Minimal Logarithmic Signatures for Finite Groups of Lie Type

Nidhi Singhi, Nikhil Singhi, Spyros Magliveras

April 20, 2009

Abstract

New methods are developed to construct algorithmically good logarithmic signatures for affine algebraic groups, using Singer subgroups. The well known conjecture about the existence of minimal logarithmic signature (MLS) for simple groups is shown to be true for some finite simple groups of Lie type.

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 $l(\alpha) = \sum_{i=1}^{s} |A_i|$.

Logarithmic signatures were first defined by Magliveras in [15] where cryptosystem PGM was proposed using LS's. Later, Magliveras, Stinson and Tran van Trung proposed cryptosystems MST_1, MST_2, and Magliveras, Lempken, Tran van Trung and Wei proposed cryptosystem MST_3 using logarithmic signatures and *covers* [16, 17]. For some interesting papers studying attacks on MST_1 and MST_2, see [4, 8].

Much earlier, logarithmic signatures were also studied, in a different context, by group theorists, who called them *group factorizations*. Perhaps Hajós was the first person to define factorizations for finite abelian groups in 1938 [10]. He used them as a tool to study the well-known Minkowski's conjecture. 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 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 [20]. 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 [8] that the length $l(\alpha)$ of a logarithmic signature α satisfies the following inequality.

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

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

An LS for which the above lower bound is sharp is called a ***minimal logarithmic signature (MLS)*** for the group G. Such optimal length logarithmic signatures are useful from both a cryptographic and a group theoretical point of view. It was observed in [9] 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 [8] that MLS's exist for all finite solvable groups and all symmetric groups S_n. It was also shown in [16] that the alternating groups A_n have MLS's. In [9] it is proved that that minimal logarithmic signatures exist for all groups of order less than 175,560. In [14], Lempken and Tran van Trung exhibit an interesting new tool to construct minimal logarithmic signatures with which they 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 [13] constructed minimal logarithmic signatures for sporadic groups $J_1, J_2, HS, M^cL, He, Co_3$.

These results make the following conjecture plausible.

Conjecture 1.2. *(MLS Conjecture) Every finite simple group has a minimal logarithmic signature.*

Before discussing the scope and content of this paper, we present in summary the classes of finite simple groups. We have taken the following classification material from Wilson [22].

1.3 Classes of finite simple groups

(i) cyclic groups of prime order

(ii) alternating group A_n, $n \geq 5$

(iii) classical groups:

  (a) linear: $PSL_n(q)$, $n \geq 2$, except $PSL_2(2)$ and $PSL_2(3)$

  (b) unitary: $PSU_n(q)$, $n \geq 3$, except $PSU_3(2)$

  (c) symplectic: $PSp_{2n}(q)$, $n \geq 2$, except $PSp_4(2)$

  (d) orthogonal: $P\Omega_{2n+1}(q)$, $n \geq 3$, q odd; $P\Omega^+_{2n}(q)$, $n \geq 4$; $P\Omega^-_{2n}(q)$, $n \geq 4$

  where q is a power of a prime

(iv) exceptional groups of Lie type

(v) the 26 sporadic simple groups

In this paper, we first define a *logarithmic signature* (LS) for an arbitrary subset A of a group G. This general definition is then used as a tool to study the MLS conjecture. Our interest is in developing general methods of constructing MLS's for simple groups and for groups in general. We then create MLS's for the projective special linear groups $PSL_n(q)$ and the projective symplectic groups $PSp_{2n}(q)$ for all $n \in \mathbb{N}$ and prime powers q. In the process we also construct MLS's for the groups $GL_n(q)$, $PGL_n(q)$, $SL_n(q)$ and $Sp_{2n}(q)$. The blocks of the LS's which we create are essentially obtained from Singer subgroups of the classical groups or their subgroups. Our methods are general and they may prove sufficiently strong as tools for constructing MLS's for all finite simple groups. Some of these aspects will be discussed in a subsequent communication [19].

The theory of algebraic groups provides tools to study classical and exceptional groups of Lie type which together are called Finite groups of Lie type. In fact much of the structure of these groups can be described using the language of algebraic groups [5, 22]. For some basic definitions such as *affine varieties*, *morphisms of varieties*, *affine algebraic groups*, the *Zariski topology*, *split BN-pairs*, see Chapters 1 and 2 of [5] for details. We do not need too many terms from algebraic group theory or Lie group theory but we do need a few basic definitions and basic results which are described in Section 2.

One can also use the Weyl group of an algebraic group to construct LS's. We had initially started with such a construction. Our construction of an LS using Weyl groups is given in [18].

Our method of creating LS's and MLS's for classical groups, as described in Sections 6, 7 and 8, actually also produces a spread in the corresponding projective or polar space. Spreads have been widely studied in various geometries and designs (see [12] for definitions and basic results). One can see that the methods described in this paper give rise to a much more general way of constructing logarithmic signatures for finite groups of Lie type using geometric objects like ovoids, spreads etc. in the corresponding geometry. This will be discussed in a subsequent paper [19].

2 Preliminaries

In this section, we describe some basic concepts for groups, permutation groups, algebraic groups, needed for our construction of Logarithmic Signatures (LS). Material for algebraic groups is mainly taken from Carter [5], Garrett [7] and Wilson [22]. Other basic material in this section is taken from Artin [1] and Biggs and White [3].

A *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 $stab_G(x)$ of G, defined by $stab_G(x) = \{g \in G \mid gx = x\}$. We may also denote $stab_G(x)$ by $stab(x)$.

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 the set $hAh^{-1} = \{hah^{-1} \mid a \in A\}$ is 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 paper we essentially consider only sharply transitive sets with respect to a given $x \in X$.

We now give, some basic definitions and notation related to groups and vector spaces. Let G be a finite group and H be a subgroup of G. We use the notation $H \leq G$ whenever H is a subgroup of G. If H is a normal subgroup of G, we write $H \trianglelefteq G$. Suppose $H \trianglelefteq G$, then $\eta : G \to G/H$ will denote a canonical homomorphism from G onto G/H. We will denote the center of G by Z_G. 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 $A = \{x^i \mid 1 \leq i \leq m\}$ 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 semidirect product of A by B.

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 and denote it by ***lt(G,H)***. We note that an $lt(G, H)$ is not unique. Similarly, we say A is an ***rt(G, H)***, when A is a right transversal of H in G.

Let $\mathbf{K}$ be an algebraically closed field. Let V be a vector space of finite dimension n, over the field K. For $v_1 \in V$, we denote by $\langle v_1 \rangle$, the one-dimensional subspace generated by v_1. $\mathcal{P}(\mathbf{V})$ denotes a projective space on V, i.e., the set of all one dimensional subspaces of V.

