The Existence of Minimal Logarithmic Signatures for Classical Groups

by

Nikhil 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

The Existence of Minimal Logarithmic Signatures for Classical Groups

by

Nikhil 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 his supervisory committee. It was submitted to the faculty of the Charles E. Schmidt College of Science and was accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

SUPERVISORY COMMITTEE:

Spyros S. Magliveras, Ph.D.
Dissertation Advisor

Lee Klingler, Ph.D.

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 deepest gratitude to my advisor Professor Spyros Magliveras. Researching with him was just one aspect. It was under his guidance that I learned to enjoy not just mathematics but many aspects of life. Moments spent with him will be an inspiring force for me throughout my 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 taking his time to read my dissertation and suggesting several improvements. I would also like to thank Professor Heinrich Niederhausen and Hanne Niederhausen for all the help and advice they provided, especially in my first years at FAU.

I would like to thank all the faculty members of Department of Mathematical Sciences at FAU. I enjoyed the courses I took from many of them. Throughout my stay here at FAU, it is the friends, who were accompanying me when I needed a companion and supporting me when I needed support. Thanks to all of them. Finally, thanks also to the office staff of Department of Mathematical Sciences at FAU, particularly Emily Cimillo and Beth Broer, for all the help they provided.

Abstract

Author:	Nikhil Singhi
Title:	The Existence of Minimal Logarithmic Signatures for Classical Groups
Institution:	Florida Atlantic University
Dissertation Advisor:	Dr. Spyros S. Magliveras
Degree:	Doctor of Philosophy
Year:	2011

A logarithmic signature (LS) for a finite group G is an ordered tuple $\alpha = [A_1, A_2, \ldots, A_n]$ of subsets A_i of G, such that every element $g \in G$ can be expressed uniquely as a product $g = a_1 a_2 \ldots, a_n$, where $a_i \in A_i$. Logarithmic signatures were defined by Magliveras in the late 1970's for arbitrary finite groups in the context of cryptography. They were also studied for abelian groups by Hajós in the 1930's. The length of an LS α is defined to be $\ell(\alpha) = \sum_{i=1}^{n} |A_i|$. It can be easily seen that for a group G of order $\prod_{j=1}^{k} {p_j}^{m_j}$, the length of any LS α for G satisfies $\ell(\alpha) \leq \sum_{j=1}^{k} m_j p_j$. An LS for which this lower bound is achieved is called a minimal logarithmic signature (MLS). The MLS conjecture states that every finite simple group has an MLS. If the conjecture is true then every finite group will have an MLS. The conjecture was shown to be true by a number of researchers for a few classes of finite simple groups. However, the problem is still wide open.

This dissertation addresses the MLS conjecture for the classical simple groups. In particular, it is shown that MLS's exist for the symplectic groups $Sp_{2n}(q)$, the orthogonal groups $O^-_{2n}(q')$ and the corresponding simple groups $PSp_{2n}(q)$ and $\Omega^-_{2n}(q')$ for all $n \in \mathbb{N}$, prime power q and even prime power q'. The existence of an MLS is also shown for all unitary groups $GU_n(q)$ for all odd n and $q = 2^s$ under the assumption that an MLS exists for $GU_{n-1}(q)$. The methods used are very general and algorithmic in nature and may be useful for studying all finite simple groups of Lie type and possibly also the sporadic groups. The blocks of logarithmic signatures constructed in this dissertation have cyclic structure and provide a sort of cyclic decomposition for these classical groups.

Dedication

This work is dedicated to my parents, Navin and Sudha Singhi, for their endless love, support and encouragement.

Contents

List of Tables

Chapter 1

Introduction

A ***logarithmic signature (LS)*** for a finite group G is an ordered tuple $\alpha = [A_1, A_2, \ldots, A_n]$ of subsets A_i of G, such that every element $g \in G$ can be expressed uniquely as a product $g = a_1 a_2 \cdots a_n$, where $a_i \in A_i$. The sets A_i, are called the ***blocks*** of the LS α. The ***length of an LS*** α is defined to be $\ell(\alpha) = \sum_{i=1}^{n} |A_i|$.

Logarithmic signatures were first defined by Magliveras in [24] where the cryptosystem PGM was proposed using LS's. In [26], the algebraic properties of logarithmic signatures and of cryptosystem PGM were discussed by Magliveras and Memon. Later, Magliveras, Stinson and Tran van Trung proposed cryptosystems MST_1, MST_2 [23], and Magliveras, Lempken, Tran van Trung and Wei proposed cryptosystem MST_3 using logarithmic signatures and *covers* [25, 22]. For some interesting papers studying attacks on MST_1, MST_2 and MST_3, see [4, 5, 12, 14, 27, 32].

Much earlier, logarithmic signatures were also studied, in a different context, by group theorists, who called them *group factorizations*. Perhaps Hajós was first to define factorizations for finite abelian groups in 1938 [15]. He used them as a tool to study the well-known Minkowski conjecture [28, 29]. Later, Rédei wrote a number of papers on factorizations of abelian groups. Rédei also proved a very interesting

theorem which says that if a finite abelian group has a factorization (i.e., an LS) in which each block has a prime number of elements and each block contains the identity element then one of the blocks is a subgroup. For these classical results on logarithmic signatures of abelian groups, see the book by Szabó [33]. Today, the term factorization is often used in the case where each block A_i is a subgroup. Hence, we will only use the term *logarithmic signature*.

It was first observed by González Vasco and Steinwandt in [14] that the length $\ell(\alpha)$ of a logarithmic signature α satisfies the following inequality.

Inequality 1.1. *Let G be a finite group and let $\alpha = [A_1, A_2, \ldots, A_k]$ be a logarithmic signature for G. Suppose $|G| = \prod_{j=1}^{k} {p_j}^{m_j}$ where the p_j are prime. Then,*

$$\ell(\alpha) \geq \sum_{j=1}^{k} m_j p_j$$

An LS for which the above lower bound is attained is called a ***minimal logarithmic signature (MLS)*** for the group G. A cryptographic significance of MLS's is the fact that they minimize memory space required for storing the underlying groups.

It was observed in [13] that if there is an MLS for a normal subgroup H of group G and also for the quotient group G/H then there is an MLS for G. Thus, if every finite simple group had an MLS, then every finite group would have an MLS.

A moderate work effort has been devoted to finding MLS's for various finite groups. It has been shown in [14] that MLS's exist for all finite solvable groups and all symmetric groups S_n. It was also shown in [25] that the alternating groups A_n have MLS's.

In [13] it is proved that minimal logarithmic signatures exist for all groups of order less than 175,560. In [21], Lempken and Tran van Trung describe an interesting new general method to construct minimal logarithmic signatures using double cosets and prove the existence of MLS's for the special linear groups $SL_n(q)$ and the projective special linear groups $PSL_n(q)$ when $gcd(n, q-1) \in \{1, 4, p \mid p \text{ a prime}\}$. They also show that, with a few exceptions, an MLS exists for all groups of order $\leq 10^{10}$. Holmes [18] constructed minimal logarithmic signatures for the sporadic groups J_1, J_2, HS, M^cL, He, and Co_3.

These results make the following conjecture plausible.

Conjecture 1.1. *(MLS Conjecture)*

Every finite simple group has a minimal logarithmic signature.

Motivated by general methods for constructing MLS's in [21], the goal of our research was to develop new general methods for constructing LS's and MLS's and applying these methods to prove the existence of MLS's in some families of simple groups.

In this dissertation, we start by studying elementary properties of LS's and MLS's and connections of LS's with other objects in group theory. We describe two general methods for constructing MLS's. We then study how one can apply these methods in symplectic, orthogonal and unitary families of groups and prove the existence of MLS's for almost all of these groups. In particular, we construct MLS's for the symplectic groups $Sp_{2n}(q)$ and $PSp_{2n}(q)$ for all $n \in \mathbb{N}, q$ a prime power. Further, we also construct MLS's for the orthogonal groups of minus type $O^-_{2n}(q)$ and $\Omega^-_{2n}(q)$ when $q = 2^s$. Finally, we discuss the results we obtained for the unitary groups $GU_n(q)$.

In Chapter 2 we first define a *logarithmic signature* for an arbitrary subset A of a group G. This general definition is then used as a tool to study the MLS conjecture. We then discuss cyclic logarithmic signatures, prove some elementary properties of logarithmic signatures and discuss the relation between sharply transitive sets and logarithmic signatures.

In Chapter 3 we give basic definitions of bilinear, quadratic and conjugate-symmetric sesquilinear forms and the corresponding classical groups. We discuss some of the properties of these groups. In Chapter 4, we define *spreads* and prove a simple result linking spreads and logarithmic signatures.

Finally, in Chapter 5, 6 and 7 we describe our constructions of LS's and MLS's for the symplectic, orthogonal and unitary families of groups.

Chapter 2

Logarithmic Signatures

Let G be a finite group and $A \subseteq G$. Let $\alpha = [A_1, A_2, \ldots, A_s]$ be an ordered s-tuple of subsets A_i of G. We say that α is a ***logarithmic signature*** (LS) for set A, if every $a \in A$ can be uniquely written as a product $a = a_1 a_2 \cdots a_s$ where $a_i \in A_i$.

