May 2018

Orthogonal Abelian Cartan Subalgebra Decompositions of Classical Lie Algebras Over Finite Commutative Rings

Songpon Sriwongsa
University of Wisconsin-Milwaukee

Orthogonal abelian Cartan subalgebra decompositions of classical Lie algebras over finite commutative rings

by

Songpon Sriwongsa

A Dissertation Submitted in
Partial Fulfillment of the
Requirements for the Degree of

Doctor of Philosophy
in
Mathematics

at

The University of Wisconsin-Milwaukee
May 2018

ABSTRACT

Orthogonal abelian Cartan subalgebra decompositions of classical Lie algebras over finite commutative rings

by

Songpon Sriwongsa

The University of Wisconsin-Milwaukee, 2018
Under the Supervision of Professor Dr. Yi Ming Zou

Orthogonal decompositions of classical Lie algebras over the complex numbers of types A, B, C and D were studied in the early 1980s and attracted further attention in the past decade, especially in the type A case, due to its application in quantum information theory. In this dissertation, we consider the orthogonal decomposition problem of Lie algebras of type A, B, C and D over a finite commutative ring with identity. We first establish the appropriate definition of orthogonal decomposition under our setting, and then derive some general properties that rely on the finite commutative rings theory. Our goal is to construct interesting orthogonal decompositions of these Lie algebras. We begin with Lie algebras of type A by searching for sufficient conditions for the existence of such an orthogonal decomposition. Our study in the special case when the ring is a finite field provides us important information that leads to the approach we develop in this dissertation. We then apply our results on the orthogonal decomposition of type A Lie algebras to obtain a construction of the orthogonal decomposition of Lie algebras of type C. We also provide methods of constructing orthogonal decompositions for Lie algebras of types B and D.

Table of Contents

ACKNOWLEDGEMENTS

First of all I would like to thank my advisor, mentor Professor Yi Ming Zou, for his patience and encouragement. He has guided me through my Ph.D. process and inspired me to learn new topics in Mathematics. His assistance has made this work possible. Also, he has made me a better mathematician.

I am also grateful to my committee members: Professors Allen Bell, Craig Guilbault, Kevin McLeod, and Jeb Willenbring. They have assisted me through the writing of this process and supported my development through my graduate study at UW-Milwaukee. Not only for this Ph.D. dissertation, they have guided me through my entire education at UW-Milwaukee. I would also like thank Dr. Supanut Chaidee from Chiang Mai University, Thailand, for his help in Mathematica programming.

Finally, I would like to thank all of my family, friends and fellow graduate students for all their help and support. I could not have gone this far without them.

Chapter 1

Background information

1.1 Introduction

Let $\mathfrak{L}$ be a Lie algebra over $\mathbb{C}$. An orthogonal decomposition (OD) of $\mathfrak{L}$ is a decomposition of $\mathfrak{L}$ into a direct sum of Cartan subalgebras which are pairwise orthogonal with respect to the Killing form. Orthogonal decompositions of Lie algebras were studied as early as in [19] by Thompson and used for the construction of a special finite simple group. The theory of such decompositions of simple Lie algebras of types A, B, C and D over $\mathbb{C}$ was developed by Kostrikin et al. in the 1980s [11, 12, 13]. The OD problem of the Lie algebras of type A_{n-1} is related to other fields such as mutually unbiased bases (MUBs) in $\mathbb{C}^n$ which have applications in information theory [6, 15]. Boykin et al. established a connection between the problem of constructing maximal collections of MUBs and the existence problem of OD of the Lie algebras of type A_{n-1} [3]. They showed that a collection of $n+1$ MUBs in $\mathbb{C}^n$ gives rise to an OD of the Lie algebras of type A_{n-1} with the converse holding if the Cartan subalgebras in an OD of the Lie algebras of type A_{n-1} are stable with respect to the $*$-operation, where $X^* = \overline{X}^T$. It was conjectured in [11], the so-called Winnie-the-Pooh conjecture, that Lie algebras of type A_{n-1} have an OD if and only if n is a power of a prime integer. This would imply the nonexistence of $n+1$ MUBs in the n-dimensional complex

space when n is not a prime power. The only if part of the conjecture is still open. On the other hand, if n is a composite number which is not a prime power, the maximum collection of pairwise orthogonal Cartan subalgebras of the Lie algebras of type A_{n-1} is unknown. This is the case even when n is the first positive non-prime power integer 6. For some more recent developments when $n = 6$, see [2]. Note that the Lie algebra of type C_3 is a subalgebra of A_5. There exists a study of the OD problem of the Lie algebra of type C_3 [20]. The OD problem for some semisimple algebras has also been studied [10].

Our main object in this dissertation is to study the problem of orthogonal decomposition of Lie algebras over finite commutative rings with identity. We will consider the Lie algebras of types A, B, C and D, since these are matrix Lie algebras and they have been the focus of study when the base ring is the field of complex numbers. Since the structure of a Lie algebra over a finite commutative ring is drastically different from the structures of those over the complex numbers, it is necessary to generalize the definition of OD to our setting. Thus we begin by introducing the needed concepts and properties.

1.2 Modular Lie algebras

In this section, we will present some elementary definitions and properties of the theory of Lie algebras over a commutative ring with identity. These Lie algebras are called modular Lie algebras. For detailed discussions on these Lie algebras, see [9, 17].

For both this section and Section 1.3, we will consider Lie algebras over a general commutative ring R with identity. For the rest of this thesis, the ring is assumed to be finite.

Definition 1.2.1. A **Lie algebra** over R is an R-module $\mathfrak{L}$ with a bilinear operation

$$[\cdot, \cdot] : \mathfrak{L} \times \mathfrak{L} \to \mathfrak{L}$$

called a **Lie bracket**, which satisfies the following axioms:

(i) Anticommutativity: $[x, x] = 0$ for all $x \in \mathfrak{L}$;

(ii) Jacobi identity: $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in \mathfrak{L}$.

An R-submodule $\mathfrak{h}$ of $\mathfrak{L}$ is a **Lie subalgebra** if it is also a Lie algebra with the same Lie bracket of $\mathfrak{L}$.

Clearly anticommutativity implies

$$[x, y] = -[y, x]$$

for all $x, y \in \mathfrak{L}$ and the converse holds if $\mathrm{char}(R) \neq 2$.

Any associative algebra A over R can become a Lie algebra with the following Lie bracket (called the **commutator**:)

$$[x, y] := xy - yx.$$

Example 1.2.2. Let V be a free R-module of rank n and let $\mathrm{End}(V)$ be the set of R-module homomorphisms $V \to V$, which is an associative algebra. With a fixed basis for V, $\mathrm{End}(V)$ can be regarded as the set of $n \times n$ matrices over R, sometimes denoted by $M_n(R)$. Equipped with the commutator, $\mathrm{End}(V)$ becomes a Lie algebra called the **general linear Lie algebra** over R, denoted by $\mathfrak{gl}_n(R)$. Any subalgebra of $\mathfrak{gl}_n(R)$ is called a **linear Lie algebra**.

The linear Lie algebras that we are interested in will be defined in Section 1.3. In order to define an orthogonal decomposition in our setting, the following concept is needed.

Definition 1.2.3. Let $\mathfrak{L}$ be a Lie algebra over R.

(1) $\mathfrak{L}$ is said to be **abelian** if $[x, y] = 0$ for all $x, y \in \mathfrak{L}$.

(2) $[\mathfrak{L}, \mathfrak{L}] := \left\{ \sum [x_i, y_i] : x_i, y_i \in \mathfrak{L} \right\}$ is called the **derived algebra** of $\mathfrak{L}$.

(3) $Z(\mathfrak{L}) := \{z \in \mathfrak{L} : [x, z] = 0 \text{ for all } x \in \mathfrak{L}\}$ is called the **center** of $\mathfrak{L}$.

(4) The **normalizer** of a subalgebra K of $\mathfrak{L}$ is defined by $N_{\mathfrak{L}}(K) := \{x \in \mathfrak{L} : [x, K] \subseteq K\}$. If $K = N_{\mathfrak{L}}(K)$, then K is called a **self-normalizer**.

(5) Set $\mathfrak{L}^1 = \mathfrak{L}$, $\mathfrak{L}^2 = [\mathfrak{L}, \mathfrak{L}]$ and in general, $\mathfrak{L}^k = [\mathfrak{L}^{k-1}, \mathfrak{L}]$ for $k \geq 2$. Then $\mathfrak{L}$ is called **nilpotent** if $\mathfrak{L}^k = 0$ for some $k \geq 1$.

