(y)|$ *for* $x \neq y$ *depends only on whether or not* x *and* y *are neighbors in* $\mathcal{G}$.

Theorem 4.1.1. *Every rank-3 graph is strongly regular.*

Proof can be found in [10].

4.1.1 Parameters of rank-3 graphs

The intersection numbers, λ and μ of a rank-3 group G are defined by

$$S_1(x) \cap S_1(y) = \begin{cases} \lambda & \text{if} \quad y \in S_1(x) = \Delta(x) \\ \mu & \text{if} \quad y \in S_2(x) = \Gamma(x). \end{cases}$$

The *adjacency matrix* for a graph with n vertices is an $n \times n$ matrix whose (i, j) entry is 1 if the i^{th} vertex and j^{th} vertex are connected, and 0 if they are not. If I, A and B are the adjacency matrices of $\mathcal{G}_I$, $\mathcal{G}_\Delta$, and $\mathcal{G}_\Gamma$ respectively, then:

1. $I + A + B = J$, where J is the $n \times n$ matrix of all ones,
2. A and B are symmetric, given that order of G is even,
3. $AA^t = kI + \lambda A + \mu B$,
4. A and B both have trace 0,
5. $A^2 - (\lambda - \mu)A - (k - \mu)I = \mu J$.

Since $\mathcal{G}_\Delta$ is regular, the row sums of A are all $|\Delta(x)| = k$, so that row sums of $(A - kI)$ are all 0 and $(A - kI)J = 0$. Hence, A satisfies the polynomial equation

$$(x - k)(x^2 - (\lambda - \mu)x - (k - \mu)) = 0.$$

Thus the spectrum of A consists of just three eigenvalues $\{k, r, s\}$ where $r, s = \frac{(\lambda-\mu) \pm \sqrt{d}}{2}$ where $d = (\lambda - \mu)^2 + 4(k - \mu)$. If we assume f and g to be the multiplicities of r and s respectively, then $n = 1 + f + g$ implies $f + g = k + \ell$. Also,

trace$(A) = 0$ implies $k + fr + gs = 0$, which gives $fr + gs = -k$. Hence,

$$f = \frac{(k+\ell)s + k}{s - r} \; ; \quad g = \frac{(k+\ell)r + k}{r - s}.$$

Since f and g must be integers, these are very strong necessary conditions for parameters n, k, ℓ, λ, μ to belong to a rank-3 graph. We call the 9-tuple $(n, k, \ell, \lambda, \mu, r, s, f, g)$ the parameters of a rank-3 graph. Furthermore, the first three parameters are related by the equation $k(k - \lambda - 1) = \ell\mu$. In fact, the left hand side is the total number of edges from $\Delta(x)$ to $\Gamma(x)$, and the right hand side is the total number of edges from $\Gamma(x)$ to $\Delta(x)$.

Let $D : G \to GL(n, \mathbb{C})$ be the matrix representation of G obtained by associating with each $g \in G$ the corresponding permutation matrix $D(g)$. Because G has rank 3, D has exactly 3 inequivalent constituents $D_1 = 1$, D_2, and D_3 each with multiplicity 1 [34]. It follows that one of the eigenvalues r, s of A has multiplicity equal to the degree f of D_2, while the other has multiplicity equal to the degree g of D_3. More detail is explained in[12].

4.1.2 An example of a family of rank-3 graphs

Let $X = \binom{n}{2}$ be a set of 2-sets for $n \geq 4$. The symmetric group on n letters, $\mathbb{S}_n$ acts transitively on X. If $x = \{a, b\} \in X$, then G_x has precisely three orbits on X, namely $I(x) = \{\{a, b\}\}$, $\Delta(x) = \{\{a, c\} : c \neq a, b\} \cup \{\{b, c\} : c \neq a, b\}$ and $\Gamma(x) = \{\{c, d\} : c \neq a, b \text{ and } d \neq a, b\}$. Hence the graph $\mathcal{G} = \mathcal{G}_\Delta$ has X as its vertex set, with two distinct elements of X being adjacent if they intersect. This is a familiar graph to graph theorists. It is the line graph of K_n, the complete graph with n vertices. When $n = 5$, the complement $\mathcal{G}_\Gamma$ of $\mathcal{G}_\Delta$ is the Peterson graph.

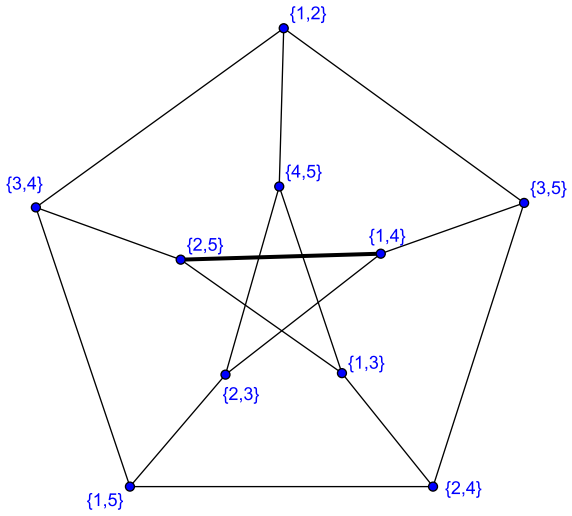

Figure 4.1: Peterson Graph

4.2 RANK-3 EXTENSIONS

The study of rank-3 extensions has been extremely important in the discovery and construction of new simple groups as rank-3 primitive extensions of particular simple groups. In order to understand how a rank-3 extension G is constructed from a group H such that stabilizer of a point of G is H, see [10, 13].

We will see one easy example. Suppose $H \cong \mathbb{S}_3$. We find that there are two graphs $\mathcal{G}_1$ with $X_1 = \{1, 2, 3\}$ and $\mathcal{G}_2 = C_6$, a 6-cycle with $X_2 = \{a, b, c, d, e, f\}$ on which H acts transitively. Below is the table of these actions.

H	Action of H on $\mathcal{G}_1$	Action of H on $\mathcal{G}_2$
h_1	1	1
h_2	(1 2 3)	(a e c)(b f d)
h_3	(1 3 2)	(a c e)(b d f)
h_4	(1 2)	(a b)(c f)(d e)
h_5	(1 3)	(a f)(b e)(c d)
h_6	(2 3)	(a d)(b c)(e f)

We now add a new vertex x and consider the set $X = \{x, 1, 2, 3, a, b, c, d, e, f\}$. Join x to each vertex in $\mathcal{G}_1$. We have $k = 3$, $\ell = 6$, $n = 10$, $\lambda = 0$ (valency of $\mathcal{G}_1$), and $k - \mu = 2$ (valency of $\mathcal{G}_2$), so, $\mu = 1$. Hence each vertex in $\mathcal{G}_1$ must be joined to $k - \lambda - 1 = 2$ vertices in $\mathcal{G}_2$ in such a way that each vertex in $\mathcal{G}_2$ is adjacent to exactly one vertex in $\mathcal{G}_1$. We first determine which vertices in $\mathcal{G}_2$ are joined to 1. The stabilizer in H of 1 is $\{h_1, h_6\}$ and this has orbits $\{a, d\}$, $\{b, c\}$, and $\{e, f\}$ on the vertices in $\mathcal{G}_2$. Let u and v denote the points in one of these orbits. If 1 is adjacent to u, then $1^{h_6} = 1$ must be adjacent to $u^{h_6} = v$. Thus, 1 must be adjacent to both points in one orbit and nonadjacent to the remaining points. If 1 is adjacent to either b and c or to e and f, then since b is adjacent to c and e is adjacent to f, vertex 1 belongs to a triangle while the vertex x does not; thus the graph $\mathcal{G}$ would not be point-symmetric. Hence 1 must be adjacent to a and d. Applying h_4, we see that $1^{h_4} = 2$ must be adjacent to $a^{h_4} = b$ and $d^{h_4} = e$. Similarly, 3 must be adjacent to c and f. Below is the graph.