Inequality 2.1. *Let G be a finite group and let $\alpha = [A_1, A_2, \ldots, A_s]$ be a logarithmic signature for $A \subseteq G$. Suppose $|A| = \prod_{j=1}^{s} {p_j}^{m_j}$ is the prime power decomposition of $|A|$. Then,*

$$\ell(\alpha) \geq \sum_{j=1}^{s} m_j p_j$$

If equality holds in the above inequality then the LS α is called a ***minimal logarithmic signature (MLS)*** for A.

The following lemma follows easily from [21] and the above definition of an MLS.

Lemma 2.1. *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 $A = A_1 A_2 \ldots A_s$. 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.*

2.1 Cyclic Sets and Cyclic Logarithmic Signatures

We say that a subset A of a group G is a ***cyclic set*** if $A = \{x^i \mid 0 \leq i < |A|\}$ for some $x \in G$ of order $\geq |A|$. The element x is called a generator of the cyclic set A. Then an LS $\alpha = [A_1, A_2, \ldots, A_k]$ for a subset A of G is called a ***cyclic logarithmic signature*** if every block A_j of α is a cyclic set. Thus a cyclic LS is completely determined by the generators x_j and the sizes $|A_j|$ of the blocks $A_j,\ 1 \leq j \leq k$. In this case, every element y of the set A can be uniquely expressed as $y = \prod_{j=1}^{k} {x_j}^{m_j}$ where $0 \leq m_j < |A_j|$ for $1 \leq j \leq k$.

All the MLS's constructed in Chapters 5 and 6 are cyclic MLS's. We observe that MLS's constructed for the groups $GL_n(q),\ PGL_n(q),\ Sp_{2n}(q), PSp_{2n}(q), O^+_{2n}(q)$ and $\Omega^+_{2n}(q)$ in [30] are also cyclic. Further, we note that the proofs of existence of MLS's for the solvable groups given in [14] and for the alternating groups A_n given in [25] imply that solvable groups and alternating groups have cyclic MLS's. Thus we have the following theorem.

Theorem 2.1. *All solvable groups have cyclic MLS's. Moreover, if $n \in \mathbb{N}$, q is any prime power and $q' = 2^s,\ s \in \mathbb{N}$, then the groups $A_n,\ GL_n(q),\ PGL_n(q),\ Sp_{2n}(q),\ PSp_{2n}(q),\ O^-_{2n}(q'),\ O^+_{2n}(q'),\ \Omega^-_{2n}(q')$ and $\Omega^+_{2n}(q')$ have cyclic MLS's.*

2.2 Properties of Logarithmic Signatures

In this section we give some basic results about logarithmic signatures that we will use in later chapters. Most of these results can be derived easily from the definitions. For most of the results, we give the proofs here. For the remaining results, proofs are given in [30]. For the case of LS's of groups, proofs are also given

for most of these results in [18], [25] and [14].

Let $H \leq G$. If $A \subseteq G$ is a complete set of left coset representatives of H in G then we say A is a *left transversal* of H in G. The collection of all left transversals of H in G is denoted by $\boldsymbol{lt(G, H)}$. In instances below where $H \trianglelefteq G$, $\eta : G \to G/H$ denotes the canonical homomorphism from G onto G/H.

Lemma 2.2. *Let $A \subseteq G$. Suppose $[A_1, A_2, \ldots, A_r]$ is an LS for A and for each A_i, $1 \leq i \leq r$, $[B_{i1}, \ldots, B_{ik_i}]$ is an LS for A_i. Then $\alpha = [B_{11}, \ldots, B_{1k_1}, \ldots, B_{r1}, \ldots, B_{rk_r}]$ is an LS for A.*

Proof. Let $a \in A$. Then by the definition of a logarithmic signature, there exist unique $a_i \in A_i, 1 \leq i \leq r$ such that $a = a_1 a_2 \ldots a_r$. Now, for each a_i there exist unique $b_{ij} \in B_{ij}, 1 \leq j \leq k_i$ such that $a_i = b_{i1} b_{i2} \ldots b_{ik_i}$. Thus, for each $a \in A$ there exist unique $b_{ij} \in B_{ij}, 1 \leq j \leq k_i, 1 \leq i \leq r$ such that $a = \prod_{i=1}^{r} (b_{i1} b_{i2} \ldots b_{ik_i})$. Therefore, α is an LS for A. □

Lemma 2.3. *[30] Let $H \leq G$ and $A \in lt(G, H)$. Then $[A, H]$ is an LS for G.*

Lemma 2.4. *[30] Let $H_1, H_2 \leq G$ be such that $G = H_1 H_2$ and $H_1 \cap H_2 = \{1\}$. Then $[H_1, H_2]$ is an LS for G.*

Lemma 2.5. *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 $B_i \subseteq G$ 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) $B_1 B_2 \cdots B_k \in lt(G, H)$.

Lemma 2.6. *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 $1 \leq i \leq k$.*

Proof. Suppose $gH \in G/H$, where $g \in G$. Then, $g = b_1 b_2 \dots b_k h$ where $b_i \in B_i, 1 \leq i \leq k$ and $h \in H$. This implies $gH = \eta(g) = \eta(b_1 b_2 \dots b_k h) = \eta(b_1)\eta(b_2) \dots (b_k)H$. Thus $gH = b_1' b_2' \dots b_k'$ where $b_i' \in \breve{B}_i, 1 \leq i \leq k$. Thus, $|G/H| \leq \prod_{i=1}^{k} |\breve{B}_i|$.

Since $H \trianglelefteq G, |\breve{B}_i| \leq |B_i|$ and $[B_1, B_2, \dots, B_k, H]$ is an LS for G, it follows that $|G/H| \geq \prod_{i=1}^{k} |\breve{B}_i|$. Thus $|G/H| = \prod_{i=1}^{k} |\breve{B}_i|$ and $[\breve{B}_1, \breve{B}_2, \dots, \breve{B}_k]$ is an LS for G/H. □

Lemma 2.7. *Let $H \leq H_1 \leq G$, $H \neq H_1$ and $H \trianglelefteq G$. Suppose $[A_1, A_2, \dots, A_k, H_1]$ is an LS for G. Let $B_i = \eta(A_i) \subseteq G/H$, for all $1 \leq i \leq k$. Then $[B_1, B_2, \dots, B_k, H_1/H]$ is an LS for G/H.*

Proof. Suppose $gH \in G/H$, where $g \in G$. Then, $g = a_1 a_2 \dots a_k h_1$ where $h_1 \in H_1$ and $a_i \in A_i, 1 \leq i \leq k$. Let $b_i = \eta(a_i) \in B_i$ for $1 \leq i \leq k$. Then $gH = \eta(g) = \eta(a_1 a_2 \dots a_k h_1) = b_1 b_2 \dots b_k h_1 H$ where $h_1 H \in H_1/H$. Thus, $|G/H| \leq (\prod_{i=1}^{k} |B_i|)|H_1/H|$.

Using the facts that $H \trianglelefteq H_1, |B_i| \leq |A_i|, 1 \leq i \leq k$ and that $[A_1, A_2, \dots, A_k, H_1]$ is an LS for G, it follows that $|G/H| \geq (\prod_{i=1}^{k} |B_i|)|H_1/H|$. Therefore, $|G/H| = (\prod_{i=1}^{k} |B_i|)|H_1/H|$ and $[B_1, B_2, \dots, B_k, H_1/H]$ is an LS for G/H. □

Lemma 2.8. *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 $[A_1, A_2, \dots, A_k]$ is an LS for A. Let $B_i = \eta(A_i) \subseteq G/H$, for $1 \leq i \leq k$. Then $[B_1, B_2, \dots, B_k]$ is an LS for $\breve{A}$.*

Proof. Consider $aH \in \breve{A}$ with $a \in A$. Then there exist $a_i \in A_i, 1 \leq i \leq k$ such that $a = a_1 a_2 \dots a_k$. This implies, $aH = b_1 b_2 \dots b_k$ where $b_i = \eta(a_i) \in B_i, 1 \leq i \leq k$. Finally, since $bH \neq cH$ for all $b, c \in A$, $b \neq c$, it follows that $[B_1, B_2, \dots, B_k]$ is an LS for $\breve{A}$. □

Lemma 2.9. [14] *If G is solvable, then G has an MLS.*

We now describe an MLS for a cyclic set.

Lemma 2.10. *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 :*

$$\text{For any list } [j_1, \ldots, j_k], \text{ such that } x^{j_i} \in A_i,\ 1 \leq i \leq k,\ \sum_{i=1}^{k} j_i < s. \qquad (2.2.1)$$

Proof. Suppose $s = p_1 p_2 \ldots p_k$ is the prime factorization for s. Then, define $A_1 = [1, x, \ldots, x^{p_1 - 1}]$ and $A_i = [1, x^{p_1 p_2 \cdots p_{i-1}}, x^{2p_1 p_2 \cdots p_{i-1}}, \ldots, x^{(p_i - 1)p_1 p_2 \cdots p_{i-1}}]$ for all $2 \leq i \leq k$. Let $m_1 = 1$ and $m_i = \prod_{j=1}^{i-1} p_j$ for $2 \leq i \leq k$. Now, given a, $1 \leq a < s$, there exist $s_1, s_2, \ldots, s_k \in \mathbb{Z}$, $0 \leq s_i < p_i$ for $1 \leq i \leq k$, such that

$$a = \sum_{i=1}^{k} m_i s_i. \quad \text{Therefore, } x^a = \prod_{i=1}^{k} x^{m_i s_i}.$$

Now, by the definition of A_i, it follows that $x^{m_i s_i} \in A_i$ for all $i \in \{1, \ldots, k\}$. Thus, x^a has a factorization, $x^a = a_1 a_2 \ldots a_k$, $a_i \in A_i$ for $1 \leq i \leq k$. Now, since $|A_i| = p_i$ for $1 \leq i \leq k$ and $\prod_{i=1}^{k} |A_i| = s = |S|$, it follows that $\gamma = [A_1, A_2, \ldots, A_k]$ is an MLS for S. Finally, from $\sum_{i=1}^{k} m_i(p_i - 1) = s - 1$, it follows that, γ satisfies (2.2.1). □

We note that the MLS γ constructed above is in fact a cyclic MLS for the cyclic set S.