Remark 1.2.4. Obviously, any abelian Lie algebra is nilpotent.

Cartan subalgebras of Lie algebras play a central role in our study; we define them next.

Definition 1.2.5. Let $\mathfrak{L}$ be a Lie algebra over R. A **Cartan subalgebra** H of $\mathfrak{L}$ is a nilpotent subalgebra which is self-normalizing.

We also need the following definition.

Definition 1.2.6. If $\mathfrak{L}$ is a Lie algebra over R, then for any $x \in \mathfrak{L}$, the map $y \mapsto [x, y], y \in \mathfrak{L}$, is an R-homomorphism of $\mathfrak{L}$ into $\mathfrak{L}$, which is denoted by $\operatorname{ad} x$ and is called the **adjoint representation**. Let $x, y \in \mathfrak{L}$, and define $K(x, y) := \operatorname{Tr}(\operatorname{ad} x \cdot \operatorname{ad} y)$, where Tr is the trace of a matrix, then K is a symmetric bilinear form on $\mathfrak{L}$, called the **Killing form**.

Definition 1.2.7. Let $\mathfrak{L}$ and $\mathfrak{M}$ be Lie algebras over R. A **Lie algebra homomorphism** of $\mathfrak{L}$ into $\mathfrak{M}$ is a mapping $\varphi : \mathfrak{L} \to \mathfrak{M}$ which is a homomorphism of R-modules and that satisfies

$$\varphi([x, y]) = [\varphi(x), \varphi(y)]$$

for all $x, y \in \mathfrak{L}$. If the mapping φ is also a bijection, then it is called an **isomorphism**. An isomorphism from $\mathfrak{L}$ onto itself is called an **automorphism.** The set of all automorphisms in $\mathfrak{L}$ forms a group denoted by $\operatorname{Aut}(\mathfrak{L})$. We say that a subalgebra H_1 is **conjugate** to a subalgebra H_2 if there exist $\phi \in \operatorname{Aut}(\mathfrak{L})$ such that $\phi(H_1) = H_2$

The following simple observation of the Killing form is useful for the study of orthogonal decomposition of Lie algebras.

Proposition 1.2.8. *The Killing form is invariant under any automorphism ϕ of a Lie algebra $\mathfrak{L}$ over R.*

Proof. For $x, y \in \mathfrak{L}$, let $z = \phi(y)$. Then $\phi([x, \phi^{-1}(z)] = [\phi(x), z])$, equivalently,

$$\operatorname{ad} \phi(x) = \phi \circ \operatorname{ad} x \circ \phi^{-1}.$$

Therefore,

$$\begin{aligned} K(\phi(x), \phi(y)) &= \operatorname{Tr}(\operatorname{ad} \phi(x) \operatorname{ad} \phi(y)) \\ &= \operatorname{Tr}(\phi \circ \operatorname{ad} x \operatorname{ad} y \circ \phi^{-1}) \\ &= \operatorname{Tr}(\operatorname{ad} x \operatorname{ad} y) \\ &= K(x, y), \end{aligned}$$

as desired. □

1.3 Linear Lie algebras

We now recall the definitions of the linear Lie algebras that will be studied and some formulas for their Killing forms.

Let e_{ij} be the $n \times n$ matrix having 1 in the (i, j) position and 0 elsewhere. Since $e_{ij}e_{kl} = \delta_{jk}e_{il}$, where δ_{jk} is the Kronecker delta, it follows that:

$$[e_{ij}, e_{kl}] = \delta_{jk}e_{il} - \delta_{li}e_{kj}.$$

We note that the Killing form formulas presented below hold in any commutative ring with identity case.

Type *A*: Let $\mathfrak{sl}_n(R)$ be the set of $n \times n$ matrices over R having trace zero. Since the trace satisfies $\operatorname{Tr}(xy) = \operatorname{Tr}(yx)$ and $\operatorname{Tr}(x + y) = \operatorname{Tr}(x) + \operatorname{Tr}(y)$, $\mathfrak{sl}_n(R)$ is a Lie subalgebra of

$\mathfrak{gl}_n(R)$, called the **special linear Lie algebra**. It is also a free R-module of rank n^2-1 generated by e_{ij} $(i \neq j)$ along with $e_{ii} - e_{i+1,i+1}$ $(1 \leq i \leq n-1)$. The Killing form is equal to

$$K(A,B) = 2n\mathrm{Tr}(AB)$$

for all $A, B \in \mathfrak{sl}_n(R)$.

Type C: Let

$$K = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

Let $\mathfrak{sp}_{2n}(R)$ be the set

$$\{X \in M_{2n}(R) : XK + KX^T = 0\}.$$

This is a Lie subalgebra of $\mathfrak{gl}_{2n}(R)$ which is called the **symplectic Lie algebra**. For $x \in \mathfrak{sp}_{2n}(R)$, write

$$x = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

for some $s, t, u, v \in \mathfrak{gl}_n(R)$. From the definition, $t^T = t, u^T = u$ and $s^T = -v$. Thus, it is a Lie subalgebra of $\mathfrak{sl}_{2n}(R)$ generated by $e_{ii} - e_{n+i,n+i}$ $(1 \leq i \leq n), e_{ij} - e_{n+j,n+i}$ $(1 \leq i \neq j \leq n), e_{i,n+i}$ $(1 \leq i \leq n), e_{i,n+j} + e_{j,n+i}$ $(1 \leq i < j \leq n), e_{n+i,i}$ $(1 \leq i \leq n)$ and $e_{n+i,j} + e_{n+j,i}$ $(1 \leq i < k \leq n)$. The Killing form is equal to

$$K(A,B) = (4n+2)\mathrm{Tr}(AB)$$

for all $A, B \in \mathfrak{sp}_{2n}(R)$.

Type B: Assume that $\mathrm{char}(R)$ is odd or 0. Recall that a matrix A is skew-symmetric if $A^T = -A$. Denoted by $\mathfrak{so}_{2n-1}(R)$, the set of $(2n-1) \times (2n-1)$ skew-symmetric matrices over R. Obviously, this is a linear Lie algebra, called the **special orthogonal Lie algebra**, and a free R-module of rank $(n-1)(2n-1)$ generated by $e_{ij} - e_{ji}, i \neq j$. The Killing form

is equal to

$$K(A,B) = (2n-3)\mathrm{Tr}(AB)$$

for all $A, B \in \mathfrak{so}_{2n-1}(R)$.

Type *D*: Assume that $\mathrm{char}(R)$ is odd or 0. Denoted by $\mathfrak{so}_{2n}(R)$, the set of $2n \times 2n$ skew-symmetric matrices over R. Obviously, this is a linear Lie algebra and a free R-module of rank $n(2n-1)$ generated by $e_{ij} - e_{ji}, i \neq j$. The Killing form is equal to

$$K(A,B) = (2n-2)\mathrm{Tr}(AB)$$

for all $A, B \in \mathfrak{so}_{2n}(R)$.

1.4 Finite commutative rings

From now on, we assume that our ring R is finite. We will investigate sufficient conditions on a given ring for the existence of orthogonal decompositions of considered Lie algebras, especially the special linear algebra in Chapter 3. We will need some basic properties of a finite commutative ring with identity, and we will briefly describe these properties next. For more details about finite commutative rings theory, we refer the reader to [1, 14]. Here, we begin by recalling the definition of a finite local ring.

Definition 1.4.1. A finite commutative ring R with identity is called **local** if R has a unique maximal ideal.

Remark 1.4.2. The characteristic of a finite local ring is a prime power integer.

Example 1.4.3. Any finite field is local. For a prime integer p and a positive integer s, $\mathbb{Z}_{p^s}$ is local.

We have the following structure theorem of finite commutative rings (Theorem VI. 2 of [14]).

Theorem 1.4.4. *Let R be a finite commutative ring with identity. Then R decomposes uniquely (up to order of summands) as a direct sum of finite local rings, i.e.*

$$R = R_1 \times R_2 \times \cdots \times R_t$$

where all $R_i's$ are finite local rings.

We can use this theorem to study the unit group group of R denoted by $R^\times$. We recall the unit group of a finite local ring and also the unit group of a finite commutative ring as direct product of unit group of each summand. First, recall the following result about the unit group of a finite field.

Theorem 1.4.5. *[1] Let $\mathbb{F}_q$ be a finite field with q elements. Then $\mathbb{F}_q^\times$ is a cyclic group of order $q-1$.*

For a finite local ring, the unit group can be described by the following theorem.