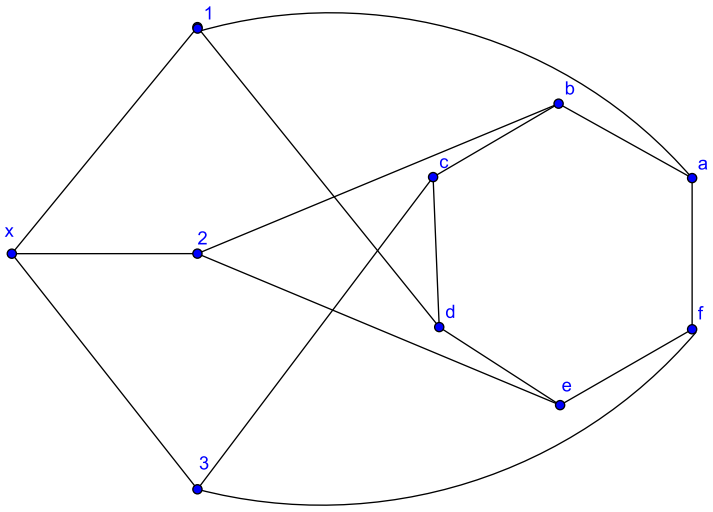

Figure 4.2: Peterson Graph

In fact the graph so formed is the Peterson Graph. The automorphism group of $\mathcal{G}$ is isomorphic to $\mathbb{S}_5$. The rank-3 extension of $H = \mathbb{S}_3$ in this case is $G = \mathbb{A}_5$, because

$|G| = |H| \cdot |X| = 6 \cdot 10 = 60$ and it is a subgroup of $\mathbb{S}_5$.

If we start with H to be simple, the rank-3 extension G must be simple if $|X|$ is not equal to the order of a direct product of isomorphic simple groups. The following theorems prove this result.

Theorem 4.2.1. *The group G is primitive if and only if both graphs $\mathcal{G}$ and $\bar{\mathcal{G}}$ are connected, i.e. if and only if $\mu \neq 0$ or k.*

For the proof of this theorem, see [11].

Theorem 4.2.2. *Assume that G is a primitive group acting on a finite set X and G_x is simple. Then either G is simple, or G contains a regular normal subgroup which is characteristically simple.*

Proof. If G is not simple, then there exists a non-trivial normal subgroup of G, which implies there is a minimal normal subgroup of G. Let N be a minimal normal subgroup of G.

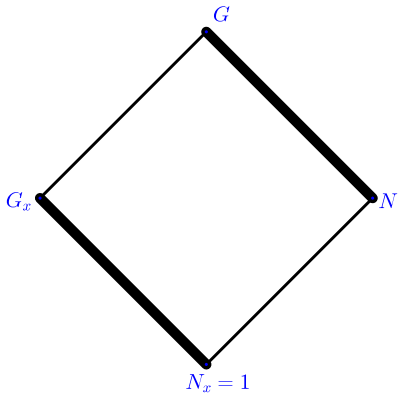

Figure 4.3: Normal subgroup diagram

Then, for $x \in X$, $N \cap G_x = N_x$ is a normal subgroup of G_x. Since G_x is simple, we must have $N_x = G_x$ or $N_x = 1$. If $N_x = G_x$, then since N is a non-trivial normal subgroup of a primitive group, it is transitive on X [34], we will get $|N| = |X| \cdot |N_x| = |X| \cdot |G_x| = |G|$. So, $N = G$, a contradiction. Therefore, $N_x = 1$ and therefore, N is

a regular minimal normal subgroup of G. But a minimal normal subgroup of a group is characteristically simple which can be written as a direct product of isomorphic simple groups. This is not possible since $|N| = |X|$ and we have that $|X|$ is not equal to an order of direct product of isomorphic simple groups. Hence, G is simple. $\square$

Several new simple groups were obtained by rank-3 extensions of a simple group. For example, the Higman-Sims group of order 44,352,000 was constructed from $H = M_{22}$[13]. In this case, the subdegrees are 1, 22 and 77. So, the corresponding Higman-Sims graph has 100 vertices. Some other groups obtained this way are McLaughlin's group with degree 275, order 898,128,000 and $H = U_4(3)$[24], Suzuki's group with degree 1782, order 448,345,497,600 and $H = E_2(4)$[32].

Another simple group $PSU(3, 5^2)$ of order 126,000, which is not really new, can also be constructed from $H = \mathbb{A}_7$. The subdegrees are 1, 7 and 42. The corresponding graph has 50 vertices, is the so called Hoffman-Singleton Graph and has been known since 1960 [14]. We have given a completely new construction of the Hoffman-Singleton graph by an approach different from the original [14] as a rank-3 graph, and using a peculiarity of $\mathbb{A}_6$ [18]. Below is the construction.

A NEW CONSTRUCTION OF the HOFFMAN-SINGLETON GRAPH

4.2.1 Introduction

The Hoffman-Singleton graph $\mathcal{H}$, a member of the small family of Moore graphs of diameter 2, is a well known 7-regular undirected graph with 50 vertices and 175 edges[14]. It is the unique strongly regular graph with parameters (50,7,0,1).

We will use the notation $G_{[x,y]}$ to denotes the pointwise stabilizer of x and y, that is $G_x \cap G_y$, and $G_{(x,y)}$ to denote the stabilizer of the 2-set $\{x, y\}$.

4.2.2 The A_5's in A_7

Let us consider the alternating group $G = \mathbb{A}_7$ acting on set $Y = \{1, \ldots, 7\}$. For $x \in Y$, the stabilizer G_x is isomorphic to $\mathbb{A}_6$, and for $x \neq y$, $G_{[x,y]} = G_{[y,x]} \cong \mathbb{A}_5$. Since G is 5-transitive, it is 2-homogeneous on Y, that is, G acts transitively on the 21 subsets of size 2 of Y. It follows that the stabilizer $G_{(x,y)}$ of an unordered pair is a subgroup of order $|G|/21 = 120$, normalizing $G_{[x,y]}$. Thus, $G_{(x,y)} \cong \mathbb{S}_5$ and there is a conjugacy class of 21 $\mathbb{A}_5$'s each fixing 2 points.

However, there is a second conjugacy class of $\mathbb{A}_5$'s in $\mathbb{A}_7$ each fixing exactly one point of Y. Consider the stabilizer $G_x \cong \mathbb{A}_6$ in its transitive representation on the points of $Y \setminus \{x\}$. We can find elements $a, b \in G_x$ such that a fixes no points of $Y \setminus \{x\}$, $|a| = 3$, $|b| = 2$, and $|ab| = 5$. For example, if $a = (1\ 2\ 3)(4\ 5\ 6)$ and $b = (1)(2)(3\ 4)(5\ 6)$, then $ab = (1\ 2\ 3)(4\ 5\ 6)(1)(2)(3\ 4)(5\ 6) = (1\ 2\ 4\ 6\ 3)(5)$. Since $|a| = 3$, $|b| = 2$ and $|ab| = 5$, the subgroup generated by a and b is isomorphic to $\mathbb{A}_5$. Moreover, since $\mathbb{A}_6$ has no subgroups of index less than 6, $N_{\mathbb{A}_6}(\mathbb{A}_5) = \mathbb{A}_5$.