We denote the group of all non-singular K-linear transformations of V by $GL(V)$. We choose a suitable

ordered basis $\mathcal{B} = \{e_1, e_2, \ldots, e_n\}$ of V. Let $x \in V, x = \sum_{i=1}^{n} x_i e_i$, $x_i \in K$. Then, we think of x also as the column vector $x = (x_1, x_2, \ldots, x_n)^t$. The vector e_i is thus identified with the column vector $e_i = (0, \ldots, 1, \ldots, 0)^t$, where the term in the i^{th} row is 1 and all other terms are 0, $1 \leq i \leq n$. Thus, the vector space V is identified with the vector space K^n, of all column vectors of length n. Then, each element of $GL(V)$, can be considered as an $n \times n$ matrix over K, acting on column vectors. Thus the group $GL(V)$ is isomorphic to the group $\boldsymbol{GL_n(K)}$ of all non-singular $n \times n$ matrices. We denote the $n \times n$ identity matrix by I_n.

We now give some basic definitions and results which we need for our construction of MLS's. See Section 4 and Section 5 for details of the groups and some basic results we consider in this paper.

Let G be an affine algebraic group. Then by a well-known result from Section 1.2 [5], we know that every affine algebraic group over an algebraically closed field is isomorphic to a closed subgroup of $GL_n(K)$, for some n and conversely. Thus, G is a subgroup of $GL_n(K)$ and acts as a permutation group on $V \setminus \{0\}$ in a natural way. A ***flag*** is defined to be a chain of subspaces ordered by inclusion (Page 102, [7]). ***Parabolic subgroups*** of G are the stabilizers of suitably chosen flags. Consider $x \in G$, then x is said be ***unipotent*** if all its eigenvalue are 1. It can be shown (Page 11, [5]) that this definition is independent of the embedding of G into $GL_n(K)$. A ***unipotent group*** is an affine algebraic group each of whose elements are unipotent.

We now give the definition of finite groups of Lie type using the Frobenius map on a *connected reductive group* [5]. The following remark will be used to define a reductive group. The reader can choose to skip the following, as the families of finite groups of Lie type that we consider in this paper will be defined separately in Section 4 in detail.

Remark 2.1. *(See Section* 1.8*, [5]) Suppose G is a connected affine algebraic group. Then, the set of all closed connected unipotent normal subgroups of G has a unique maximal element called the unipotent radical $R_u(G)$ of G.*

A connected affine algebraic group G is said to be *reductive* if $G \neq 1$ and $R_u(G) = 1$.

Let G be a connected reductive group over an algebraically closed field of characteristic p. Then, we know that G is isomorphic to a closed subgroup of $GL_n(K)$ for some n. Let $q = p^e$, $e \geq 1$ and F_q be the map of $GL_n(K)$ into itself given by $F_q : (a_{ij}) \rightarrow (a_{ij}^q)$. The map F_q is a homomorphism of $GL_n(K)$ into itself. A homomorphism $F : G \rightarrow G$ is called a *standard Frobenius map*, if there exists an injective homomorphism $i : G \rightarrow GL_n(K)$ for some n, such that $i(F(g)) = F_q(i(g))$ for some $q = p^e$ and for all $g \in G$. A homomorphism $F : G \rightarrow G$ is called a *Frobenius map* if some power of F is a standard Frobenius map. If $F : G \rightarrow G$ is a Frobenius map, define G^F as follows.

$$G^F = \{g \in G | F(g) = g\}$$

G^F is a finite subgroup of G. Following [5], we call, finite groups G^F arising from a Frobenius map $F : G \rightarrow G$ on a connected reductive group G, *finite groups of Lie type*.

3 LS and MLS

From now on, we assume that group G is finite. We now give few basic definitions and lemmas related to Logarithmic Signatures and Minimal Logarithmic Signatures.

Let $A \subseteq G$. 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 a set*** A, if every $a \in A$ can be uniquely written as a product $a = a_1 a_2 \cdots a_s$ where $a_i \in A_i$. Suppose $|A| = \prod_{j=1}^{k} {p_j}^{m_j}$ where p_j's are prime. If $l(\alpha) = \sum_{j=1}^{k} m_j p_j$ then α is said to be a ***Minimal Logarithmic Signature (MLS) for a subset*** A of G.

Following remark easily follows from [14] and the above definition of an MLS.

Remark 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. 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 basic results about logarithmic signatures that we will use in the later sections. The results can be derived easily from the definitions. Proofs are also given for most of these results in [13],[16] and [8], for the case of LS for groups. It is easy to see that these proofs can be extended to LS for a subset of a group.

Remark 3.2. *Let $A \subseteq G$. Suppose $[A_1, A_2, \ldots, A_r]$ is an LS for A and $[B_{i1}, \ldots, B_{ik_i}]$ is an LS for each A_i, $0 \leq i \leq r$. Then $\alpha = [B_{i1}, \ldots, B_{ik_1}, \ldots, B_{r1}, \ldots, B_{rk_r}]$ is an LS for A.*

Remark 3.3. *Let $H \leq G$ and A be an $lt(G, H)$. Then $[A, H]$ is an LS for G.*

Remark 3.4. *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.*

Remark 3.5. *Suppose $H \trianglelefteq G$ and $[B'_1, B'_2, \ldots, B'_k]$ is an LS for G/H. For each $i \in \{1, \ldots, k\}$, let $B_i \subseteq G$ be such that $\eta(B_i) = B'_i$ and $|B_i| = |B'_i|$. Then,*

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

Remark 3.6. *Let $H \trianglelefteq G$ and $[B_1, B_2, \ldots, B_k, H]$ be an LS for G. Then, $[B'_1, B'_2, \ldots, B'_k]$ is an LS for G/H, where $B'_i = \eta(B_i)$, for all $1 \leq i \leq k$.*

Remark 3.7. *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.*

Remark 3.8. *Let $H \trianglelefteq G$ and $A \subseteq G$ be such that $aH \neq bH$ for all $a, b \in A$, $a \neq b$. Let $A' = \eta(A)$. Suppose $[A_1, A_2, \ldots, A_k]$ is an LS for A. Let $B_i = \eta(A_i) \subseteq G/H$, for all $1 \leq i \leq k$. Then $[B_1, B_2, \ldots, B_k]$ is an LS for A'.*

Remark 3.9. *[8] If G is solvable, then G has an MLS.*

We now describe an MLS for a cyclic set.