2.3 Group Actions and Permutation Groups

In this section, we will first give definitions related to group actions and permutation groups. Later on, we describe one of the methods we use to construct MLS's.

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 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.

Let $x \in X$. 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, under the action of G, 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 $y = gx$.

Definition 2.1. *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 $x \in X$.

Lemma 2.11. [30] *Let $G|X$ be a transitive permutation group. Suppose $A \subseteq G$ is a sharply transitive set on X with respect to $x \in X$. Then, $[A, G_x]$ is an LS for G.*

The above lemma is one of the main tools we use to construct MLS's for the classical groups. We choose X suitably so that $G|X$ is a transitive permutation group. Singer cyclic groups (see the next chapter for more details) in these classical groups provide the main component for the sharply transitive set A.

G_x generally turns out to be a *parabolic subgroup*; however, in this dissertation, for studying G_x we have preferred using geometric objects like *spreads* or algebraic structures like *inner product spaces* and *quadratic spaces*. These terms will be formally described in the next chapters.

Chapter 3

Bilinear, Conjugate-Symmetric Forms and Singer Groups

In this chapter we define bilinear, conjugate-symmetric sesquilinear and quadratic forms. We describe some of the properties of these forms and define the corresponding classical groups. The last section of this chapter is devoted to Singer groups in the classical groups. Most of the material given in this chapter related to the forms and the corresponding classical groups is taken from Wilson's book [35].

3.1 Bilinear and Conjugate-Symmetric Forms

Let V be a finite dimensional vector space over a finite field K. 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 $f(u, \lambda v + w) = \lambda f(u, v) + f(u, w)$, $\lambda \in K$, $u, v, w \in V$. A *conjugate-symmetric sesquilinear form* on V over $K = \mathbb{F}_{q^2}$ is a map f satisfying the following properties: $f(\lambda u + v, w) = \lambda f(u, w) + f(v, w)$ and $f(w, v) = (f(v, w))^q$, $\lambda \in K$ and $u, v, w \in V$. The pair (V, f) is called an *inner-product space*.

Now consider an n-dimensional vector space V over K and bilinear or sesquilinear form f. A *norm* of v is defined as $f(v,v)$. A non-zero vector $v \in V$ is said to be an *isotropic vector* if the norm of v is zero. A vector of non-zero norm is called an *anisotropic vector*. For a subspace W of V, $W^{\perp} = \{v \in V \mid f(v,w) = 0 \; for \; all \; w \in W\}$. W is said to be a *totally isotropic subspace* of V if $W \subseteq W^{\perp}$.

Let J_n be an $n \times n$ matrix whose $(i,j)^{th}$ entry is $f(e_i, e_j)$ where $\{e_1, \ldots, e_n\}$ is an ordered basis of V. Now suppose, $x = (x_1, x_2, \ldots, x_n)^t$ and $y = (y_1, y_2, \ldots, y_n)^t$ with respect to the basis $\{e_1, \ldots, e_n\}$. Then, $f(x,y) = y^t J_n x$ when f is a bilinear form and $f(x,y) = (y^q)^t J_n x$ when f is a conjugate-symmetric sesquilinear form. Thus the form f is uniquely determined by the matrix J_n. The matrix J_n is called the matrix of the form f with respect to the ordered basis $\{e_1, \ldots, e_n\}$.

When V is a vector space over the field $K = \mathbb{F}_{q^2}$, we define the matrix $g^q \in GL(V)$ by $g^q = ((g_{ij})^q)$ where $g = (g_{ij}) \in GL(V)$.

Radical of a form f, denoted by $rad(f)$, is $V^{\perp}$. Form f is said to be *non-singular* if $rad(f) = \langle 0 \rangle$. An element $g \in GL(V)$ is said to be an *isometry* of f if $f(gu, gv) = f(u,v)$ for all $u, v \in V$. The *isometry group* of an inner product space (V, f) is defined to be the subgroup of $GL(V)$, consisting of all elements $g \in GL(V)$ preserving the form f i.e. $g^t J_n g = J_n$ in case of bilinear form f and $(g^q)^t J_n g = J_n$ in case of conjugate-symmetric sesquilinear form f.

There are three interesting types of bilinear forms. A bilinear form f is said to be *symmetric* if $f(u,v) = f(v,u)$ for all $u, v \in V$. It is called *skew-symmetric* if $f(u,v) = -f(v,u)$ for all $u, v \in V$ and *alternating* if $f(v,v) = 0$ for all $v \in V$. It is easy to check that an alternating bilinear form is always skew-symmetric.

Definition 3.1. *Let (V, f) be an inner product space where f is a non-singular*

alternating bilinear form and V is a vector space over the field $K = \mathbb{F}_q$. A basis $\mathcal{B} = \{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ satisfying the following conditions is called a ***symplectic basis*** *of V.*

For all $i, j \in \{1, 2, \ldots, n\}$,

(i) $f(e_i, e_j) = f(f_i, f_j) = 0$

(ii) $f(e_i, f_j) = -f(f_j, e_i) = \delta_{ij}$

where δ_{ij} is the Kronecker delta function.

It can be shown that a symplectic basis exists for any non-singular alternating bilinear form (See Section 3.4.4, [35]). There exists a similar basis in the case of a non-singular conjugate-symmetric sesquilinear form.

Lemma 3.1. *[35, Section 3.6.2] Let (V, f) be an inner product space where f is a non-singular conjugate-symmetric sesquilinear form and V is an n-dimensional vector space over the field $K = \mathbb{F}_{q^2}$.*

(i) If $n = 2m + 1$, then there exists a basis $\mathcal{B} = \{e_1, e_2, \ldots, e_m, w, f_1, f_2, \ldots, f_m\}$ for V satisfying the following conditions.

(a) $f(e_i, e_j) = f(f_i, f_j) = 0$

(b) $f(e_i, f_j) = -f(f_j, e_i) = \delta_{ij}$

(c) $f(e_i, w) = f(f_i, w) = 0$ *and* $f(w, w) = 1$

(ii) If $n = 2m$, then there exists a basis $\mathcal{B} = \{e_1, e_2, \ldots, e_m, f_1, f_2, \ldots, f_m\}$ for V such that $\mathcal{B}$ satisfies the conditions (a) and (b) mentioned above.

We now state the well-known theorem of Witt.

Theorem 3.1. *(Witt's Theorem) If (V, f) and (W, g) are isometric spaces, with f and g nonsingular, and either alternating bilinear, or conjugate-symmetric sesquilinear, or symmetric bilinear in odd characteristic, then any isometry between a subspace X of V and a subspace Y of W extends to an isometry of V with W.*

Now, the following lemma is an immediate consequence of Witt's theorem.

Lemma 3.2. *Let V be a $2n$-dimensional vector space and f a non-singular alternating bilinear form on V. Let W be a maximal totally isotropic subspace of V. Then W has dimension n. Further, a basis $\{e_1, \ldots, e_n\}$ of W can be extended to a basis $\mathcal{B} = \{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ of V such that $\mathcal{B}$ is a symplectic basis of V.*

We now give the definitions of the symplectic and unitary families of groups.

Definition 3.2. *Let (V, f) be an inner product space of dimension $2m$. If f is a non-singular alternating bilinear form then the isometry group of (V, f) is called the **symplectic group** $\mathbf{Sp_{2n}(q)}$. The quotient group $Sp_{2n}(q)/Z(Sp_{2n}(q))$ is called the **projective symplectic group** $\mathbf{PSp_{2n}(q)}$.*

We note that, the center $Z(Sp_{2n}(q))$ is $\{\pm I_{2n}\}$.

Definition 3.3. *Let (V, f) be an inner product space where f is a non-singular conjugate-symmetric sesquilinear form and V is an n-dimensional vector space over the field $K = \mathbb{F}_{q^2}$. The isometry group of (V, f) is called the **(general) unitary group** $\mathbf{GU_n(q)}$. The **special unitary group** $\mathbf{SU_n(q)}$ is $SL_n(q^2) \cap GU_n(q)$. The quotient group $SU_n(q)/Z(SU_n(q))$ is called the **projective special unitary group** $\mathbf{PSU_n(q)}$.*

3.2 Quadratic Forms

A *quadratic form* $Q : V \to K$ is a function 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 the associated bilinear form. Clearly, f is symmetric. The pair (V, Q) is called a *quadratic space*. The radical of Q is $rad(Q) := \{v \in rad(f) \mid Q(v) = 0\}$. The quadratic form Q is called *non-singular*, if $rad(Q) = \langle 0 \rangle$. The quadratic space (V, Q) is called *non-degenerate*, if f is non-singular, where f is the associated bilinear form. If $\text{char}(K) \neq 2$, then $4Q(v) = Q(2v) = Q(v + v) = 2Q(v) + f(v, v) \Rightarrow Q(v) = \frac{1}{2} f(v, v)$. Thus, for q odd, one can recapture the symmetric bilinear form f from the quadratic form Q. For q even, the symmetric bilinear form f becomes alternating.