It follows that the number of conjugates in $\mathbb{A}_6$ of an $\mathbb{A}_5$ fixing no points of $Y \setminus \{x\}$, is $[\mathbb{A}_6 : N_{\mathbb{A}_6}(\mathbb{A}_5)] = 6$.

There are 7 conjugate $G_x \cong \mathbb{A}_6$ in $\mathbb{A}_7$. Hence, there are in all $7 \times 6 = 42$ $\mathbb{A}_5$'s each fixing exactly one point, six in each G_x. These constitute a single conjugacy class of subgroups, which we denote by Q. Thus the collection of 63 $\mathbb{A}_5$'s in $\mathbb{A}_7$ splits into two conjugacy classes of sizes 21 and 42.

Below is the list of elements of an $\mathbb{A}_5$ fixing 1 :

Elements of order 2	Elements of order 3	Elements of order 5_1	Elements of order 5_2
(1)(2)(3)(4 7)(5 6)	(1)(2 3 4)(5 6 7)	(1)(2)(3 5 4 7 6)	(1)(2)(3 4 6 5 7)
(1)(2)(4)(3 6)(5 7)	(1)(2 4 3)(5 7 6)	(1)(2)(3 6 7 4 5)	(1)(2)(3 7 5 6 4)
(1)(2)(5)(3 4)(6 7)	(1)(2 5 6)(3 4 7)	(1)(3)(2 6 4 7 5)	(1)(3)(2 4 5 6 7)
(1)(2)(6)(3 7)(4 5)	(1)(2 6 3)(4 5 7)	(1)(3)(2 5 7 4 6)	(1)(3)(2 7 6 5 4)
(1)(2)(7)(3 5)(4 6)	(1)(2 4 6)(3 7 5)	(1)(4)(2 5 6 3 7)	(1)(4)(2 6 7 5 3)
(1)(3)(4)(2 5)(6 7)	(1)(2 7 6)(3 4 5)	(1)(4)(2 7 3 6 5)	(1)(4)(2 3 5 7 6)
(1)(3)(5)(2 7)(4 6)	(1)(2 6 4)(3 5 7)	(1)(5)(2 3 7 6 4)	(1)(5)(2 7 4 3 6)
(1)(3)(6)(2 4)(5 7)	(1)(2 3 5)(4 6 7)	(1)(5)(2 4 6 7 3)	(1)(5)(2 6 3 4 7)
(1)(3)(7)(2 6)(4 5)	(1)(2 4 7)(3 6 5)	(1)(6)(2 3 4 5 7)	(1)(6)(2 5 3 7 4)
(1)(4)(5)(2 6)(3 7)	(1)(2 5 4)(3 6 7)	(1)(6)(2 7 5 4 3)	(1)(6)(2 4 7 3 5)
(1)(4)(6)(2 7)(3 5)	(1)(2 6 5)(3 7 4)	(1)(7)(2 6 5 3 4)	(1)(7)(2 3 6 4 5)
(1)(4)(7)(2 3)(5 6)	(1)(2 7 3)(4 5 6)	(1)(7)(2 4 3 5 6)	(1)(7)(2 5 4 6 3)
(1)(5)(6)(2 3)(4 7)	(1)(2 3 6)(4 7 5)		
(1)(5)(7)(2 4)(3 6)	(1)(2 4 5)(3 7 6)		
(1)(6)(7)(2 5)(3 4)	(1)(2 5 3)(4 7 6)		
	(1)(2 7 5)(3 4 6)		
	(1)(2 3 7)(4 6 5)		
	(1)(2 6 7)(3 5 4)		
	(1)(2 5 7)(3 6 4)		
	(1)(2 7 4)(3 5 6)		

4.2.3 Constructing the Hoffman-Singleton Graph

Let $W = \{1, 2, \ldots, 6\}$, and define $Q = \{q_{xi} : x \in Y \text{ and } i \in W\}$ be the conjugacy class of $\mathbb{A}_5$'s in G each of which fixes exactly one point $x \in Y$. Note that $q_{xi} \leq G_x$ for $x \in Y$ and $i \in W$. It should be noted that although G acts on the elements of Y, the elements of W, as used here, are simply indices.

Lemma 4.2.1. *Suppose that for $x \in Y$, $Q_x = \{q_{xi} : i \in W\}$. For a given $i \in W$, and $y \in Y \setminus \{x\}$ we have*

$$q_{xi} \cap q_{yj} \cong \begin{cases} D_{10} & for\ exactly\ one\ j \in W \\ \mathbb{Z}_2 & for\, the\, remaining\, indices\, j. \end{cases}$$

Proof. We observe the intersection $q_{xi} \cap q_{yj}$ by analyzing the elements by order.

1. An element of order 3 in q_{xi} is of cycle type $(x)(a\,b\,c)(d\,e\,f)$. So that an element of order 3 in q_{xi} fixes exactly one point x whereas an element of order 3 in q_{yj} fixes exactly one point y and $y \neq x$. So, there is no elements of order 3 in $q_{xi} \cap q_{yj}$.

2. Let F be the set of 24 elements of order 5 in q_{xi}. All of the elements of F fix $x \in Y$, and for each $y \in Y \setminus \{x\}$ exactly 4 elements of F also fix y. So, the only possible elements of order 5 in $q_{xi} \cap q_{yj}$ are elements of type $(x)(y)(a\,b\,c\,d\,e)$. Hence, either there are no elements of order 5 or exactly 4 elements of order 5 in $q_{xi} \cap q_{yj}$, which comprise the non-identity elements of a cyclic subgroups of order 5. Moreover, for a given q_{xi} and $y \in Y \setminus \{x\}$ and for $(x)(y)(a\,b\,c\,d\,e) \in q_{xi}$, there is exactly one $j \in W$ for which $(x)(y)(a\,b\,c\,d\,e) \in q_{yj}$.

Notice that an $\mathbb{A}_5$ always contains a D_{10}, dihedral subgroup of order 10. There are precisely 6 different D_{10}'s in an $\mathbb{A}_5$. So, If $q_{xi} \cap q_{yj}$ contains 4 elements of order 5, then the corresponding elements of order 2 formed by pentagon reflections also lie in the intersection. Hence $q_{xi} \cap q_{yj} \cong D_{10}$. If $q_{xi} \cap q_{yj}$ does not contain an element of order 5, there exists exactly one element of order 2 in the intersection obtained by two different pentagons reflections one from each of q_{xi} and q_{yj}, both fixing x and y. In this case, $q_{xi} \cap q_{yj} \cong \mathbb{Z}_2$. □

Lemma 4.2.2. *Let $x, y \in Y$, $x \neq y$ and $i \in W$. If the cyclic subgroup of order 5 in q_{xi} fixing x and y is generated by the cycle $(z\,a\,b\,c\,d)$ for $z, a, b, c, d \in Y \setminus \{x, y\}$, then the cyclic subgroup of order 5 in q_{xi} fixing x and z is generated by the cycle $(y\,a\,c\,b\,d)$.*

Proof. Let $\langle (x)(y)(z\,a\,b\,c\,d)\rangle \leq q_{xi}$. Then $(x)(y)(z)(a\,d)(b\,c)$ is an element of order 2 in q_{xi} which is the reflection of the pentagon formed by the cycle $(z\,a\,b\,c\,d)$ with the axis of reflection passing through z. Since there is exactly one element of order 2 in q_{xi} fixing given 3 points, the possible 5 cycles in q_{xi} fixing x and z are the first 4 powers of $(y\,a\,b\,c\,d)$, and the first 4 powers of $(y\,a\,c\,b\,d)$. If $(x)(z)(y\,a\,b\,c\,d) \in q_{xi}$, then $\underbrace{(x)(y)(z\,a\,b\,c\,d)}\,\underbrace{(x)(z)(y\,a\,b\,c\,d)}\,\underbrace{(x)(z)(y\,a\,b\,c\,d)} = (x)(y\,b)(a\,d\,z\,c) \in q_{xi}$ which is an

element of order 4 in $\mathbb{A}_5$, a contradiction. Hence, we must have $\langle (x)(z)(y\,a\,c\,b\,d)\rangle \leq q_{xi}$.