Lemma 3.10. *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 $S = \{x^i | 0 \leq i < s\}$. Then S has an MLS, $\gamma = [A_1, A_2, \ldots, A_k]$, satisfying the following property.*

$$\text{For any list } [j_1, \ldots, j_k], \text{ such that } x^{j_i} \in A_i,\ 1 \leq i \leq k,\ \sum_{i=1}^{k} j_i < s \tag{3.10.1}$$

Proof. Suppose $s = p_1p_2 \ldots p_k$ is the prime factorization for s. Then, define $A_1 = [1, x, \ldots, x^{p_1-1}]$ and $A_i = [1, x^{p_1p_2\ldots p_{i-1}}, x^{2p_1p_2\ldots p_{i-1}}, \ldots, x^{(p_i-1)p_1p_2\ldots p_{i-1}}]$ for all $2 \leq i \leq k$. Now, given a, $1 \leq a < s$, there exists $s_1, s_2, \ldots, s_k \in \mathbb{Z}$, $0 \leq s_i < p_i$ for $1 \leq i \leq k$, such that $a = \sum_{i=1}^{k} \left(\prod_{j=1}^{i-1} p_j \right) s_i$. Therefore,

$$x^a = \prod_{i=1}^{k} x^{\left(\prod_{j=1}^{i-1} p_j\right) s_i}.$$

Now, by definition of A_i, it follows that $x^{\left(\prod_{j=1}^{i-1} p_j\right) s_i} \in A_i$ for all $1 \leq i \leq k$. Thus, x^a has a factorization, $x^a = a_1 a_2 \dots a_k$, $a_i \in A_i$ 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 $\gamma = [A_1, A_2, \dots, A_k]$ is an MLS for S. Finally, using the fact that $\sum_{i=1}^{k} \left(\prod_{j=1}^{i-1} p_j\right)(p_i - 1) = s - 1$, it follows that, γ satisfies (3.10.1).

□

Lemma 3.11. *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 $P = stab_G(x)$. 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 Orbit-Stabilizer Theorem, it follows that $|G| = |A| \cdot |P|$. Hence, $[A, P]$ is an LS for G.

□

The following remark essentially follows from the discussion about *parabolic subgroups and the Levi decomposition* of algebraic groups as well as finite groups of Lie type given on pages 62-63 in Carter's Book [5].

Remark 3.12. *Let G be a finite group of Lie type and P be 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 the complement L is a subgroup of P called the standard Levi subgroup of P.*

Now using the above Remark 3.12 and Remark 3.4 we get the following.

Remark 3.13. *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 called the unipotent group, and L is the standard Levi subgroup of P.*

We note that the standard Levi subgroup L of a finite group of Lie type G itself has a decomposition of similar type as that of Remark 3.12. Thus the above remark gives us a good inductive tool to create logarithmic signatures for the finite groups of Lie type. In the sections that follow, we describe parabolic subgroups, sharply transitive sets and standard Levi subgroups for these groups and the corresponding simple groups. We then use the above remark as a tool to create MLS's and other interesting LS's for such groups. We plan to explore the MLS conjecture for the remaining classical groups and other groups of Lie type in the subsequent paper.

4 Inner-product spaces

In this section, we describe basic concepts related to inner-product spaces and the symplectic group $Sp_{2n}(q)$ which we will need in the later sections.

Let $i, n \in \mathbb{N}$ be such that $i|n$ and 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 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 $f(u, \lambda v + w) = \lambda f(u, v) + f(u, w)$, $\lambda \in K$, $u, v \in V$. The pair (V, f) is called the *inner-product space.*

A vector $v \in V$ is said to be an ***isotropic vector*** if $f(v,v) = 0$. For a subspace W of V, $W^{\perp} = \{v \in V \mid f(v,w) = 0 \text{ for all } w \in W\}$. W is said to be an ***isotropic subspace*** of V if $W \subseteq W^{\perp}$.

Let f be any bilinear form. 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. 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 $\{e_1, \ldots, e_n\}$.

A form f is said to be *non-singular* if $V^{\perp} = \{0\}$. 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. $g^t J_n g = J_n$.

Bilinear form f is of the following three types. Bilinear form is *symmetric* if $f(u,v) = f(v,u)$, *skew-symmetric* if $f(u,v) = -f(v,u)$ and *alternating* if $f(v,v) = 0$. It is easy to check that an alternating bilinear form is always skew-symmetric. In this paper, we will be only interested in the alternating bilinear form.

Remark 4.1. *Let (V, f) be an inner product space. If f is a non-singular alternating bilinear form then the isometry group of (V, f) is called the* ***symplectic group*** $\mathbf{Sp_{2n}(q)}$.

Remark 4.2. *(Section 3.4.4, [22]) 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 $K = \mathbb{F}_q$. Then there is a basis of V, $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ where $f(e_i, e_j) = f(f_i, f_j) = 0$ for all $1 \leq i, j \leq n$, $f(e_i, f_j) = -f(f_j, e_i) = \delta_{ij}$ where δ_{ij} is the Kronecker delta function. Any such basis is called a* ***symplectic basis*** *for the inner product space (V, f).*

It is well known that any maximal isotropic subspace of V with respect to a non-singular alternating bilinear form has dimension n (See Section 8.1 in [7]). The following lemma easily follows from Witt's theorem [7].

Lemma 4.3. *Let V be a $2n$-dimensional vector space and f be a non-singular alternating bilinear form on V. Let W be a maximal isotropic subspace of V. Let $\{e_1, \ldots, e_n\}$ be any basis of W. Then, there exist $f_i \in V$, $1 \leq i \leq n$, such that $\mathcal{B} = \{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ is a symplectic basis of V with respect to the bilinear form f.*

Suppose, as above f is a non-singular alternating bilinear form. Then, $\pm I_{2n}$ are the only scalar matrices in $Sp_{2n}(q)$. Hence, the center $Z_{Sp_{2n}(q)}$ is $\{\pm I_{2n}\}$. The ***projective symplectic group*** $\mathbf{PSp_{2n}(q)} = Sp_{2n}(q)/Z_{Sp_{2n}(q)}$ is a simple group of Lie type.

5 LS's for Parabolic subgroups

Suppose G is a finite group of Lie type. Then from the discussion in Section 2, it follows that G is a subgroup of $GL_n(q)$. Let $V = \mathbb{F}_{q^n}$ be the field of order q^n viewed as an n-dimensional vector space over $\mathbb{F}_q$. Then, G acts as a permutation group on $V \setminus \{0\}$ as well as on projective space $\mathcal{P}(V)$. Also note that, $1 \in V \setminus \{0\}$ and $\langle 1 \rangle \in \mathcal{P}(V)$ where 1 is the multiplicative identity of the field $\mathbb{F}_{q^n}$. Let P_G denote the parabolic subgroup of G (in the sense of Remarks 3.12 and 3.13) defined by $P_G := stab_G(\langle 1 \rangle)$.

In this section we describe the structure of the parabolic subgroup P_G for the groups $G = GL_n(q)$, $PGL_n(q)$, $SL_n(q)$, $PSL_n(q)$, $Sp_{2n}(q)$, $PSp_{2n}(q)$ and obtain an LS for P_G. We then use this LS to construct an MLS for all the above mentioned groups G in the next sections.

We choose a suitable ordered basis $\mathcal{B} = \{e_1, e_2, \ldots, e_n\}$ of V. As noted in Section 2, we identify elements of V with the $n \times 1$ column vectors and the group $GL(V)$ with the group $GL_n(q)$.

