On the Minimal Logarithmic Signature Conjecture

by

Nidhi Singhi

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, Florida

May 2011

On the Minimal Logarithmic Signature Conjecture

by

Nidhi Singhi

This dissertation was prepared under the direction of the candidate's dissertation advisor, Dr. Spyros S. Magliveras of the Department of Mathematical Sciences, and it has been approved by the members of her 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.

Stephen Locke, Ph.D.

Ronald C. Mullin, Ph.D.

Rainer Steinwandt, Ph.D.

Lee Klingler, Ph.D.
Chair, Department of Mathematical Sciences

Gary W. Perry, Ph.D.
Dean, The Charles E. Schmidt College of Science

Barry T. Rosson, Ph.D.
Dean, Graduate College

April 7, 2011
Date

Acknowledgments

First, I would like to express my deepest gratitude to my advisor Professor Spyros Magliveras, for all his inspiration, his teachings and his affection. My researching world was illuminated with his guidance. He taught me how to enjoy all aspects of mathematics as well as those of life. His inspiring style will provide guidance to me in all walks of life.

I would like to thank the members of my supervisory committee - Professors Lee Klingler, Stephen Locke, Ronald Mullin and Rainer Steinwandt - for their invaluable advice on several occasions. Special thanks to Professor Hoffman for patiently going through my dissertation and suggesting several improvements. I would like to thank Hanne Niederhausen and Professor Heinrich Niederhausen for all their help and guidance. I will truly treasure the time I have spent in their humble company.

Thanks to all the faculty members of Department of Mathematical Sciences at FAU for sharing their valuable insights in different areas of mathematics. I would also like to thank members of the administrative staff, Beth and Emily for all their help. I am grateful to all my dear friends at FAU, for their constant support and all their smiles :). I will always cherish the ecstatic moments I have passed in their warm company.

Abstract

Author:	Nidhi Singhi
Title:	On The Minimal Logarithmic Signature Conjecture
Institution:	Florida Atlantic University
Dissertation Advisor:	Dr. Spyros S. Magliveras
Degree:	Doctor of Philosophy
Year:	2011

The minimal logarithmic signature conjecture states that in any finite simple group there are subsets A_i, $1 \leq i \leq s$ such that the size $|A_i|$ of each A_i is a prime or 4 and each element of the group has a unique expression as a product $\prod_{i=1}^{s} a_i$ of elements $a_i \in A_i$. Logarithmic signatures have been used in the construction of several cryptographic primitives since the late 1970's [3, 15, 17, 19, 16]. The conjecture is shown to be true for various families of simple groups including cyclic groups, A_n, $PSL_n(q)$ when $\gcd(n, q-1)$ is 1, 4 or a prime and several sporadic groups [10, 9, 12, 14, 18]. This dissertation is devoted to proving that the conjecture is true for a large class of simple groups of Lie type called classical groups. The methods developed use the structure of these groups as isometry groups of bilinear or quadratic forms. A large part of the construction is also based on the Bruhat and Levi decompositions of parabolic subgroups of these groups.

In this dissertation the conjecture is shown to be true for the following families of simple groups: the projective special linear groups $PSL_n(q)$, the projective symplectic groups $PSp_{2n}(q)$ for all n and q a prime power, and the projective orthogonal groups of positive type $\Omega^+_{2n}(q)$ for all n and q an even prime power. During the process, the existence of minimal logarithmic signatures (MLS's) is also proven for the linear groups: $GL_n(q)$, $PGL_n(q)$, $SL_n(q)$, the symplectic groups: $Sp_{2n}(q)$ for all n and q a prime power, and for the orthogonal groups of plus type $O^+_{2n}(q)$ for all n and q an even prime power. The constructions in most of these cases provide cyclic MLS's. Using the relationship between finite groups of Lie type and groups with a split BN-pair, it is also shown that every finite group of Lie type can be expressed as a disjoint union of sets, each of which has an MLS.

Dedication

Dedicated to my parents Sudha and Navin Singhi for their endless love, encouragement and support.

Contents

List of Tables

Chapter 1

Introduction

Public key cryptosystems such as RSA, ElGamal over a finite field $\mathbb{F}_q$ or an elliptic curve, rely on the difficulty of certain problems in finite abelian groups, which have been thoroughly studied. In 2002, P. Nguyen [20] stated that "Due to Shor's algorithms for computing prime factorizations and discrete logarithms on quantum computers, most of the present day public key cryptosystems must be considered insecure, if sufficiently large quantum computers became available". Nguyen further suggests: "...One interesting line of research in this direction is the use of computational problems in non-abelian groups..." [20]. In this context, cryptosystems based on non-abelian groups become an important part of "post-quantum" cryptography.

In the late 1970's, Magliveras invented a private key cryptosystem called Permutation Group Mappings (PGM), which was based on a special kind of factorizations called, ***Logarithmic Signatures*** for finite permutation groups [17]. In the decade 2000-2010, Magliveras, Stinson, Trung, and Wei proposed new public-key cryptosystems MST_1, MST_2 and MST_3 based on logarithmic signatures and *covers* for finite non-abelian groups [16, 15, 18].

Let G be a finite group and $A \subseteq G$. Let $\alpha = [A_1, \ldots, A_s]$ be an ordered tuple of

subsets A_i of G, $1 \leq i \leq s$; $s \in \mathbb{N}$. Then, α is said to be:

(i) a ***Cover*** for A, if every $a \in A$, can be expressed as a product of the form $a_1 a_2 \dots a_s$, where $a_i \in A_i$, $1 \leq i \leq s$.

(ii) a ***Logarithmic Signature (LS)*** for A, if every $a \in A$ can be uniquely expressed as a product of the form $a_1 a_2 \dots a_s$, where $a_i \in A_i$, $1 \leq i \leq s$.

Let $\alpha = [A_1, \dots, A_s]$ be an LS for a finite group G. Then, the subsets A_i are called the *blocks* of α and the *length* of α is defined as $\ell(\alpha) = \sum_{i=1}^{s} |A_i|$. In [10], while discussing the security of MST_1 and MST_2, González Vasco and Steinwandt gave the following straightforward lower bound for $\ell(\alpha)$. If $|G| = \prod_{j=1}^{k} p_j^{m_j}$ where the p_j are primes, then $\ell(\alpha) \geq \sum_{i=1}^{k} m_j p_j$.

If the equality holds in the above bound, then α is called a ***Minimal Logarithmic Signature (MLS)***. Motivated by finding short keys for MST_1, in [9], González Vasco, Rötteler and Steinwandt showed the existence of ***Minimal Logarithmic Signatures*** for all groups of order $< 175,560$, the order of Janko's first sporadic group. They also noted that, if an MLS exists for a normal subgroup H of G, and also for the quotient group G/H, then there is an MLS for G. Therefore, if every finite simple group had an MLS then, every finite group would have an MLS.

At the beginning of our research, finding MLS's for finite simple groups had already become an intriguing question for researchers playing with logarithmic signatures both from the mathematical and the cryptographic point of view. In [10], González Vasco and Steinwandt derived the existence of MLS's for solvable groups and the symmetric groups S_n. Magliveras proved that an MLS exists for alternating groups A_n [18]. Later, Lempken and Trung presented an elegant approach, using double coset decompositions, to construct MLS's for all groups of order $\leq 10^{10}$. In

particular, they proved the existence of an MLS for all simple groups G of order $175,560 \leq |G| \leq 10^{10}$ (with the few exception of eight groups) [14]. They also proved that MLS's exist for $PSL_n(q)$ where $\gcd(n, q-1) = \{1, 4\}$ or a prime. In [12], Holmes constructed MLS's for the sporadic groups J_1, J_2, HS, M^cL, He, Co_3.

By 2008, the smallest group for which the existence of an MLS (as mentioned in [14]) was unknown was the Tits group of order $17,971,200$. Structurally Tits group is very similar to finite groups of Lie type. Inspired by the above mentioned interesting results, we began researching the MLS conjecture i.e., "Every finite simple group has a Minimal Logarithmic Signature". Our efforts were focused on the large class of finite groups of Lie type.

One aspect that became clear to us was that the methods developed so far to construct MLS's were not sufficient to handle the MLS conjecture. We began by observing groups of Lie type as permutation groups acting transitively on certain sets. For example, the set of all *isotropic points* in the projective space with respect to the *bilinear* form associated with the symplectic group.

Then, as shown in this dissertation, constructing MLS's for a permutation group is equivalent to finding *sharply transitive sets* and *stabilizers* that have an MLS. We noticed that the stabilizers of these points in finite groups of Lie type are precisely the *Parabolic subgroups*. We could see Lempken and Trung's theorem in a new light [14]. Our proofs for the existence of an MLS are quite different from those in [14] and in the case of $G = PSL_n(q)$, we remove the Lempken-Trung restriction on n and q.

Parabolic subgroups led us to *Bruhat* and *Levi decompositions* of the groups of

Lie type. This also gave us an inductive step to construct MLS's and other partitions for these groups. At some stage, we found a link between sharply transitive sets and objects like *spreads* and *ovals* in the geometry corresponding to these groups. The results of these geometric objects and Levi decompositions depend heavily on the type of group, the field characteristic, as well as the dimension.

Thus, even though our methods are universal and might work for all finite groups of Lie type and possibly the sporadic groups, in actual constructions of MLS's, we have to consider each family of groups of Lie type separately. Therefore, in this dissertation we focus on classical groups.

We now summarize the results described in this dissertation. We first apply our methods to *special linear groups* to generalize the result of Lempken and Trung [14]. We then prove the existence of MLS's for $GL_n(q)$, $PGL_n(q)$, $SL_n(q)$ and $PSL_n(q)$ for any $n \in \mathbb{N}$ and q a prime power. Subsequently we use spreads to construct MLS's for the symplectic and the orthogonal families of classical groups. In particular, we construct MLS's for $Sp_{2m}(q)$, $PSp_{2m}(q)$ for any $m \in \mathbb{N}$; q a prime power, and for $O^+_{2m}(q)$ and $\Omega^+_{2m}(q)$ for any $m \in \mathbb{N}$, q a power of 2.

In the concluding section, we also give a general method to construct partitions of a finite group of Lie type. We show that any finite group of Lie type can be expressed as a disjoint union of sets, each of which has an MLS.

In Chapter 2, we give definitions pertaining to finite groups of Lie type. We also discuss the relationship between classical groups as isometry groups of bilinear, *quadratic*, *sesquilinear forms*, and as seen as groups with a *split BN-pair*.

In Chapter 3, we describe properties of logarithmic signatures and give our basic

method of constructing MLS's for permutation groups.

In Chapter 4, we construct MLS's for the linear family of of classical groups. In Chapters 5 and 6 we establish the existence of MLS's for the symplectic groups over any field $\mathbb{F}_q$ and for the orthogonal groups of plus type over the field of characteristic 2.

In the last chapter, we use the relationship between finite groups of Lie type and groups with a split BN-pair. We use a natural expression for an element of a group with a split BN-pair (obtained by Bruhat and Levi decompositions) to construct a cover and a partition for finite groups of Lie type.

Chapter 2

Preliminaries

In this chapter, we begin by providing the definitions and theory needed to define finite groups of **Lie type**. We then define these groups in Section 2.5. Finite groups of Lie type are classified into two main classes: Classical groups and Exceptional groups of Lie type. A substantial part of this dissertation focuses on the classical groups. In Section 2.6, we give the necessary background to define classical groups as isometry groups. We use this structure to construct MLS's in the subsequent chapters. The last two sections are devoted to describing the relationship between finite groups of Lie type and finite groups with a split BN-pair. The results stated in Section 2.7 use this relationship and help us to construct partitions for all finite groups of Lie type in the later chapters.

2.1 Permutation groups and sharply transitive sets

In this section, we explain a few basic concepts related to permutations groups and sharply transitive sets. Let G be a finite group. A *(left) group action* is a triple (G, X, ϕ) where G is a group, X is a set, and ϕ is a map from $G \times X$ onto X satisfying the following two axioms: i) $\phi(1, x) = x$ for all $x \in X$, where 1 is

the identity of G, and ii) $\phi(g, \phi(h, x)) = \phi(gh, x)$ for all $g, h \in G$ and all $x \in X$. By suppressing ϕ we simplify notation so that $\phi(g, x)$ is denoted by gx. Then, the two axioms simply become i) $1x = x$ for all $x \in X$, 1 the identity of G, and ii) $g(hx) = (gh)x$, for all $g, h \in G$ and $x \in X$. Further, we denote the group action by $G|X$ and say that G *acts* on X. The *kernel* of the group action $G|X$ is $K = K_{G|X} = \{g \in G \mid gx = x \text{ for all } x \in X\}$. It is easy to see that a group action $G|X$ amounts to a homomorphism of G into the symmetric group S_X with kernel K. The action $G|X$ is said to be *faithful* if $K_{G|X} = 1$. When $G|X$ is faithful, the homomorphism becomes an isomorphism and we identify G with its image in S_X. In the latter case we also say that G is a *permutation group* on X.

Suppose that $G|X$ is a group action and $x \in X$. The set $O(x) = \{gx \mid g \in G\}$ is called the *orbit of* x in X, under the action of G. The *stabilizer of* x, is the subgroup G_x of G, defined by $G_x = \{g \in G \mid gx = x\}$.

A group action $G|X$ is said to be *transitive* if $G|X$ has exactly one orbit. Moreover, $G|X$ is said to be *sharply transitive* if for every $x, y \in X$, there exists a *unique* $g \in G$ such that $y = gx$. Let $A \subseteq G$, $Y \subseteq X$ and $x \in Y$. We say that A is a *sharply transitive set on* Y, *with respect to* x, if for each $y \in Y$, there exists a unique $a \in A$ such that $ax = y$. We note that if A is a sharply transitive set on X with respect to $x \in X$ and $hx = y$ for some $h \in G$, then for any $g \in G$, the set $gAh^{-1} = \{gah^{-1} \mid a \in A\}$ is a sharply transitive set on X, with respect to y. The set A is said to be *sharply transitive on* X, if A is a sharply transitive set on X with respect to every $x \in X$. In this research work, we only consider sharply transitive sets with respect to a given $x \in X$.