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 $g : V \to V$.

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, $Isom(V, f) = Isom(V, Q)$ [35, Section 3.7].

A vector $v \in V$ is said to be *singular* if $Q(v) = 0$ and *non-singular* if $Q(v) \neq 0$. A subspace W of V is called *totally singular* if every vector in W is singular. 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.

By an *orthogonal group* we mean the isometry group of a non-degenerate quadratic space (V, Q). When the dimension n of the vector space V is odd, there is a unique non-degenerate quadratic form.

Definition 3.4. *Let (V, Q) be a non-degenerate quadratic space of dimension $2m+1$. The isometry group of the form Q is called the* ***orthogonal group*** *and is denoted by* $\mathbf{O_{2m+1}(q)}$.

If $n = 2m$, the quadratic form Q is said to be of *plus type* if the dimension of a maximal totally singular subspace W is m, and of *minus type* if the dimension of W is $m - 1$.

Definition 3.5. *Let (V, Q) be a non-degenerate quadratic space of dimension $2m$. The isometry group of a non-degenerate quadratic form Q of plus type is called the* ***orthogonal group of plus type*** *and is denoted by* $\mathbf{O^+_{2m}(q)}$. *Similarly, the isometry group of a non-degenerate quadratic form Q of minus type is called the* ***orthogonal group of minus type*** *and is denoted by* $\mathbf{O^-_{2m}(q)}$.

Let $G = O_n(q)$ be any orthogonal group ($O_{2m+1}(q)$, $O^+_{2m}(q)$, $O^-_{2m}(q)$). For $g \in G$, $det(g) = \pm 1$ when q is odd, and 1 when q is even. The group $\mathbf{SO_n(q)} := G \cap SL_n(q)$ is called the ***special orthogonal group***, and is a subgroup of index 2 in G for q odd. For q even, $SO_n(q) = G$. Let, I_n denote the $n \times n$ identity matrix. Then, $-I_n \in SO_n(q)$ if and only if n is even. Further, $Z(G) = \{\pm I_n\}$ or $\{I_n\}$ depending on whether q is odd or even. The corresponding quotient groups $G/Z(G)$, $SO_n(q)/Z(SO_n(q))$ are the ***projective orthogonal group*** $\mathbf{PO_n(q)}$, and

the ***projective special orthogonal*** group $\mathbf{PSO_n(q)}$ respectively. Unlike other families of classical groups, the aforementioned groups are generally not simple. There is a subgroup of index 2 in $SO_n(q)$ denoted by $\Omega_n(q)$. The group $\mathbf{\Omega_n(q)}$ is the commutator subgroup of $O_n(q)$. The corresponding quotient groups $\mathbf{P\Omega_{2m+1}(q)}$, $\mathbf{P\Omega^-_{2m}(q)}$ and $\mathbf{P\Omega^+_{2m+1}(q)}$ are usually simple. We note that, for q even, $P\Omega^\epsilon_n(q) = \Omega^\epsilon_n(q)$.

3.3 Singer Groups

In this section we give the definition of Singer cyclic groups. These cyclic groups are crucial in our construction of MLS's.

Definition 3.6. *An element of $GL_n(q)$ of order $q^n - 1$ is called a* ***Singer cycle****. The subgroup generated by a Singer cycle is called a* ***Singer cyclic subgroup of $GL_n(q)$*** *(or just Singer subgroup of $GL_n(q)$).*

Let G be any classical subgroup of $GL_n(q)$ and S be a Singer subgroup of $GL_n(q)$. A Singer subgroup of G is defined as the intersection of S with G. A Singer subgroup of G can be equivalently defined as the irreducible cyclic subgroup of G of maximal possible order. Singer subgroups exist in symplectic groups, orthogonal groups of minus type and in odd-dimensional unitary groups.

Now, the image of a Singer cyclic group of $GL_n(q)$ in $PGL_n(q)$ under the canonical homomorphism is called a Singer cyclic group of $PGL_n(q)$. Similarly one can define Singer subgroups in the projective groups corresponding to the classical groups.

Below, we list the orders of the Singer subgroups in all the classical groups.

$GL_n(q)$	$q^n - 1$	$PGL_n(q)$	$\frac{q^n-1}{q-1}$
$SL_n(q)$	$\frac{q^n-1}{q-1}$	$PSL_n(q)$	$\frac{q^n-1}{(q-1)(n,\ q-1)}$
$Sp_{2n}(q)$	$q^n + 1$	$PSp_{2n}(q)$	$\frac{q^n+1}{(2,\ q+1)}$
$O^-_{2n}(q)$	$q^n + 1$	$\Omega^-_{2n}(q)$	$\frac{q^n+1}{(2,\ q+1)}$
$GU_n(q); n$ odd	$q^n + 1$	$PU_n(q); n$ odd	$\frac{q^n+1}{q+1}$
$SU_n(q); n$ odd	$\frac{q^n+1}{q+1}$	$PSU_n(q); n$ odd	$\frac{q^n+1}{(q+1)(n,\ q+1)}$

Table 3.1: Orders of Singer subgroups in the classical groups

Chapter 4

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 S in V, let $\widetilde{S} = \{\mathcal{P}(W) \mid W \in S\}$. Then $\widetilde{S}$ is called an *$(r-1)$-partial spread* in $\mathcal{P}(V)$. When S is an r-spread in V, $\widetilde{S}$ is called an *$(r-1)$-partial 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.

Spreads and partial spreads are very interesting geometric objects which have been widely studied. Partial spreads partitioning the set of all singular points of $\mathcal{P}(V)$ with respect to a quadratic form are also called spreads in a related polar geometry. They can also be considered as duals of ovoids. There are many well known results and unsolved problems related to them (See [7, 17, 34]). Spreads

have also been used in many other areas of mathematics. One of the classical methods of constructing projective planes uses spreads (See Kantor [19]). In fact a well known spread, the so called classical spread, was constructed by André [1] and independently by Bruck and Bose [6] in the context of projective planes.

The classical spreads have also been used to study finite groups. Dye has several interesting papers in this context [8, 9, 10]. We now describe the classical spread.

Suppose $V = \mathbb{F}_{q^{2n}}$ is the field of order q^{2n}, viewed as a vector space over $\mathbb{F}_q$. Let α be a primitive element of the field $\mathbb{F}_{q^{2n}}$. Consider the subfield $W = \mathbb{F}_{q^n}$ as a subspace of V. For every $x \in V$, define $Wx := \{wx \mid w \in W\}$. The following lemma can be easily verified.

Lemma 4.1. *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 n-spread in V.

Proposition 4.1. *Let $W_i = W\alpha^{(q^n-1)i} = \{w\alpha^{(q^n-1)i} \mid w \in W\},\ 0 \leq i \leq q^n$. Then it is easy to see that the spread S can also be described as follows: $S = \{W_i \mid 0 \leq i \leq q^n\}$.*

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 4.1. *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

Lemma 4.2. *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 4.1. Let* S *be an* r*-partial spread in* V*, which viewed projectively partitions* L*. Let* $W \in S$*,* $w \in L \cap \mathcal{P}(W)$ *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*.*

Proof. Let $w_1 \in L$. Then $w_1 \in \mathcal{P}(W_1) \cap L$ for some $W_1 \in S$. From condition (i) in the statement of the above lemma it follows that there exists a unique $a \in A$ such that $a(W) = W_1$. Let $w' = a^{-1}(w_1)$. Then clearly $w' \in W$ and from condition (ii) it follows that there exists a unique $b \in B$ such that $b(w) = w'$. Thus, $ab(w) = a(w') = w_1$. From this it follows that AB is sharply transitive on L with respect to w. Lemma 2.11 now implies that $[A,\ B,\ G_w]$ is an LS for G where G_w is a stabilizer of w in G. □

Chapter 5

Symplectic Groups

The main goal in this chapter is to show the existence of minimal logarithmic signatures for the symplectic groups $Sp_{2n}(q)$ and the projective symplectic groups $PSp_{2n}(q)$ for all $n \in \mathbb{N}$ and prime powers q. We summarize our method for the construction of MLS's for $Sp_{2n}(q)$ and $PSp_{2n}(q)$ in the following paragraph.

We consider a transitive action of $G = Sp_{2n}(q)$ on $\mathcal{P}(V)$, where V is a vector space of dimension $2n$. We fix $w \in \mathcal{P}(V)$ and describe the structure of the stabilizer in G of w, G_w. We then use Singer cycles in $Sp_{2n}(q)$ an $GL_n(q)$ to construct a subset $A \subseteq G$ which is sharply transitive on $\mathcal{P}(V)$ with respect to w. Then, Lemma 2.11 implies that $[A, G_w]$ is an LS for G. Finally we show that A and G_w have MLS's and therefore using Lemma 2.2 we have that G has an MLS. In a similar fashion we show that $PSp_{2n}(q)$ has an MLS.