Let $G := GL_n(q)$. We assume that $e_1 = 1$. Remark 3.13 implies that P_G has an LS $[U_G, L_G]$. The structures of the groups U_G and L_G can easily be obtained by applying the definitions (For details see Section 3.3.3 in Wilson [22]). Here, $U_G = \{\begin{pmatrix} 1 & u \\ 0 & I_{n-1} \end{pmatrix} \mid u \in \mathbb{F}_q^{n-1}\}$ is an elementary abelian group of order q^{n-1} and $L_G = \{\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \mid a \in \mathbb{F}_q^*,\ A \in GL_{n-1}(q)\}$. It is also known that $Z_G = \{kI_n \mid k \in \mathbb{F}_q^*\}$ is a cyclic group of order $q-1$.

Let $L_1 = \{\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \mid A \in GL_{n-1}(q)\}$. Then, it is easy to see that $L_1 \leq L_G$ and $L_G = L_1 Z_G$. Also, $L_1 \cap Z_G = \{I_n\}$. Thus, from Remark 3.4, $[L_1, Z_G]$ is an LS for L_G. Now, using Remark 3.2 we can replace L_G in $[U_G, L_G]$ by $[L_1, Z_G]$. Hence, we have proved the following lemma.

Lemma 5.1. *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 the cyclic group of order $q-1$.*

Let $G := PGL_n(q) = GL_n(q)/Z_1$ and let $\eta : GL_n(q) \to G$ be the canonical homomorphism from $GL_n(q)$ onto G. Then, $P_G = stab_G(\langle 1 \rangle) = P_1/Z_1$. We note that $U_1 \cap Z_1 = L_1 \cap Z_1 = \{I_n\}$. Therefore, $U_2 := \eta(U_1)$ and $L_2 := \eta(L_1)$ are subgroups of G isomorphic to U_1 and L_1 respectively. Thus, from the above lemma and Remark 3.6, we get the following.

Lemma 5.2. *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 $L_2 \cong GL_{n-1}(q)$.*

Now, let $G := SL_n(q)$. Then, $Z_G = Z_1 \cap G$ and $P_G = P_1 \cap G$. From Remark 3.13, it follows that P_G has an LS $[U_G, L_G]$. It is easy to show that $U_G = U_1$ and $L_G = \{\begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \mid A \in GL_{n-1}(q),\ a = det(A)^{-1}\}$. Also, $Z_G = \{kI_n \mid k^n = 1,\ k \in \mathbb{F}_q^*\} = \{\begin{pmatrix} k & 0 \\ 0 & kI_{n-1} \end{pmatrix} \mid k^n = 1,\ k \in \mathbb{F}_q^*\}$. Note that, $k^n = 1$ implies $det(kI_{n-1})^{-1} = (k^{n-1})^{-1} = k$. Thus, $Z_G \leq L_G$ and hence $Z_G \leq Z_{L_G}$.

From the above description of Z_G and L_G it is easy to see that Z_G is a cyclic group of order $d = gcd(n, q-1)$ and $L_G \cong GL_{n-1}(q)$. Also, note that Z_{L_G} is a cyclic group of order $q-1$ and $L_G/Z_{L_G} \cong PGL_{n-1}(q)$.

Now using Remark 3.3, L_G has an LS $[L_3, Z_{L_G}]$ where L_3 is any $lt(L_G, Z_{L_G})$. Also, Z_{L_G} has an LS $[L_3', Z_G]$, where L_3' is any $lt(Z_{L_G}, Z_G)$. Thus we can apply Remark 3.2 and replace L_G in $[U_G, L_G]$ by $[L_3, L_3', Z_G]$. Hence, we have the following lemma.

Lemma 5.3. *Let $G := SL_n(q)$. Then $P_3 := P_G$ has an LS $[U_3, L_3, L_3', Z_3]$, where U_3 is an elementary abelian group of order q^{n-1}, $Z_3 := Z_G$ is a cyclic group of order $d = (n, q-1)$, L_3 is any $lt(L_G, Z_{L_G})$ and L_3' is any $lt(Z_{L_G}, Z_G)$. Further Z_{L_G} is a cyclic subgroup of order $q-1$, $L_G \cong GL_{n-1}(q)$ and $L_G/Z_{L_G} \cong PGL_{n-1}(q)$.*

Now, let $\eta : SL_n(q) \to PSL_n(q)$ be the canonical homomorphism from $SL_n(q)$ onto $PSL_n(q)$. Note that $U_3 \cap Z_3 = \{I_n\}$. Hence $U_4 := \eta(U_3)$ and $L_4' := \eta(L_3') = Z_{L_G}/Z_G$ are subgroups of G/Z_G. Also, using the fact that $(L_G/Z_G)/(Z_{L_G})/Z_G) \cong L_G/Z_{L_G} \cong PGL_{n-1}(q)$, it can be easily checked that $L_4 := \eta(L_3)$ is an $lt(L_G/Z_G, Z_{L_G}/Z_G)$. The above lemma and Remark 3.6 now imply the following lemma.

Lemma 5.4. *Let $G := SL_n(q)$. Then $G/Z_G = PSL_n(q)$ and $P_4 := P_{G/Z_G}$ has an LS $[U_4, L_4, L_4']$, where U_4 is an elementary abelian group of order q^{n-1}, $L_4 = \eta(L_3)$ is an $lt(L_G/Z_G, Z_{L_G}/Z_G)$, $(L_G/Z_G)/(Z_{L_G}/Z_G) \cong PGL_{n-1}(q)$ and $L_4' = Z_{L_G}/Z_G$ is a cyclic group of order $(q-1)/d$, $d = (n, q-1)$.*

We now describe LS's for the parabolic subgroups of the symplectic group $Sp_{2n}(q)$ and the projective symplectic group $PSp_{2n}(q)$.

Let $V = \mathbb{F}_{q^{2n}}$ be the field of order q^{2n} viewed as an $2n$-dimensional vector space over $\mathbb{F}_q$. Let f be a non-singular alternating bilinear form on V. Let $e_1 := 1, f_1 \in V$ be such that $f(e_1, f_1) = 1$. Now, choose $e_2, \ldots, e_n, f_2, \ldots, f_n \in V$ such that $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ is a symplectic basis of V [22]. Let $\mathcal{B} = \{e_1, f_1, e_2, \ldots, e_n, f_2, \ldots, f_n\}$ be an ordered basis of V. Let W be the subspace of V generated by $\{e_2, \ldots, e_n, f_2, \ldots, f_n\}$ and $f' = f|_{W\times W}$. Then, the inner product space (W, f') has a symplectic basis $\mathcal{B}' = \{e_2, \ldots, e_n, f_2, \ldots, f_n\}$. The matrix of the bilinear form f with respect to the basis $\mathcal{B}$ 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 $\mathcal{B}'$.