Let G be a group and $H \subseteq G$. If H is a subgroup of G, we write $H \leq G$. If H is a normal subgroup of G, we write $H \trianglelefteq G$, and throughout, we denote by

$\eta : G \to G/H$ the canonical homomorphism from G onto the quotient group G/H. We will denote the center of G by Z_G or simply by Z when the context is clear. For $x \in G$, $\langle x \rangle$ denotes the cyclic subgroup of G generated by x. We say that a subset A of a group G is a *cyclic set*, if $A = \{x^i \mid 0 \leq i \leq m\}$ for some $x \in G$ and for some $m \leq |\langle x \rangle|$. For $A, B \subseteq G$, $AB = \{ab \mid a \in A,\ b \in B\}$ denotes the product of complexes A and B in G. If $A \trianglelefteq G$, $B \leq G$ and $A \cap B = 1$, we use $A \cdot B$ to denote the split extension of A by B. For elements g, h of a group G, the commutator of g and h is $g^{-1}h^{-1}gh$. The *commutator subgroup* of G is the subgroup generated by all the commutators of G and is denoted by G'. Group G is said to *perfect* if and only if $G = G'$.

Let $H \leq G$. If $A \subseteq G$ is a complete set of left coset representatives of H in G then we say that A is a *left transversal* of H in G. The collection of all left transversals of H in G is denoted by $\boldsymbol{lt(G, H)}$. We note that $|lt(G, H)| = |H|^{|A|}$. Similarly, we define a *right transversal* of H in G, and denote the collection of all right transversals by $\boldsymbol{rt(G, H)}$. For further notions related to group actions such as primitivity, the reader is referred to [1].

2.2 General Linear groups

In this section, we illustrate the underlying structure of the first infinite family of classical groups: The linear groups $PSL_n(q)$. Let q be a prime power. Let V be a vector space of dimension n over the field $\mathbb{F}_q$ of order q. The *general linear group* $GL(V)$ is the set of invertible linear maps from V onto itself. Without loss of generality, we may take V as the vector space $\mathbb{F}_{q^n}$ of n-tuples of elements of $\mathbb{F}_q$, and identify $GL(V)$ with the group of invertible $n \times n$ matrices over $\mathbb{F}_q$, denoted by

$GL_n(q)$.

Now, an invertible matrix takes a basis to a basis, and is determined by the image of an ordered basis. The only condition on this basis is that the ith vector be linearly independent from all the previous ones. These (previous vectors) span a subspace of dimension $i-1$ which contains exactly q^{i-1} vectors. Thus, the order of $GL_n(q)$ is,

$$|GL_n(q)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) = q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1)$$

We denote the $n \times n$ identity matrix by I_n. The center of $GL_n(q)$ consists of all scalar matrices, $Z = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\}$, and is a cyclic normal subgroup of $GL_n(q)$ of order $q-1$. The quotient group $GL_n(q)/Z$ is called the *projective general linear group*, and is denoted by $PGL_n(q)$. Clearly, $|PGL_n(q)| = |GL_n(q)|/(q-1)$.

Suppose that $A, B \in GL_n(q)$. Then, $det(AB) = det(A)det(B)$, that is, the determinant map is a group homomorphism from $GL_n(q)$ onto the multiplicative group of the field $\mathbb{F}_q$. The kernel of this determinant map is another normal subgroup of $GL_n(q)$, called the *special linear group*. This subgroup is denoted by $SL_n(q)$ and consists of all matrices of determinant 1. It is clear that $|SL_n(q)| = |PGL_n(q)|$.

In $\mathbb{F}_q^*$, the number of scalars λ for which, $\lambda^n = 1$ is $gcd(n, q-1)$. Thus, the center of $SL_n(q)$, $Z = \{\lambda I_n \mid \lambda^n = 1, \lambda \in \mathbb{F}_q^*\}$ is a subgroup of order $gcd(n, q-1)$. The corresponding quotient group $SL_n(q)/Z$ is called the *projective special linear group* $PSL_n(q)$ and is of order $|SL_n(q)|/gcd(n, q-1)$. Thus,

$$|PSL_n(q)| = \frac{q^{n(n-1)/2}}{(n, q-1)} \prod_{i=2}^{n} (q^i - 1)$$

For $n \geq 2$, all members of this infinite family of $PSL_n(q)$ groups are simple, except for $PSL_2(2) \cong S_3$ and $PSL_2(3) \cong A_4$. One of the key results in proving the simplicity of these groups as well as of other finite classical groups is known as *Iwasawa's Lemma*.

Lemma 2.1. *If G is a finite perfect group, acting faithfully and primitively on a set X, such that the point stabilizer H has a normal abelian subgroup A whose conjugates generate G, then G is simple.*

For the proof of the above lemma, please refer to Section 3.3.2 of [24]. We now move our discussion to algebraic groups.

2.3 Affine algebraic groups as subgroups of $GL_n(q)$

In the subsections that follow, most of the material on algebraic groups is taken from [6, 8] and that of isometry groups from [24]. Let K be an algebraically closed field and K^n be the vector space of n-tuples over K. Then, the polynomial ring $K[x_1, \ldots, x_n]$ gives rise to a ring of functions from K^n into K. For any subset S of $K[x_1, \ldots, x_n]$, we denote by $\vartheta(S)$ the set of $v \in K^n$ such that $f(v) = 0$ for all $f \in S$. Then, $\vartheta(S)$ is a subspace of K^n, and $\vartheta(S) = \vartheta(I)$ where I is the ideal of $K[x_1, \ldots, x_n]$ generated by S. A subspace of K^n of the form $\vartheta(I)$ for some ideal I is called an *affine variety*.

Given an affine variety V in K^n, we define its ideal I to be the set of all $f \in K[x_1, \ldots, x_n]$ with $f(v) = 0$ for all $v \in$ V. Thus every ideal I determines an affine variety ϑ(I) and every affine variety V determines an ideal I(V). The affine

sub-varieties of V form the closed sets in a topology called the Zariski topology. Any topological properties mentioned in what follows such as connectedness are with respect to Zariski topology. The concept of an *"algebraic variety"* is much broader than that of an affine variety. For our results, we just need the notion of affine varieties. For definitions and some basic theorems on algebraic varieties and morphisms of varieties see Chapter 1 of [6].

An *algebraic group* over K is a set G, which is an algebraic variety over K and is also a group, such that the maps: $(x, y) \to xy$ and $x \to x^{-1}$ are morphisms of varieties. If G is an affine variety then G is called an *affine algebraic group.*

Let H_1, H_2 be affine algebraic groups. A map $\alpha : H_1 \to H_2$ is called a homomorphism of affine algebraic groups, if α is a morphism of varieties and also a homomorphism of groups. A map α is an isomorphism of affine algebraic groups, if α is bijective and both α and α^{-1} are homomorphisms of affine algebraic groups. If G is an affine algebraic group and H is a closed subgroup of G then H will also be an affine algebraic group. If H_1 and H_2 are affine algebraic groups then the direct product of $H_1 \times H_2$ will also be an affine algebraic group.

Consider $GL_n(K)$. Then, $GL_n(K) = \{(a_{ij}) \in K^{n^2} : det(a_{ij}) \neq 0\}$ can be regarded as a subset of K^{n^2}. $GL_n(K)$ is an open set in K^{n^2} and can be regarded as an affine algebraic variety as follows:

$$GL_n(K) = \{(a_{11}, \ldots, a_{nn}, b) \in K^{n^2+1} \mid det(a_{ij}) = 1\}.$$

Thus $GL_n(K)$ may be regarded as an affine algebraic variety as well as a group,

and hence is an affine algebraic group. Therefore any closed subgroup of $GL_n(K)$ is also an affine algebraic group and vice versa:

Proposition 2.1. *Every affine algebraic group is isomorphic to a closed subgroup of $GL_n(K)$ for some n and conversely.*

2.4 Unipotent and reductive algebraic groups

Let V be a finite dimensional vector space over K and consider $GL(V)$. An element $x \in GL(V)$ is called *semisimple*, if x is diagonalizable, and *unipotent* if all its eigen-values are equal to 1. Let G be a connected affine algebraic group. Then, by Proposition 2.1, G is isomorphic to a closed subgroup of $GL_n(K)$. It can be shown that the unipotence and semisimplicity condition of an element $x \in G$ is independent of the embedding of G into $GL_n(K)$ [6]. A *unipotent group* is an affine algebraic group each of whose elements are unipotent. Thus we have the following proposition.

Proposition 2.2. *[4] Any unipotent algebraic group is isomorphic to a closed subgroup of upper triangular matrices with diagonal entries* 1 *and conversely any such group is unipotent.*

From [6], it is known that the set of closed connected unipotent normal subgroups of G has a unique maximal element called the *unipotent radical* $R_u(G)$. A connected affine algebraic group G is said to be *reductive* if $R_u(G) = 1$.

2.5 Finite groups of Lie type

We now come to the key idea that relates finite groups of Lie type to the corresponding affine algebraic groups. Let G be a connected reductive group over an algebraically closed field K of characteristic p. Then from Proposition 2.1, G is isomorphic to a closed subgroup of $GL_n(K)$ for some n. Let $q = p^e$, $e \geq 1$, and $\tau_q : (a_{ij}) \to (a_{ij}^q)$ be a homomorphism of $GL_n(q)$ into itself.

A homomorphism $\tau : G \to G$ is called a *standard Frobenius map* if there exists an injective homomorphism $\sigma : G \to GL_n(K)$ for some n, such that $\sigma(\tau(g)) = \tau_q(\sigma(g))$ for some $q = p^e$ and all $g \in G$. A homomorphism $\sigma : G \to G$ is called a *Frobenius map* if some power of σ is a standard Frobenius map. Although the Frobenius map, σ is a surjective homomorphism of algebraic groups, it is not an isomorphism of algebraic groups. It is, however an isomorphism of abstract groups.

If $\sigma : G \to G$ is a Frobenius map, we define G^σ by $G^\sigma = \{g \in G : \ \sigma(g) = g\}$. Then, G^σ is a finite subgroup of G. The finite groups G^σ arising from a Frobenius map σ on a connected reductive group G are called the *finite groups of Lie type*.

Finite groups of Lie type are primarily classified into two main classes:

(i) Classical groups

- Linear: $PSL_n(q)$
- Symplectic: $PSp_{2n}(q)$
- Unitary: $PSU_n(q)$
- Orthogonal: $P\Omega_{2n+1}(q)$; $P\Omega_{2n}^+(q)$; $P\Omega_{2n}^-(q)$

(ii) Exceptional groups of Lie type

Since the primary focus of this thesis is on classical groups, we skip the definitions and details regarding the Exceptional groups of Lie type.

There are various constructions for finite groups of Lie type. All groups of Lie type except for the Suzuki and the Ree groups, can be obtained using the standard Frobenius map, as defined above. These groups are then classified based on their 'root-system' and the corresponding Dynkin diagram. Later on, Jacques Tits introduced axioms of a split BN-pair for a group to obtain uniform proofs for all groups of Lie type. In Section 2.2, we defined the $PSL_n(q)$ family of classical groups. In Section 2.6, we define the remaining families of classical groups. These families are defined in terms of bilinear, sesquilinear and quadratic forms on a vector space. As proved in [6], if G is a connected reductive algebraic group and $F : G \to G$ is a Frobenius map then both G and G^F (as defined in this section) are groups with a split BN-pair. In the section that follows, we give axioms for group G with a split BN-pair and briefly describe the structures of several important subgroups of G. These structures and propositions are then used to construct MLS's for classical groups and partitions for all finite groups of Lie type that have a split BN-pair.

2.6 Classical groups as Isometry groups

We now provide the material needed to define symplectic, unitary and orthogonal groups. Let $i, n \in \mathbb{N}$ be such that $i|n$ and let q be a prime power. We denote the unique subfield of order q^i in $\mathbb{F}_{q^n}$ by $\mathbb{F}_{q^i}$. Let K be an algebraically closed field, V a finite dimensional vector space over K, and $\mathcal{P}(V)$ the corresponding projective space.

A *bilinear form* on V over K is a map $f : V \times V \to K$ satisfying the laws

$f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$ and $f(u, \lambda v + w) = \lambda f(u, v) + f(u, w)$, $\lambda \in K$, $u, v \in V$. A bilinear form is called *symmetric* if $f(u, v) = f(v, u)$, *skew symmetric* if $f(u, v) = -f(v, u)$ and *alternating* if $f(v, v) = 0$, $\forall u, v \in V$. An alternating bilinear form, is always skew-symmetric, since $f(u, v) + f(v, u) = f(u + v, u + v) = 0$. The converse is also true, when the characteristic of the field K is not 2, since then $f(v, v) = -f(v, v)$. The pair (V, f) is called an *inner-product space*.

A *quadratic form* is a function $Q : V \to K$ satisfying $Q(\lambda u + v) = \lambda^2 Q(u) + \lambda f(u, v) + Q(v)$, for all $u, v \in V$, $\lambda \in K$ where f is a symmetric bilinear form. Thus, a quadratic form always determines a symmetric bilinear form, called the *associated bilinear form*. If $\text{char}(K)$ is not 2, the quadratic form can be recovered from the symmetric bilinear form as $Q(v) = \frac{1}{2} f(v, v)$. If $\text{char}(K) = 2$, then the associated bilinear form is actually alternating, since $0 = Q(2v) = Q(v + v) = 2Q(v) + f(v, v) = f(v, v)$. The pair (V, Q) is called a *quadratic space*.