Theorem 1.4.6. *[14] Let R be a finite local ring with the maximal ideal M and residue field $k = R/M$. Then*

$$R^\times \cong (1+M) \times k^\times.$$

For a general finite commutative ring with identity, the unit group can be described by:

Theorem 1.4.7. *[14] Let $R = R_1 \times R_2 \times \cdots \times R_t$ be a direct product of finite local rings. Then $R^\times$ is the direct product of groups*

$$R^\times \cong R_1^\times \times R_2^\times \times \cdots \times R_t^\times.$$

1.5 Symplectic spaces and quadratic spaces

We now recall some basics about symplectic spaces and quadratic spaces, for more details, see [5, 21]. These materials will be needed in the construction of the orthogonal decomposition

of $\mathfrak{sp}_{2^{m+1}}$ in Chapter 4.

Definition 1.5.1. Let V be a vector space over a field F. A **symplectic form** is a nondegenerate bilinear map $\langle \cdot, \cdot \rangle : V \times V \to F$ such that $\langle v, v \rangle = 0$ for all $v \in V$. We call the order pair $(V, \langle \cdot, \cdot \rangle)$ a **symplectic space**.

The following subspace will be considered.

Definition 1.5.2. Let $(V, \langle \cdot, \cdot \rangle)$ be a symplectic space over a field F and let W be a linear subspace of V. Then W is called **totally isotropic** if $\langle u, v \rangle = 0$ for all $u, v \in W$.

We will only work with symplectic form over a finite fields, especially over $\mathbb{Z}_2$. The following fact about the dimension of a totally isotropic subspace over a finite field is well-known (see for example [21])

Theorem 1.5.3. *Let $\mathbb{F}_q$ be a finite field. Totally isotropic subspaces of $\mathbb{F}_q^{2m}$ are of dimension $\leq m$, and there exist totally isotropic subspaces of dimension m. Hence, maximal totally isotropic subspaces are of dimension m. Moreover, any totally isotropic subspace is contained in a maximal totally isotropic subspace.*

In what follows, we introduce a quadratic space over a field and its special subspaces, the so-called totally singular subspaces.

Definition 1.5.4. Let V be a vector space over a field F. A map $q : V \to F$ is a **quadratic form** if:

- $q(cv) = c^2 q(v)$ for all $c \in F, v \in V$;
- the map $\beta(u, v) := q(u + v) - q(u) - q(v)$ for all $u, v \in V$, is a symmetric bilinear form on V.

The ordered pair (V, q) is called a **quadratic space**. Moreover, q is said to be **nondegenerate** if β is nondegenerate.

Definition 1.5.5. Let q be a quadratic form on V. A subspace W of V is **totally singular** if $q(w) = 0$ for all $w \in W$. The maximum dimension of a totally singular subspace of V is called the **Witt index** of V.

1.6 Thesis outline

The remainder of this dissertation is organized as follows.

In Chapter 2, we precisely define an orthogonal decomposition of Lie algebras that will be considered in this dissertation and provide some simple examples. Since a finite commutative ring with identity is a direct sum of local rings, we describe a relationship between an orthogonal decomposition and the decomposition of the ring.

In Chapter 3, we begin with the investigation of a special type of orthogonal decomposition (we call it classical) of $\mathfrak{sl}_n, n = 2, 3$, over a finite field. These small cases provide insight to some sufficient conditions on the ring that will permit an orthogonal decomposition of $\mathfrak{sl}_n$ over that ring. On the other hand, the results of Chapter 2 lead us to necessary conditions on rings to admit an orthogonal decomposition of $\mathfrak{sl}_n$. We will also write a Magma code for the purpose of finding the maximum number of classical components for some small cases. Another special type of orthogonal decompositions that we construct in this chapter is called the $\mathbb{J}$-decomposition. We will finish this chapter by computing the number of orbits of this type of decompositions under conjugacy for $n = 2, 3$ over a finite field.

In Chapter 4, we construct an orthogonal decomposition of $\mathfrak{sp}_{2^{m+1}}$ over a finite commutative ring of odd characteristic with identity through the restriction of the decomposition of $\mathfrak{sl}_n$ given in Chapter 3. To do this, we need to use tools from the theories of symplectic spaces and quadratic spaces we discussed earlier.

In Chapter 5, we describe an orthogonal decomposition of $\mathfrak{so}_n$ over a finite commutative ring of odd characteristic with identity. We show that standard basis elements of this algebra form an orthogonal decomposition.

Chapter 2

Orthogonal decompositions of Lie algebras over finite commutative rings

In an orthogonal decomposition of a Lie algebra, the components are Cartan subalgebras. Over the complex numbers, Cartan subalgebras are abelian subalgebras [7]. However, for a modular Lie algebra over a general commutative ring, a Cartan subalgebra is not necessary abelian, thus, we will only consider decomposition that is formed by abelian Cartan subalgebras. Therefore, we will introduce the orthogonal decomposition into abelian Cartan subalgebras of Lie algebras over a finite commutative ring R with identity in this chapter. We use the abbreviation ODAC for this type of orthogonal decompositions (AC for "abelian Cartan"). We will begin with the definition of ODAC and some simple examples.

2.1 Definitions and examples

Definition 2.1.1. Let $\mathfrak{L}$ be a Lie algebra over a finite commutative ring R with 1. An **orthogonal decomposition into abelian Cartan subalgebras** (abbreviated as ODAC) of $\mathfrak{L}$ is a direct sum R-module decomposition

$$\mathfrak{L} = H_0 \oplus H_1 \oplus \ldots \oplus H_k, k \in \mathbb{N},$$

where the H_i's are pairwise orthogonal abelian Cartan subalgebras of $\mathfrak{L}$ with respect to the Killing form.

Example 2.1.2. Any abelian Lie algebra obviously has an ODAC with one component which is itself.

We give an ODAC for $\mathfrak{L} = \mathfrak{sl}_2(R)$ whose verification is straightforward in the next example.

Example 2.1.3. Assume that $2 \nmid \mathrm{char}(R)$. Then $\mathfrak{sl}_2(R)$ has an ODAC

$$\mathfrak{sl}_2(R) = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_R \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle_R \oplus \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle_R.$$

In this example, the assumption that 2 does not divide the characteristic of R is necessary for the sum being direct.

Definition 2.1.4. Suppose that

$$\mathfrak{L} = H_1 \oplus H_2 \oplus \cdots \oplus H_k$$

and

$$\mathfrak{L} = H_1' \oplus H_2' \oplus \cdots \oplus H_{k'}'.$$

are two ODACs of $\mathfrak{L}$. We say that these two ODACs are **conjugate** if $k = k'$ and there exists an automorphism $\phi \in \mathrm{Aut}(\mathfrak{L})$ such that for all $i \in \{1, 2, \ldots, k\}$, there exists a unique $j \in \{1, 2, \ldots, k\}$ such that $\phi(H_i) = H_j'$, i.e., H_i is conjugate to H_j.

The notion of ODAC conjugation will be helpful for the discussion of the ODAC problem of $\mathfrak{sl}_n$ over finite fields in Section 3.1 which will provide us significant information that leads us to the main results in Section 3.2.

2.2 Orthogonal decompositions over finite direct products of finite local rings

We will use the fact that a finite commutative ring R with identity is a direct product of a finite number of finite local rings to relate the problem of ODAC of a Lie algebra over R with that of the finite local rings. Let $R = R_1 \times R_2 \times \cdots \times R_t$, where R_i is a finite local ring. For each $i = 1, 2, \ldots, t$, let L_i be a module over R_i. Then $L = L_1 \oplus L_2 \oplus \cdots \oplus L_t$ is an R-module by defining the scalar multiplication as follows: for all $r = (r_1, r_2, \ldots, r_t) \in R$, where $r_i \in R_i$,

$$r.(x_1, x_2, \ldots, x_t) := (r_1x_1, r_2x_2, \ldots, r_tx_t)$$

where $(x_1, x_2, \ldots, x_t) \in L$. If each L_i is a Lie algebra over R_i, then we can naturally define the Lie bracket on L by taking the componentwise bracket.

Lemma 2.2.1. *Let $\mathfrak{L}_i$ be a Lie algebra over $R_i, i = 1, 2, \ldots, t$. Then*

$$L = \mathfrak{L}_1 \oplus \mathfrak{L}_2 \oplus \cdots \oplus \mathfrak{L}_t$$

is a Lie algebra over R with the bracket defined by

$$[(x_1, x_2, \ldots, x_t), (y_1, y_2, \ldots, y_t)] := ([x_1, y_1], [x_2, y_2], \ldots, [x_t, y_t]),$$

where $(x_1, x_2, \ldots, x_t), (y_1, y_2, \ldots, y_t) \in L$.