We now describe the group G in a language suitable for our construction. Let $V = \mathbb{F}_{q^{2n}}$ be the field of order q^{2n} viewed as a $2n$-dimensional vector space over $\mathbb{F}_q$. For $y \in V$, we denote y^{q^n} by $\overline{y}$. For $s \in V$, T_s denotes the linear transformation $T_s : V \to V$ defined by $T_s(v_1) = sv_1$, for all $v_1 \in V$. Let α be a primitive element of the field $\mathbb{F}_{q^{2n}}$ and $x \in GL_{2n}(q)$ be the matrix corresponding to the linear transformation

T_α.

Define a bilinear form $f : V \times V \to \mathbb{F}_q$ by $f(x, y) = tr_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q} ax\overline{y} = \sum_{i=1}^{2n} (ax\overline{y})^{q^i}$, where $a \in \mathbb{F}^*_{q^{2n}}$ is such that $a + \overline{a} = 0$. Then, it can easily be seen that f is a non-singular alternating bilinear form (see proof of Theorem 5.6 in [16]). The group $G = Sp_{2n}(q)$ is the isometry group of the inner product space (V, f). Let W be the subspace of V defined by $W = \{x \in V \mid \overline{x} = x\}$. Then, $W = \mathbb{F}_{q^n}$. It is easy to verify that W is a maximal totally isotropic subspace of V. Let $\{e_1, \ldots, e_n\}$ be any basis of W with $e_1 = 1$. Then, using Lemma 3.2, we can form a symplectic basis $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ of V.

5.1 Structure of the Stabilizer Subgroup

Consider the ordered basis $\mathcal{A} = \{e_1, f_1, e_2, \ldots, e_n, f_2, \ldots, f_n\}$ of V. Let Y be the subspace of V generated by $\{e_2, \ldots, e_n, f_2, \ldots, f_n\}$ and $f' = f|_{Y \times Y}$. Then, the inner product space (Y, f') has a symplectic basis $\mathcal{A}' = \{e_2, \ldots, e_n, f_2, \ldots, f_n\}$. The matrix of the bilinear form f with respect to the basis $\mathcal{A}$ is given by

$$J'_{2n} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & J_{2n-2} \end{pmatrix},$$

where J_{2n-2} is the matrix of bilinear form f' with respect to the basis $\mathcal{A}'$.

Let $w = \langle e_1 \rangle$ and $g = (g_{ij})_{2n \times 2n} \in G_w$. Then $g(w) = w$. This implies that the first column of g is $(g_{11}, 0, \ldots, 0)^t$. From the fact that $g(e_i)$, $g(f_i) \in \langle 1 \rangle^\perp$ for $2 \leq i \leq n$, it follows that the second row of g is of the form $(0, g_{22}, 0, \ldots, 0)$. Now let $g_1 = g|_Y$. If we consider g_1 as a matrix with respect to the basis $\mathcal{A}'$, then we see

that ${g_1}^t\ J_{2n-2}\ g_1 = J_{2n-2}$. Hence $g_1 \in Sp_{2n-2}(q)$.

Using these facts and similar arguments given in [35] and [11], one can verify the following about the structure of G_w. The subgroup $G_w = U \cdot (L_1 \times L_2)$, where U is a p-group of order q^{2n-1} ,

$$L_1 = \left\{ \begin{pmatrix} I_2 & 0 \\ 0 & A \end{pmatrix} \mid A \in Sp_{2n-2}(q) \right\}, \text{ and } \quad L_2 = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & I_{2n-2} \end{pmatrix} \mid a \in \mathbb{F}_q^* \right\}.$$

Thus, $L_1 \cong Sp_{2n-2}(q)$ and L_2 is a cyclic group of order $q-1$. Now, the following lemma follows from Lemma 2.4.

Lemma 5.1. *Let $G := Sp_{2n}(q)$. Then, G_w has an LS $[U, L_1, L_2]$, where U is a p-group of order q^{2n-1}, $L_1 \cong Sp_{2n-2}(q)$, and L_2 is a cyclic group of order $q-1$.*

Now, $Z_G = \{\pm I_{2n}\}$. Thus, $|Z_G| = 2$ or 1, for q odd or even respectively. Let q be an odd prime power and $\eta : Sp_{2n}(q) \to PSp_{2n}(q)$ be the canonical homomorphism from $Sp_{2n}(q)$ onto $PSp_{2n}(q)$.

Let

$$K_1 := \left\{ \begin{pmatrix} I_2 & 0 \\ 0 & \pm I_{2n-2} \end{pmatrix} \right\} \quad \text{and} \quad K_2 := \left\{ \begin{pmatrix} \pm I_2 & 0 \\ 0 & I_{2n-2} \end{pmatrix} \right\}.$$

Then, $K_1 \trianglelefteq L_1$, $K_2 \trianglelefteq L_2$ and $K := K_1 \times K_2$ is an elementary abelian subgroup of G of order 4. Moreover, $Z_G \trianglelefteq K$ and $K \trianglelefteq L = L_1 \times L_2$. Let $M := K/Z_G$.

Further, we note that $(L/Z_G)/M \cong L/K \cong (L_1/K_1) \times (L_2/K_2)$. Hence, using

Lemma 2.4, it follows that $(L/Z_G)/M$ has an LS $[M_1, M_2]$, where M_1 and M_2 are subgroups of $(L/Z_G)/M$, $M_1 \cong L_1/K_1 \cong PSp_{2n-2}(q)$ and $M_2 \cong L_2/K_2$ is a cyclic group of order $(q-1)/2$.

Now, $U \cap Z_G = \{I_{2n}\}$. Hence, $U_1 := \eta(U)$ is a subgroup of G/Z_G and is isomorphic to U. Let $\overline{G} = PSp_{2n}(q)$. Then, using the facts that $[U, L]$ is an LS for G_w and $Z_G \leq L \leq G_w$, together with Lemma 2.7, we obtain that $\overline{G}_w = G_w/Z_G$ has an LS $[U_1, L/Z_G]$. Hence we have the following lemma.

Lemma 5.2. *Let* $G := Sp_{2n}(q)$ *and* $\overline{G} = PSp_{2n}(q)$.

(i) If q is a power of 2, then $\overline{G}_w = G_w$ has an LS $[U, L_1, L_2]$, where U is a 2-group of order q^{2n-1}, $L_1 \cong Sp_{2n-2}(q)$ and L_2 is a cyclic group of order $q-1$.

(ii) If q is an odd prime power, then, $\overline{G}_w$ has an LS $[U_1, L/Z_G]$, where U_1 is a p-group of order q^{2n-1} and L/Z_G has a normal subgroup M of order 2. Further, $(L/Z_G)/M = M_1 \times M_2$, where M_1, M_2 are subgroups of $(L/Z_G)/M$, $M_1 \cong PSp_{2n-2}(q)$ and M_2 is a cyclic group of order $(q-1)/2$.

5.2 Sharply Transitive Set A

We will again consider the symplectic basis $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ of V, as defined in the beginning of this chapter. Let $\mathcal{B} = \{e_1, \ldots, e_n, f_1, \ldots, f_n\}$. Then, the matrix of the bilinear form f with respect to the ordered basis $\mathcal{B}$ of V is given by $\left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$. From here through the end of this chapter, we consider the elements of $GL_{2n}(q)$ as linear transformations on V, with respect to the ordered basis $\mathcal{B}$.

Let $x_1 = x^{q^n-1} \in GL_{2n}(q)$ be the matrix corresponding to the linear transformation $T_{\alpha^{q^n-1}}$. Let $C \in GL_n(q)$ be the matrix corresponding to the linear transformation $T_{\alpha^{q^n+1}}|_W$ of W with respect to the ordered basis $\{e_1, e_2, \ldots, e_n\}$ of W. Let $x_2 = \begin{pmatrix} C & 0 \\ 0 & (C^t)^{-1} \end{pmatrix} \in GL_{2n}(q)$. We note that, since 1 is in W, $x_2\langle 1\rangle = \langle T_{\alpha^{q^n+1}}(1)\rangle = \langle \alpha^{q^n+1}\rangle$. Now by using the definition of the bilinear form f, one can easily prove that $x_1 = x^{q^n-1}$ preserves f. Also, $x_2^t J_{2n} x_2 = J_{2n}$ implies that x_2 preserves the bilinear form f. Thus, $x_1,\ x_2 \in G$.

Let $H_1 = \langle x_1\rangle,\ H_2 = \langle x_2\rangle$ be the cyclic subgroups of G generated by x_1 and x_2 respectively. Then it follows that H_1 is of order $q^n + 1$ and H_2 is of order $q^n - 1$. Therefore, H_1 is the Singer group of $Sp_{2n}(q)$ and H_2 is isomorphic to the Singer group of $GL_n(q)$. We now use these subgroups to construct a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$.

Let $H_3 = \langle x_2^{\frac{q^n-1}{q-1}}\rangle$ be the subgroup of H_2 of order $q-1$. Recall that the center Z_G of G is $\{I_{2n}, -I_{2n}\}$ if q is odd, and $\{I_{2n}\}$ if q is even. Let $\breve{H}_1 \in lt(H_1, Z_G)$ and $\breve{H}_2 \in lt(H_2, H_3)$. Then $|\breve{H}_1| = \frac{q^n+1}{2}$ if q is odd, and $|\breve{H}_1| = q^n + 1$ if q is even. Also, $|\breve{H}_2| = \frac{q^n-1}{q-1}$. Further, $\breve{H}_1$ and $\breve{H}_2$ can be chosen so that $\breve{H}_1 \cap \breve{H}_2 = \{1\}$ and both are cyclic sets. Thus, $|\breve{H}_1\breve{H}_2| = \frac{q^{2n}-1}{2(q-1)}$ if q is odd, and $|\breve{H}_1\breve{H}_2| = \frac{q^{2n}-1}{q-1}$ if q is even.