We now suppose that $K = \mathbb{F}_{q^2}$. We write $\overline{x} = x^q$ for every element $x \in K$. Then, a *conjugate-symmetric sesquilinear form* over a vector space V defined over K is a map $f : V \times V \to K$ satisfying, $f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$ and $f(w, v) = \overline{f(v, w)}$. This implies $f(u, \lambda v + w) = \overline{\lambda} f(u, v) + f(u, w)$.

Let f be a bilinear form, and Q be a quadratic form defined over V. If V is of dimension n, then form f is determined by its values $f(e_i, e_j)$ on the basis $\{e_1, \ldots, e_n\}$ of V. The $n \times n$ matrix J_n, whose $(i, j)^{th}$ entry is $f(e_i, e_j)$ is called the matrix of the form f w.r.t. this ordered basis. It is easy to show that if $g : f_i \to e_i$ is a base-change matrix then the matrix of the form w.r.t. the new basis $\{f_1, \ldots, f_n\}$ is $g^T J_n g$.

A non-zero vector $v \in V$ is said to be *isotropic* if $f(v, v) = 0$, *singular* if $Q(v) = 0$

and *non-singular* if $Q(v) \neq 0$. A point $\langle v \rangle \in \mathcal{P}(V)$ is called a ***singular point*** if v is a singular vector. Similarly, $\langle v \rangle$ is called a ***non-singular point*** if v is a non-singular vector and $\langle v \rangle$ is called an ***isotropic point*** if v is an isotropic vector. A subspace W of V is said to be *totally isotropic* if $f(u, v) = 0$ for all $u, v \in W$ and *totally singular* if $Q(w) = 0$ for all $w \in W$.

The radical of f, denoted by *rad(f)*, is defined to be $V^{\perp} = \{u \in V \mid f(u, v) = 0, \forall\ v \in V\}$ and the radical of Q is defined as $rad(Q) := \{v \in rad(f) \mid Q(v) = 0\}$. A Bilinear form f is said to be *non-singular*, if $\text{rad}(f) = \langle 0 \rangle$ i.e the matrix J_n of the form f is non-singular. A quadratic form Q is said to be non-singular, if $\text{rad}(Q) = \langle 0 \rangle$. A quadratic space (V, Q) is called *non-degenerate* if the associated bilinear form f is non-singular.

An *isometry* from an inner-product space (V, f) onto (V, f') is a non-singular linear map, $g : V \to V$ such that $f'(g(u), g(v)) = f(u, v)$, for all $u, v \in V$. An *isometry* from a quadratic space (V, Q) onto (V, Q') is a non-singular linear map $g : V \to V$ such that $Q'(g(v)) = Q(v)$, for all $v \in V$. Two quadratic spaces (V, Q) and (V, Q') are said to be *equivalent*, if there exists an isometry $g : V \to V$. For any n, up to equivalence, there are exactly two non-singular quadratic forms, Q_1 and Q_2 (for details, see Section 3.4.6, 3.4.7 in [24]). Let f_1 and f_2 be the associated bilinear forms corresponding to the quadratic forms Q_1 and Q_2 respectively. An isometry from a quadratic space (V, Q) onto (V, Q) is called an isometry of the quadratic space (V, Q).

It is clear that an isometry of a quadratic space (V, Q) is an isometry of the inner-product space (V, f), where f is the associated bilinear form. For q odd, the converse is also true, i.e., an isometry of an inner-product space (V, f) is also an isometry of the quadratic space (V, Q). We denote, the group of all isometries of

an inner-product space (V, f), by $Isom(V, f)$ and that of a quadratic space (V, Q) by $Isom(V, Q)$. Then, $Isom(V, Q) \leq Isom(V, f) \leq GL(V)$ and when q is odd, $Isom(V, f) = Isom(V, Q)$ [24, Section 3.7].

One of the important results that plays a vital role in the study of the geometry of these spaces is *Witt's Theorem*. Below we state the theorem and for the proof the reader is referred to [24].

Proposition 2.3. *If (V, f) and (W, g) are isometric spaces, with f and g non-singular, and either alternating bilinear, or conjugate-symmetric sesquilinear or symmetric bilinear form in odd characteristic, then any isometry α between subspaces X of V and Y of W extends to an isometry of V with W.*

We now define symplectic groups that can be obtained as isometry groups of non-singular bilinear forms.

2.6.1 Symplectic group: $Sp_{2m}(q)$

In this subsection, we first construct a so called *'symplectic basis'*, which we then use to define the symplectic group. Let V be an n dimensional vector space over $\mathbb{F}_q$. Let f be an alternating bilinear form defined on V. If there are any vectors $u, v \in V$, with $f(u, v) = \lambda \neq 0$, then we choose u and $v' = \lambda^{-1}v$ as the first two basis vectors say, e_1 and f_1. Then w.r.t the basis $\{e_1, f_1\}$ the alternating bilinear form f satisfies:

$$f(e_1, e_1) = f(f_1, f_1) = 0 \text{ and } f(e_1, f_1) = -f(f_1, e_1) = 1$$

By restricting the form f to $\{u, v\}^{\perp}$ and continuing in the same fashion we get basis vectors $e_1, \ldots, e_m$ and $f_1, \ldots, f_m$ where $f(e_i, e_j) = f(f_i, f_j) = 0$ for all $1 \leq i, j \leq m$ and $f(e_i, f_i) = -f(f_i, e_i) = 1$. Now, either, we have a basis for V, in which case f is non-singular and $\dim(V) = n = 2m$ is even. Else $f(u, v) = 0$ for all $u, v \in \{e_1, e_2, \ldots, e_m, f_1, f_2, \ldots, f_m\}^{\perp} \neq 0$, hence f is singular, and we can complete $e_1, e_2, \ldots, e_m, f_1, f_2, \ldots, f_m\}$ to a basis in any way we choose. For our research, we will only consider non-singular forms, where as seen above we have decomposed V as an orthogonal direct sum of m non-singular subspaces $\langle e_i, f_i \rangle$ of dimension 2, called the *hyperbolic planes*.

Proposition 2.4. *(Section* 3.4.4, [24]*) Let f be a non-singular alternating bilinear form over a vector space V defined over the field $K = \mathbb{F}_q$. Then there is a basis of V, $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ where $f(e_i, e_j) = f(f_i, f_j) = 0$ for all $1 \leq i, j \leq m$, $f(e_i, f_j) = -f(f_j, e_i) = \delta_{ij}$ where δ_{ij} is the Kronecker delta function. Any such basis is called a symplectic basis for V w.r.t. the bilinear form f.*

The *symplectic group* $Sp_{2m}(q)$ is the isometry group of a non-singular alternating bilinear form f on $V \cong \mathbb{F}_q^{2m}$. From the above proposition, we know that V has a symplectic basis $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$. By counting the number of ways of choosing an ordered symplectic basis $e_1, \ldots, f_m$ [24], the order of $Sp_{2m}(q)$ is:

$$|Sp_{2m}(q)| = \prod_{i=1}^{m} (q^{2i} - 1) q^{2i-1} = q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1).$$

Suppose λ is a scalar matrix in $Sp_{2m}(q)$, then $f(\lambda u, \lambda v) = \lambda^2 f(u, v) = f(u, v) \Leftrightarrow \lambda = \pm 1$. Thus the, center of $Sp_{2m}(q)$ is $Z = \{\pm I_{2m}\}$ when q is odd, and $Z = \{I_{2m}\}$

when q is even. The quotient group $Sp_{2m}(q)/Z$ is a finite group of Lie type called the *projective symplectic group* $PSp_{2m}(q)$ and is simple for all $m \geq 1$, except $PSp_2(2)$, $PSp_2(3)$ and $PSp_4(2)$.

2.6.2 Orthogonal groups

For a complete description of orthogonal groups of finite dimension over a finite field, the reader is referred to [23].

2.7 Finite groups with a split BN-pair

We represent the axioms given by Jacques Tits which define groups with a split BN-pair. Let G be a group with two subgroups B and N. These form a BN-pair for G if the following axioms are satisfied.

(i) $G = \langle B, N \rangle$

(ii) $T = B \cap N$ is normal in N

(iii) $N/T = W$ is generated by a set of involutions, $S = \{s_i\}_{i \in I}$, where I is some finite indexing set

(iv) If $n_i \in N$ maps to $s_i \in S$ under the natural homomorphism $\eta : N \to W$, then $n_i B n_i \neq B$

(v) For each $n \in N$ and each n_i, $n_i Bn \subseteq Bn_i nB \cup BnB$

A finite group G is said to have a *split BN-pair of characteristic p* if the following axioms are satisfied:

(i) G has subgroups B and N that form a BN-pair

(ii) $B = U \cdot T$ where U is a normal p-subgroup of B and T is an abelian subgroup of order prime to p

(iii) $\bigcap_{n \in N} nBn^{-1} = T$

In the above axioms, subgroup B is known as the *Borel subgroup* of G, U as the *unipotent sugroup* of B, T as the *torus* of G and W as the *Weyl group* of the BN pair of G. We now give necessary definitions and theorems pertaining to these groups, that are needed for our constructions (proofs can be found in Chapter 4 of [5] and [6, 8]).

2.7.1 Borel Subgroup, Maximal Tori and the Weyl group

Historically, the formal axioms for groups with a BN-pair came after a well developed theory of algebraic groups using the specific concepts we describe below. Let G be a connected reductive group over an algebraically closed field K of characteristic p and $\sigma : G \to G$ be the Frobenius map. Then as defined in Section 2.5, $G^\sigma = \{g \in G \ : \ \sigma(g) = g\}$ is a finite group of Lie type. A *Borel subgroup* B of G is defined as a maximal closed connected solvable subgroup of G. A *torus* of G is a closed subgroup isomorphic to $K^* \times \ldots \times K^*$, where K^* is the multiplicative group of the field K. A torus T is called a *maximal torus*, if it is not contained in any larger torus of G. The group $W := N_G(T)/T$ is called the *Weyl group* of G, where $N_G(T)$ is the normalizer of a maximal torus T of G.

A subgroup $H \leq G$ is said to be σ-stable if and only if $\sigma(H) = H$. A *Borel subgroup* of a finite group of Lie type G^σ is defined to be a subgroup of the form B^σ where B is a σ-stable Borel subgroup of G. Similarly, the *maximal torus* and

the *Weyl group* of G^σ is defined as T^F, where T is a σ-stable maximal torus of G and $W^\sigma = N_G(T)^\sigma/T^\sigma$. All finite groups of Lie type have a BN-pair and a split BN-pair [6]. Since, all classical groups are subgroups of $GL_n(q)$ where q is a power of p, we consider some examples to understand the structure of the aforementioned groups.

Example 2.1. *Let $G = GL_n(q)$, then the following forms a BN-pair for G:*

(i) B is the group of all upper triangular matrices

(ii) N is the group of monomial matrices

(iii) $T = B \cap N$ group of diagonal matrices, and

(iv) $W = N/T \cong S_n$

Example 2.2. *Let n be odd and $G = SO_n(q) \leq GL_n(q)$ be the special orthogonal group. Then, $B \cap G$ and $N \cap G$ form a BN-pair of G, where B and N are as defined above for $GL_n(q)$.*

For $G = GL_n(q)$, the following forms a split BN-pair:

(i) B and N as defined for G above form a BN-pair,

(ii) U is the group of upper triangular unipotent matrices, a p-Sylow subgroup of G

(iii) T is the group of diagonal matrices

The Weyl group of the BN-pair of G is also a finite *Coxeter group* [8] with respect to the finite generating set $S = \{s_i\}_{i \in I}$. The *length* of an element $w \in W$,

denoted by $l(w)$ with respect to S is the least integer n so that w has an expression $w = s_1 s_2 \dots s_m$. In particular, $l(w) = 0$ if and only if $w = 1$.

Proposition 2.5. *[8] For the Weyl group W of G, there is a unique element w_0 in W of maximal length.*

For the proof the above proposition, reader is referred to the first chapter in [8].

Proposition 2.6. *[6] Let G be a group with a BN-pair. Then $G = BNB$.*

Proposition 2.7. *([6], Proposition 2.5.1) Let G be a group with a split BN-pair. Then, U is a maximal unipotent subgroup of G.*

Proposition 2.8. *([6], Proposition 2.1.4) Let J be a subset of the index set I. Let W_J be the subgroup of W generated by the elements s_i with $i \in J$ and let N_J be the subgroup of N satisfying $N_J/(T \cap N_J) = W_J$. Then BN_JB is a subgroup of G.*

We will denote BN_JB by P_J. Then, $P_I = G$ and $P_\emptyset = B$. By a *parabolic subgroup* of G we mean any subgroup conjugate to P_J for some subset $J \subseteq I$.

2.7.2 Parabolic subgroups

Above, we defined parabolic subgroups for any group G with a split BN-pair. Since in our research we are dealing with subgroups of $GL_n(q)$, we now give an equivalent definition of parabolic subgroups seen as subgroups of $GL_n(q)$. A classical group is a subgroup of $GL_n(K)$ and acts as a permutation group on $V \setminus \{0\}$ in a natural way. A *flag* F in V is a chain $V_{d_1} \subset V_{d_2} \subset \ldots \subset V_{d_m}$ of subspaces ordered by inclusion, where V_i is of dimension d_i with $d_1 < d_2 < \ldots < d_m$. (Section 7.1, [8])

A *Parabolic subgroup* P_G in $GL_n(q)$ is the stabilizer of a flag $V_{d_1} \subset V_{d_2} \subset \ldots \subset V_{d_m}$ i.e. $P_G = \{g \in GL_n(q) \ : \ gV_{d_i} = V_{d_i} \ \forall \ i\}$. In the case of classical groups defined by a bilinear or quadratic form, flag F is called an *isotropic flag* in V if V_{d_i} is a totally isotropic subspace of V for each $1 \leq i \leq m$. Then, Parabolic subgroups are precisely the stabilizers of isotropic flags. Parabolic subgroups of an arbitrary finite group with a split BN-pair can be further decomposed into corresponding unipotent and *Levi subgroups*. This decomposition is called the *Levi decomposition*. As proven in Section 2.6 of [6], the Levi subgroup itself is a group with a split BN-pair. We use this decomposition property of Parabolic and Levi subgroups many times in our construction of MLS's.