□

From the proof of lemma 4.2.2, we can conclude that $(x)(y)(z\,a\,b\,c\,d) \in q_{xi}$ implies that $(x)(z)(y\,a\,c\,b\,d) \in q_{xi}$ whereas $(x)(z)(y\,a\,b\,c\,d) \notin q_{xi}$.

Theorem 4.2.3. *Let $X = \{\infty\} \cup Y \cup Q$ for some point ∞ not in $Y \cup Q$. Join ∞ with each element of Y. Join x with each element of Q_x. Join q_{xi} with q_{yj} $(x \neq y)$ if and only if $q_{xi} \cap q_{yj} \cong D_{10}$ for $x, y \in Y$ and $i, j \in W$. Then the graph so formed is the Hoffman-Singleton graph.*

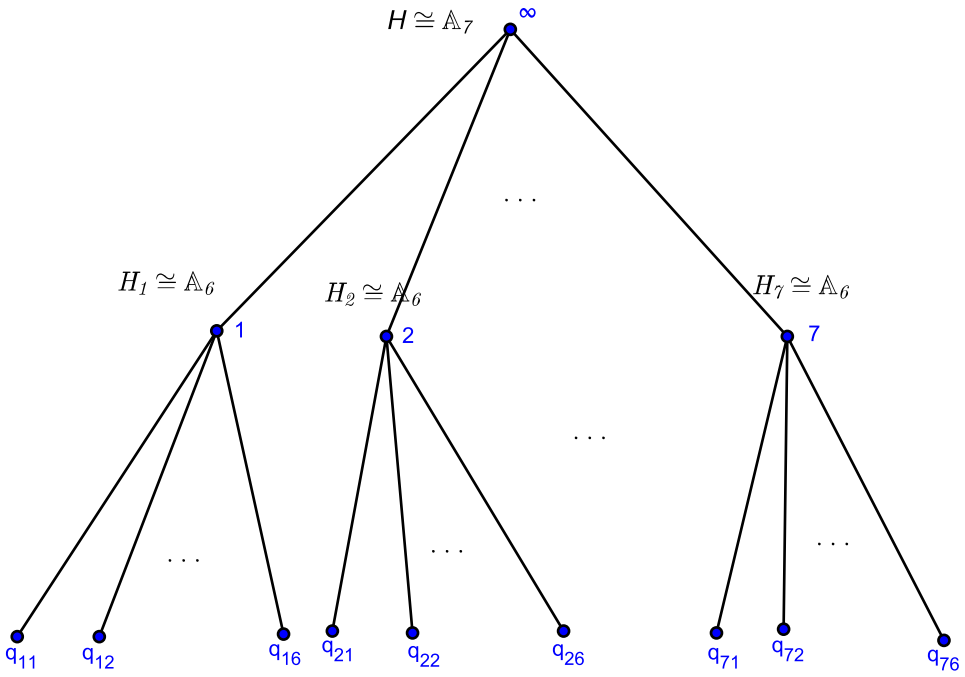

Figure 4.4: Hoffman-Singleton Graph

Proof. It is clear from the construction that the diameter of the graph is 2. We will prove that the parameters $(50, 7, 0, 1)$ of the Hoffman-Singleton graph are satisfied. Clearly the total number of vertices is $|X| = |\{\infty\} \cup Y \cup Q| = 1 + 7 + 42 = 50$. By construction, the degree of ∞ and each of $x \in Y$ is 7. Each q_{xi} is joined with x and exactly 6 q_{yj}'s for each $y \in Y \setminus \{x\}$. So, the degree of each q_{xi} is 7.

To show $\lambda = 0$, we need to show that $|S_1(u) \cap S_1(v)| = 0$ if $d(u, v) = 1$. We first notice that, for $x \in Y$, $d(\infty, x) = 1$ and $|S_1(\infty) \cap S_1(x)| = 0$ and also for $i \in W$, $d(x, q_{xi}) = 1$ and $|S_1(x) \cap S_1(q_{xi})| = 0$. We also need to prove that $|S_1(q_{xi}) \cap S_1(q_{yj})| = 0$ for q_{xi} and q_{yj} with $d(q_{xi}, q_{yj}) = 1$. It is sufficient to show that there is no triangle among the elements of Q. So, let $q_{xi}, q_{yj} \in S_1(q_{zk})$ for $x, y, z \in Y$ all distinct and $i, j, k \in W$. We just need to show that $q_{xi} \cap q_{yj} \cong \mathbb{Z}_2$. Now, by construction, $q_{xi} \in S_1(q_{zk})$ implies $q_{xi} \cap q_{zk} \cong D_{10}$. So that, $q_{xi} \cap q_{zk}$ contains an element of order 5 which fixes x and z, say $(x)(z)(y\,a\,b\,c\,d)$, for some $a, b, c, d \in Y \setminus \{x, y, z\}$. Then, by lemma 4.2.2, $(x)(y)(z\,a\,c\,b\,d) \in q_{xi}$ and $(z)(y)(x\,a\,c\,b\,d) \in q_{zk}$. But $q_{yj} \in S_1(q_{zk})$. So, $q_{yj} \cap q_{zk} \cong D_{10}$ which implies that $(z)(y)(x\,a\,c\,b\,d) \in q_{yj}$. Again, by lemma 4.2.2, $(y)\ (x)\ (z\,a\,b\,c\,d) \in q_{yj}$. Therefore, an element of order 5 in q_{xi} fixing x and y is of type $(x)(y)(z\,a\,c\,b\,d)$ whereas an element of order 5 in q_{yj} fixing y and x is of type $(y)(x)(z\,a\,b\,c\,d)$ each of which are elements of different cyclic groups of order 5. Hence, by lemma 4.2.1, $q_{xi} \cap q_{yj} \cong \mathbb{Z}_2$.

Now, we will prove that $\mu = 1$. We will prove this for all possible cases of distance 2. Clearly $d(\infty, q_{xi}) = 2$ for $x \in Y$ and $i \in W$ and $S_1(\infty) \cap S_1(q_{xi}) = \{x\}$. So that $|S_1(\infty) \cap S_1(q_{xi})| = 1$. Also, $d(x, y) = 2$ for $x, y \in Y$, $x \neq y$ and $S_1(x) \cap S_1(y) = \{\infty\}$, which implies $|S_1(x) \cap S_1(y)| = 1$. Furthermore, for $x, y \in Y$ with $x \neq y$ and $j \in W$, we have $d(x, q_{yj}) = 2$ and $S_1(x) \cap S_1(q_{yj}) = \{q_{xi}\}$ for exactly one $i \in W$ and So, $|S_1(x) \cap S_1(q_{yj})| = 1$. The only remaining case is $S_1(q_{xi}) \cap S_1(q_{yj})$, given that $d(q_{xi}, q_{yj}) = 2$. We will first prove that there is no 4-cycle in the subgraph induced by Q.