Lemma 5.3. *The subset $\breve{H}_1\breve{H}_2 = \{h_1h_2 \mid h_1 \in \breve{H}_1,\ h_2 \in \breve{H}_2\}$ of $Sp_{2n}(q)$ is a sharply transitive set on X with respect to $\langle 1\rangle$, where $X = \{\langle \alpha^{2i}\rangle \mid 0 \le i < \frac{q^{2n}-1}{2(q-1)}\}$ if q is odd, and $X = \mathcal{P}(V) = \{\langle \alpha^i\rangle \mid 0 \le i < \frac{q^{2n}-1}{q-1}\}$ if q is even.*

Proof. Suppose q is odd and $X = \{\langle \alpha^{2i}\rangle \mid 0 \le i < \frac{q^{2n}-1}{2(q-1)}\}$. Consider $\langle \alpha^{2i}\rangle$ for some $i,\ 0 \le i < \frac{q^{2n}-1}{2(q-1)}$. Let $m_1 = -1,\ m_2 = 1$. Now, there exist $h_1 \in \breve{H}_1,\ h_2 \in \breve{H}_2$ such

that $h_1\langle v\rangle = x_1^{m_1 i}\langle v\rangle$ for all $v \in V$ and $h_2\langle 1\rangle = x_2^{m_2 i}\langle 1\rangle$. Thus,

$$h_1h_2\langle 1\rangle = x_1^{m_1 i}x_2^{m_2 i}\langle 1\rangle = x_1^{-i}x_2^{i}\langle 1\rangle = x_1^{-i}\langle \alpha^{(q^n+1)i}\rangle = \langle \alpha^{(q^n-1)(-i)}\alpha^{(q^n+1)i}\rangle = \langle \alpha^{2i}\rangle.$$

Now, since $|\breve{H}_1\breve{H}_2| = \frac{q^{2n}-1}{2(q-1)} = |X|$, it follows that $\breve{H}_1\breve{H}_2$ is a sharply transitive set on X with respect to $\langle 1\rangle$.

Similarly, when q is even, by taking $m_1 = m_2 = q^n/\ 2$ in the above proof, we can show that $\breve{H}_1\breve{H}_2$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$. $\square$

Now, suppose q is odd. We recall that α is the primitive element of the field $\mathbb{F}_{q^{2n}}$. Define subspace W' of V by $W' = \alpha W = \{\alpha w \mid w \in W\}$. Then, clearly W' is a maximal totally isotropic subspace of V, and $\{e'_i := \alpha e_i \mid 1 \leq i \leq n\}$ forms a basis of W'. Now, using Lemma 3.2 we can find $f'_i,\ 1 \leq i \leq n$, such that $\mathcal{B}' = \{e'_1, \ldots, e'_n, f'_1, \ldots, f'_n\}$ forms a symplectic basis of V with respect to the bilinear form f. Let $r \in GL_{2n}(q)$ be the matrix corresponding to the linear transformation T' defined by $T'(v) = \sum_{i=1}^{n}(a_i e'_i + a_{i+n}f'_i)$ for all $v = \sum_{i=1}^{n}(a_i e_i + a_{i+n}f_i) \in V$. Then, from the definition of r and the basis $\mathcal{B}'$ of V, it follows that $r \in Sp_{2n}(q)$.

Now, using Lemma 5.3, we can show that $\breve{H}_1 r \breve{H}_2 = \{h_1 r h_2 \mid h_1 \in \breve{H}_1,\ h_2 \in \breve{H}_2\}$ is a sharply transitive set on X' with respect to $\langle 1\rangle$, where $X' = \{\langle \alpha^{2i+1}\rangle \mid 0 \leq i < \frac{q^{2n}-1}{2(q-1)}\}$. Let $M := \{1,\ r\} \subseteq Sp_{2n}(q)$. Then, from the above discussion and Lemma 5.3, we have the following theorem.

Theorem 5.1. *Let $\breve{H}_1, \breve{H}_2$ and M be the subsets of $Sp_{2n}(q)$ as defined above.*

(i) If q is odd, then the set $\breve{H}_1 M \breve{H}_2 = \{h_1 m h_2 \mid h_1 \in \breve{H}_1,\ m \in M,\ h_2 \in \breve{H}_2\}$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$.

(ii) If q is even, then the set $\breve{H}_1\breve{H}_2 = \{h_1h_2 \mid h_1 \in \breve{H}_1,\ h_2 \in \breve{H}_2\}$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$.

Now, $\breve{H}_1$ and $\breve{H}_2$ are cyclic sets. Thus, by Lemma 2.10 it follows that $\breve{H}_1$ and $\breve{H}_2$ have an MLS. Also, $|M| = 2$, a prime. Hence, we have the following lemma.

Lemma 5.4. *Let $\breve{H}_1, \breve{H}_2, M$ be as defined above. The sets $\breve{H}_1M\breve{H}_2$ and $\breve{H}_1\breve{H}_2$ have an MLS.*

5.3 MLS's for $Sp_{2n}(q)$ and $PSp_{2n}(q)$

We now have all the tools to prove the existence of MLS's for $Sp_{2n}(q)$ and $PSp_{2n}(q)$.

Theorem 5.2. *Let q be a prime power and $n \in \mathbb{N}$. Then, the groups $Sp_{2n}(q)$ and $PSp_{2n}(q)$ have an MLS.*

Proof. Suppose q is odd. We will first prove by induction on n that $Sp_{2n}(q)$ has an MLS. For $n = 2$, we know that $Sp_2(q) = SL_2(q)$. Since $SL_2(q)$ has an MLS [31], this implies that $Sp_2(q)$ has an MLS. Now let $n > 2$, $G = Sp_{2n}(q)$ and $w = \langle 1\rangle$. From Theorem 5.1, Lemma 5.4 and Lemma 2.11, it follows that G has an LS $[\breve{H}_1M\breve{H}_2, G_w]$, where $\breve{H}_1M\breve{H}_2$ has an MLS. Now, Lemma 5.1 implies that G_w has an LS $[U, L_1, L_2]$, where U, L_2 are solvable subgroups of G and $L_1 \cong Sp_{2n-2}(q)$. Thus, using Lemma 2.9, U and L_2 have an MLS. Using the induction hypothesis we can assume that $Sp_{2n-2}(q)$ has an MLS. Hence, by induction on n and using Lemma 2.2, it follows that $Sp_{2n}(q)$ has an MLS.

Similarly, when q is even, by replacing $\breve{H}_1M\breve{H}_2$ with $\breve{H}_1\breve{H}_2$ in the above proof, we can show that $Sp_{2n}(q)$ has an MLS.

Now, consider $PSp_{2n}(q)$. Suppose q is odd. We will again prove by induction on n that $PSp_{2n}(q)$ has an MLS. Let $\overline{G} = PSp_{2n}(q)$. Let $\overline{A} = \eta(\breve{H}_1 M \breve{H}_2)$, where $\eta : Sp_{2n}(q) \to PSp_{2n}(q)$ is the canonical homomorphism onto $PSp_{2n}(q)$. Then using Lemma 2.8, Lemma 5.4 and Theorem 5.1, we deduce that $\overline{A}$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to w, and that $\overline{A}$ has an MLS. Next, using Lemma 5.2(ii), $\overline{G}_w$ has an LS $[U_1, L/Z_G]$, where U_1 is a solvable subgroup of G and L/Z_G has a normal subgroup M of order 2. Further, $(L/Z_G)/M = M_1 \times M_2$, where M_1, M_2 are subgroups of $(L/Z_G)/M$, $M_1 \cong PSp_{2n-2}(q)$ and M_2 is a cyclic group of order $\frac{q-1}{2}$. By Lemma 2.9, U_1 and M_2 have an MLS. Also, by the induction hypothesis, we can assume that M_1 has an MLS. Thus, using Lemma 2.2, $(L/Z_G)/M$ has an MLS. Now, clearly M has an MLS. Hence, by taking $H = M$ and $G = L/Z_G$ in Lemma 2.5 and using Lemma 2.2, it follows that L/Z_G has an MLS. This implies, $\overline{G}_w$ has an MLS. Finally, using Lemma 2.11 and Lemma 2.2, and by induction on n, $\overline{G}$ has an MLS.

In the case when q is even, $PSp_{2n}(q) \cong Sp_{2n}(q)$, and therefore, $PSp_{2n}(q)$ has an MLS. □

Chapter 6

Orthogonal Groups of Minus type

In this chapter we construct MLS's for $O^-_{2n}(q)$ and $\Omega^-_{2n}(q)$, when q is even. We will use the classical spread described in Chapter 4 and Lemma 4.2 for constructing these minimal logarithmic signatures.