Proposition 2.9. *[6] Let G be a group with a split BN-pair and P a parabolic subgroup of G. Then $P = U \cdot L$ where U is the largest normal unipotent p-subgroup of P, p a prime and where the complement L is a subgroup of P called the* standard Levi subgroup *of P.*

2.8 Spreads

Let V be an n-dimensional vector space and $\mathcal{P}(V)$ the corresponding projective space. For a subspace W of V, we denote the corresponding subspace in $\mathcal{P}(V)$ by $\mathcal{P}(W)$. An *r-partial spread* in V is a set $S = \{W_i \mid 1 \leq i \leq t\}$ of r-dimensional subspaces W_i such that for $i \neq j$, $W_i \cap W_j = \langle 0 \rangle$. Such a partial spread is said to be an *r-spread* in V if $\bigcup_{i=1}^{t} W_i = V$. For an r-partial spread / r-spread S in V, let $\widetilde{S} = \{\mathcal{P}(W) \mid W \in S\}$. Then $\widetilde{S}$ is called an *$(r-1)$-partial spread/ $(r-1)$-spread* in $\mathcal{P}(V)$. With some abuse of notation, since no ambiguity arises, we denote a partial spread $\widetilde{S}$ in $\mathcal{P}(V)$ also by S. It is clear that, when S is a spread in $\mathcal{P}(V)$ it

partitions $\mathcal{P}(V)$ into $(r-1)$-dimensional subspaces of $\mathcal{P}(V)$. We will also consider partial spreads partitioning the set of all singular points of $\mathcal{P}(V)$ corresponding to a quadratic form.

We now describe the classical spread. Suppose $V = \mathbb{F}_{q^{2m}}$ is the field of order q^{2m}, viewed as a vector space over $\mathbb{F}_q$. Let α be a primitive element of the field $\mathbb{F}_{q^{2m}}$. Consider the subfield $W = \mathbb{F}_{q^m}$ as a subspace of V. For every $x \in V$, define $Wx := \{wx \mid w \in W\}$. Then:

Lemma 2.2. *For $x, y \in V \setminus \{0\}$,*

$$Wx \cap Wy = \begin{cases} \langle 0 \rangle & \text{if } y \notin Wx \\ Wx & \text{if } y \in Wx \end{cases}$$

The above lemma implies that the set S of distinct subspaces $Wx,\ x \in V \setminus \{0\}$ forms an m-spread in V.

Proposition 2.10. *Let $W_i = W\alpha^{(q^m-1)i} = \{w\alpha^{(q^m-1)i} \mid w \in W\},\ 0 \leq i \leq q^m$. Then, spread S can also be described as follows: $S = \{W_i \mid 0 \leq i \leq q^m\}$.*

Chapter 3

Logarithmic signatures and minimal logarithmic signatures

Let G be a finite group. Let $\alpha = [A_1, A_2, \ldots, A_s]$ be an LS for a subset A of G, $A_i \subseteq G$. Suppose $|A| = \prod_{j=1}^{k} {p_j}^{m_j}$ where the p_j are primes. If $l(\alpha) = \sum_{j=1}^{k} m_j p_j$, then α is said to be a *minimal logarithmic signature* (MLS) for the subset A of G. The following proposition follows from [14] and the above definition of an MLS.

Lemma 3.1. *Let G be a finite group. Let $A \subseteq G$ and $\alpha = [A_1, A_2, \ldots, A_s]$ be an LS for A, so that $A = A_1 A_2 \ldots A_n$. Then, α is an MLS for A if and only if for all $1 \leq i \leq s$, $|A_i|$ is a prime or 4.*

We now mention some elementary results about logarithmic signatures that we will use in the later chapters. The results can be derived easily from the definitions. For the case of LSs of groups, proofs are also given for most of these results in [12], [18] and [10].

Proposition 3.1. *[23] Let $A \subseteq G$. Suppose $\alpha = [A_1, A_2, \ldots, A_r]$ is an LS for A and for each A_i, $1 \leq i \leq r$, suppose that $\beta = [B_{i1}, \ldots, B_{ik_i}]$ is an LS for A_i. Then $\gamma = [B_{i1}, \ldots, B_{ik_1}, \ldots, B_{r1}, \ldots, B_{rk_r}]$ is an LS for A.*

Proposition 3.2. *Let $H \leq G$ and $A \in lt(G, H)$. Then $[A, H]$ is an LS for G.*

Proof. Now, $G = \bigcup_{a \in A} aH$ and $|G| = |A||H|$. Hence, $[A, H]$ is an LS for G. □

Proposition 3.3. *Let $H_1, H_2 \leq G$ be such that $G = H_1H_2$ and $H_1 \cap H_2 = \{1\}$. Then, $[H_1, H_2]$ is an LS for G.*

Proof. For $g \in G$, $g = h_1h_2$ for some $h_1 \in H_1$, $h_2 \in H_2$. If for some $h_3 \in H_1$, $h_4 \in H_2$, $h_1h_2 = h_3h_4 \Rightarrow h_1(h_3)^{-1} \in H_2 \Rightarrow h_1 = h_3$ and similarly $h_2 = h_4$, since $H_1 \cap H_2 = \{1\}$. Hence, $[H_1, H_2]$ is an LS for G. □

Proposition 3.4. *[23] Suppose that $H \trianglelefteq G$ and that $[\breve{B}_1, \breve{B}_2, \ldots, \breve{B}_k]$ is an LS for G/H. For each $i \in \{1, \ldots, k\}$, suppose that $B_i \subseteq G$ be such that $\eta(B_i) = \breve{B}_i$ and $|B_i| = |\breve{B}_i|$. Then,*

(i) $[B_1, B_2, \ldots, B_k, H]$ is an LS for G and (ii) $B_1B_2 \cdots B_k \in lt(G, H)$.

Proposition 3.5. *[23] Let $H \trianglelefteq G$ and suppose that $[B_1, B_2, \ldots, B_k, H]$ is an LS for G. Then, $[\breve{B}_1, \breve{B}_2, \ldots, \breve{B}_k]$ is an LS for G/H, where $\breve{B}_i = \eta(B_i)$, for all $1 \leq i \leq k$.*

Proposition 3.6. *[23] Let $H \leq H_1 \leq G$, $H_1 \neq H$ and $H \trianglelefteq G$. Suppose $[A_1, A_2, \ldots, A_k, H_1]$ is an LS for G. Let $B_i = \eta(A_i) \subseteq G/H$, for all $1 \leq i \leq k$. Then $[B_1, B_2, \ldots, B_k, H_1/H]$ is an LS for G/H.*

Proposition 3.7. *[23] Let $H \trianglelefteq G$ and $A \subseteq G$ such that $a, b \in A$, $a \neq b$ imply that $aH \neq bH$. Let $\breve{A} = \eta(A)$, and suppose that $[A_1, A_2, \ldots, A_k]$ is an LS for A. Let $B_i = \eta(A_i) \subseteq G/H$, for $1 \leq i \leq k$. Then $[B_1, B_2, \ldots, B_k]$ is an LS for $\breve{A}$.*

Proposition 3.8. [10] *If G is solvable, then G has an MLS.*

Lemma 3.2. *[23] Let G be a finite group and $x \in G$ be an element of order t. For $s \in \mathbb{N}$, $s \leq t$, let $S = \{x^i \mid 0 \leq i < s\}$. Then S has an MLS $\gamma = [A_1, A_2, \ldots, A_k]$, satisfying the following property :*

$$\text{For any list } [j_1, \ldots, j_k], \text{ such that } x^{j_i} \in A_i,\ 1 \leq i \leq k, \quad \sum_{i=1}^{k} j_i < s \tag{3.0.1}$$

Lemma 3.3. *Let $G|X$ be a transitive permutation group. Suppose $A \subseteq G$ is a sharply transitive set on X with respect to $x \in X$ and $P = G_x$. Then, $[A, P]$ is an LS for G.*

Proof. For $g \in G$, let $y \in X$ be such that $gx = y$. Now, there exists a unique $a \in A$ such that $ax = y$. Let $p = a^{-1}g$. Then, clearly $p \in P$ and $g = ap$ and by the Orbit-Stabilizer Theorem, it follows that $|G| = |A| \cdot |P|$. Hence, $[A, P]$ is an LS for G. □

The next proposition follows from Proposition 2.9 and Lemma 3.3.

Proposition 3.9. *Let G be a finite group of Lie type. Let P be a parabolic subgroup of G. Then P has an LS $[U, L]$ where U is a p-group, the unipotent group, and L is the standard Levi subgroup of P.*

Let V be a finite dimensional vector space over $\mathbb{F}_q$, f a non-singular bilinear form and Q a non-degenerate quadratic form. Let L be a subset of $\mathcal{P}(V)$ satisfying the following condition.

Condition 3.1. *L is one of the following sets.*

(a) the set of all points of $\mathcal{P}(V)$,

(b) the set of all isotropic points of $\mathcal{P}(V)$ with respect to the bilinear form f,

(c) the set of all singular points of $\mathcal{P}(V)$ with respect to the quadratic form Q,

(d) the set of all non-singular points of $\mathcal{P}(V)$ with respect to the quadratic form Q.

For a proof of the lemma mentioned below, the reader is referred to Chapter 4 of [23].

Lemma 3.4. *Suppose $G|L$ is a transitive permutation group such that G is a subgroup of $GL(V)$ and $L \subseteq \mathcal{P}(V)$ satisfies Condition 3.1. Let S be an r-partial spread in V, which viewed projectively partitions L. Let $W \in S$, $w \in \mathcal{P}(W)$ and G_w be the stabilizer of w in G. Suppose there exist sets $A, B \subseteq G$ such that*

(i) A acts sharply transitively on S with respect to W under the action of G on the set of all r-dimensional subspaces of V.

(ii) B acts sharply transitively on $L \cap \mathcal{P}(W)$ with respect to w under the action of G on $\mathcal{P}(W)$.

Then, $[A,\ B,\ G_w]$ is an LS for G.

Lemma 3.4 is the main tool we use in Chapter 5 and 6 to create MLS's for the groups $Sp_{2m}(q)$ for any q, $O^+_{2m}(q)$ for q even, and their corresponding simple groups: $PSp_{2m}(q)$ and $\Omega^+_{2m}(q)$.

Chapter 4

Linear groups

In this chapter, we first describe the structure of parabolic subgroups of $GL_n(q)$, $PGL_n(q)$, $SL_n(q)$ and $PSL_n(q)$ for any $n \in \mathbb{N}$ and q a prime power. Using these structures, we construct an LS for these parabolic subgroups. We then use these LS's in Sections 4.2, 4.3 to construct MLS's for the aforementioned infinite family of groups.

4.1 Logarithmic signature for parabolic subgroups

Let $V = \mathbb{F}_{q^n}$ be the field of order q^n viewed as an n-dimensional vector space over $\mathbb{F}_q$. We choose a suitable ordered basis $\mathcal{B} = \{e_1, e_2, \ldots, e_n\}$ of V. Suppose G is a finite group of Lie type. Then from the discussion in Section 2.3 and 2.5, it follows that G is a subgroup of $GL_n(q)$. Thus, G acts as a permutation group on $V \setminus \{0\}$ as well as on the projective space $\mathcal{P}(V)$. Now, $1 \in V \setminus \{0\}$ and $\langle 1 \rangle \in \mathcal{P}(V)$ where 1 is the multiplicative identity of the field $\mathbb{F}_{q^n}$. We denote by P_G, a parabolic subgroup $P_G := G_{\langle 1 \rangle}$ of G.

Let $G := GL_n(q)$. We assume that $e_1 = 1$. From Proposition 3.9, we have an LS $[U_G, L_G]$ for P_G. The structures of the groups U_G and L_G can easily be obtained by

applying the definitions (Section 3.3.3 in Wilson [24]). Here, $U_G = \{\left(\begin{smallmatrix} 1 & u \\ 0 & I_{n-1} \end{smallmatrix}\right) \mid u \in \mathbb{F}_q^{n-1}\}$ is an elementary abelian group of order q^{n-1} and $L_G = \{\left(\begin{smallmatrix} a & 0 \\ 0 & A \end{smallmatrix}\right) \mid a \in \mathbb{F}_q^*,\ A \in GL_{n-1}(q)\}$. The center of G is $Z_G = \{kI_n \mid k \in \mathbb{F}_q^*\}$ which is a cyclic group of order $q-1$.

Let $L_1 = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & A \end{smallmatrix}\right) \mid A \in GL_{n-1}(q)\}$. Then, we note that $L_1 \leq L_G$ and $L_G = L_1 Z_G$. Also, $L_1 \cap Z_G = \{I_n\}$. Thus, from Proposition 3.3, $[L_1, Z_G]$ is an LS for L_G. Now, using Proposition 3.1, we can replace the block L_G in $[U_G, L_G]$ by $[L_1, Z_G]$. Hence, we have proved the following lemma.