Let us take $q_{xi}, q_{yj}, q_{zk}, q_{wl} \in Q$ with x, y, z, w distinct elements of Y and $i, j, k, l \in W$ and assume that $q_{xi} \cap q_{yj} \cong D_{10}$, $q_{yj} \cap q_{zk} \cong D_{10}$, and $q_{zk} \cap q_{wl} \cong D_{10}$. We will show that $q_{wl} \cap q_{xi} \cong \mathbb{Z}_2$. Now, suppose $(x)(y)(z\,w\,a\,b\,c) \in q_{xi} \cap q_{yj}$ for $a, b, c \in Y \setminus \{x, y, z, w\}$, then, by lemma 4.2.2, $(y)(z)(x\,w\,b\,a\,c) \in q_{yj}$ and hence $(y)(z)(x\,w\,b\,a\,c) \in q_{yj} \cap q_{zk}$. But $(y)(z)(x\,w\,b\,a\,c) = (y)(z)(w\,b\,a\,c\,x)$, so that by the same argument,

$(z)(w)(y\,b\,c\,a\,x) \in q_{zk} \cap q_{wl}$. Again $(z)(w)(y\,b\,c\,a\,x) = (z)(w)(x\,y\,b\,c\,a)$. So, $(x)(w)(z\,y\,c\,b\,a) \in q_{wl}$. But, $(x)(y)(z\,w\,a\,b\,c) \in q_{xi}$, and $(x)(y)(z\,w\,a\,b\,c) = (x)(y)(w\,a\,b\,c\,z)$. So, we must have $(x)(w)(y\,a\,c\,b\,z) \in q_{xi}$ and hence $q_{xi} \cap q_{wl} \cong \mathbb{Z}_2$ since $(x)(w)(z\,y\,c\,b\,a)$ and $(x)(w)(y\,a\,c\,b\,z)$ are elements of distinct cyclic groups of order 5. Finally, we will prove that $|S_1(q_{xi}) \cap S_1(q_{yj})| = 1$ when $d(q_{xi}, q_{yj}) = 2$. Assume that $q_{yj'} \in S_1(q_{xi})$ for $j' \in W$ and $j' \neq j$ and $q_{vm} \in S_1(q_{xi})$ for each $v \in Y \setminus \{x, y\}$ and some $m \in W$. Then $q_{yj'} \notin S_1(q_{vm})$ for each q_{vm} because there are no triangles in Q. But, $|S_1(q_{vm}) \cap Q_y| = 1$ for each of 5 q_{vm}'s where $|Q_y| = 6$ and $q_{yj}, q_{yj'} \in Q_y$. Hence there is at least one q_{vm} such that $q_{yj} \in S_1(q_{vm})$. There can not be more than one q_{vm} such that $q_{yj} \in S_1(q_{vm})$ because there is no 4-cycle in the subgraph induced by Q. So there is exactly one q_{vm} such that $q_{yj} \in S_1(q_{vm})$. Therefore $|S_1(q_{xi}) \cap S_1(q_{yj})| = 1$ and hence $\mu = 1$. □

4.2.4 Remark

This construction of the Hoffman-Singleton graph and perhaps even its existence, is based on the unique property of $n = 6$ for $\mathbb{A}_n$ to have two conjugacy classes of $\mathbb{A}_{n-1}$. For every other n, $\mathbb{A}_n$ has exactly one conjugacy class of $\mathbb{A}_{n-1}$'s. One could now proceed to obtain a primitive rank-3 extension of $\mathbb{A}_7$, where $\mathbb{A}_7$ is the stabilizer of a point[10, 12]. We would then arrive at simple group $U_3(5) = PSU_3(5^2)$ of order 126,000 acting as a rank-3 group on X. The full automorphism group of $\mathcal{H}$ turns out to be $P\Sigma U_3(5^2)$, of order 252,000.

CHAPTER 5

COLLISION PROBLEM IN $PSL(2, p)$

There have been several recent cryptographic and cryptanalytic works on Cayley hashing schemes. For example, in 2010, M. Grassl, I. Ilić, S. Magliveras, and R. Steinwandt [8] constructed collisions for the Tillich and Zémor's hash function [33]. This approach also yields collisions for related proposals by Petit et al. from ICECS 08 [27] and CT-RSA 09 [26]. It would be of considerable value if we were able to construct a Cayley hashing scheme which is secure under cryptanalysis.

We are interested to work with Cayley hashing scheme in the projective special linear group, $PSL(2, p)$ for an odd prime p. Such a hashing scheme would be very similar to that of Tillich and Zémor construction. We describe below the proposed scheme.

Let $G = PSL(2, p) = \langle a, b \rangle$ generated by two elements a and b. Then a binary bitstring $v = b_1 \dots b_m \in \{0, 1\}^*$ is hashed by applying $h : \{0, 1\}^* \to G$ by:

$$0 \mapsto a$$

$$1 \mapsto b.$$

For example, $h(010010110) = abaababba \in G$. Since the order of G is approximately $\frac{p^3}{2}$ the hash value will be encoded into approximately a $[3 \log_2(p) - 1]$-bit hash value.

As discussed in 2.4.1, a secure cryptographic hash function has to possess three important properties: pre-image resistance, second pre-image resistance and collision resistance. Our attention is on collision resistance.

5.1 COLLISION IN $PSL(2, p)$

For an odd prime p, let $G = PSL(2, p)$ be the projective special linear group and suppose that G is generated by two elements a and b, i.e. $G = \langle a, b\rangle$. For any word $w(a, b)$, in a and b, let $\overline{w}$ denote the evaluation of $w(a, b)$ as an element of G. The *collision problem* in G is to find two different words $w_1(a, b)$ and $w_2(a, b)$ such that $\overline{w_1} = \overline{w_2}$. If the length $|w|$ of a word w is the total number of a's and b's appearing in w (only non-negative exponents can be used), the length of collision $\overline{w_1} = \overline{w_2}$, is the integer $\rho := |w_1| + |w_2|$. We are always interested in a collision of shortest length. So, without loss of generality, we assume that ρ is the length of a shortest collision.

Suppose that $G = \langle a, b\rangle$. For non-negative integer k we define B_k, the *block of words of length* k in a and b, to be the collection of all words of length k whose evaluation as element of G do not have a representation as words in a and b of length strictly less than k.

If we employ brute force to find a collision, we start forming blocks of words. We set $B_0 = [1]$, where 1 is the identity of G. Then, the block of words of length 1 is :

$$B_1 = [a, b]$$

To obtain B_k from B_{k-1} we form the ordered collection

$$B_k = B_{k-1}a \cup B_{k-1}b$$

Thus, in particular

$$B_2 = B_1a \cup B_1b = [aa, ba, ab, bb]$$

We continue this way to compute B_k from B_{k-1} . If in the process of computing B_k we find a word $w \in B_k$ whose evaluation $\overline{w}$ is equal to the evaluation $\overline{v}$ of an earlier computed word in $v \in B_i$ for $i \leq k$, then we have found a collision: $v \equiv w$, in which case we stop the process. Otherwise we continue computing new members of

B_k and if no collisions have been found by the end of the process, we have that :

$$|B_k| = 2|B_{k-1}| = 2^k$$

and we proceed to compute the block B_{k+1}.