Let q be a power of 2 and $V = \mathbb{F}_{q^{2n}}$. As before, we consider V as a $2n$-dimensional vector space over $\mathbb{F}_q$. Recall that, for $y \in V$, $\overline{y}$ denotes y^{q^n}. We use the notations T_s and x as defined in the previous chapter. Define a bilinear map $f : V \times V \to \mathbb{F}_q$ by $f(x, y) = tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x\overline{y} + \overline{x}y) = \sum_{i=0}^{n-1}(x\overline{y} + \overline{x}y)^{q^i}$. The bilinear form f is symmetric and since q is even, f is also alternating. Define a quadratic form $Q : V \to \mathbb{F}_q$ by $Q(x) = tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x\overline{x}) = \sum_{i=0}^{n-1}(x\overline{x})^{q^i}$. It can easily be shown that the number of non-zero singular points in $\mathcal{P}(V)$ with respect to the quadratic space (V, Q) is $(q^n+1)(q^{n-1}-1)/(q-1)$ (see proof of Theorem 5.6 in [16]). From this it follows that the quadratic form Q is of minus type (Section 3.7.2 [35]). Thus, (V, Q) is a non-degenerate quadratic space with quadratic form Q of minus type and associated bilinear form f. Let G be the group of all isometries of (V, Q). Then, $G \cong O^-_{2n}(q)$ and G is a permutation group acting transitively on singular points [35, Section 3.7.2].

Now, $W = \mathbb{F}_{q^n}$ is an n-dimensional totally isotropic subspace of V. It can be

easily checked that W has an $(n-1)$-dimensional totally singular subspace W' (see Section 3.4.7 in [35]). Since Q is a quadratic form of minus type, it follows that W' is a maximal totally singular subspace of W. Now, we choose singular vectors $e_1,\ e_2,\ \ldots,\ e_{n-1} \in W'$ so that $\{e_1,\ e_2,\ \ldots,\ e_{n-1}\}$ is a basis for W'. Then we extend this basis to a symplectic basis $\mathcal{B} = \{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ for V such that $\{e_1,\ e_2,\ \ldots,\ e_n\}$ is a basis for W. We will write the elements of G as matrices with respect to the ordered basis $\mathcal{B}$.

We now define two cyclic subgroups of G which are very similar to the cyclic groups described in the previous chapter. Let $a = x^{q^n-1} \in GL_{2n}(q)$ be the matrix corresponding to the linear transformation $T_{\alpha^{q^n-1}}$. Let $C \in GL(W')$ be a generator of the Singer cyclic subgroup of $GL(W')$. Let $b \in GL_{2n}(q)$ be defined as follows.

$$b = \begin{pmatrix} C & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (C^t)^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Then it follows from [2] and [31] that $a, b \in G$. Let $A = \langle a \rangle,\ B = \langle b \rangle$ be the cyclic subgroups of G generated by a and b respectively. Then, A is of order $q^n + 1$ and B is of order $q^{n-1} - 1$. We note that the cyclic subgroup A is the same as the cyclic subgroup H_1 defined in the previous chapter.

Let $B_1 = \langle b^{\frac{q^{n-1}-1}{q-1}} \rangle$ be the subgroup of order $q-1$ of B . Since B_1 is a cyclic subgroup of the cyclic group B, $\breve{B} \in lt(B, B_1)$ can be chosen so that $\breve{B}$ is a cyclic set. Then from Lemma 2.10 it follows that A and $\breve{B}$ have MLS's.

We will now consider the classical spread described in Proposition 4.1, $S =$

$\{W_i \mid 0 \leq i \leq q^n\}$. Recall that, $W_i = W\alpha^{(q^n-1)i} = \{w\alpha^{(q^n-1)i} \mid w \in W\}$. We know that S partitions the set of all points of $\mathcal{P}(V)$. Now, with respect to the bilinear form f, each of the W_i's is an n-dimensional totally isotropic subspace. Also, it can be shown that with respect to the quadratic form Q, for each $i,\ 0 \leq i \leq q^n,\ W_i$ has an $(n-1)$-dimensional totally singular subspace W_i'. Let $S' = \{W_i' \mid 0 \leq i \leq q^n\}$. Then, the partial spread S' partitions the set of all singular points of $\mathcal{P}(V)$.

Now, Lemma 3.1(ii) in [31] implies that the group A is sharply transitive on S' with respect to W'. Also, from the definition of B, it is clear that B is isomorphic to the Singer cyclic subgroup of $GL_{n-1}(q)$. Thus, $\breve{B}$ is sharply transitive on $\mathcal{P}(W')$ with respect to $\langle e_1 \rangle$ (Lemma 6.1, [31]). Hence we have the following lemma.

Lemma 6.1. *Let $A, \breve{B} \subseteq O_{2n}^-(q)$, S' be the partial spread, and W' the subspace of V as defined above. Let $w = \langle e_1 \rangle$. Then,*

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

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

We are now ready to prove that the orthogonal group $O_{2n}^-(q)$ with q even has an MLS.

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

Proof. Let $G = O_{2n}^-(q)$. We will use induction on n to show that G has an MLS. First we observe that $O_2^-(q) \cong D_{q+1}$, a dihedral group of order $2(q+1)$. Thus using Lemma 2.9, $O_2^-(q)$ has an MLS. Now assume that $n > 1$. We apply Lemma 4.2 with $G = O_{2n}^-(q),\ A = A,\ B = \breve{B},\ w = \langle e_1 \rangle$ where $A, \breve{B} \subseteq G$ and $e_1 \in W'$ are as defined

above. We also take L to be the set of all singular points of $\mathcal{P}(V)$. From Lemma 6.1 it follows that conditions (i) and (ii) of Lemma 4.2 are satisfied. Thus, $[A,\ \breve{B},\ G_w]$ is an LS for G. From Section 3.7.4 in [35], the stabilizer G_w is a semi-direct product of a 2-group of order q^{2n-2} and $GL_1(q) \times O^-_{2n-2}(q)$. Now from Lemma 2.9 it follows that 2-groups and $GL_1(q)$ have MLS's. Further, by the induction hypothesis, we can assume that $O^-_{2n-2}(q)$ has an MLS. Thus, G_w has an MLS. Also, as noted above, the sets A and $\breve{B}$ have MLS's. Hence, using Lemma 2.2, G has an MLS. □

We now show that an MLS exists for each of the groups, $\Omega^-_{2n}(q),\ n \in \mathbb{N},\ q$ even.

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

Proof. Let $G = O^-_{2n}(q)$ and G' be the commutator subgroup of G. Then $G' \cong \Omega^-_{2n}(q)$. Consider the sets $A, \breve{B} \subseteq G$ and elements $b \in G$ and $e_1 \in W'$ as defined above. It is easy to verify that $A \leq G'$ (see [3], for example). Now, an element g in $O^-_{2n}(q)$ is in $\Omega^-_{2n}(q)$ if and only if the rank of the matrix $I_{2n} + g$ is even (see Section 3.8.1 in [35]). It is easy to see that the matrix b satisfies the above condition. Thus, $b \in G'$. Hence, $\breve{B} \subseteq G'$.

Now, G' acts on $\mathcal{P}(V)$. Thus, just as in the previous theorem $[A,\ \breve{B},\ G'_w]$ is an LS for G' where $w = \langle e_1 \rangle$. Also, the stabilizer G'_w is a semi-direct product of a 2-group of order q^{2n-2} and $GL_1(q) \times \Omega^-_{2n-2}(q)$ (Proposition 4.1.20 in [20]). From these facts and by using the same arguments as used to prove Theorem 6.1 above, we see that G' has an MLS. □

Chapter 7

Unitary Groups

In this chapter we apply the methods we have developed to the unitary groups $GU_n(q)$. The basic ideas are very similar to those used in the previous chapter. We consider only the case when n is odd and q is even. We consider the classical spread and action of the unitary group on the set of all vectors of norm 1, with respect to the conjugate-symmetric sesquilinear form. Using the partition of this set, induced by the classical spread, we obtain a logarithmic signature for the unitary group $GU_n(q)$, in which all the blocks have MLS's except for one block which is isomorphic to $GU_{n-1}(q)$. Thus we reduce the problem of constructing an MLS for $GU_n(q)$ to a case in smaller dimension.

Let n be odd and q be a power of 2. Let $V = \mathbb{F}_{q^{2n}}$ be the field of order q^{2n}. Now, V can be viewed as an n-dimensional vector space over $\mathbb{F}_{q^2}$ and $2n$-dimensional vector space over $\mathbb{F}_q$. We will use notations $\overline{y}, \alpha$ and T_s as defined in Chapter 5. Define a map $f : V \times V \to \mathbb{F}_{q^2}$ by $f(x,y) = tr_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^2}} x\overline{y} = \sum_{i=0}^{n-1} (x\overline{y})^{q^{2i}}$. It can be easily shown that f is a non-singular conjugate-symmetric sesquilinear form (See Hestenes [16], where he has extensively used this form). Let Y be the set of all anisotropic vectors of norm 1 in V, with respect to the form f. Let G be the isometry group of

the inner product space (V, f). Then $G \cong GU_n(q)$.