Proof. It is clear that the bracket operation is bilinear and satisfies anticommutativity. For any $(x_1, x_2, \ldots, x_t), (y_1, y_2, \ldots, y_t), (z_1, z_2, \ldots, z_t) \in L$, we have

$$[[(x_1, x_2, \ldots, x_t), (y_1, y_2, \ldots, y_t)], (z_1, z_2, \ldots, z_t)] = ([[x_1, y_1], z_1], [[x_2, y_2], z_2], \ldots, [[x_t, y_t], z_t]).$$

By the Jacobi identity of each component, this bracket satisfies the Jacobi identity. □

We will first prove the necessity and sufficiency for the existence of ODAC of a general Lie algebra over R in terms of its R_i form, that is, a Lie algebra obtained by restricting the coefficients to R_i, for each i. Then we will consider the linear Lie algebras in the latter part of this section. We will utilize the projection maps to obtain the desired results. Let Proj_i denote the projection map onto the ith coordinate. Then we have:

Lemma 2.2.2. *For $i \in \{1, 2, \ldots, t\}$, let $\mathfrak{L}_i$ be a Lie algebra over R_i and let $\mathfrak{L}$ be a Lie algebra over R. With the bracket in Lemma 2.2.1, assume that $\mathfrak{L} \cong \mathfrak{L}_1 \oplus \mathfrak{L}_2 \oplus \cdots \oplus \mathfrak{L}_t$ as Lie algebras over R via an isomorphism ϕ. If H is an abelian Cartan subalgebra of $\mathfrak{L}$, then $\mathrm{Proj}_i(\phi(H))$ is an abelian Cartan subalgebra of $\mathfrak{L}_i$ for all $i = 1, 2, \ldots, t$.*

Proof. It suffices to prove the case $t = 2$ and $i = 1$ since similar arguments hold for the other cases. It is clear that $\mathrm{Proj}_1(\phi(H))$ is an R_1-submodule of $\mathfrak{L}_1$. Let $x, y \in \mathrm{Proj}_1(\phi(H))$. Using the scalar $(1, 0)$, we observe that $(x, 0)$ and $(y, 0)$ are in $\phi(H)$. Since H is abelian, so is $\phi(H)$ and

$$[x, y] = \mathrm{Proj}_1([x, y], [0, 0]) = \mathrm{Proj}_1[(x, 0), (y, 0)] = \mathrm{Proj}_1(0, 0) = 0.$$

Thus, $\mathrm{Proj}_1(\phi(H))$ is an abelian subalgebra of $\mathfrak{L}_1$ and so it is nilpotent.

We show that $\mathrm{Proj}_1(\phi(H))$ is a self-normalizer of $\mathfrak{L}_1$. For convenience, we denote $H_i := \mathrm{Proj}_i(\phi(H))$ for all $i = 1, 2$. Let $x \in N_{\mathfrak{L}_1}(H_1)$. Then $[x, H_1] \subseteq H_1$. For any $h \in H$,

$$\begin{aligned}
[(x, 0), \phi(h)] &= [(x, 0), (\mathrm{Proj}_1(\phi(h)), \mathrm{Proj}_2(\phi(h)))] \\
&= ([x, \mathrm{Proj}_1(\phi(h))], [0, \mathrm{Proj}_2(\phi(h))]) \\
&= ([x, \mathrm{Proj}_1(\phi(h))], 0) \in (H_1, H_2) = \phi(H).
\end{aligned}$$

Then, $[(x, 0), \phi(H)] \subseteq \phi(H)$. Since H is a self-normalizer, so is $\phi(H)$. Thus, $(x, 0) \in \phi(H)$. Therefore, $N_{\mathfrak{L}_1}(H_1) = H_1$. □

Theorem 2.2.3. *For $i \in \{1, 2, \ldots, t\}$, let $\mathfrak{L}_i$ and $\mathfrak{L}$ be as in Lemma 2.2.2. Then $\mathfrak{L}$ has an ODAC if and only if $\mathfrak{L}_i$ has an ODAC for all $i = 1, 2, \ldots, t$.*

Proof. Assume that $\mathfrak{L} = H_1 \oplus H_2 \oplus \cdots \oplus H_k$ is an ODAC of $\mathfrak{L}$. We show that $\mathfrak{L}_1$ has an ODAC

$$\mathfrak{L}_1 = \mathrm{Proj}_1(\phi(H_1)) \oplus \mathrm{Proj}_1(\phi(H_2)) \oplus \cdots \oplus \mathrm{Proj}_1(\phi(H_k)).$$

Similar arguments work for the other $\mathfrak{L}_i$'s. By Lemma 2.2.2, each $\mathrm{Proj}_1(\phi(H_j))$ is an abelian Cartan subalgebra of $\mathfrak{L}_1$. Let $x \in \mathfrak{L}_1$ and $x_0 \in \mathfrak{L}$ such that $\phi(x_0) = (x, 0, \ldots, 0)$. Due to the ODAC of $\mathfrak{L}$, we have

$$x_0 = x_{0,1} + x_{0,2} + \cdots + x_{0,k},$$

for some $x_{0,j} \in H_j$, and

$$x = \mathrm{Proj}_1(\phi(x_0)) = \mathrm{Proj}_1(\phi(x_{0,1})) + \mathrm{Proj}_1(\phi(x_{0,2})) + \cdots + \mathrm{Proj}_1(\phi(x_{0,k})).$$

So, $\mathfrak{L}_1 \subseteq \sum_{j=1}^{k} \mathrm{Proj}_1(\phi(H_j))$. On the other hand, it is clear that $\mathfrak{L}_1 \supseteq \sum_{j=1}^{k} \mathrm{Proj}_1(\phi(H_j))$. Next, let $j_0 \in \{1, 2, \ldots, k\}$ and $x \in \mathrm{Proj}_1(\phi(H_{j_0})) \cap \sum_{j \neq j_0} \mathrm{Proj}_1(\phi(H_j))$. Then there exist $(h_2, \ldots, h_t), (h'_2, \ldots, h'_t) \in \sum_{i=2}^{t} \mathfrak{L}_i$ such that

$$(x, h_2, \ldots, h_t) \in \phi(H_{j_0}) \text{ and } (x, h'_2, \ldots, h'_t) \in \sum_{j \neq j_0} \phi(H_j).$$

Let $r = (1, 0, \ldots, 0) \in R_1 \times R_2 \times \cdots \times R_t$. So,

$$(x, 0, \ldots, 0) = r(x, h_2, \ldots, h_t) = r(x, h'_2, \ldots, h'_t) \in \phi(H_{j_0}) \cap \sum_{j \neq j_0} \phi(H_j)$$

and hence $x = 0$, i.e., the sum is direct. Let K_i be the Killing form for $\mathfrak{L}_i$. Then the Killing form K for $\mathfrak{L}$ is equal to

$$K(x, y) = K_1(x_1, y_1) + K_2(x_2, y_2) + \cdots + K_t(x_t, y_t)$$

for all $x = (x_1, x_2, \ldots, x_t), y = (y_1, y_2, \ldots, y_t) \in \mathfrak{L}$. Finally, we prove that $\mathrm{Proj}_1(\phi(H_{j_1}))$ is orthogonal to $\mathrm{Proj}_1(\phi(H_{j_2}))$ with respect to the Killing from K_1 if $j_1 \neq j_2$. Let $x \in \mathrm{Proj}_1(\phi(H_{j_1}))$ and $y \in \mathrm{Proj}_1(\phi(H_{j_2}))$. Then $(x, 0, \ldots, 0) \in \phi(H_{j_1})$ and $(y, 0, \ldots, 0) \in \phi(H_{j_2})$. Moreover,

$$K_1(x, y) + K_2(0, 0) + \ldots + K_t(0, 0) = K((x, 0, \ldots, 0), (y, 0, \ldots, 0)) = 0.$$

Therefore, $K_1(x, y) = 0$.