Let $G = Sp_{2n}(q)$ be the symplectic group as described in the previous section. Consider the parabolic subgroup $P_G = stab_G(\langle 1\rangle)$. Let $g = (g_{ij})_{2n\times 2n} \in P_G$. Then $g(\langle 1\rangle) = \langle 1\rangle$. This implies that the first column of g is $(g_{11}, 0, \ldots, 0)^t$. Using the fact that $g(e_i)$, $g(f_i) \in \langle 1\rangle^{\perp}$ for $2 \le i \le n$, it follows that second row of g is of the form $(0, g_{22}, 0, \ldots, 0)$. Now let $g_1 = g|_W$. If we consider g_1 as a matrix with respect to the basis $\mathcal{B}'$, then one can easily verify 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 (see [22] and [7] for details), one can verify the following about the structure of the parabolic subgroup P_G. The parabolic subgroup $P_G = U_5 \cdot (L_5 \times L'_5)$, where U_5 is a p-group of order q^{2n-1}, $L_5 = \{\begin{pmatrix} I_2 & 0 \\ 0 & A \end{pmatrix} \mid A \in Sp_{2n-2}(q)\}$ and $L'_5 = \{\begin{pmatrix} a & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & I_{2n-2} \end{pmatrix} \mid a \in \mathbb{F}_q^*\}$. Thus, $L_5 \cong Sp_{2n-2}(q)$ and L'_5 is a cyclic group of order $q-1$. Also, $L_G = L_5 \times L'_5$ is the standard Levi subgroup. Now, the following lemma follows from Remark 3.4.

Lemma 5.5. *Let $G := Sp_{2n}(q)$. Then, $P_5 := P_G$ has an LS $[U_5, L_5, L'_5]$, where U_5 is a p-subgroup of G of order q^{2n-1}, $L_5 \cong Sp_{2n-2}(q)$, L'_5 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 $H_{5,1} := \{\begin{pmatrix} I_2 & 0 \\ 0 & \pm I_{2n-2} \end{pmatrix}\} \trianglelefteq L_5$ and $H_{5,2} := \{\begin{pmatrix} \pm I_2 & 0 \\ 0 & I_{2n-2} \end{pmatrix}\} \trianglelefteq L'_5$. Then, $H_{5,3} := H_{5,1} \times H_{5,2}$ is clearly an elementary abelian subgroup of G of order 4. Also, $Z_G \trianglelefteq H_{5,3}$ and $H_{5,3} \trianglelefteq L_G = L_5 \times L'_5$. Let $H_6 := H_{5,3}/Z_G$.

Then, note that $(L_G/Z_G)/H_6 \cong L_G/H_{5,3} \cong (L_5/H_{5,1}) \times (L'_5/H_{5,2})$. Hence, using Remark 3.4, it follows that $(L_G/Z_G)/H_6$ has an LS $[L_{6,1}, L_{6,2}]$, where $L_{6,1}$ and $L_{6,2}$ are subgroups of $(L_G/Z_G)/H_6$ and $L_{6,1} \cong L_5/H_{5,1} \cong PSp_{2n-2}(q)$ and $L_{6,2} \cong L'_5/H_{5,2}$ is a cyclic group of order $(q-1)/2$.

Now, $U_5 \cap Z_G = \{I_{2n}\}$. Hence, $U_6 := \eta(U_5)$ is a subgroup of G/Z_G isomorphic to U_5. Let $P_6 = P_{PSp_{2n}(q)} = stab_{PSp_{2n}(q)}(\langle 1\rangle)$. Then, using the facts that $[U_5, L_G]$ is an LS for P_5, $Z_G \le L_G \le P_5$ and Remark 3.7, it follows that $P_6 = P_5/Z_G$ has an LS $[U_6, L_G/Z_G]$. Hence we have the following lemma.

Lemma 5.6. *Let $G := Sp_{2n}(q)$. Consider $G/Z_G = PSp_{2n}(q)$ and $P_6 := P_{G/Z_G} = stab_{PSp_{2n}(q)}(\langle 1\rangle)$. Then, we have the following.*

(i) Suppose q is a power of 2. Then, $P_6 = P_5$ has an LS $[U_5, L_5, L'_5]$, where U_5 is a p-subgroup of $PSp_{2n}(q)$

of order q^{2n-1}, $L_5 \cong Sp_{2n-2}(q)$ *and* L_5' *is a cyclic group of order* $q-1$.

(ii) Suppose q *is an odd prime power. Then,* P_6 *has an LS* $[U_6, L_G/Z_G]$, *where* U_6 *is a* p*-subgroup of* G *of order* q^{2n-1} *and* L_G/Z_G *has a normal subgroup* H_6 *of order* 2. *Further,* $(L_G/Z_G)/H_6 = L_{6,1} \times L_{6,2}$, *where* $L_{6,1}$, $L_{6,2}$ *are subgroups of* $(L_G/Z_G)/H_6$, $L_{6,1} \cong PSp_{2n-2}(q)$ *and* $L_{6,2}$ *is a cyclic group of order* $(q-1)/2$.

6 MLS 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 will then use to construct an MLS for $SL_n(q)$ and $PSL_n(q)$ for all $n \in \mathbb{N}$ and q a prime power. We note that MLS's for $GL_n(q)$ and $PGL_n(q)$ have already been obtained by Lempken and Trung [14], using a slightly different method.

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 $\boldsymbol{\alpha}$ 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 $\boldsymbol{x} \in G$ 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 $\alpha_{\mathbf{1}} = det(x)$. Let $\mathbf{H} = \langle x \rangle$ 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 $\mathbf{H'} = H/Z_G$. Then $H' = \langle xZ_G \rangle$ is the cyclic group generated by xZ_G. Let $\mathbf{M} := \{x^i \mid 0 \leq i < \frac{q^n-1}{q-1}\}$. The first two statements in the remark below follow from results in [2, 6, 21]. The third statement follows from the second statement and the facts that $Z_G \leq stab_G(\langle 1 \rangle)$ and M is an $lt(H, Z_G)$.

Remark 6.1.

(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) $H' = \langle xZ_G \rangle$ *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 $\mathbf{d} = |Z_{SL_n(q)}| = gcd(n, q-1)$. Then $d \mid \frac{q^n-1}{q-1}$. Define M_1, $M_2 \subseteq M$ as $\mathbf{M_1} := \{x^{dj} \mid 0 \leq j < \frac{q^n-1}{(q-1)d}\}$ and $\mathbf{M_2} := \{x^j \mid 0 \leq j < d\}$. Then, $[M_1, M_2]$ is an LS for M. Using Lemma 3.10, 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 (3.10.1). Then, by Remark 3.2, $\beta = [A_1, A_2, \ldots, A_{k_1}, B_1, B_2, \ldots, B_{k_2}]$ is an MLS for M.

The following remark follows immediately from the above discussion and Lemma 3.11.

Remark 6.2. *(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.

Using Lemma 5.1, we know that 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 Remark 3.9, U_1 and Z_1 have an MLS. Also, we know that $GL_1(q)$ is a cyclic group of order $q-1$. Hence, $GL_1(q)$ has an MLS. Therefore, using Remarks 6.2, 3.2 and induction on n, we have the following theorem.