Consider, the subspace $W = \mathbb{F}_{q^n}$ of the vector space V over $\mathbb{F}_q$. Thus, $W = \{x \in V \mid \overline{x} = x\}$. Now, when we restrict the map f to W, we have the following.

$$f|_W(x, y) = \sum_{i=0}^{n-1} (x\overline{y})^{q^{2i}} = \sum_{i=0}^{n-1} (xy)^{q^{2i}} = tr_{\mathbb{F}_{q^n}/\mathbb{F}_q} xy$$

Lemma 7.1. *Let f, W and Y be as defined above. Then, $|W \cap Y| = q^{n-1}$. That is, with respect to the conjugate-symmetric sesquilinear form f, the number of anisotropic vectors in W of norm 1 is q^{n-1}.*

Proof. Define a map $Q : V \to \mathbb{F}_{q^2}$ by $Q(v) = f(v, v)$. Let $Q_1 = Q|_W$. By the definition of f, it follows that $Q_1 \neq 0$. Since q is even, Q_1 is also a linear map. Thus, $Q_1(W) = \mathbb{F}_q$ and $W' := ker(Q_1)$ is an $(n-1)$-dimensional subspace of W. Therefore, $|W \setminus W'| = q^n - q^{n-1} = q^{n-1}(q-1)$. From this we can conclude that $|W \cap Y| = q^{n-1}$. □

Using the proof of the lemma above, we can choose an ordered basis $\mathcal{B} = \{e_1, e_2, \ldots, e_m, w, f_m, f_{m-1}, \ldots, f_1\}$ of V satisfying the conditions given in Lemma 3.1, and such that $f_1, w \in W$. Then the matrix of the conjugate-symmetric sesquilinear form with respect to the basis $\mathcal{B}$ is given by

$$J_n = \begin{pmatrix} 0 & 0 & \ldots & 1 \\ \vdots & \vdots & \iddots & \vdots \\ 0 & 1 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{pmatrix}.$$

Now, consider the classical spread $S = \{W_i \mid 0 \leq i \leq q^n\}$ in V over $\mathbb{F}_q$ as

described in Proposition 4.1. Recall that $W_i = \{w\alpha^{(q^n-1)i} \mid w \in W\}$ where α is a primitive element of the field $\mathbb{F}_{q^{2n}}$. Let $Y_i = Y \cap W_i$ for $0 \leq i \leq q^n$. Clearly $S' = \{Y_i \mid 0 \leq i \leq q^n\}$ partitions the set Y.

Let x_1 be the matrix of the linear transformation $T_{\alpha^{q^n-1}}$ with respect to the basis $\mathcal{B}$. It is easy to check that x_1 preserves f. Thus $x_1 \in G$. Let $H_1 = \langle x_1 \rangle$ be the cyclic subgroup of G generated by x_1. Then, H_1 is of order $q^n + 1$. The following lemma is an immediate consequence of the definition of S' and the classical spread S.

Lemma 7.2. *Let H_1 and S' be as defined above. Then, H_1 is sharply transitive on S'.*

Let ϕ be the automorphism of the field $\mathbb{F}_{q^2}$ defined by $\phi(x) = x^q$. For a matrix $A = (a_{ij})$, the matrix A^ϕ is defined by $A^\phi = (\phi(a_{ij})) = (a_{ij}^q)$. Let z be an $(n-2)$ - dimensional column vector with entries in $\mathbb{F}_q$ and $s \in \mathbb{F}_q$. Define the matrix $x_{z,s} \in GL_n(q^2)$ as follows,

$$x_{z,s} = \begin{pmatrix} 1 & (z^\phi)^t J_{n-2} & s - (z^\phi)^t \ J_{n-2} \ z \\ 0 & I_{n-2} & z \\ 0 & 0 & 1 \end{pmatrix}.$$

Since $(x_{z,s}^\phi)^t J_n x_{z,s} = J_n$, it follows that $x_{z,s} \in G$. For more details about this matrix, see Chapter 8 in [11]. Now, let H_2 be the subgroup of G defined by, $H_2 = \{x_{z,s} \mid z^t \in (\mathbb{F}_q)^{n-2},\ s \in \mathbb{F}_q\}$. Clearly, H_2 is a subgroup of G of order q^{n-1}.

Lemma 7.3. *Let $Y_0 \subseteq \mathbb{F}_{q^n}, H_2, w$ and f_1 be as defined above. Then, H_2 is sharply transitive on Y_0 with respect to $w + f_1$.*

Proof. Let $w' = w + f_1$. Since $H_2 \leq G$, it follows that $hw' \in Y_0$ for all $h \in H_2$.

Now suppose, $h, h' \in H_2$. Then $h = x_{z,s}, h' = x_{z',s'}$ for some $z^t, z'^t \in (\mathbb{F}_q)^{n-2}$ and $s, s' \in \mathbb{F}_q$. Then, by calculating hw' and $h'w'$ one can easily check that if $hw' \neq h'w'$, then at least one of the following is true: $z \neq z'$ or $s \neq s'$. This implies $h \neq h'$. This proves the lemma. □

We will now use Lemma 7.2 and Lemma 7.3 to show that when n is odd and q a power of 2, $GU_n(q)$ has an MLS if $GU_{n-1}(q)$ has an MLS.

Theorem 7.1. *Let n be odd and q be even. Then,*

(i) the group $GU_n(q)$ has an LS $[H_1,\ H_2,\ H_3]$ where H_1 a cyclic subgroup of $GU_n(q)$ and H_2 a 2-group are as defined above and $H_3 \cong GU_{n-1}(q)$.

(ii) $GU_n(q)$ has an MLS if $GU_{n-1}(q)$ has an MLS.

Proof. We will consider $G := GU_n(q)$ as a permutation group acting on the set Y of all anisotropic vectors of norm 1. Lemma 7.2 and Lemma 7.3 imply that the subset $H_1H_2 \subseteq G$ acts sharply transitively on Y with respect to w', where $H_1, H_2 \leq G$ and w' are as defined above.

From the results given in Section 3.6.2 of [35] about the stabilizer of a one dimensional anisotropic subspace, it follows that stabilizer $G_{w'}$ in G of w' is a subgroup isomorphic to $GU_{n-1}(q)$. Now by applying Lemma 2.11, we have that $[H_1, H_2, G_{w'}]$ is an LS for G. This proves the first part of the theorem.

Now since H_1 is cyclic and H_2 is a 2-group, using Lemma 2.9 it follows that each of H_1 and H_2 has an MLS. Thus the group $GU_n(q)$ has an MLS, if $GU_{n-1}(q)$ has an MLS. □

In this thesis we have only considered $GU_n(q)$. If we consider $PSU_n(q)$, perhaps methods similar to those we used for $PSL_n(q)$ in [31] can be used to modify the above construction for that case. When q is odd, one can prove using the classical spread and similar methods as above, that the number of anisotropic vectors of norm 1 is the same. The subgroup of matrices we have used above for showing sharp transitivity can also be constructed in a similar way. Thus it is quite possible that the these methods can be used to give similar results in these cases also.

In fact our method of obtaining MLS's by using a decomposition of the group into sharply transitive sets and stabilizers of suitable geometric objects like spreads is quite widely applicable. It can possibly be used to get MLS's for all finite simple groups.

Bibliography

[1] Johannes André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.*, 60:156–186, 1954.

[2] László Babai, Péter P. Pálfy, and Jan Saxl. On the number of p-regular elements in finite simple groups. *LMS J. Comput. Math.*, 12:82–119, 2009.

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

[4] Simon R. Blackburn, Carlos Cid, and Ciaran Mullan. Cryptanalysis of the MST_3 public key cryptosystem. *J. Math. Cryptology*, 3:321–338, 2009.

[5] 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.

[6] R. H. Bruck and R. C. Bose. The construction of translation planes from projective spaces. *J. Algebra*, 1:85–102, 1964.

[7] J. De Beule, A. Klein, K. Metsch, and L. Storme. Partial ovoids and partial spreads of classical finite polar spaces. *Serdica Math. J.*, 34(4):689–714, 2008.

[8] R. H. Dye. Partitions and their stabilizers for line complexes and quadrics. *Ann. Mat. Pura Appl. (4)*, 114:173–194, 1977.

[9] R. H. Dye. Maximal subgroups of finite orthogonal groups stabilizing spreads of lines. *J. London Math. Soc. (2)*, 33(2):279–293, 1986.

[10] R. H. Dye. Spreads and classes of maximal subgroups of $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$. *Ann. Mat. Pura Appl. (4)*, 158:33–50, 1991.

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

[12] María Isabel González Vasco, Angel L. Pérez del Pozo, and Pedro Taborda Duarte. A note on the security of MST_3. *Designs, Codes and Cryptography*, 55:189–200, 2010. 10.1007/s10623-010-9373-0.

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

[14] 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).

[15] G. Hajós. Többméretű terek befedése kockaráccsal. *Mat. Fiz. Lapok*, 45:171–190, 1938.

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

[17] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

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

[19] William M. Kantor. Spreads, translation planes and Kerdock sets. I. *SIAM J. Algebraic Discrete Methods*, 3(2):151–165, 1982.

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

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

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

[27] Spyros S. Magliveras, Pavol Svaba, Tran van Trung, and Pavol Zajac. On the security of a realization of cryptosystem MST_3. *Tatra Mt. Math. Publ.*, 41:65–78, 2008. TATRACRYPT '07.

[28] Hermann Minkowski. *Geometrie der Zahlen.* Teubner, Leipzig, 1896.

[29] Hermann Minkowski. *Diophantische Approximationem.* Teubner, Leipzig, 1907.

[30] Nidhi Singhi. *On the Minimal Logarithmic Signature Conjecture.* PhD thesis, Florida Atlantic University, 2011.

[31] 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.

[32] Pavol Svaba and Tran van Trung. Public key cryptosystem MST_3: cryptanalysis and realization. *J. Math. Cryptology*, 4:271–315, 2010.

[33] Sándor Szabó. *Topics in factorization of abelian groups.* Birkhäuser Verlag, Basel, 2004.

[34] J. A. Thas. Ovoids and spreads of finite classical polar spaces. *Geom. Dedicata*, 10(1-4):135–143, 1981.

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