Lemma 4.1. *Let $G := GL_n(q)$. Then, $P_1 := P_G$ has an LS $[U_1, L_1, Z_1]$ where $U_1 := U_G$ is an elementary abelian group of order q^{n-1}, $L_1 \cong GL_{n-1}(q)$ and $Z_1 := Z_G$ is a cyclic group of order $q-1$.*

We proceed to state and prove the following related lemma:

Lemma 4.2. *Let $G := PGL_n(q)$. Then, $P_2 := P_G$ has an LS $[U_2, L_2]$ where U_2 is an elementary abelian group of order q^{n-1} and $L_2 \cong GL_{n-1}(q)$.*

Proof. Let P_1,U_1,L_1,Z_1 be as defined in Lemma 4.1. Then, $P_G = G_{\langle 1 \rangle} = P_1/Z_1$. We note that $U_1 \cap Z_1 = L_1 \cap Z_1 = \{I_n\}$. Therefore, $U_2 := \eta(U_1) \cong U_1$ and $L_2 := \eta(L_1) \cong L_1$ are subgroups of G, where $\eta : GL_n(q) \to G$ is the canonical homomorphism from $GL_n(q)$ onto G . Thus, from Lemma 4.1 and Proposition 3.5, P_G has an LS $[U_2, L_2]$. □

Further, we state and prove similar lemmas for the groups $SL_n(q)$ and $PSL_n(q)$. In the proofs we consider P_1, Z_1, U_1, L_1 defined as above.

Lemma 4.3. *Let $G := SL_n(q)$. Then $P_3 := P_G$ has an LS $[U_3, L_3, \breve{L}_3, Z_3]$, where U_3 is an elementary abelian group of order q^{n-1}, $Z_3 := Z_G$ is a cyclic group of order*

$d = gcd(n, q-1)$, $L_3 \in lt(L_G, Z_{L_G})$ and $\breve{L}_3 \in lt(Z_{L_G}, Z_G)$. Further Z_{L_G} is a cyclic subgroup of order $q-1$, $L_G \cong GL_{n-1}(q)$ and $L_G/Z_{L_G} \cong PGL_{n-1}(q)$.

Proof. For G, $Z_G = Z_1 \cap G$ and $P_G = P_1 \cap G$. From Proposition 3.9, P_G has an LS $[U_G, L_G]$. Moreover, we see that $U_G = U_1$ and $L_G = \{\left(\begin{smallmatrix} a & 0 \\ 0 & A \end{smallmatrix}\right) \mid A \in GL_{n-1}(q),\ a = det(A)^{-1}\}$. Also, $Z_G = \{kI_n \mid k^n = 1,\ k \in \mathbb{F}_q^*\} = \{\left(\begin{smallmatrix} k & 0 \\ 0 & kI_{n-1} \end{smallmatrix}\right) \mid k^n = 1,\ k \in \mathbb{F}_q^*\}$. Since $k^n = 1$ implies $det(kI_{n-1})^{-1} = (k^{n-1})^{-1} = k$, thus, $Z_G \leq L_G$ and $Z_G \leq Z_{L_G}$. Hence Z_G is a cyclic group of order $d = gcd(n, q-1)$ and $L_G \cong GL_{n-1}(q)$. Also, Z_{L_G} is a cyclic group of order $q-1$ and $L_G/Z_{L_G} \cong PGL_{n-1}(q)$. Now using Proposition 3.2, L_G has an LS $[L_3, Z_{L_G}]$ where $L_3 \in lt(L_G, Z_{L_G})$. Also, Z_{L_G} has an LS $[\breve{L}_3, Z_G]$, where $\breve{L}_3 \in lt(Z_{L_G}, Z_G)$. Thus by applying Proposition 3.1 and replacing L_G in $[U_G, L_G]$ by $[L_3, \breve{L}_3, Z_G]$, we get P_G has an LS $[U_3, L_3, \breve{L}_3, Z_3]$. □

Lemma 4.4. *Let $G := SL_n(q)$. Then $G/Z_G = PSL_n(q)$ and $P_4 := P_{G/Z_G}$ has an LS $[U_4, L_4, \breve{L}_4]$, where U_4 is an elementary abelian group of order q^{n-1}, $L_4 = \eta(L_3) \in lt(L_G/Z_G, Z_{L_G}/Z_G)$, $(L_G/Z_G)/(Z_{L_G}/Z_G) \cong PGL_{n-1}(q)$ and $\breve{L}_4 = Z_{L_G}/Z_G$ is a cyclic group of order $(q-1)/d$, $d = (n, q-1)$.*

Proof. Let $\eta : G \to G/Z_G$ be the canonical homomorphism from G onto Z_G. For U_3, Z_3 as defined in Lemma 4.3, $U_3 \cap Z_3 = \{I_n\}$. Therefore $U_4 := \eta(U_3)$ and $\breve{L}_4 := \eta(\breve{L}_3) = Z_{L_G}/Z_G$ are subgroups of G/Z_G. Using the fact that $(L_G/Z_G)/(Z_{L_G}/Z_G) \cong L_G/Z_{L_G} \cong PGL_{n-1}(q)$, we note that $L_4 := \eta(L_3) \in lt(L_G/Z_G, Z_{L_G}/Z_G)$. Lemma 4.3 and Proposition 3.5 then imply that $P_4 := P_{G/Z_G}$ has an LS $[U_4, L_4, \breve{L}_4]$. □

4.2 MLS's for $GL_n(q)$ and $PGL_n(q)$

In this section we construct MLS's for $GL_n(q)$ and $PGL_n(q)$, which we then use to construct MLS's for $SL_n(q)$ and $PSL_n(q)$ for all $n \in \mathbb{N}$ and q a prime power.

Let $V = \mathbb{F}_{q^n}$ be the field of order q^n viewed as an n-dimensional vector space over $\mathbb{F}_q$. Let α be a primitive element of $\mathbb{F}_{q^n}$. We fix an ordered basis $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ for V. Let $G := GL_n(q)$ and $x \in G$ be the matrix corresponding to the linear transformation $T_\alpha : V \to V$ defined by $T_\alpha(v_1) = \alpha v_1$, for all $v_1 \in V$. Let $\alpha_1 = det(x)$. Let $H = \langle x \rangle$ be the cyclic subgroup of G generated by x. As noted in the last section $Z_G = \{kI_n \mid k \in \mathbb{F}_q^*\}$. Using the fact $\mathbb{F}_q^* = \langle \alpha^{\frac{q^n-1}{q-1}} \rangle$, it follows that $Z_G \leq H$ and $Z_G = \langle x^{\frac{q^n-1}{q-1}} \rangle$. Define $\breve{H} = H/Z_G$. Then $\breve{H} = \langle xZ_G \rangle$ is the cyclic group generated by the coset xZ_G. Let $M := \{x^i \mid 0 \leq i < \frac{q^n-1}{q-1}\}$. The first two statements in the proposition below follow from results in [2, 7, 21]. The third statement follows from the second statement and the facts that $Z_G \leq G_{\langle 1 \rangle}$ and $M \in lt(H, Z_G)$.

Proposition 4.1.

(i) H is the well known Singer subgroup of $GL_n(q)$ of order $q^n - 1$ acting sharply transitively on $V \setminus \{0\}$.

(ii) $\breve{H} = \langle xZ_G \rangle$ is a Singer subgroup of $PGL_n(q)$ of order $\frac{q^n-1}{q-1}$ acting sharply transitively on $\mathcal{P}(V)$.

(iii) The set M is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1 \rangle$.

Now, assume that $d = |Z_{SL_n(q)}| = gcd\ (n, q-1) \ \Rightarrow\ q \equiv 1 \mod d$ and $n \equiv 0 \mod d$. Since, $\frac{q^n-1}{q-1} = 1 + q + q^2 + \ldots + q^n - 1$, thus, $\frac{q^n-1}{q-1}\ mod\ d \ \equiv\ n \cdot 1\ mod\ d$. Hence, $d \mid \frac{q^n-1}{q-1}$. Define $M_1, M_2 \subseteq M$ as $M_1 := \{x^{dj} \mid 0 \leq j < \frac{q^n-1}{(q-1)d}\}$ and

$M_2 := \{x^j \mid 0 \leq j < d\}$. Then, $[M_1, M_2]$ is an LS for M. Using Lemma 3.2, we have MLS's $\beta_1 = [A_1, A_2, \ldots, A_{k_1}]$ for M_1 and $\beta_2 = [B_1, B_2, \ldots, B_{k_2}]$ for M_2 satisfying Equation (3.0.1). Then, by Proposition 3.1, $\beta = [A_1, A_2, \ldots, A_{k_1}, B_1, B_2, \ldots, B_{k_2}]$ is an MLS for M.

The following proposition follows immediately from the above discussion and Lemma 3.3.

Proposition 4.2.

(i) $\beta = [A_1, A_2, \ldots, A_{k_1}, B_1, B_2, \ldots, B_{k_2}]$ *is an MLS for* M.

(ii) $[A_1, \ldots, A_{k_1}, B_1, \ldots, B_{k_2}, P_1]$ *is an LS for* $G := GL_n(q)$, *where* P_1 *is a parabolic subgroup of* G.

Theorem 4.1. *Let* $n \in \mathbb{N}$ *and* q *be a prime power. Then* $GL_n(q)$ *has an MLS.*

Proof. By Lemma 4.1, P_1 has an LS $[U_1, L_1, Z_1]$ where U_1 is an elementary abelian subgroup of G, $L_1 \cong GL_{n-1}(q)$ and $Z_1 = Z_G$ is a cyclic group. Further, by Proposition 3.8, U_1 and Z_1 have an MLS. We also know that $GL_1(q)$ is a cyclic group of order $q - 1$. Hence, $GL_1(q)$ has an MLS. Therefore, using Propositions 4.2, 3.1 and induction on n, we have that $GL_n(q)$ has an MLS for any $n \in \mathbb{N}$ and q a prime power. □

Theorem 4.2. *Let* $n \in \mathbb{N}$ *and* q *be a prime power. Then* $PGL_n(q)$ *has an MLS.*

Proof. Let $G := PGL_n(q)$ and $\eta : GL_n(q) \to PGL_n(q)$ be the canonical homomorphism from $GL_n(q)$ onto $PGL_n(q)$. Then, $P_2 = G_{\langle 1 \rangle} = P_1/Z_1$. Let $\breve{M} = \eta(M)$. Then, Proposition 4.1 *(iii)* implies that $\breve{M}$ acts sharply transitively on $\mathcal{P}(V)$ with

respect to $\langle 1 \rangle$. Also, $\breve{M}$ satisfies the conditions of Proposition 3.7 with $G = GL_n(q)$ and $H = Z_1$. Let $\overline{A}_i = \eta(A_i),\ 1 \leq i \leq k_1$, and $\overline{B}_j = \eta(B_j),\ 1 \leq j \leq k_2$. From Propositions 4.2 *(i)* and 3.7, it follows that $[\overline{A}_1, \ldots, \overline{A}_{k_1}, \overline{B}_1, \ldots, \overline{B}_{k_2}]$ is an MLS for $\breve{M}$. Further, from Lemma 3.3, it follows that $[\breve{M}, P_2]$ is an LS for $PGL_n(q)$. Lemma 4.2 implies that P_2 has an LS $[U_2, L_2]$ where U_2 is an elementary abelian subgroup of G and $L_2 \cong GL_{n-1}(q)$. Now, Proposition 3.8 implies that U_2 has an MLS and Theorem 4.1 implies that L_2 has an MLS. Finally, using Proposition 3.1 we have that $PGL_n(q)$ has an MLS. □

4.3 MLS's for $SL_n(q)$ and $PSL_n(q)$

We continue using the notation of the previous sections. In particular we assume that β is as defined in Proposition 4.2. Let $a, b \in \mathbb{Z}$ be such that $d = a(q-1) + bn$. Define $f_1 = \alpha_1^{-b} I_n = \ (det(x))^{-b} I_n$. Next, fix an element $c \in B_1 \subseteq M,\ c \neq I_n$. From , M acts sharply transitively on $\mathcal{P}(V)$ wrt $\langle 1 \rangle$, Then, $c = x^m$ for some $m \neq 0$, $m < d$. Hence, $c(\langle 1 \rangle) = x^m(\langle 1 \rangle) = \langle \alpha^m \rangle$. Let $f_2 = (a_{ij})_{n \times n} \in GL_n(q)$ be the diagonal matrix defined as follows.

$$a_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \neq m+1 \\ \alpha_1^{-1} & \text{if } i = j = m+1. \end{cases} \tag{4.3.1}$$

Lemma 4.5. *$f_2^j(\langle \alpha^i \rangle) = \langle \alpha^i \rangle$ for all $i \neq m$, $0 \leq i < d$, and for all $j \in \mathbb{Z}$.*

Proof. Consider α^i, $i \neq m$, $0 \leq i < d \leq n$. We observe that the column vector representing $\alpha^i \in \mathcal{B}$ has 0 in the $(m+1)^{th}$ row. Equation (4.3.1) now implies that,

$f_2^j(\langle\alpha^i\rangle) = \langle\alpha^i\rangle$ for all $j \in \mathbb{Z}$. $\square$

Lemma 4.6. *Let* $x^{s_j} \in B_j,\ 1 \le j \le k_2$. *Then,*

$$\left(\prod_{j=1}^{k_2}\left(x^{s_j} f_2^{s_j}\right)\right)(\langle 1\rangle) = \left(\prod_{j=1}^{k_2} x^{s_j}\right)(\langle 1\rangle). \tag{4.3.2}$$

Proof. Let $x^{s_j} \in B_j$, $1 \le j \le k_2$. If $k_2 = 1$, then (4.3.2) follows from Lemma 4.5 and the fact that $m \neq 0$. Now suppose $k_2 > 1$. Define $y_r = \prod_{j=k_2-r}^{k_2} x^{s_j}$, $y'_r = \prod_{j=k_2-r}^{k_2}(x^{s_j} f_2^{s_j})$ for $0 \le r \le k_2 - 1$. We want to show that $y_{k_2-1}(\langle 1\rangle) = y'_{k_2-1}(\langle 1\rangle)$. We will prove by induction on r, $0 \le r \le k_2 - 1$, that

$$y'_r(\langle 1\rangle) = y_r(\langle 1\rangle). \tag{4.3.3}$$

When $r = 0$, using Lemma 4.5 and the fact that $m \neq 0$ we obtain that $f_2^{s_{k_2}}(\langle 1\rangle) = f_2^{s_{k_2}}(\langle\alpha^0\rangle) = \langle 1\rangle$. Hence, $y'_0(\langle 1\rangle) = y_0(\langle 1\rangle)$. Now by the induction hypothesis, assume that (4.3.3) is true for all i, $0 \le i \le r < k_2 - 1$. We show that (4.3.3) is true for $r + 1 \le k_2 - 1$.