Theorem 6.3. *Let* $n \in \mathbb{N}$ *and* q *be a prime power. Then* $GL_n(q)$ *has an MLS.*

Now, 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, $P_2 = stab_G(\langle 1\rangle) = P_1/Z_1$. Let $M' = \eta(M)$. Then, Remark 6.1*(iii)* implies that M' acts sharply transitively on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$. Also, M' satisfies the conditions of Remark 3.8 with $G = GL_n(q)$ and $H = Z_1$. Let $\overline{A}_i = \eta(A_i),\ 1 \le i \le k_1$ and $\overline{B}_j = \eta(B_j),\ 1 \le j \le k_2$. Using Remarks 6.2*(i)* and 3.8, it follows that $[\overline{A}_1, \ldots, \overline{A}_{k_1}, \overline{B}_1, \ldots, \overline{B}_{k_2}]$ is an MLS for M'. Also, using Lemma 3.11, it follows that $[M', P_2]$ is an LS for $PGL_n(q)$. Lemma 5.2 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, Remark 3.9 implies that U_2 has an MLS and Theorem 6.3 implies that L_2 has an MLS. Finally, using Remark 3.2 we have the following result.

Theorem 6.4. *Let $n \in \mathbb{N}$ and q be a prime power. Then $PGL_n(q)$ has an MLS.*

7 MLS for $SL_n(q)$ and $PSL_n(q)$

We continue with the notations from the previous section. In particular we assume that β is as defined in Remark 6.2. Let $a, b \in \mathbb{Z}$ be such that $d = a(q-1) + bn$. Define $\mathbf{f_1} = \alpha_1^{-b} I_n$. Also, fix an element $c \in B_1$, $c \neq I_n$. 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 $\mathbf{f_2} = (a_{ij})_{n\times n} \in GL_n(q)$ be the diagonal matrix defined as follows.

$$a_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \neq m+1 \\ \alpha_1^{-1} & \text{if } i = j = m+1. \end{cases} \tag{7.0.1}$$

Lemma 7.1. *$f_2^j(\langle \alpha^i\rangle) = \langle \alpha^i\rangle$ for all $i \neq m$, $0 \le i < d$ and for all $j \in \mathbb{Z}$*

Proof. Consider α^i, $i \neq m$, $0 \le i < d \le n$. It follows that, the column vector representing $\alpha^i \in \mathcal{B}$ has 0 in the $(m+1)^{th}$ row.

The Equation (7.0.1) now implies that, $f_2^j(\langle \alpha^i\rangle) = \langle \alpha^i\rangle$ for all $j \in \mathbb{Z}$.

□

Lemma 7.2. *Let $x^{s_j} \in B_j, 1 \le j \le k_2$. Then,*

$$\left(\prod_{j=1}^{k_2} \left(x^{s_j} f_2^{s_j}\right)\right)(\langle 1\rangle) = \left(\prod_{j=1}^{k_2} x^{s_j}\right)(\langle 1\rangle). \tag{7.2.1}$$

Proof. Let $x^{s_j} \in B_j$, $1 \le j \le k_2$. If $k_2 = 1$, then (7.2.1) follows from Lemma 7.1 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

$$y'_r(\langle 1\rangle) = y_r(\langle 1\rangle). \tag{7.2.2}$$

When $r = 0$, using Lemma 7.1 and the fact that $m \neq 0$ we get, $f_2^{s_{k_2}}(\langle 1\rangle) = f_2^{s_{k_2}}(\langle \alpha^0\rangle) = \langle 1\rangle$. Hence, $y'_0(\langle 1\rangle) = y_0(\langle 1\rangle)$. Now by induction hypothesis, assume that (7.2.2) is true for all i, $0 \le i \le r < k_2 - 1$. We show that (7.2.2) 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 $M_2 = \{x^j | 0 \le j < d\}$ with $I_n \in B_i$, $1 \le i \le k_2$, it follows that,

$$x^m \neq \prod_{j=k_2-r}^{k_2} x^{s_j}. \tag{7.2.3}$$

Now $x^m, \prod_{j=k_2-r}^{k_2} x^{s_j} \in M$ and using Remark 6.1, M is sharply transitive on $\mathcal{P}(V)$. Hence, (7.2.3) implies that, $(\prod_{j=k_2-r}^{k_2} x^{s_j})(\langle 1\rangle) = \langle \alpha^s\rangle$ for some $s \neq m, 0 \le s < d$.

Finally, using Lemma 7.1 it follows that,

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

□

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

Theorem 7.3. *Let A'_i, $1 \leq i \leq k_1$ and B'_i, $1 \leq i \leq k_2$ be defined as above. Then,*

(i) $A'_i, B'_j \subseteq SL_n(q)$ for all $1 \leq i \leq k_1$ and for all $1 \leq j \leq k_2$.

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

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

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

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

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

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

Hence, $B'_i \subseteq SL_n(q)$ 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

$$x^t(\langle 1\rangle) = \langle v_1\rangle. \tag{7.3.1}$$

From Remark 6.2(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,

$$x^t = \prod_{i=1}^{k_1} x^{dr_i} \prod_{j=1}^{k_2} x^{s_j}. \tag{7.3.2}$$

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

$$\left(\prod_{i=1}^{k_1} x^{dr_i} f_1^{r_i}\right)(\langle v\rangle) = \left(\prod_{i=1}^{k_1} x^{dr_i}\right)(\langle v\rangle) \text{ for all } v \in V. \tag{7.3.3}$$

Also, using Lemma 7.2 we have,

$$\left(\prod_{j=1}^{k_2} x^{s_j} f_2^{s_j}\right)(\langle 1\rangle) = \left(\prod_{j=1}^{k_2} x^{s_j}\right)(\langle 1\rangle). \tag{7.3.4}$$

Hence, from (7.3.1), (7.3.2), (7.3.3) and (7.3.4) 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, $[A'_1, \ldots, A'_{k_1}, B'_1, \ldots, B'_{k_2}]$ is an LS for $\mathcal{A}$. Now, $|A'_i| = |A_i|$ for all $1 \leq i \leq k_1$ and $|B'_j| = |B_j|$ for all $1 \leq j \leq k_2$. Hence, using Remark 6.2(i), it follows that $[A'_1, \ldots, A'_{k_1}, B'_1, \ldots, B'_{k_2}]$ is an MLS for $\mathcal{A}$. □

The following remark easily follows from Theorem 7.3, Remark 3.8 and the fact that $Z_{SL_n(q)} \subseteq stab_{SL_n(q)}(\langle 1\rangle)$.

Remark 7.4. *Let $G = SL_n(q)$ and $\mathcal{A}'$ be the subset of $PSL_n(q)$ defined by $\mathcal{A}' = \eta(\mathcal{A}) = \{aZ_G | a \in \mathcal{A}\}$, where $\mathcal{A} \subseteq SL_n(q)$ is as defined in the previous theorem. Then, $\mathcal{A}'$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$ and $\mathcal{A}'$ has an MLS.*

Now we are ready to prove the main theorem of this section.