Since $2 + 2^2 + ... + 2^k$ will exceed $|G|$ for some k, it is not possible that we will continue to have full blocks of length 2^i without any collisions. That is, in the worst case if k is such that $\sum_{i=1}^{k} 2^k > |G|$ there are two words in the union $w_1, w_2 \in B_1 \cup B_2 \cup \cdots \cup B_k$, such that $w_1 \neq w_2$ and $\overline{w_1} = \overline{w_2}$. In other words, we will get a collision. From $2 + 2^2 + 2^3 + \cdots + 2^k \geq |G|$ we get $2(2^k - 1) \geq |G|$, which gives, $2^{k+1} \geq |G| + 2 \geq |G|$, and hence $k \geq log_2|G| - 1$. Hence, we get the following lemma.

Lemma 5.1.1. *If $k > log_2(|G|)$ then there is a collision $\overline{w_1} = \overline{w_2}$ for some $w_1, w_2 \in B_1 \cup \cdots \cup B_k$, $w_1 \neq w_2$.*

In case of $G = PSL(2, p)$, we can approximate the value of k in terms of p. Since $|PSL(2, p)| = \frac{p(p^2-1)}{2} \approx \frac{p^3}{2}$, we will get, $k \approx 3log_2 p$. For example, if $p \approx 2^{10}$, then $k \approx 30$, which means that we will get a collision if we reach to the block of length 30. So, the number of computation required maybe as high as 2^{31}. Since the number of computations and required storage grows exponentially, a brute force method becomes infeasible as the value of p becomes sufficiently large. This information motivates us to try to find such a generating pairs whose collision length is sufficiently large.

We call a collision to be *long* if $\rho \approx O(log|G|)$. The name long is in the sense that the computation becomes infeasible for sufficient large values of p. Otherwise, we call it *short*. To evaluate the possible utility of hash functions for $PSL(2, p)$ described above, it is important to understand the distributional collision length characteristics, over all possible pairs of generators (a, b) of $PSL(2, p)$. Our goal is to characterize the generating pairs in $PSL(2, p)$ having short and long collisions.

5.2 ANALYSIS OF ORBITALS

It is infeasible to check the collision characteristics for all possible pairs (a, b), such that $\langle a, b\rangle = G$, because the number of such pairs is extremely large.

If we choose at least one of a or b, of small order, we get a trivial collision. By *trivial collision*, we mean, a collision $g = g\underbrace{g\cdots g}_{i}$ of length $1 + (1 + i) = i + 2$, for a generator g of order i. So, both of a and b must be of higher order. If at least one of a and b is of order p, then the non-abelian discrete logarithm problem in $PSL(2, p)$ can be solved by I. Ilić algorithm, [15] and hence collision is achieved. Even if none of a and b are of order p, if we are able to obtain an element of order p as a short word in a and b, we can go back to above condition and hence a collision can be found. By a short word in a and b we mean the computation is feasible. Finding an element of order p as a word in a and b is called the $p-$*depth problem*. It is in a sense similar to collision problem. There is an investigation of the $p-$depth problem in [15].

So, our interest is on the pairs (a, b) where both a and b are of order $\frac{p-1}{2}$. The reason is also because, there is high probability that two randomly selected elements of order $\frac{p-1}{2}$ generate whole group. The following theorem substantiates this statement.

Theorem 5.2.1. *The probability that two randomly selected elements generate whole group $G = PSL(2, p)$ among all possible pairs of elements of order $\frac{p-1}{2}$ is $\frac{(p-1)(p-2)}{p(p+1)}$.*

Proof is in [15].

So, let X be the set of all elements of order $d = \frac{p-1}{2}$. Then, since there are $\frac{p(p+1)}{2}$ conjugate cyclic subgroups of order d and each cyclic subgroup has $\phi(d)$ elements of order d, the total number of elements of order of d in G is $\frac{p(p+1)}{2}\phi(d)$. So, we have $|X| = \frac{\phi(d)p(p+1)}{2}$ and hence $|X \times X| = (\frac{\phi(d)p(p+1)}{2})^2$, which is still a very big number of pairs to check for collision.

Let us consider the induced action of G on $X \times X$ by conjugation.

Lemma 5.2.1. *The length of collision ρ is invariant under conjugation.*

Proof. Let $\rho = \rho(a,b)$ be the length of a collision with respect to a generating pair (a,b). Let $g \in G$ and let $(a,b)^g = (a^g, b^g) = (g^{-1}ag, g^{-1}bg) = (a',b')$. Note that if $(w(a,b))^g = g^{-1}w(a,b)g$, then $(w(a,b))^g = w(a,b)^g = w(a',b')$. Also, $|w(a',b')| = |w(a,b)|$. Moreover, $w_1(a,b) = w_2(a,b)$ implies $w_1(a,b)^g = (w_1(a,b))^g = (w_2(a,b))^g = w_2(a,b)^g$. Hence $\rho = |w_1(a,b)| + |w_2(a,b)| = |w_1(a,b)^g| + |w_2(a,b)^g| = |w_1(a',b')| + |w_2(a',b')|$. □

So that, we achieve considerable computational gain by selecting representatives of orbits under conjugation of the action $G|(X \times X)$. We are interested in the number of orbits of $G|(X \times X)$.

Theorem 5.2.2. *The number of orbits of the action $G|(X \times X)$ is*

$$\eta = \frac{\phi(d)^2(p+3)}{2}$$

Proof. Let H be any particular fixed subgroup of G of order d. If $t = \frac{\phi(d)}{2}$, the elements of order d in H can be arranged in conjugate pairs as

$$\{(x_1, x_1^{-1}), \ldots, (x_i, x_i^{-1}), \ldots, (x_t, x_t^{-1})\}$$

with x_i conjugate to x_j if and only if $i = j$. Let $Y = \{x_1, \ldots, x_t\}$. Let Z be a collection of orbit representatives of H acting on X by conjugation. By elementary group theory, we can show that the pairs in $Y \times Z$ constitute a complete set of distinct representatives of the G-orbits on $X \times X$. Looking at the action $H|X$ by conjugation, we see that H commutes with the $\phi(d)$ elements of order d in H, thus these elements are fixed under conjugation by H. The remaining $|X| - \phi(d)$ elements of X fall into orbits of length d under H, because no element of H fixes under conjugation (i.e. commute with) any element of order d besides the elements of order d in H. This yields, $\phi(d) + \frac{|X|-\phi(d)}{d}$ $H-$orbits on X. Thus, $\eta = |Y \times Z| = |Y| \cdot |Z|$. Hence we have, $\eta = \frac{\phi(d)}{2}\left(\phi(d) + \frac{|X|-\phi(d)}{d}\right) = \frac{\phi(d)}{2}\left(\phi(d) + \frac{\frac{\phi(d)p(p+1)}{2} - \phi(d)}{d}\right) = \frac{\phi(d)^2(p+3)}{2}$.

□

As explained in the proof of the above theorem, we prepare $\frac{\phi(d)^2(p+3)}{2}$ representative pairs and check to see which pairs generate the whole group. Theorem 5.2.1 is the witness of the fact that a lot of them will generate the whole group. We collect all the generating pairs and for each we perform and experiment to check for the length of the collision. We use APL to perform all these computations.