Now, since $k_2 - r \ge 2$ and $[B_1, \ldots, B_k]$ is an MLS for the set $M_2 = \{x^j \mid 0 \le j < d\}$, with $I_n \in B_i$, $1 \le i \le k_2$, it follows that

$$x^m \neq \prod_{j=k_2-r}^{k_2} x^{s_j}. \tag{4.3.4}$$

Next, x^m, $\prod_{j=k_2-r}^{k_2} x^{s_j} \in M$ and from Proposition 4.1, M is sharply transitive on $\mathcal{P}(V)$. Hence, (4.3.4) implies that $(\prod_{j=k_2-r}^{k_2} x^{s_j})(\langle 1\rangle) = \langle\alpha^s\rangle$ for some $s \neq$

$m,\ 0 \leq s < d$. Finally, using Lemma 4.5 we have :

$$\begin{aligned} y'_{r+1}(\langle 1\rangle) &= (x^{s_{k_2-(r+1)}} f_2^{s_{k_2-(r+1)}} \prod_{j=k_2-r}^{k_2} x^{s_j})(\langle 1\rangle) \\ &= (x^{s_{k_2-(r+1)}}) f_2^{s_{k_2-(r+1)}}(\langle \alpha^s\rangle) \\ &= x^{s_{k_2-(r+1)}}(\langle \alpha^s\rangle) \\ &= y_{r+1}(\langle 1\rangle). \end{aligned}$$

□

Now, define $\breve{A}_i = \{x^{dj} f_1^j \mid x^{dj} \in A_i\}$ for $1 \leq i \leq k_1$, and $\breve{B}_i = \{x^j f_2^j \mid x^j \in B_i\}$ for $1 \leq i \leq k_2$.

Theorem 4.3. *Let* $\breve{A}_i,\ 1 \leq i \leq k_1$ *and* $\breve{B}_i,\ 1 \leq i \leq k_2$ *be defined as above. Then,*

(i) $\breve{A}_i \subseteq SL_n(q)$ *for all* $1 \leq i \leq k_1$ *and* $\breve{B}_i \subseteq SL_n(q)$ *for all* $1 \leq i \leq k_2$.

(ii) $\mathcal{A} = (\prod_{i=1}^{k_1} \breve{A}_i).(\prod_{j=1}^{k_2} \breve{B}_j)$ *is a sharply transitive set on* $\mathcal{P}(V)$ *with respect to* $\langle 1\rangle$.

(iii) $[\breve{A}_1, \ldots, \breve{A}_{k_1}, \breve{B}_1, \ldots, \breve{B}_{k_2}]$ *is an MLS for* $\mathcal{A}$.

Proof. For the first part, let $x^{dj} f_1^j \in \breve{A}_i$, for any $i,\ 1 \leq i \leq k_1$. Then,

$$\begin{aligned} det(x^{dj} f_1^j) &= det(x^{dj})\, det(f_1^j) = (det(x))^{dj}\, (det(\alpha_1^{-b} I_n))^j \\ &= \alpha_1^{dj} \alpha_1^{-bnj} = \alpha_1^{(a(q-1)+bn)j} \alpha_1^{-bnj} \qquad (\text{ since } d = a(q-1)+bn) \\ &= \alpha_1^{a(q-1)j} = 1 \qquad\qquad (\text{ since } \alpha_1 \in \mathbb{F}_q^* \ ) \end{aligned}$$

Thus, $\breve{A}_i \subseteq SL_n(q)$ for all $i,\ 1 \leq i \leq k_1$. Similarly, for $x^j f_2^j \in \breve{B}_i,\ 1 \leq i \leq k_2$,

we have

$$det(x^j f_2^j) = (det(x))^j \, (det(f_2))^j = \alpha_1^j \alpha_1^{-j} = 1$$

Hence, $\breve{B}_i \subseteq SL_n(q)$ for all $i,\ 1 \leq i \leq k_2$.

For the second part, let $\langle v_1 \rangle$ be any one dimensional subspace of V. Since $M = \{x^t \mid 0 \leq t < \frac{q^n-1}{q-1}\}$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1 \rangle$, there exists a unique $x^t,\ 0 \leq t < \frac{q^n-1}{q-1}$ such that

$$x^t(\langle 1 \rangle) = \langle v_1 \rangle. \tag{4.3.5}$$

From Proposition 4.2 (i), it follows that there exist unique $x^{dr_i} \in A_i,\ 1 \leq i \leq k_1$ and $x^{s_j} \in B_j,\ 1 \leq j \leq k_1$, such that,

$$x^t = \prod_{i=1}^{k_1} x^{dr_i} \prod_{j=1}^{k_2} x^{s_j}. \tag{4.3.6}$$

Now, since $f_1 \in Z_{GL_n(q)}$ and $Z_{GL_n(q)} \subseteq GL_n(q)_{\langle v \rangle} u$ for all $v \in V$, we have,

$$\left(\prod_{i=1}^{k_1} x^{dr_i} f_1^{r_i} \right) (\langle v \rangle) = \left(\prod_{i=1}^{k_1} x^{dr_i} \right) (\langle v \rangle) \text{ for all } v \in V. \tag{4.3.7}$$

Also, using Lemma 4.6 we have,

$$\left(\prod_{j=1}^{k_2} x^{s_j} f_2^{s_j} \right) (\langle 1 \rangle) = \left(\prod_{j=1}^{k_2} x^{s_j} \right) (\langle 1 \rangle). \tag{4.3.8}$$

Hence, from (4.3.5), (4.3.6), (4.3.7) and (4.3.8) we have,

$$\left(\prod_{i=1}^{k_1}\left(x^{dr_i}f_1^{r_i}\right)\prod_{j=1}^{k_2}\left(x^{s_j}f_2^{s_j}\right)\right)(\langle 1\rangle) = x^t(\langle 1\rangle) = \langle v_1\rangle.$$

Therefore, $\{a(\langle 1\rangle) \mid a \in \mathcal{A}\} = \mathcal{P}(V)$. Now since $|\mathcal{A}| = \frac{q^n-1}{q-1} = |\mathcal{P}(V)|$, $\mathcal{A}$ is clearly a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$.

For the third part, by the definition of $\mathcal{A}$ it follows that, $[\breve{A}_1, \ldots, \breve{A}_{k_1}, \breve{B}_1, \ldots, \breve{B}_{k_2}]$ is an LS for $\mathcal{A}$. Now, $|\breve{A}_i| = |A_i|$ for all $1 \leq i \leq k_1$ and $|\breve{B}_j| = |B_j|$ for all $1 \leq j \leq k_2$. Hence, using Proposition 4.2 (i), it follows that $[\breve{A}_1, \ldots, \breve{A}_{k_1}, \breve{B}_1, \ldots, \breve{B}_{k_2}]$ is an MLS for $\mathcal{A}$. □

The following proposition easily follows from Theorem 4.3, Proposition 3.7 and the fact that $Z_{SL_n(q)} \subseteq SL_n(q)_{\langle 1\rangle}$.

Proposition 4.3. *Let $G = SL_n(q)$ and $\breve{\mathcal{A}}$ be the subset of $PSL_n(q)$ defined by $\breve{\mathcal{A}} = \eta(\mathcal{A}) = \{(aZ_G) \mid a \in \mathcal{A}\}$, where $\mathcal{A} \subseteq SL_n(q)$ is as defined in the previous theorem. Then, $\breve{\mathcal{A}}$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$ and $\breve{\mathcal{A}}$ has an MLS.*

Theorem 4.4. *Let $n \in \mathbb{N}$ and q be a prime power. Then, the groups $SL_n(q)$ and $PSL_n(q)$ have MLS's.*

Proof. Let $G = SL_n(q)$ and $P_3 = G_{\langle 1\rangle}$. Using Theorem 4.3 and Lemma 3.3, it follows that G has an LS $[\mathcal{A}, P_3]$ and $\mathcal{A}$ has an MLS. From Proposition 4.3, we have that P_3 has an LS $[U_3, L_3, \breve{L}_3, Z_3]$. Here, U_3 and Z_3 are abelian groups hence using Proposition 3.8, it follows that both have an MLS. Now, $L_3 \in lt(L_G, Z_{L_G})$ and $L_G/Z_{L_G} \cong PGL_{n-1}(q)$. Thus, using Theorem 4.2 and Proposition 3.4, we can

choose L_3 so that it has an MLS. Now, $\breve{L}_3 \in lt(Z_{L_G}, Z_3)$. We know that Z_{L_G}/Z_3 is an abelian group, hence it has an MLS. Thus, using Proposition 3.4, we can choose $\breve{L}_3$ so that $\breve{L}_3$ has an MLS. Finally, using Proposition 3.1 it follows that $SL_n(q)$ has an MLS.

Now consider $PSL_n(q) = G/Z_G$ and $P_4 = P_{G/Z_G}$. Then from Lemma 4.4 and Propositions 4.3, 3.3 and 3.1, it follows that $PSL_n(q)$ has an LS $[\breve{\mathcal{A}}, U_4, L_4, \breve{L}_4]$ and that $\breve{\mathcal{A}}$ has an MLS. Note that U_4 and $\breve{L}_4$ are abelian groups. Hence, using Proposition 3.8, both U_4 and $\breve{L}_4$ have an MLS. Further, $L_4 = \eta(L_3)$. Hence, using Proposition 3.7 and the fact that L_3 has an MLS, it follows that L_4 has an MLS. The above facts together with Proposition 3.1 imply that $PSL_n(q)$ has an MLS. $\square$

Chapter 5

Symplectic groups

In this chapter, we construct MLS's for the symplectic group $Sp_{2m}(q)$ and the corresponding simple group $PSp_{2m}(q)$ for any $m \in \mathbb{N}$ and q a power of a prime. In [23], using a similar construction as described in the previous chapter, MLS's for $Sp_{2m}(q)$ and $PSp_{2m}(q)$ were constructed. In this chapter, we use the geometric language of spreads to construct MLS's for the aforementioned groups. This provides us with an interesting link between MLS's and spreads in a projective space, and also helps us in constructing MLS's for other classical groups as we will see in the next chapter.

We first describe the group $G = Sp_{2m}(q)$ in a language suitable for our construction. Let $V = \mathbb{F}_{q^{2m}}$ be the field of order q^{2m} viewed as a $2m$-dimensional vector space over $\mathbb{F}_q$. For $y \in V$, $\overline{y}$ denotes y^{q^m}. For $s \in V$, T_s denotes the linear transformation $T_s : V \to V$ defined by $T_s(v) = sv$, for all $v \in V$. Let α be a primitive element of the field $\mathbb{F}_{q^{2m}}$ and $x \in GL_{2m}(q)$ be the matrix corresponding to the linear transformation T_α. Define a bilinear form $f : V \times V \to \mathbb{F}_q$ by $f(x, y) = tr_{\mathbb{F}_{q^{2m}}/\mathbb{F}_q}(ax\overline{y}) = \sum_{i=1}^{2m}(ax\overline{y})^{q^i}$, where $a \in \mathbb{F}^*_{q^{2m}}$ is such that $a + \overline{a} = 0$. Then, f is a non-singular alternating bilinear form (see proof of Theorem 5.6 in

[11]). The group $G = Sp_{2m}(q)$ is the isometry group of the inner product space (V, f).

The subspace $W = \mathbb{F}_{q^m}$ is a maximal totally isotropic subspace of V with respect to the alternating bilinear form f. Let, $\mathcal{B}_1 = \{e_1, \ldots, e_m\}$ be any ordered basis for W. Then, using Proposition 2.3 (Witt's Theorem), one can extend the basis $\mathcal{B}_1$ of W to a symplectic basis $\mathcal{B} = \{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ of V. We consider the elements of $GL_{2m}(q)$ as linear transformations on V, with respect to the ordered basis $\mathcal{B}$.

We now describe some cyclic subgroups of G that we use to construct a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1 \rangle$. Let $a_1 = x^{q^m-1} \in GL_{2m}(q)$, be the matrix corresponding to the linear transformation $T_{\alpha^{q^m-1}}$. Let $C \in GL_m(q)$ be the matrix corresponding to the linear transformation $T_{\alpha^{q^m+1}}|_W$ of W with respect to the ordered basis $\mathcal{B}_1$. Let $b_1 = \left(\begin{smallmatrix} C & 0 \\ 0 & (C^t)^{-1} \end{smallmatrix}\right) \in GL_{2m}(q)$. Then, it has been shown that $a_1, b_1 \in G$ [23].

Let $A_1 = \langle a_1 \rangle$, $B_1 = \langle b_1 \rangle$ be the cyclic subgroups of G generated by a_1 and b_1 respectively. It follows that A_1 is of order $q^m + 1$ and B_1 of order $q^m - 1$. We note that A_1 is the *Singer group* of $Sp_{2m}(q)$ and B_1 is isomorphic to the *Singer group* of $GL_m(q)$. Let $C_1 = \langle b_1^{\frac{q^m-1}{q-1}} \rangle$ be the subgroup of B_1 of order $q - 1$. Now for q odd, $Z_G = \{I_{2m}, -I_{2m}\}$ and for q even, $Z_G = \{I_{2m}\}$. Let $\breve{A}_1 \in lt(A_1, Z_G)$ and $\breve{B}_1 \in lt(B_1, C_1)$. Thus for q odd, $|\breve{A}_1| = \frac{q^m+1}{2}$ and for q even, $|\breve{A}_1| = q^m + 1$. Also, $|\breve{B}_1| = \frac{q^m-1}{q-1}$. Further, $\breve{A}_1$ and $\breve{B}_1$ are cyclic sets and can be chosen so that $\breve{A}_1 \cap \breve{B}_1 = \{1\}$. Hence, by Lemma 3.2, $\breve{A}_1$ and $\breve{B}_1$ have MLS's.