Theorem 7.5. *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 $P_3 = stab_G(\langle 1\rangle)$. Using Theorem 7.3 and Lemma 3.11, it follows that G has an LS $[\mathcal{A}, P_3]$ and $\mathcal{A}$ has an MLS. From Remark 5.3, we have that P_3 has an LS $[U_3, L_3, L'_3, Z_3]$. Here, U_3 and Z_3 are abelian groups hence using Remark 3.9, it follows that both have an MLS. Now, L_3 is any $lt(L_G, Z_{L_G})$ and $L_G/Z_{L_G} \cong PGL_{n-1}(q)$. Thus, using Theorem 6.4 and Remark 3.5, it follows that we can choose L_3 such that it has an MLS. Now, L'_3 is any $lt(Z_{L_G}, Z_3)$. We know that Z_{L_G}/Z_3 is an abelian group, hence it has an MLS. Thus, using Remark 3.5, we can choose L'_3 such that L'_3 has an MLS. Finally, using Remark 3.2 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 using Lemma 5.4 and Remarks 7.4, 3.11 and 3.2, it follows that $PSL_n(q)$ has an LS $[\mathcal{A}', U_4, L_4, L'_4]$ and $\mathcal{A}'$ has an MLS. Also, U_4 and L'_4 are abelian groups. Hence, using Remark 3.9, both U_4 and L'_4 have an MLS. Further, $L_4 = \eta(L_3)$. Hence, using Remark 3.8 and the fact that L_3 has an MLS, it follows that L_4 has an MLS. The above facts together with Remark 3.2 imply that $PSL_n(q)$ has an MLS. □

As already noted in Section 1, the existence of MLS's for $SL_n(q)$ and $PSL_n(q)$, for the particular cases when $gcd(n, q-1)$ is 1, 4 or a prime number, was proved by Lempken and Trung [14] using a different method, by studying double cosets.

8 MLS for $Sp_{2n}(q)$ and $PSp_{2n}(q)$

Let $\mathbf{V} = \mathbb{F}_{q^{2n}}$. As before, we consider V as a $2n$-dimensional vector space over $\mathbb{F}_q$. For $y \in V$, we denote y^{q^n} by $\overline{\mathbf{y}}$. For $s \in V$, $\mathbf{T_s}$ 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 $\mathbf{x} \in GL_{2n}(q)$ be the matrix corresponding to the linear transformation T_α.

Define a bilinear form $\mathbf{f} : V \times V \to \mathbb{F}_q$ 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 be easily seen that f is a non-singular alternating bilinear form (See proof of Theorem 5.6 in [11]). 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 isotropic subspace of V. Let $\{e_1, \ldots, e_n\}$ be any basis of W. Then, using Lemma 4.3 we have a symplectic basis $\mathcal{B} = \{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ of V. Then, the matrix of the bilinear form f with respect to the ordered basis $\mathcal{B}$ of V is given by $J_{2n} = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$.

We consider 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 $A \in GL_n(q)$ 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 $x_2 = \begin{pmatrix} A & 0 \\ 0 & (A^t)^{-1} \end{pmatrix} \in GL_{2n}(q)$. 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, $x_1,\ x_2 \in Sp_{2n}(q)$.

Let $G = Sp_{2n}(q)$. Then, $Z_G = \{I_{2n}, -I_{2n}\}$ if q is odd and $Z_G = \{I_{2n}\}$ if q is even. 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 $q^n - 1$. Let $H_3 = \langle x_2^{\frac{q^n-1}{q-1}}\rangle$ be the subgroup of H_2 of order $q - 1$. We note that, 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 $\langle 1\rangle$, which we will then use to create MLS's for $Sp_{2n}(q)$ and $PSp_{2n}(q)$.

Let H_1' and H_2' be $lt(H_1, Z_G)$ and $lt(H_2, H_3)$ respectively. Then $|H_1'| = \frac{q^n+1}{2}$ if q is odd and $|H_1'| = q^n + 1$ if q is even. Also, $|H_2'| = \frac{q^n-1}{q-1}$. Further, H_1' and H_2' can be chosen so that $H_1' \cap H_2' = \{1\}$ and both are cyclic sets. Thus, $|H_1'H_2'| = \frac{q^{2n}-1}{2(q-1)}$ if q is odd and $|H_1'H_2'| = \frac{q^{2n}-1}{q-1}$ if q is even.

Lemma 8.1. *The subset $H_1'H_2' = \{h_1h_2 \mid h_1 \in H_1',\ h_2 \in H_2'\}$ of $Sp_{2n}(q)$ is a sharply transitive set on Y with respect to $\langle 1\rangle$, where $Y = \{\langle \alpha^{2i}\rangle \mid 0 \le i < \frac{q^{2n}-1}{2(q-1)}\}$ if q is odd and $Y = \mathcal{P}(V) = \{\langle \alpha^i\rangle \mid 0 \le i < \frac{q^{2n}-1}{q-1}\}$ if q is even.*

Proof. Suppose q is odd and $Y = \{\langle \alpha^{2i}\rangle \mid 0 \le i < \frac{q^{2n}-1}{2(q-1)}\}$. 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 exists $h_1 \in H_1'$, $h_2 \in H_2'$ 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 $|H_1'H_2'| = \frac{q^{2n}-1}{2(q-1)} = |Y|$, it follows that $H_1'H_2'$ is a sharply transitive set on Y 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 $H_1'H_2'$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$. □

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 isotropic subspace of V and $\{e_i' := \alpha e_i \mid 1 \le i \le n\}$ forms a basis of W'. Now, using Lemma 4.3 we can find f_i', $1 \le i \le n$, 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 $p \in GL_{2n}(q)$ be the matrix corresponding to the linear transformation T' defined by $T'(v) = \sum_{i=1}^{n}(a_ie_i' + a_{i+n}f_i')$ for all $v = \sum_{i=1}^{n}(a_ie_i + a_{i+n}f_i) \in V$. Then, from the definition of p and the basis $\mathcal{B}'$ of V, it follows that, $p \in Sp_{2n}(q)$.

Now, using Lemma 8.1 one can easily prove that, $H_1'pH_2' = \{h_1ph_2 \mid h_1 \in H_1',\ h_2 \in H_2'\}$ is a sharply transitive set on Y' with respect to $\langle 1\rangle$, where $Y' = \{\langle \alpha^{2i+1}\rangle \mid 0 \leq i < \frac{q^{2n}-1}{2(q-1)}\}$. Let $M := \{1,\ p\} \subseteq Sp_{2n}(q)$. Then, from the above discussion and Lemma 8.1, we have the following theorem.