Conversely, we suppose that each $\mathfrak{L}_i, i = 1, 2, \ldots, t$, has an ODAC with k_i components. We can add the zero submodules to the ODAC of each $\mathfrak{L}_i$ and assume that all direct sums have the same number of terms, say k. For each $i = 1, 2, \ldots, t$ and $j = 1, 2, \ldots, k$, let H_{ij} be the jth component of ODAC of $\mathfrak{L}_i$ if $j \leq k_i$ and $H_{ij} = 0$ if $j > k_i$. Then $\mathfrak{L}$ has an ODAC

$$\mathfrak{L} = H_1 \oplus H_2 \oplus \cdots \oplus H_k,$$

where $H_j = \phi^{-1}(H_{1j}, H_{2j}, \ldots, H_{tj})$. □

We will relate the decomposition of the ring R to that of a linear Lie algebra. Note that the multiplication

$$((a_{ij}^{(1)}), (a_{ij}^{(2)}), \ldots, (a_{ij}^{(t)})) \cdot ((b_{ij}^{(1)}), (b_{ij}^{(2)}), \ldots, (b_{ij}^{(t)})) = ((a_{ij}^{(1)})(b_{ij}^{(1)}), (a_{ij}^{(2)})(b_{ij}^{(2)}), \ldots, (a_{ij}^{(t)})(b_{ij}^{(t)})),$$

defines an R-algebra structure on $\mathfrak{gl}_n(R_1) \oplus \mathfrak{gl}_n(R_2) \oplus \cdots \oplus \mathfrak{gl}_n(R_t)$. Consequently, we can define the bracket $[\cdot, \cdot]$ on it to be the componentwise commutator and immediately see that this bracket is a finite tuple of Lie brackets from each component. From Lemma 2.2.1, it follows that this R-algebra is a Lie algebra over R. Note that for each $a \in R$, we can write $a = (a^{(1)}, a^{(2)}, \ldots, a^{(t)})$ uniquely. Define

$$\phi : \mathfrak{gl}_n(R) \longrightarrow \mathfrak{gl}_n(R_1) \oplus \mathfrak{gl}_n(R_2) \oplus \cdots \oplus \mathfrak{gl}_n(R_t)$$

$$(a_{ij}) \longmapsto ((a_{ij}^{(1)}), (a_{ij}^{(2)}), \ldots, (a_{ij}^{(t)}))$$

for all $(a_{ij}) \in \mathfrak{gl}_n(R)$. Clearly, ϕ is an R-module isomorphism.

Let $A = (a_{ij}), B = (b_{ij}) \in \mathfrak{gl}_n(R)$. Then

$$\begin{aligned}
\phi(AB) &= \phi((a_{ij})(b_{ij})) \\
&= \phi((\sum_l a_{il}b_{lj})) \\
&= ((\sum_l a_{il}^{(1)}b_{lj}^{(1)}), (\sum_l a_{il}^{(2)}b_{lj}^{(2)}), \ldots, (\sum_l a_{il}^{(t)}b_{lj}^{(t)})) \\
&= ((a_{ij}^{(1)})(b_{ij}^{(1)}), (a_{ij}^{(2)})(b_{ij}^{(2)}), \ldots, (a_{ij}^{(t)})(b_{ij}^{(t)})) \\
&= ((a_{ij}^{(1)}), (a_{ij}^{(2)}), \ldots, (a_{ij}^{(t)})) \cdot ((b_{ij}^{(1)}), (b_{ij}^{(2)}), \ldots, (b_{ij}^{(t)})) \\
&= \phi((a_{ij}))\phi((b_{ij})) = \phi(A)\phi(B).
\end{aligned}$$

So, $\phi([A, B]) = \phi(AB - BA) = \phi(AB) - \phi(BA) = \phi(A)\phi(B) - \phi(B)\phi(A) = [\phi(A), \phi(B)]$. Thus, we have the following corollary.

Corollary 2.2.4. *Let $R = R_1 \times R_2 \times \cdots \times R_t$ be a finite direct product of finite local rings. Then we have the following:*

(i) There is a Lie algebra (over R) isomorphism

$$\phi : \mathfrak{gl}_n(R) \longrightarrow \mathfrak{gl}_n(R_1) \oplus \mathfrak{gl}_n(R_2) \oplus \cdots \oplus \mathfrak{gl}_n(R_t).$$

(ii) If $\mathfrak{g}$ is a Lie subalgebra of $\mathfrak{gl}_n(R)$, then

$$\mathfrak{g} \cong \mathrm{Proj}_1(\phi(\mathfrak{g})) \oplus \mathrm{Proj}_2(\phi(\mathfrak{g})) \oplus \cdots \oplus \mathrm{Proj}_t(\phi(\mathfrak{g})).$$

Moreover, $\mathfrak{g}$ has an ODAC *if and only if* $\mathrm{Proj}_i(\phi(\mathfrak{g}))$ *has an* ODAC *for all* $i = 1, 2, \ldots, t$.

Chapter 3

Orthogonal decompositions of Lie algebras of type A

In this chapter, we consider the ODAC problem of the special linear Lie algebra $\mathfrak{sl}_n(R)$. In Section 3.1, due to the availability of tools for modular Lie algebras over fields of characteristic $p > 0$ (see [17]), we will first explore the special type of ODAC (the so-called classical) of $\mathfrak{sl}_n$ over a finite field when $n = 2, 3$. The observations in these special cases will then be used in Section 3.2 to derive the main results for $n \geq 2$. These results provide sufficient conditions for the existence of an ODAC of $\mathfrak{sl}_n$ over a finite commutative ring with identity. In the cases of a finite local ring and a finite field, the verifications of these conditions are straight forward for the given ring and field since the needed information is readily obtained from their structures.

3.1 Classical orthogonal decompositions of $\mathfrak{sl}_n, n = 2, 3$ over finite fields

For a prime integer $p \neq 2, 3$ and a positive integer m, let $\mathbb{F}_q$ be a finite field of $q = p^m$ elements.

Definition 3.1.1. A Lie algebra $\mathfrak{L}$ over $\mathbb{F}_q$ is called **classical** if:

1. the center of $\mathfrak{L}$ is zero;
2. $[\mathfrak{L}, \mathfrak{L}] = \mathfrak{L}$;
3. $\mathfrak{L}$ has a abelian Cartan subalgebra H, relative to which:
   (a) $\mathfrak{L} = \oplus \mathfrak{L}_\alpha$, where $\mathfrak{L}_\alpha := \{x \in \mathfrak{L} : [h, x] = \alpha(x)x \text{ for all } h \in H\}$;
   (b) if $\alpha \neq 0$ is a root, $[\mathfrak{L}_\alpha, \mathfrak{L}_{-\alpha}]$ is one-dimensional;
   (c) if α and β are roots, and if $\beta \neq 0$, then not all $\alpha + k\beta$ are roots, where $1 \leq k \leq p-1$.

   An abelian Cartan subalgebra H satisfying (a), (b) and (c) is called a **classical** Cartan subalgebra.

It is known that all classical Cartan subalgebras of a classical Lie algebra $\mathfrak{L}$ over $\mathbb{F}_q$ are conjugate [17].

Suppose that $\mathfrak{L} = H + \sum_\alpha \mathfrak{L}_\alpha$ the root subspace decomposition relative to a classical Cartan subalgebra H. Let $G'(\mathfrak{L})$ be the group of automorphisms of $\mathfrak{L}$ generated by all $\exp(\operatorname{ad} x_\alpha)$ where $x_\alpha \in \mathfrak{L}_\alpha,\ \alpha \neq 0$.

Theorem 3.1.2. *[17] Let H_1, H_2 be classical Cartan subalgebras of $\mathfrak{L}$. Then there exists a $\sigma \in G'(\mathfrak{L})$ such that $\sigma(H_1) = H_2$.*

We now define a classical ODAC.

Definition 3.1.3. An ODAC of a Lie algebra $\mathfrak{L}$ over $\mathbb{F}_q$ is said to be **classical** if all of its components are classical Cartan subalgebras.

Example 3.1.4. From Example 2.1.3, $\mathfrak{sl}_2(\mathbb{Z}_7)$ has an ODAC

$$\mathfrak{sl}_2(\mathbb{Z}_7) = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{Z}_7} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}_7} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}_7}.$$

However, it is not classical because $\sqrt{-1}$ is undefined here and so the adjoint action of the second matrix is not semisimple, i.e., $\mathfrak{sl}_2(\mathbb{Z}_7)$ does not have a root subspace decomposition relative to the second summand.

In this section, we investigate the classical ODAC problem for a classical $\mathfrak{sl}_n(\mathbb{F}_q), n = 2, 3$. Since we assume that $\mathfrak{sl}_n(\mathbb{F}_q)$ is classical, $\mathrm{char}(\mathbb{F}_q)$ is not equal to n. Let H_0 be the classical Cartan subalgebra of $\mathfrak{sl}_n(\mathbb{F}_q)$ consisting of the diagonal matrices. We suppose that $\mathfrak{sl}_n(\mathbb{F}_q)$ has a classical ODAC, then by Proposition 1.2.8, we can assume that one of the components is H_0. It is clear that K is non-degenerate because $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$. Since each $\mathrm{ad}(h), h \in H_0$, has all its characteristic roots in $\mathbb{F}_q$, we have:

Proposition 3.1.5. *[17] Under the above hypotheses, the restriction to H_0 of K is nondegenerate.*

Let H be a classical Cartan subalgebra of $\mathfrak{sl}_n(\mathbb{F}_q)$ orthogonal to H_0 with respect to K. Since H and H_0 are conjugate, $K_{|_H}$ is also non-degenerate. In the next lemma, we give a description of H.