Now, suppose q is odd. Define subspace W' of V by $W' = \alpha W = \{\alpha w \mid w \in W\}$. Then, W' is a maximal isotropic subspace of V and $\{e_i' := \alpha e_i \mid 1 \leq i \leq m\}$ forms a

basis of W'. Now, we can find $f'_i,\ 1 \leq i \leq m$, such that $\mathcal{B}' = \{e'_1, \ldots, e'_m, f'_1, \ldots, f'_m\}$ forms a symplectic basis for V with respect to the bilinear form f. Let $t \in GL_{2m}(q)$ be the matrix corresponding to the linear transformation T' defined by $T'(v) = \sum_{i=1}^{m}(a_i e'_i + a_{i+m} f'_i)$ for all $v = \sum_{i=1}^{m}(a_i e_i + a_{i+m} f_i) \in V$. It has been shown in [23] that, $t \in Sp_{2m}(q)$. Let $M := \{1,\ t\} \subseteq Sp_{2m}(q)$.

Now, consider the classical spread $S = \{W_i \mid 0 \leq i \leq q^m\}$, as described in Proposition 2.10. With respect to the bilinear form f, the W_i are m-dimensional totally isotropic subspaces of V. Also note that $W_0 = W$. For the structure of G_w, stabilizer of $w = \langle 1 \rangle$ in G, reader is referred to Section 5.1 of [23]. The following lemma follows from the results given in [23].

Lemma 5.1. *Let S be the spread, W be the subspace of V as defined above and $\breve{A}_1, \breve{B}_1, M \subseteq Sp_{2m}(q)$. Let $w = \langle 1 \rangle$.*

(i) If q is odd, then the set $\breve{A}_1 M = \{a_1 m \mid a_1 \in \breve{A}_1,\ m \in M\}$ is a sharply transitive set on S with respect to W.

(ii) If q is even, then the set $\breve{A}_1$ is a sharply transitive set on S with respect to W.

(iii) $\breve{B}_1$ is a sharply transitive set on $\mathcal{P}(W)$ with respect to w.

We now state and prove the following theorem:

Theorem 5.1. *Let $G = Sp_{2m}(q)$ and $\breve{A}_1, \breve{B}_1, M \subseteq Sp_{2m}(q)$ be as defined above. Let $w = \langle 1 \rangle$.*

(i) If q is odd, then $[\breve{A}_1 M,\ \breve{B}_1,\ G_w]$ is an LS for $Sp_{2m}(q)$.

(ii) If q is even, then $[\breve{A}_1,\ \breve{B}_1,\ G_w]$ is an LS for $Sp_{2m}(q)$.

Proof. Let $L = \mathcal{P}(V)$, and q be odd. If $A = \breve{A}_1 M$, $B = \breve{B}_1$ and G_w is the stabilizer of w in G, then, from Lemma 5.1, conditions of Lemma 3.4 are satisfied. Thus, for q odd, $[\breve{A}_1 M,\ \breve{B}_1,\ G_w]$ is an LS for $Sp_{2m}(q)$. Similarly, for q even, if $A = \breve{A}_1$ and $B = \breve{B}_1$, then $[\breve{A}_1,\ \breve{B}_1,\ G_w]$ is an LS for $Sp_{2m}(q)$. □

Theorem 5.2. *Suppose $\breve{G} = PSp_{2m}(q)$. Let $\breve{A}_1, \breve{B}_1, M \subseteq Sp_{2m}(q)$ and $\eta : Sp_{2m}(q) \to PSp_{2m}(q)$ be the canonical homomorphism onto $PSp_{2m}(q)$. Let $w = \langle 1 \rangle$.*

(i) If q is odd, then $[\eta(\breve{A}_1 M),\ \eta(\breve{B}_1),\ \breve{G}_w]$ is an LS for $PSp_{2m}(q)$.

(ii) If q is even, then $[\eta(\breve{A}_1),\ \eta(\breve{B}_1),\ \breve{G}_w]$ is an LS for $PSp_{2m}(q)$.

Proof. The theorem follows from Proposition 3.7 and Theorem 5.1. □

The following proposition is essential for the next theorem and follows from Lemma 5.1 and Lemma 5.2 in [22].

Proposition 5.1. *For $m > 2$, suppose that $Sp_{2m-2}(q)$ and $PSp_{2m-2}(q)$ have MLS's. Then the parabolic subgroups G_w and $\breve{G}_w$ have MLS's, where $G = Sp_{2m}(q)$, $\breve{G} = PSp_{2m}(q)$ and $w = \langle 1 \rangle$.*

We now prove that the groups $Sp_{2m}(q)$ and $PSp_{2m}(q)$ have MLS's.

Theorem 5.3. *Let q be a prime power and $m \in \mathbb{N}$. Then, the groups $Sp_{2m}(q)$ and $PSp_{2m}(q)$ have MLS's.*

Proof. Let $G = Sp_{2m}(q)$ and $\breve{G} = PSp_{2m}(q)$. Also assume that the subsets $\breve{A}_1,\ \breve{B}_1$, $M \subseteq G$ and the map η are as defined earlier. We will use induction on m, Theorem 5.1 and Theorem 5.2 to obtain an MLS for G and $\breve{G}$. We observe that

$Sp_2(q) \cong SL_2(q)$ and $PSp_2(q) \cong PSL_2(q)$. Then from Section 4.3, $Sp_2(q)$ and $PSp_2(q)$ have MLS's. Using the induction hypothesis we can assume that $Sp_{2m-2}(q)$ and $PSp_{2m-2}(q)$ have MLS's. Thus using Proposition 5.1, we obtain that G_w and $\breve{G}_w$ have MLS's. We also observe that since $\breve{A}_1$, $\breve{B}_1$ are cyclic sets and $|M| = 2$, the sets $\breve{A}_1, \breve{A}_1 M$ and $\breve{B}_1$ have MLS's. Further, using Proposition 3.7, it follows that $\eta(\breve{A}_1),\ \eta(\breve{A}_1 M),\ \eta(\breve{B}_1) \subseteq PSp_{2m}(q)$ have MLS's. Finally, using Theorem 5.1 and Theorem 5.2, we have an MLS for G and $\breve{G}$. $\square$

Chapter 6

Orthogonal groups of 'plus' type

Let $V = \mathbb{F}_{q^{2m}}$ be the field of order q^{2m} viewed as a $2m$-dimensional vector space over the field $\mathbb{F}_q$, q even. Let α be a primitive element of the field $\mathbb{F}_{q^{2m}}$. Let $W := \mathbb{F}_{q^m}$, a subspace of V. Let $\beta = \alpha^{q^m-1}$. Then clearly $\mathcal{B}_1 = \{1, \beta\}$ is the basis for V over $\mathbb{F}_{q^m}$. Define a bilinear form $f : V \times V \to \mathbb{F}_q$ by $f(x, y) = f(x_1 + x_2\beta, y_1 + y_2\beta) = tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x_1y_2 + x_2y_1) = \sum_{i=0}^{m-1}(x_1y_2 + x_2y_1)^{q^i}$. Then, it can be verified that f is a non-singular symmetric bilinear form. Define a quadratic form, $Q : V \to \mathbb{F}_q$ by $Q(x) = Q(x_1 + x_2\beta) = tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x_1x_2) = \sum_{i=0}^{m-1}(x_1x_2)^{q^i}$. Now for $w \in W$, $Q(w) = Q(w \cdot 1 + 0 \cdot \beta) = tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(w \cdot 0) = 0$. Thus, W is an m-dimensional totally singular subspace and Q is a quadratic form of *plus type*. Hence, (V, Q) is a non-degenerate quadratic space with quadratic form Q of plus type and the associated bilinear form f.

Let G be the isometry group of the quadratic space (V, Q) as defined above. Then, $G \cong O^+_{2m}(q)$ and G is a permutation group acting transitively on the set of all singular points as well as on the set of all non-singular points of $\mathcal{P}(V)$ [24, Section 3.7.2]. As shown in [24], $|G| = 2q^{m(m-1)}(q^m - 1)\prod_{i=1}^{m-1}(q^{2i} - 1)$. Let L be the set of all non-singular points in $\mathcal{P}(V)$. The total number of singular points in $\mathcal{P}(V)$

is $(q^m-1)(q^{m-1}+1)/(q-1)$ [24, Section 3.7.2]. Thus, $|L| = q^{m-1}(q^m-1)$.

Consider the action of G on L. We will again use the classical spread $S = \{W_i \mid 0 \leq i \leq q^m\}$, with $W_i = W\alpha^{(q^m-1)i}$ as described in Proposition 2.10. We note that, $W_0 = W$ and $W_1 = W\beta$ are totally singular subspaces. Let $S' = S \setminus \{W_0, W_1\}$. We will first construct the subgroups A_3 and B_3 of G such that A_3 is sharply transitive on the partial spread S' with respect to W_2 and B_3 is sharply transitive on $L \cap \mathcal{P}(W_2)$ with respect to a non-singular point $w \in \mathcal{P}(W_2)$. We then use Lemma 3.4 to get MLS's for the groups $O^+_{2m}(q)$ and $\Omega^+_{2m}(q)$.

Let H be the multiplicative group of the field $\mathbb{F}_{q^m}$. Then $|H| = q^m - 1$. Let λ be a generator of the group H. For $h \in H$, define a linear transformation $t_h : V \to V$ by $t_h(x_1 + x_2\beta) = hx_1 + h^{-1}x_2\beta$. For $x = x_1 + x_2\beta$, $Q(t_h(x)) = Q(t_h(x_1 + x_2\beta)) = Q(hx_1 + h^{-1}x_2\beta) = tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(hh^{-1}x_1x_2) = Q(x)$. Thus, t_h preserves the quadratic form Q for every $h \in H$. Further, using the fact that $\beta \notin W$, we see that $t_{h_1} \neq t_{h_2}$ for $h_1 \neq h_2,\ h_1, h_2 \in H$. Therefore, $A_3 := \langle t_\lambda \rangle$ is a cyclic subgroup of G of order $q^m - 1$.

Now, for $x \in V,\ t_h(Wx) = Wt_h(x)$. Also, since $\beta \notin W$, $t_h(W_2) \in S'$. Further, it is easy to see that $t_{h_1}(W_2) = t_{h_2}(W_2)$ if and only if $h_1 = h_2$. Hence, using the fact that $|S'| = |A_3| = q^m - 1$, it follows that A_3 is sharply transitive on S' with respect to W_2. In fact, A_3 is a sharply transitive group on S'.

Our next step is to construct the subgroup B_3 of G. From the fact that the subspaces W_i are totally isotropic, follows that the dimension of a maximal totally singular subspace in $W_i,\ 2 \leq i \leq q^m$ is at least $m-1$ (See [24, Section 3.4.7]).

Now suppose that there is a subspace $W_j,\ 2 \leq j \leq q^m$ such that W_j is an m-dimensional totally singular subspace. The group A_3 is transitive on S', thus, it would follow that all subspaces of S' would be totally singular. This would imply that all points of $\mathcal{P}(V)$ are singular points, a contradiction to the fact that there are non-singular points in $\mathcal{P}(V)$. Hence, the dimension of a maximal totally singular subspace in $W_i,\ 2 \leq i \leq q^m$ is $m-1$. Let W' be an $(m-1)$-dimensional maximal totally singular subspace of W_2. It follows that the number of non-singular points in $\mathcal{P}(W_2)$ is q^{m-1}.

Choose an ordered basis $\{e_1, \ldots, e_{m-1}, d\}$ for W_2 such that, $\{e_1, \ldots, e_{m-1}\}$ is an ordered basis for W'. Clearly, the e_i, for $1 \leq i \leq m-1$ are singular vectors and d is a non-singular vector in W_2. Now, from Proposition 2.3 and [24, Section 3.4.7], one can extend the basis $\{e_1, \ldots, e_{m-1}\}$ of W' to a symplectic basis $\mathcal{B} = \{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ of V where $Q(e_i) = Q(f_i) = 0$ for all $i,\ 1 \leq i \leq m$.

Suppose $d = \sum_{i=1}^{m}(\alpha_i e_i + \beta_i f_i)$, $\alpha_i, \beta_i \in \mathbb{F}_q$. Since W_2 is a totally isotropic subspace, $f(d, e_i) = 0$, thus $\beta_i = 0$ for all $i,\ 1 \leq i \leq m-1$. Then, $d = \alpha_1 e_1 + \ldots + \alpha_m e_m + \beta_m f_m$. Also, as $Q(d) \neq 0,\ \alpha_m \neq 0 \neq \beta_m$. Let $z = d - (\alpha_1 e_1 + \ldots + \alpha_{m-1} e_{m-1}) = \alpha_m e_m + \beta_m f_m$, then clearly $\langle z \rangle \in \mathcal{P}(W_2)$. Here, $Q(z) = \alpha_m \beta_m \neq 0$, thus $\langle z \rangle$ is a non-singular point in $\mathcal{P}(W_2)$. We write the vector z as a column vector $(0, \ldots, 0, \alpha_m, 0, \ldots, 0, \beta_m)^t$ with respect to the basis $\mathcal{B}$ of V.