5.2.1 Computation

The ksims algorithm

In 1968, Professor Charles Sims published a remarkable algorithm which facilitates computation with finite permutation groups. Various improved versions were developed since then. The current version of the algorithm used in this thesis was developed by Leo Chouinard, Jr. and Spyros Magliveras in the late 1970's at the University of Nebraska, Lincoln, and is based on a non-deterministic procedure. The algorithm is called *ksims* in honor of Donald Knuth and Charles Sims. This algorithm is of polynomial time complexity, where the input is the set of generators for a permutation group G, and the output is the order of the group, and in the predefined variable, for example G, it stores three objects; the prescribed name of the group, the set of generators of the group, and a *logarithmic signature* of the group. By a logarithmic signature of a group we mean the following: Let G be a finite group. The ordered set $\alpha = [A_1, A_2, \ldots, A_s]$ where $A_i \subseteq G$, A_i ordered, for $1 \leq i \leq s$, is called a *logarithmic signature* of G if and only if every element $g \in G$ can be represented uniquely as $g = g_1 g_2 \cdots g_s$ where $g_i \in A_i$ for $1 \leq i \leq s$. Other characteristics of the algorithm include the following: given an element $x \in \mathbb{S}_n$, there is an efficient way to decide whether $x \in G$ or not. Also, using the logarithmic signature, there is an efficiently computable bijective mapping $\sigma : G \to \mathbb{Z}_{|G|}$.

5.2.2 The collision algorithm

Given as input two generators a and b of $G = PSL(2, p)$, the output is the length of a collision, which is the sum of the lengths of two different words in a and b that represent the same group element. Let v be a vector of zeros of length $|G|$. Let B_k be the block of words of length k and let $Z_k = \sigma(B_k)$, i.e. the set of images under σ of the group elements $\overline{w}$, for $w \in B_k$. We can find the set Z_k by means of the logarithmic signature. We start by assigning the value 1 to the Z_1 positions of v. Recall that we form the block B_k from the block B_{k-1} by $B_k = B_{k-1}a \cup B_{k-1}b$. Recursively, assume we have assigned the value $k-1$ to the Z_{k-1} positions of v. To check for a collision in the k^{th} step, we check to see if all the values of v in the Z_k positions are zero or not. If not, there is a collision of length $k+i$, where $i < k$ is the non-zero value assigned in v in the i^{th} step. Even if all the values of v in the Z_k positions are zero, if $|Z_k| < 2^k$, we will get a collision of length $k + k = 2k$ in the B_k^{th} block with itself. Otherwise, there is no collision, in which case we assign the value k to the Z_k positions of v and iterate. The termination of iteration is guaranteed by the lemma 5.1.1.

The earliest and the shortest collision

The first collision we obtain by the above algorithm may not necessarily be the shortest, because the collision length is the sum of two block lengths. For example we may get collision of type $9 + 11 = 20$, whereas there may exist the shortest collision of type $3 + 13 = 16$ after two blocks. So, we call the first collision occurring the *earliest collision*. The earliest collision is of equal importance as the shortest collision. Our algorithm continues to check to see if there exist collisions shorter than the earliest collision.

Space-time tradeoff

Note that $|B_{k+1}| = 2|B_k| = 2^{k+1}$. So, the workspace requirement grows exponentially. Since the number of computations can be higher, we can run out of space very soon. So, for relatively large values of p, we can undertake a space-time tradeoff. Instead of saving B_k, which is the block of words of length k where each element is a permutations on $p+1$ points, we just save the vector Z_k, the image under σ set of B_k in $\mathbb{Z}_{|G|}$. An integer consumes much less space compared to a permutation on $p+1$ points. The element of B_k can be recovered one at a time as σ^{-1} is efficiently computable by an appropriate *ksims* function. Nonetheless, we have to perform element-wise multiplication by a and b instead of block-wise multiplication, so we loose time. The logarithmic signature subroutines handle the job of mapping $\sigma : G \mapsto \mathbb{Z}_{|G|}$ and vice versa.

The table below is the list of minimum and maximum earliest collisions and the shortest collisions inside a $PSL(2, p)$ for primes $19 \leq p \leq 113$.

Prime (p)	$\|G\|$	$log_2\|G\|$	min. earliest, shortest collision	max. earliest collision	max. shortest collision
19	3420	11.74	6	14	11
23	6072	12.57	6	17	13
29	12180	13.57	6	16	16
31	14880	13.86	6	21	17
37	25308	14.63	6	20	20
41	34440	15.07	6	18	18
43	39732	15.28	6	20	20
47	51888	15.66	6	24	22
53	74412	16.18	6	22	22
59	102660	16.65	6	25	23
61	113460	16.79	6	24	24
67	150348	17.20	6	24	24
71	178920	17.45	6	26	24
73	194472	17.57	6	23	23
79	246480	17.91	6	25	23
83	285852	18.13	6	24	24
89	352440	18.43	6	24	24
97	456288	18.80	6	23	23
101	515100	18.98	6	26	26
103	546312	19.06	6	26	26
107	612468	19.22	6	26	26
109	647460	19.30	6	26	26
113	721392	19.46	6	27	27

Table 5.1: Min. and Max. length of the earliest and the shortest collision for $19 \leq p \leq 113$

Below is the frequency distribution of the earliest and the shortest collision length for $PSL(2, 113)$.

collision	6	7	8	9	10	11	12	13	14	15	16
E. Coll. freq.	24	16	302	72	650	250	2324	576	3688	732	8288
S. Coll. freq.	288	16	1100	74	1358	1276	2630	890	5322	1806	7774
Collision	17	18	19	20	21	22	23	24	25	26	27
E. Coll. freq.	1092	7912	892	4576	188	340	14	16	8	2	6
S. Coll. freq.	3280	4370	1022	668	48	16	8	10	8	2	2

Table 5.2: Freq. dist. of the earliest collision and the shortest collision for $PSL(2, 113)$

The same table in bar diagram form:

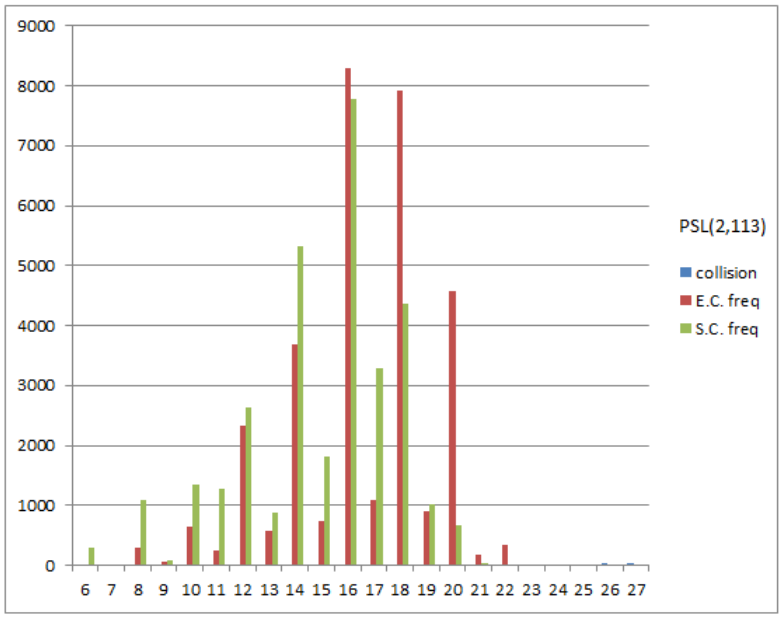

Figure 5.1: The earliest collision and the shortest collision for $PSL(2, 113)$

5.3 OBSERVATION

There always exists a generating pair (a, b) such that the order of ab is 2. This gives the trivial collision $a = aabab$ whose length is 1+5=6. There always exists a shortest collision of length greater than $log_2|G|$. If the order of ab is small, we get a short collision. The reason is because, if $|ab| = i$, then $a = a\underbrace{\underline{ab}\cdots\underline{ab}}_{i}$ is the obvious collision and its length is $1 + (1 + 2i) = 2 + 2i$.