Lemma 3.1.6. *Under the above setting, we have the following statements.*

(1) If $n = 2$, then

$$H = \left\langle \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}$$

for some $a \neq 0$.

(2) If $n = 3$, then

$$H = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & a \\ ab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ ab & 0 & 0 \\ 0 & b & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}$$

for some $a, b \neq 0$.

Proof. We only provide the proof for $n = 3$ since similar arguments apply to the case $n = 2$. We first prove the following assertions:

(a) Every matrix in H has a zero diagonal.

(b) Every nonzero matrix in H has no zero row nor zero column.

(c) H admits a basis $\{A_2, A_3\}$ satisfying the conditions below, $k = 2, 3$:

(i) The first row of A_k has 1 in the k-th position and 0 elsewhere.

(ii) The first position of the k-th column of A_k is the only nonzero element in that column.

(iii) The j-th row of A_k coincides with the k-th row of A_j.

First note that (a) holds since H is orthogonal to H_0 and the characteristic of the field is not equal to 2 or 3. If we assume (b), then it follows that H has a basis $\{A_2, A_3\}$ with property (i). We use the commutativity of H to prove (iii). By (i), the j-th row of A_k equals the first row of the product A_jA_k, but $A_jA_k = A_kA_j$, so it equals the k-th row of A_j. To prove (ii), we note that for $j \geq 2$, the j-th element of the k-th column of A_k is the k-th element of the j-th row of A_k, so by (iii), it is equal to the k-th element of the k-th row of A_j, and therefore it is zero by (a). To prove (b), we assume the contrary. Without loss of generality, we may assume that there exists a nonzero matrix $A \in H$ whose first row is zero, i.e.

$$A = \begin{pmatrix} 0 & 0 & 0 \\ a & 0 & b \\ c & d & 0 \end{pmatrix},$$

where a, b, c, d are not all zero. Note that H has dimension two. Let B be a nonzero matrix such that $H = \langle A, B \rangle_{\mathbb{F}_q}$. Write

$$B = \begin{pmatrix} 0 & x & y \\ u & 0 & z \\ v & w & 0 \end{pmatrix},$$

where x, y, z, u, v, w are not all zero, then

$$[A, B] = \begin{pmatrix} -ax - cy & -dy & -bx \\ bv - cz & bw + ax - dz & ay \\ du - aw & cx & -bw + cy + dz \end{pmatrix} \tag{3.1}$$

equals zero because H is abelian. If the product $abcd$ is zero, then it can be verified that the Killing form would be degenerate on H. This can be done either by considering different cases or using computational algebra packages. Using the latter method, it is straightforward that the determinant of the Killing form is contained in the ideal $J \subset \mathbb{Z}[a, b, c, d, x, y, z, u, v, w]$ generated by the entries of $[A, B]$ and $abcd$. Codes in both Sage and Magma are provided in Appendix A for this purpose. Therefore, all a, b, c and d are nonzero. Now, by (3.1), $x = y = 0$ and we may assume that $a = 1$. So, we have $bv = cz, bw = dz$ and $du = w$. These can be reduced to $z = bu$ and $v = cu$. Since $B \neq 0$, $u \neq 0$. Again, we may assume that $u = 1$. Then $d = w, b = z$ and $c = v$, i.e., $A = B$, which contradicts the choice of B. Therefore, (b) holds.

From the above discussions, H admits a basis of the form

$$\left\{ \begin{pmatrix} 0 & 1 & 0 \\ x & 0 & a \\ * & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ * & 0 & 0 \\ y & b & 0 \end{pmatrix} \right\}$$

where $a, b \neq 0$. Since H is abelian, $x = y = 0$ and $* = ab$. □

The above lemma leads us to the existence of an ODAC of $\mathfrak{sl}_n(\mathbb{F}_q)$, when $n = 2, 3$. For $n = 2$, the decomposition (some cases are classical) always exists because $\mathrm{char}(\mathbb{F}_q) \neq 2$ (see Example 2.1.3). Moreover, we note that any classical ODAC of $\mathfrak{sl}_2(\mathbb{F}_q)$(if one exists) is

conjugate to

$$\mathfrak{sl}_2(\mathbb{F}_q) = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{F}_q} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}, \tag{3.2}$$

for some $a \neq 0$. For $n = 3$, we state the result as a theorem.

Theorem 3.1.7. *Let $\mathbb{F}_q$ be a finite field of $q = p^m$ elements with characteristic $p \neq 2, 3$. Then $\mathfrak{sl}_3(\mathbb{F}_q)$ has a classical ODAC if and only if $3|(q-1)$. In that case, for any primitive cube root of unity $u \in \mathbb{F}_q$, we have the following classical ODAC:*

$$\mathfrak{sl}_3(\mathbb{F}_q) = H_0 \oplus H_1 \oplus H_2 \oplus H_3,$$

where

$$H_1 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q},$$

$$H_2 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & u \\ u^2 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ u^2 & 0 & 0 \\ 0 & u & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q},$$

$$H_3 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & u^2 \\ u & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ u & 0 & 0 \\ 0 & u^2 & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}.$$

Proof. Assume that $3|(q-1)$. Since the unit group $\mathbb{F}_q^\times$ is cyclic and $|\mathbb{F}_q^\times| = q-1$, there exists a primitive cube root of unity $u \in \mathbb{F}_q$. The verification that the given decomposition is an ODAC of $\mathfrak{sl}_3(\mathbb{F}_q)$ is straightforward. Let

$$X = \begin{pmatrix} 1 & 1 & u \\ u & 1 & 1 \\ 1 & u & 1 \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} u & u & 1 \\ u & 1 & u \\ u & u^2 & u^2 \end{pmatrix}.$$

Then both X and Y are nonsingular. Note that conjugation by X (resp. X^2), changes H_2

(resp. H_3) to H_0, and conjugation by Y changes H_1 to H_0. Since H_0 is a classical Cartan subalgebra, so are H_1, H_2 and H_3. Thus, this decomposition is classical.

Conversely, suppose that $3 \nmid (q-1)$ but $\mathfrak{sl}_3(\mathbb{F}_q)$ possesses a classical ODAC. Note that the decomposition of $\mathfrak{sl}_3(\mathbb{F}_q)$ has 4 components. Then, up to conjugacy, we can assume that H_0 is one of the components and, by Lemma 3.1.6, all other components are of the forms

$$H_1' = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & a \\ ab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ ab & 0 & 0 \\ 0 & b & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}$$

$$H_2' = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & c \\ cd & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ cd & 0 & 0 \\ 0 & d & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}$$

$$H_3' = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & e \\ ef & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ ef & 0 & 0 \\ 0 & f & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}$$

for some $a, b, c, d, e, f \neq 0$. By the orthogonality between H_1' and H_2', we have $cd + ad + ab = 0$ and $cd + cb + ab = 0$. Then $d = a^{-1}cb$. Substituting d in the first equation, we get $c^2 + ac + a^2 = 0$. However, since $3 \nmid (q-1)$, there is no primitive cube root of unity in $\mathbb{F}_q$, so the polynomial $x^2 + ax + a^2$ has no root in $\mathbb{F}_q$. This is a contradiction. □

Remark 3.1.8. By the above theorem, if $\mathbb{F}_q$ does not have a primitive cube root of unity, then the number of pairwise classical orthogonal Cartan subalgebras in $\mathfrak{sl}_3(\mathbb{F}_q)$ is at most two. If H_0 and H_1' is such a pair, then they must have the forms described in the theorem, and by [17], H_0 and H_1' are conjugate. However, the two matrices listed in H_1' are not diagonalizable over $\mathbb{F}_q$, so there is no orthogonal pair of classical Cartan subalgebras in $\mathfrak{sl}_3(\mathbb{F}_q)$ in this case.

Remark 3.1.9. If $\mathfrak{sl}_3(\mathbb{F}_q)$ has a classical ODAC, by the arguments in the proof of the above theorem, it must be, up to conjugacy, of the form

$$\mathfrak{sl}_3(\mathbb{F}_q) = H_0 \oplus H_1 \oplus H_2 \oplus H_3, \tag{3.3}$$

where

$$H_1 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & a \\ ab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ ab & 0 & 0 \\ 0 & b & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q},$$

$$H_2 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & ua \\ u^2ab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ u^2ab & 0 & 0 \\ 0 & ub & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q},$$

$$H_3 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & u^2a \\ uab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ uab & 0 & 0 \\ 0 & u^2b & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q},$$

for some nonzero a, b and a primitive cube root u of unity.