Theorem 8.2. *Let H_1', H_2' and M be the subsets of $Sp_{2n}(q)$ as defined above.*

(i) If q is odd, then the set $H_1'MH_2' = \{h_1mh_2 \mid h_1 \in H_1',\ m \in M,\ h_2 \in H_2'\}$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$.

(ii) If q is even, then the set $H_1'H_2' = \{h_1h_2 \mid h_1 \in H_1',\ h_2 \in H_2'\}$ is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$.

Now, H_1' and H_2' are cyclic sets. Thus, by Lemma 3.10 it follows that H_1' and H_2' have an MLS. Also, $|M| = 2$, a prime. Hence, we have the following lemma.

Lemma 8.3. *Let H_1', H_2', M be as defined above. The sets $H_1'MH_2'$ and $H_1'H_2'$ have an MLS.*

Now, we can prove that the groups $Sp_{2n}(q)$ and $PSp_{2n}(q)$ have an MLS.

Theorem 8.4. *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. Let $G = Sp_{2n}(q)$ and $P_G = stab_{Sp_{2n}(q)}(\langle 1\rangle)$. Using Theorem 8.2, Lemma 8.3 and Lemma 3.11, it follows that G has an LS $[H_1'MH_2', P_G]$ where $H_1'MH_2'$ has an MLS. Now, Lemma 5.5 implies that P_G has an LS $[U_5, L_5, L_5']$ where U_5, L_5' are solvable subgroups of G and $L_5 \cong Sp_{2n-2}(q)$. Thus, using Remark 3.9, U_5 and L_5' have an MLS. Using induction hypothesis we can assume that $Sp_{2n-2}(q)$ has an MLS. Also, from Theorem 7.5 and the fact that $Sp_2(q) = SL_2(q)$, it follows that, $Sp_2(q)$ has an MLS. Hence, by induction on n and using Lemma 3.2, it follows that $Sp_{2n}(q)$ has an MLS.

Similarly, when q is even, by replacing $H_1'MH_2'$ with $H_1'H_2'$ 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 $G' = PSp_{2n}(q)$ and $P_{G'} = stab_{PSp_{2n}(q)}(\langle 1\rangle)$. Let $A' = \eta(H_1'MH_2')$, where $\eta : Sp_{2n}(q) \to PSp_{2n}(q)$ is the canonical homomorphism onto $PSp_{2n}(q)$. Then using Remark 3.8, Lemma 8.3 and Theorem 8.2, it follows that A' is a sharply transitive set on $\mathcal{P}(V)$ with respect to $\langle 1\rangle$ and A' has an MLS. Next, using Lemma 5.6(ii), $P_{G'}$ has an LS $[U_6, L_G/Z_G]$, where U_6 is a solvable subgroup of G and L_G/Z_G has a normal subgroup H_6 of order 2. Further, $(L_G/Z_G)/H_6 = L_{6,1} \times L_{6,2}$, where $L_{6,1},\ L_{6,2}$ are subgroups of $(L_G/Z_G)/H_6$, $L_{6,1} \cong PSp_{2n-2}(q)$ and $L_{6,2}$ is a cyclic group of order $\frac{q-1}{2}$. By Remark 3.9, U_6 and $L_{6,2}$ have an MLS. Also, by the induction hypothesis we can assume that $L_{6,1}$ has an MLS. Thus, using Remark 3.2, $(L_G/Z_G)/H_6$ has an MLS. Now, clearly H_6 has an MLS. Hence, by taking $H = H_6$ and $G = L_G/Z_G$ in Remark 3.5 and using Remark 3.2, it follows that L_G/Z_G has an MLS. This implies, $P_{G'}$ has an MLS. Finally, using Lemma 3.11 and Remark 3.2 and by induction on n, 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. □

References

[1] Michael Artin. *"Algebra."* Prentice Hall Inc, 1991.

[2] Áron Bereczky. *"Maximal Overgroups of Singer Elements in Classical Groups."* J. Algebra **234**, 187-206(2000).

[3] Norman Biggs and Arthur T. White *"Permutation groups and combinatorial structures."* Cambridge University Press, Cambridge-New York, 1979

[4] Jens-Matthias Bohli, Rainer Steinwandt, Mańia Isabel González Vasco and Consuelo Martínez. *"Weak Keys in MST_1."* Designs, Codes and Cryptography **37**, 509 - 524(2005).

[5] Roger W. Carter. *"Finite groups of Lie type: Conjugacy Classes and Complex Characters."* John Wiley & Sons Ltd, New York, 1985.

[6] A. Cossidente and M. J. De Resmini. *"Remarks on Singer Cyclic Groups and Their Normalizers."* Designs, Codes and Cryptography **32**, 97 - 102(2004).

[7] Paul Garrett. *"Buildings and Classical Groups"* Chapman & Hall, London, 1997.

[8] Mańia Isabel González Vasco and Rainer Steinwandt. *"Obstacles in Two Public Key Cryptosystems Based on Group Factorizations."* Tatra Mountains Math. Pub. **25**, 2337(2002).

[9] Mańia Isabel González Vasco, Martin Rötteler and Rainer Steinwandt. *"On Minimal Length Factorizations of Finite Groups."* Experimental Math. **12**, 1-12(2003).

[10] G. Hajós *"Többméretű terek befedése kockaráccsal"* Mat. Fiz. Lapok. **45**, 171-190(1938). Canad. J. Math. **22**, 492-513(1970).

[11] Marshall D. Hestenes. *"Singer Groups"* Canad. J. Math. **22**, 492-513(1970).

[12] J. W. P. Hirschfeld *"Projective Geometries Over Finite Fields"* The Clarendon Press Oxford University Press, New York, 1998.

[13] P. E. Holmes. *"On Minimal Factorisations of Sporadic Groups"* Experimental Math. **13**, 435-440(2004).

[14] Wolfgang Lempken and Tran van Trung. *"On Minimal Logarithmic Signatures of Finite Groups."* Experimental Math. **14**, 257-269(2005).

[15] Spyros S. Magliveras. *"A Cryptosystem from Logarithmic Signatures of Finite Groups."* In Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972975. Amsterdam: Elsevier Publishing Company, 1986.

[16] Spyros S. Magliveras. *"Secret and Public-Key Cryptosystems from Group Factorizations."* Tatra Mountains Math. Pub. **25**, 1122(2002).

[17] Wolfgang Lempken, Spyros S. Magliveras, Tran van Trung and Wandi Wei. *"A Public Key Cryptosystem Based on Non-abelian Finite Groups."* to appear in the J. Cryptology (2009).

[18] Spyros S. Magliveras, Nidhi Singhi and Nikhil Singhi. *"*** - A paper on Almost Minimal Logarithmic Signatures."* ***** In preparation.

[19] Spyros S. Magliveras, Nidhi Singhi and Nikhil Singhi. *"*** - Logarithmic Signatures and Spreads."* ***** In preparation.

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

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

[22] Robert A. Wilson. *The finite simple groups.* In preparation. http://www.maths.qmul.ac.uk/ raw/fsgs.html