5.4 CONCLUSION

5.4.1 Bad generators

The generating pairs for which the collision found is short ($\rho < log_2|G|$) are called *bad generators*. Bad generators are not collision resistant. For this reason, it is extremely important for a cryptographer to have prior knowledge of bad generators, so that they can avoid those pairs while choosing the pair (a, b) for a hashing scheme.

Theorem 5.4.1. *The following are some sufficient conditions for a generating pair* (a, b) *to be a bad generator:*

1. *at least one of* a *or* b *is of small order,*
2. *the product* ab *is of small order,*
3. *at least one of* a *or* b *is of order* p*,*
4. *there exists an element of order* p *as a short word in* a *and* b*.*

5.4.2 Good generators

The generating pairs for which the earliest collision is long ($\rho > log_2|G|$) are called *good generators*, or *secure generators*. If there exist a good generating pair, the time complexity (number of computations), to find a collision is $\approx 2^{log_2|G|} = |G|$, which is computationally infeasible because the prime we use is approximately 2^{1000}. So, the number of computation required is approximately 2^{3000} which is infeasible using the most modern computers. Hence, they are collision resistant. In our experiment we always obtain secure generators.

Moreover, for each prime, we obtain several good generators and bad generators. For example, for $p = 113$, we categorize length of the shortest collision as follows:

collision length	$6 - 14$	$15 - 19$	$20 - 27$
category of generators	bad	fair	secure
probability	40%	57 %	3%

We will end this section with the following conjecture.

Conjecture 5.4.2. *There always exists a secure generating pair* (a, b) *in a group* $PSL(2, p)$.

BIBLIOGRAPHY

[1] Burnside, W., *Theory of Groups of Finite Order*, Dover, New York (1955).

[2] John H. Conway, *A perfect group of order 8,315,553,613,086,720,000 and the sporadic simple groups*, Proceedings of the National Academy of Sciences of the United States of America 61 (2): 398-400 (1968).

[3] Leonard Eugene Dickson with an introduction by Wilhelm Magnus, *Linear Groups with an exposition of the Galois field theory*, Dover Publications, Inc., New York (1958).

[4] Banai Eiichi, Ito Tatsuro, *Algebraic Combinatorics I and Association Schemes*, The Benjamin/Cummings Publishing Company, Inc., California (1984).

[5] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren, *Cryptographic hash functions from expander graphs*, J. Cryptology 22, no. 1, 93-113 (2009).

[6] Whitfield Diffie and Martin Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory 22 (6): 644-654 (1976).

[7] Walter Feit, *Characters of Finite groups*, W. A. Benjamin, Inc., New York (1967).

[8] Markus Grassl, Ivana Ilić, Spyros Magliveras, and Rainer Steinwandt, *Cryptanalysis of the Tillich-Zémor hash function*, Journal of Cryptology (2010).

[9] M. Hall Jr., *The Theory of Groups*, Macmillan, New York (1959).

[10] Marshall D. Hestenes, *On the use of Graphs in Group Theory*, New Direction in the Theory of Graphs, Academic Press, New York and London, pp. 97-128 (1973).

[11] Marshall D. Hestenes and Donald G. Higman, *Rank-3 groups and strongly regular graphs*, Computers in Algebra and Number Theory, SIAM-AMS Proceedings 4, pp. 141-159 (1971).

[12] Donald G. Higman, *Finite Permutation Groups of Rank-3*, Math. Zeitschr. 86, pp. 145-156 (1964).

[13] Donald G. Higman and Charles C. Sims, *A Simple Group of Order 44,352,000*, Mathematische Zeitschrift 105 (2): 110-113 (1968).

[14] A.J. Hoffman, R.R. Singleton, *On Moore Graphs with Diameters 2 and 3*, IBM Journal of Research and Development 4, 497-504 (1960).

[15] Ivana Ilić, *The Discrete Logarithm Problem in Non-abelian Group*, Dissertation (Ph.D.) Florida Atlantic University (2010).

[16] Wolfgang Lempken, Spyros S. Magliveras, Tran van Trung and Wandi Wei, *A public key cryptosystem based on non-abelian finite groups*, J. Cryptology, 22, pp 62-74 (2009).

[17] Neal Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation 48 (177): 203-209 (1987).

[18] Krishna B. Thapa Magar and Spyros S. Magliveras, *A new construction of the Hoffman-Singleton graph using a well known peculiarity of* $\mathbb{A}_6$, Congressus Numerantium 215, pp. 97-103 (2013).

[19] Spyros S. Magliveras, *Classnotes on Group Actions*, personal communic. (2010).

[20] Spyros S. Magliveras *Secret- and Public-key Cryptosystems from Group Factorizations*, Tatra Mt. Math. Pub., 25, pp. 11-22 (2002).

[21] Spyros S. Magliveras and Nasir D. Memon *Properties of Cryptosystem PGM*, Advances in Cryptology, Lecture Notes in Comp. Sc., Springer Verlag 435, pp 447-460, (1989).

[22] Spyros S. Magliveras, B. A. Oberg, and A. J. Surkan *A new random number generator from permutation groups*, Rendiconti del Seminario, Mathematico e Fisico, di Milano, Vol. Liv (1984).

[23] Spyros S. Magliveras and Tran Van Trung and Douglas R. Stinson *New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups*,J. Cryptology,15, pp. 285-297 (2002).

[24] J. McLaughlin, *A simple group of order 898,128,000*, Theory of Finite Groups,(R. Brauer, ed.) Benjamin, New York, pp. 109-111 (1969).

[25] Victor S. Miller, *Use of elliptic curves in cryptography*, CRYPTO. Lecture Notes in Computer Science 85: 417-426 (1985).

[26] Christophe Petit, Jean-Jacques Quisquater, Jean-Pierre Tillich, and Gilles Zémor, *Hard and easy Components of Collision Search in the Zémor-Tillich Hash Function: new Attacks and Reduced Variants with Equivalent Security.*, M. Fischlin, editor, Topics in Cryptology CT-RSA 2009, volume 5473 of Lecture Notes in Computer Science, pages 182-194. Springer-Verlag, (2009).

[27] Christophe Petit, Nicolas Veyrat-Charvillon, and Jean-Jacques Quisquater, *Efficiency and Pseudo-Randomness of a Variant of Zémor-Tillich Hash Function*, IEEE International Conference on Electronics, Circuits, and Systems ICECS (2008).

[28] James Thomas Renfrow , *A study of rank-4 permutation groups*, Dissertation (Ph.D.) California Institute of Technology (1969).

[29] Ron Rivest, Adi Shamir, and Leonard Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21 (2): 120-126 (1978).

[30] Joseph J. Rotman, *An Introduction to the Theory of Groups*, isbn 3-540-94285-8, Springer-Verlag, 4th edition, pp. i - 513 (1999).

Rudvalis, A. (1973), "A new simple group of order 214 33 53 7 13 29", Notices of the American Mathematical Society (20): A95

[31] Arunas Rudvalis, *A new simple group of order* $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$, Notices of the American Mathematical Society (20): A-95 (1973).

[32] M. Suzuki, *A simple group of order 448,345,497,600*,Theory of Finite Groups,(R. Brauer, ed.) Benjamin, New York, pp. 113-119 (1969).

[33] Jean Pierre Tillich, Gilles Zémor. *Hashing with* SL_2. In Y. Desmedt, editor, Advances in Cryptology CRYPTO'94, volume 839 of Lecture Notes in Computer Science, pages 40-49 (1994).

[34] Wielandt, H.,*Finite Permutation Groups*, Academic Press, New York (1964).

[35] Wielandt, H., Endliche *k-homogene Permutationsgruppen*, Math. Z. 101 (1967).