The collection of ODACs of the forms in (3.2) and (3.3) over finite fields will be considered again in Section 3.5. We will count the number of them up to conjugacy.

3.2 Orthogonal decompositions of $\mathfrak{sl}_n$ over finite commutative rings

We note that every matrix described in Theorem 3.1.7 is a product of a diagonal matrix and a permutation matrix. Let u be a primitive cube root of unity and let

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & u^2 \end{pmatrix} \text{ and } P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

then each matrix in Theorem 3.1.7 is of the form D^aP^b for some $a, b \in \{0, 1, 2\}$. We show that an ODAC of $\mathfrak{sl}_n(R)$ can be constructed under assumptions similar to the $n = 3$ case using the $n \times n$ version of matrices D and P.

The matrices D and P play a key role in the construction of OD for $\mathfrak{sl}_n(\mathbb{C})$ when $n = p^m$

for a prime integer p and a positive integer m [11]. To use them in our construction here, some of the differences must be noted. The matrix D requires the existence of a primitive pth root u of unity, which always exists in the complex number case. But for a general finite commutative ring, the existence of u needs to be assumed. Moreover, $u^{p-1} + \ldots + u + 1 = 0$ holds in $\mathbb{C}$, but this may not hold in a general finite commutative ring unless $u - 1$ is a unit. In addition, one can use Lie's theorem to verify that the constructed decomposition is an OD in the complex number case [11], but Lie's theorem is not available in the general cases considered here.

We will use the Kronecker product of matrices for the construction of ODAC in the next theorem. Recall that the Kronecker product (denoted by $\otimes$) of two matrices is the matrix obtained by multiplying each element from the left matrix by the whole right matrix e.g.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} x & y \\ u & v \end{bmatrix} = \begin{bmatrix} a \begin{bmatrix} x & y \\ u & v \end{bmatrix} & b \begin{bmatrix} x & y \\ u & v \end{bmatrix} \\ c \begin{bmatrix} x & y \\ u & v \end{bmatrix} & d \begin{bmatrix} x & y \\ u & v \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} ax & ay & bx & by \\ au & av & bu & bv \\ cx & cy & dx & dy \\ cu & cv & du & dv \end{bmatrix}.$$

Theorem 3.2.1. *Let R be a finite commutative ring with identity. For a prime power $n = p^m$, if there exists a primitive pth root of unity $u \in R^\times$ such that $u - 1 \in R^\times$, then $\mathfrak{sl}_n(R)$ has an* ODAC

$$\mathfrak{sl}_n(R) = H_\infty \oplus H_0 \oplus H_1 \oplus \cdots \oplus H_{n-1}.$$

Proof. We first consider the case $m = 1$. For $n = 2$, see Example 2.1.3. Assume that $p > 2$.

Let

$$D = \mathrm{diag}(1, u, \ldots, u^{p-1}) \text{ and } P = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Since $u^p - 1 = 0$ and $u - 1 \in R^\times$, $\mathrm{Tr}(D) = 1 + u + u^2 + \ldots + u^{p-1} = 0$. Thus, D and P are matrices in $\mathfrak{sl}_p(R)$ and p is the smallest positive integer such that $D^p = P^p = I$. For any $a, b \in \mathbb{Z}_p$, let $J_{(a,b)} = D^a P^b$. We have

$$\mathrm{Tr} J_{(a,b)} = 0 \Leftrightarrow (a, b) \neq (0, 0) \tag{3.4}$$

and

$$P^b D^a = u^{-ab} D^a P^b. \tag{3.5}$$

The last equation implies

$$J_{(a,b)} J_{(c,d)} = u^{-bc} J_{(a+c,b+d)} \text{ and} \tag{3.6}$$

$$[J_{(a,b)}, J_{(c,d)}] = (u^{-bc} - u^{-ad}) J_{(a+c,b+d)} \tag{3.7}$$

for $a, b, c, d \in \mathbb{Z}_p$. For $a, k \in \mathbb{Z}_p$ with $a \neq 0$, $J_{(a,ka)}$ and $J_{(0,a)}$ are elements of $\mathfrak{sl}_p(R)$ by (3.4). For a fixed $k \in \mathbb{Z}_p$, it follows immediately from the definitions of D and P that $J_{(1,k)}, J_{(2,2k)}, \ldots, J_{(p-1,k(p-1))}$ are linearly independent. Construct the following free R-submodules:

$$H_k = \langle J_{(a,ka)} | a \in \mathbb{Z}_p^\times \rangle_R, k \in \mathbb{Z}_p \text{ and}$$

$$H_\infty = \langle J_{(0,a)} | a \in \mathbb{Z}_p^\times \rangle_R = \langle P, P^2, \ldots, P^{p-1} \rangle_R.$$

By (3.7), H_∞ and H_k are Lie subalgebras of $\mathfrak{sl}_p(R)$.

Let

$$X = \begin{bmatrix} 1 & u^{\frac{p(p-1)}{2}} & u^{\frac{(p-1)(p-2)}{2}} & \cdots & u^3 & u \\ u & 1 & u^{\frac{p(p-1)}{2}} & \cdots & u^6 & u^3 \\ u^3 & u & 1 & \cdots & u^{10} & u^6 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ u^{\frac{(p-1)(p-2)}{2}} & u^{\frac{(p-2)(p-3)}{2}} & u^{\frac{(p-3)(p-4)}{2}} & \cdots & 1 & u^{\frac{p(p-1)}{2}} \\ u^{\frac{p(p-1)}{2}} & u^{\frac{(p-1)(p-2)}{2}} & u^{\frac{(p-2)(p-3)}{2}} & \cdots & u & 1 \end{bmatrix}.$$

Since $p > 2$ and $1 - u$ is a unit, X is invertible over R. It is straightforward to verify that $X^{-1}DPX = D$ and $X^{-1}PX = P$. Thus by (3.5), conjugation by the matrix X shifts $H_0, H_1, \ldots, H_{p-1}$ cyclically and fixes H_∞. We show that

$$\mathfrak{sl}_p(R) = H_\infty \oplus H_0 \oplus H_1 \oplus \cdots \oplus H_{p-1}. \tag{3.8}$$

It is clear from the construction that $H_0 \cap \sum_{j \neq 0} H_j = \{0\}$. In particular, the sum is direct for H_0 and H_∞. Thus, the sums for all H_i's are also direct, and we have $H_\infty \oplus H_0 \oplus H_1 \oplus \cdots \oplus H_{p-1}$, which is a free $R-$submodule of $\mathfrak{sl}_p(R)$. But we also have

$$|\mathfrak{sl}_p(R)| = |H_\infty \oplus H_0 \oplus H_1 \oplus \cdots \oplus H_{p-1}|.$$

Therefore, the equality (3.8) holds.

We prove that the decomposition (3.8) is pairwise orthogonal with respect to the Killing form $K(A, B) = 2p\mathrm{Tr}(AB)$. It is obvious that H_∞ is orthogonal to all others H_i's. Let $a, b \in \mathbb{Z}_p^\times, k_1, k_2 \in \mathbb{Z}_p$ with $k_1 \neq k_2$. Then $(a + b, k_1 a + k_2 b) \neq (0, 0)$ and so by (3.6),

$$\begin{aligned} K(J_{(a,k_1a)}, J_{(b,k_2b)}) &= 2p\mathrm{Tr}(J_{(a,k_1a)} J_{(b,k_2b)}) \\ &= 2pu^{-k_1ab}\mathrm{Tr}(J_{(a+b,k_1a+k_2b)}) \\ &= 0. \end{aligned}$$

Thus, H_i and H_j are orthogonal for all $i, j \in \mathbb{Z}_p$ and $i \neq j$.