We can now show that there is a subgroup of unipotent matrices of G, that acts sharply transitively on the set of all non-singular points of $\mathcal{P}(W_2)$ with respect to $\langle z \rangle$. Let $y = (y_1, \ldots, y_{m-1})^t$, $y_i \in \mathbb{F}_q$. Define $u_y \in GL_{2m}(q)$ as follows.

$$u_y := \begin{pmatrix} I_{m-1} & y & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & I_{m-1} & 0 \\ 0 & 0 & y^t & 1 \end{pmatrix}$$

Let $B_3 = \{u_y \mid y \in W'\}$ and $y' \in V$ be the column vector $(y_1, \ldots, y_{m-1}, 0, \ldots, 0)^t$. Then, it can be easily verified that $B_3 \leq G$ is a 2-group and for $u_y \in B_3$, $u_y(\langle z \rangle) = \langle \alpha_m y' + z \rangle$. Clearly for $y_1 \neq y_2$, $u_{y_1}(\langle z \rangle) \neq u_{y_2}(\langle z \rangle)$. Also, $|B_3| = q^{m-1}$ which is the same as the number of non-singular points in W_2. Hence B_3 acts sharply transitively on $L \cap \mathcal{P}(W_2)$ with respect to the non-singular point $\langle z \rangle$. Thus we have the following theorem.

Lemma 6.1. *Let $A_3, B_3 \leq O^+_{2m}(q)$, S' be the partial spread, and W' the subspace of V as defined above. Let $w = \langle z \rangle$. Then,*

(i) A_3 is a sharply transitive set on S' with respect to W'.

(ii) B_3 is a sharply transitive set on $L \cap \mathcal{P}(W_2)$ with respect to w.

The above lemma allows us to prove the following theorem.

Theorem 6.1. *Let q be a power of 2 and $m \in \mathbb{N}$. Then, the orthogonal group $O^+_{2m}(q)$ has an MLS.*

Proof. Let $G = O^+_{2m}(q)$. We apply Lemma 3.4 with $G = O^+_{2m}(q)$, $A = A_3$, $B = B_3$, $w = \langle z \rangle$, where subgroups A_3, $B_3 \leq G$ and $z \in G$ are as defined before Lemma 6.1. From Lemma 6.1 it follows that the conditions of Lemma 3.4 are satisfied. Thus, $[A_3,\ B_3,\ G_w]$ is an LS for G. Let G' be the commutator subgroup of

G. Then $G' \cong \Omega^+_{2m}(q)$. From Proposition 4.1.7 in [13], it follows that the stabilizer in $\Omega^+_{2m}(q)$ of a non-singular point is $Sp_{2m-2}(q)$. Now, consider the reflection $t_z : V \to V$ defined by $t_z(v) = v + \frac{f(v,z)}{Q(z)}z$ corresponding to the non-singular vector z. We check that the linear transformation $t_z \in G_w$ and since each element of G' is a product of an even number of reflections, $t_z \notin G'_w$. From the order of the orthogonal groups of plus type and the number of non-singular points in $\mathcal{P}(V)$, it follows that G_w is a semi-direct product of a group of order 2 and $Sp_{2m-2}(q)$. Therefore, using Theorem 5.3, it follows that G_w has an MLS. Using Proposition 3.8 and Lemma 3.2, we obtain that A_3 and B_3 have MLS's. Finally, using Proposition 3.1, we have an MLS for the group G. □

We now show that for q even, the group $\Omega^+_{2m}(q)$ has an MLS.

Theorem 6.2. *Let q be a power of 2 and $m \in \mathbb{N}$. Then, the orthogonal group $\Omega^+_{2m}(q)$ has an MLS.*

Proof. Let $G = O^+_{2m}(q)$ and G' be the commutator subgroup of G isomorphic to $\Omega^+_{2m}(q)$. Also assume that the subgroups $A_3,\ B_3 \leq G$ and the set L are as defined before. Now, we know that G' acts transitively on L. Also, an element x in $O^+_{2m}(q)$ is in $\Omega^+_{2m}(q)$ if and only if the rank of $I_{2m} + x$ is even [24, Section 3.8.1]. From the definition of B_3, it follows that for every $u_y \in B_3$, the rank of $1 + u_y$ is 2. Thus, $B_3 \leq G'$. Similarly, we can show that $A_3 \leq G'$. Then by applying Lemma 3.4, we have that $[A_3,\ B_3,\ G'_w]$ is an LS for G'. As mentioned in the proof of the previous theorem, the stabilizer G'_w is $Sp_{2m-2}(q)$ and therefore Theorem 5.3 implies that G'_w has an MLS. We already know that A_3 and B_3 have MLS's. Hence, using Proposition 3.1, we obtain that G' has an MLS. □

Chapter 7

Partitions of finite groups of Lie type

So far, among all finite simple groups of Lie type, we have shown the existence of MLS's for the following groups:

(i) $PSL_n(q)$ for any $n \in \mathbb{N}$ and q a power of a prime

(ii) $PSp_{2m}(q)$ for any $n \in \mathbb{N}$ and q a power of a prime

(iii) $\Omega^-_{2m}(q)$ for any $n \in \mathbb{N}$ and q a power of 2, [23]

(iv) $\Omega^+_{2m}(q)$ for any $n \in \mathbb{N}$ and q a power of 2.

For unitary groups, we have partial results [23], i.e. the general Unitary group $GU_n(q)$ has an MLS for n odd; q even, if $GU_{n-1}(q)$ has an MLS.

Let G be any finite group of Lie type. We end the dissertation with the discussion on how one can use the properties and structure of finite groups of Lie type to partition G into parts, each of which has an MLS. We note that results proven in this section hold for any finite group of Lie type. Because of the algorithmic nature of these results, we feel they are likely to be useful in cryptography, while at the same time being interesting from group theoretic point of view.

We now discuss one such proven result from [6] about finite groups with a split BN-pair. Let G be a finite group of Lie type. Then, as discussed in Section 2.7,

G has a split BN-pair. Therefore, we have $\eta : N \to W$, a canonical homomorphism from N onto $N/T := W$ as defined before. From Proposition 2.5, there exists a unique element $w_0 \in W$ of maximal length. Let $n_0 \in N$ be a pre-image of w_0 under the map η. For $x, y \in G$, let $x^y := y^{-1}xy$. For each $w \in W$, define:

$$U_w := U \cap U^{n_0\dot{w}}, \text{ where } \dot{w} \in N \text{ such that } \eta(\dot{w}) = w \in W$$

From Proposition 2.7, U is a maximal unipotent subgroup (a p-group), $U_w \leq U$ for every $w \in W$, the torus subgroup T is an abelian group, and W the Weyl group of G, generated by a set of involutions $S = \{s_i\}_{i=1}^{\ell}$.

For the proof of the following proposition, the reader is referred to [6].

Proposition 7.1. *[6] Let G be a group with a split BN-pair. Then, every element $g \in G$ can be uniquely written as $g = ut\dot{w}u'$ for $u \in U$, $t \in T$, $w \in W$ and $u' \in U_w$.*

Now, we see that the above proposition gives us a cover for every finite group of Lie type, as follows. From Section 2.7, if G is a finite group of Lie type then, G has a split BN-pair. Thus, for every $g \in G$, $g = ut\dot{w}u'$ where $u \in U$, $t \in T$, $w \in W$ and $u' \in U_w$. Now for every $w \in W$, we fix a pre-image $\dot{w} \in N$ under the map η. Let $\dot{W}$ denote the set of all such fixed pre-images $\dot{w} \in N$ and $U_W = \bigcup_{w \in W} U_w$. Then, by Theorem 7.1, $[U, T, \dot{W}, U_W]$ is a cover for the group G.

Theorem 7.1. *Let G be a finite group of Lie type, then G has a cover.*

Theorem 7.2. *Let G be a finite group of Lie type. Then, $G = \bigcup_{w \in W} A_w$, where $A_{w_1} \cap A_{w_2} \neq \phi$, if $w_1 \neq w_2$ and each $A_w \subseteq G$ has an MLS.*

Proof. From Section 2.7, G has a split BN-pair. Then, from Theorem 7.1 for every $g \in G$, $g = utwu'$ for $u \in U$, $t \in T$, $w \in W$ and $u' \in U_w$. Now, U is a p-group, T is an abelian group, and $U_w \leq U$ for every $w \in W$. Thus, U, T and U_w, $w \in W$, are all solvable and have an MLS (from Proposition 3.8). Suppose $\alpha_1 = [U_1, \ldots, U_{k_1}]$ is an MLS for U, $\alpha_2 = [T_1, \ldots, T_{k_2}]$ an MLS for T and, for $w \in W$, $\alpha_w = [B_{w_1}, \ldots, B_{w_{k_3}}]$ an MLS for U_w. Then, for every $w \in W$, $[U_1, \ldots, U_{k_1}, T_1, \ldots, T_{k_2}, \dot{w}B_{w_1}, \ldots, B_{w_{k_3}}]$ is an MLS for some subset A_w of G, where $\dot{w} \in \dot{W}$. Concluding, from Proposition 7.1, $A_{w_1} \neq A_{w_2}$ for any $w_1 \neq w_2$; $w_1, w_2 \in W$ and $G = \bigcup_{w \in W} A_w$. □

To give an intuition of the above theorem, we give here a few examples of the orders of finite groups of Lie type and their corresponding Weyl groups:

$\lvert G\rvert$	$\lvert W\rvert$
$\lvert SO_5(2^3)\rvert = 2^{12}\ 3^4\ 5\ 7^2\ 13$	$\lvert W\rvert = 2^3 = 8$
$\lvert PGL_5(3^2)\rvert = 2^9\ 3^{10}\ 5\ 11^2\ 13$	$\lvert W\rvert = 2^3\ 3\ 5 = 120$
$\lvert PGL_4(5)\rvert = 2^9\ 3^2\ 5^6\ 13\ 31$	$\lvert W\rvert = 2^3\ 3 = 24$
$\lvert PGL_3(2^3)\rvert = 2^9\ 3^2\ 7^2\ 73$	$\lvert W\rvert = 6$
$\lvert SO_5(3^2)\rvert = 2^9\ 3^8\ 5^2\ 41$	$\lvert W\rvert = 2^3 = 8$
$\lvert PGL_5(3^2)\rvert = 2^9\ 3^{10}\ 5\ 11^2\ 13$	$\lvert W\rvert = 6$
$\lvert P(CO)_8(3^2)\rvert = 2^{14}\ 3^{12}\ 5^2\ 7\ 13$	$\lvert W\rvert = 2^6\ 3 = 120$

Table 7.1: Orders of Weyl groups

We note that, the number of components mentioned in the above partition of G is equal to the number of elements in the Weyl group of G. We also observe that in a few examples tabulated above, the size of the Weyl group is considerably smaller as compared to $|G|$. Thus, if one thinks of an MLS as an optimal factorization for a finite group, then the above construction gives us a partition of finite groups of Lie type, quite close to an optimal one.

Bibliography

[1] Michael Artin. *Algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[2] Áron Bereczky. Maximal overgroups of Singer elements in classical groups. *J. Algebra*, 234(1):187–206, 2000.

[3] Jens-Matthias Bohli, Rainer Steinwandt, María Isabel González Vasco, and Consuelo Martínez. Weak keys in MST_1. *Des. Codes Cryptogr.*, 37(3):509–524, 2005.

[4] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[5] Nicolas Bourbaki. *Éléments de mathématique: groupes et algèbres de Lie*. Masson, Paris, 1982. Chapitre 9. Groupes de Lie réels compacts. [Chapter 9. Compact real Lie groups].

[6] Roger W. Carter. *Finite groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.

[7] A. Cossidente and M. J. de Resmini. Remarks on Singer cyclic groups and their normalizers. *Des. Codes Cryptogr.*, 32(1-3):97–102, 2004.

[8] Paul Garrett. *Buildings and classical groups*. Chapman & Hall, London, 1997.

[9] María Isabel González Vasco, Martin Rötteler, and Rainer Steinwandt. On minimal length factorizations of finite groups. *Experiment. Math.*, 12(1):1–12, 2003.

[10] María Isabel González Vasco and Rainer Steinwandt. Obstacles in two public key cryptosystems based on group factorizations. *Tatra Mt. Math. Publ.*, 25:23–37, 2002. TATRACRYPT '01 (Liptovský Ján).

[11] Marshall D. Hestenes. Singer groups. *Canad. J. Math.*, 22:492–513, 1970.

[12] P. E. Holmes. On minimal factorisations of sporadic groups. *Experiment. Math.*, 13(4):435–440, 2004.

[13] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[14] Wolfgang Lempken and Tran van Trung. On minimal logarithmic signatures of finite groups. *Experiment. Math.*, 14(3):257–269, 2005.

[15] Wolfgang Lempken, Tran van Trung, Spyros S. Magliveras, and Wandi Wei. A public key cryptosystem based on non-abelian finite groups. *J. Cryptology*, 22(1):62–74, 2009.

[16] S. S. Magliveras, D. R. Stinson, and Tran van Trung. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *J. Cryptology*, 15(4):285–297, 2002.

[17] Spyros S. Magliveras. A cryptosystem from logarithmic signatures of finite groups. In *Proceedings of the 29th Midwest Symposium on Circuits and Systems*, pages 972–975. Elsevier Publishing Company, Amsterdam, 1986.

[18] Spyros S. Magliveras. Secret- and public-key cryptosystems from group factorizations. *Tatra Mt. Math. Publ.*, 25:11–22, 2002. TATRACRYPT '01 (Liptovský Ján).

[19] Spyros S. Magliveras and Nasir D. Memon. Algebraic properties of cryptosystem PGM. *J. Cryptology*, 5(3):167–183, 1992.

[20] P. Nguyen. *New Trends in Cryptology*. European project STORK - "Strategic roadmap for Crypto". IST-2002-38273.

[21] James Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938.

[22] Nidhi Singhi, Nikhil Singhi, and Spyros Magliveras. Minimal logarithmic signatures for finite groups of Lie type. *Des. Codes Cryptogr.*, 55(2-3):243–260, 2010.

[23] Nikhil Singhi. *The Existence of Minimal Logarithmic Signatures for Classical Groups*. PhD thesis, Florida Atlantic University, 2011.

[24] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2009.