We now show that $H_k, (k \in \mathbb{Z}_p)$ and H_∞ are abelian Cartan subalgebras. It is clear from the construction that both H_0 and H_∞ are abelian. Moreover, H_0 is a Cartan subalgebra. Since $H_0, H_1, \ldots, H_{p-1}$ are conjugate, they are all abelian Cartan subalgebras. It remains to verify that H_∞ is self normalizing. Recall that for all $k \in \mathbb{Z}_p$ and $a, b \in \mathbb{Z}_p^\times$, $[J_{(a,ka)}, J_{(0,b)}] = (1 - u^{-ab})J_{(a,ka+b)}$ is in H_c for some $c \in \mathbb{Z}_p$. Now, let $A \in N_{\mathfrak{sl}_p(R)}(H_\infty)$. Then by (3.8), we can write

$$A = \sum_{c=1}^{p-1} \Big(\sum_{j=0}^{p-1} (\alpha_{(c,j)} J_{(c,jc)}) + \beta_c J_{(0,c)} \Big),$$

where $\alpha_{(c,j)}, \beta_c \in R$. For any basis element $J_{(0,a)}$ of H_∞, we have

$$[A, J_{(0,a)}] = \sum_{c=1}^{p} \Big(\sum_{j=0}^{p} (\alpha_{(c,j)} [J_{(c,jc)}, J_{(0,a)}]) + \beta_c [J_{(0,c)}, J_{(0,a)}] \Big) \in H_\infty.$$

This implies

$$\sum_{c=1}^{p-1} \sum_{j=0}^{p-1} (\alpha_{(c,j)} (1 - u^{-ac}) J_{(c,jc+a)}) = \sum_{c=1}^{p-1} \sum_{j=0}^{p-1} (\alpha_{(c,j)} [J_{(c,jc)}, J_{(0,a)}]) \in H_\infty.$$

This summation is also in $\oplus_{i=0}^{p-1} H_i$. Then by (3.8), it must be zero. For any $c \in \mathbb{Z}_p^\times, j \in \mathbb{Z}_p$, we can choose $a = -c^{-1}$ so the scalar $1 - u^{-ac} = 1 - u$ is a unit in R. So, $\alpha_{(c,j)} = 0$. Hence, $H_\infty = N_{\mathfrak{sl}_p(R)}(H_\infty)$. This completes the proof for the case $m = 1$.

Next suppose that $m \geq 2$. Let $W = \mathbb{F}_{p^m} \oplus \mathbb{F}_{p^m}$ be a $2m$-dimensional vector space over $\mathbb{F}_p$ equipped with a symplectic form $\langle \cdot, \cdot \rangle : W \times W \to \mathbb{F}_p$ defined by the field trace as follows: for any elements $\vec{w} = (\alpha; \beta), \vec{w}' = (\alpha'; \beta') \in W$,

$$\langle \vec{w}, \vec{w}' \rangle = Tr_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\alpha\beta' - \alpha'\beta). \tag{3.9}$$

Then, by Corollary 3.3 of [21], W possesses a symplectic basis $\mathcal{B} = \{\vec{e}_1, \ldots, \vec{e}_m, \vec{f}_1, \ldots, \vec{f}_m\}$ where $\{\vec{e}_1, \ldots, \vec{e}_m\}$ and $\{\vec{f}_1, \ldots, \vec{f}_m\}$ span the first and the second factor, respectively, such

that

$$\langle \vec{w}, \vec{w}' \rangle = \sum_{i=1}^{m} (a_i b_i' - a_i' b_i), \tag{3.10}$$

where $\vec{w} = \sum_{i=1}^{m} (a_i \vec{e_i} + b_i \vec{f_i})$ and $\vec{w}' = \sum_{i=1}^{m} (a_i' \vec{e_i} + b_i' \vec{f_i})$. With the basis $\mathcal{B}$, write each vector $\vec{w} \in W$ as

$$\vec{w} = (a_1, \ldots, a_m; b_1, \ldots, b_m),$$

and associate it with a matrix

$$\mathcal{J}_{\vec{w}} = J_{(a_1,b_1)} \otimes J_{(a_2,b_2)} \otimes \cdots \otimes J_{(a_m,b_m)},$$

where $\otimes$ denotes the Kronecker product of matrices, and $J_{(a_i,b_i)}$ is given as in the case $m = 1$ with a given primitive pth root of unity $u \in R^\times$ such that $u - 1 \in R^\times$ for all $i = 1, 2, \ldots, m$. Then the set $\{\mathcal{J}_{\vec{w}} : 0 \neq \vec{w} \in W\}$ forms a basis of $\mathfrak{sl}_{p^m}(R)$ as a free R-module of rank $p^m + 1$. By the properties of Kronecker product, we have the following:

$$\mathcal{J}_{\vec{w}} \mathcal{J}_{\vec{w}'} = u^{-\mathfrak{B}(\vec{w},\vec{w}')} \mathcal{J}_{\vec{w}+\vec{w}'} \quad \text{and} \tag{3.11}$$

$$\begin{aligned} [\mathcal{J}_{\vec{w}}, \mathcal{J}_{\vec{w}'}] &= (u^{-\mathfrak{B}(\vec{w},\vec{w}')} - u^{-\mathfrak{B}(\vec{w}',\vec{w})}) \mathcal{J}_{\vec{w}+\vec{w}'} \\ &= u^{-\mathfrak{B}(\vec{w}',\vec{w})} (u^{\langle \vec{w},\vec{w}' \rangle} - 1) \mathcal{J}_{\vec{w}+\vec{w}'}, \end{aligned} \tag{3.12}$$

where

$$\mathfrak{B}(\vec{w}, \vec{w}') = \sum_{i=1}^{m} a_i' b_i$$

for all $\vec{w} = (a_1, \ldots, a_m; b_1, \ldots, b_m), \vec{w}' = (a_1', \ldots, a_m'; b_1', \ldots, b_m') \in W$.

Write $\vec{w} = (\alpha; \beta) \in W$, where $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_m)$. Define

$$H_\infty = \langle \mathcal{J}_{(0;\lambda)} | \lambda \in \mathbb{F}_{p^m}^\times \rangle_R \quad \text{and} \quad H_\alpha = \langle \mathcal{J}_{(\lambda;\alpha\lambda)} | \lambda \in \mathbb{F}_{p^m}^\times \rangle_R,$$

where $\alpha \in \mathbb{F}_{p^m}$. Since the $\mathcal{J}_{\vec{w}}$'s are basis elements, we have

$$\mathfrak{sl}_{p^m}(R) = H_\infty \oplus (\oplus_{\alpha \in \mathbb{F}_{p^m}} H_\alpha) \tag{3.13}$$

We show that all component H_i's are pairwise orthogonal abelian Cartan subalgebras. It is clear that $\langle(\lambda;\alpha\lambda),(\lambda';\alpha\lambda')\rangle = \langle(0;\lambda),(0;\lambda')\rangle = 0$, so by (3.12), all H_α and H_∞ are abelian. To see that they are pairwise orthogonal, note that if $(\gamma;\delta) \neq (-\alpha;-\beta)$, then $\mathrm{Tr}(\mathcal{J}_{(\alpha;\beta)}\mathcal{J}_{(\gamma;\delta)}) = 0$. Indeed, if $\lambda = (a_1,\ldots,a_m), \beta = (b_1,\ldots,b_m), \gamma = (a'_1,\ldots,a'_m), \delta = (b'_1,\ldots,b'_m)$ and $a_i \neq -a'_i$ for some $i \in \{1,\ldots,m\}$, then $a_i + a'_i \neq 0$ and $\mathrm{Tr}J_{(a_i+a'_i,b_i+b'_i)} = 0$ (as in the case $m = 1$). By (3.11) and the trace property of Kronecker product,

$$\begin{aligned}
\mathrm{Tr}(\mathcal{J}_{(\alpha;\beta)}\mathcal{J}_{(\gamma;\delta)}) &= u^{-\mathfrak{B}((\alpha;\beta),(\gamma;\delta))}\mathrm{Tr}(\mathcal{J}_{(a_1+a'_1,\ldots,a_m+a'_m;b_1+b'_1,\ldots,b_m+b'_m)}) \\
&= u^{-\mathfrak{B}((\alpha;\beta),(\gamma;\delta))}\mathrm{Tr}(\otimes_{j=1}^m J_{(a_j+a'_j,b_j+b'_j)}) \\
&= u^{-\mathfrak{B}((\alpha;\beta),(\gamma;\delta))}\prod_{j=1}^m \mathrm{Tr}(J_{(a_j+a'_j,b_j+b'_j)}) \\
&= 0.
\end{aligned}$$

Thus they are pairwise orthogonal. It remains to show that all H_α's and H_∞ are their own normalizers. We first show that for $\alpha \neq \alpha' \in \mathbb{F}_{p^m}$ and $\lambda' \in \mathbb{F}_{p^m}^\times$,

(i) there is an $\lambda \in \mathbb{F}_{p^m}^\times$ such that $\langle(\lambda;\alpha\lambda),(\lambda';\alpha'\lambda')\rangle = 1$ and

(ii) there is an $\lambda \in \mathbb{F}_{p^m}^\times$ such that $\langle(\lambda;\alpha\lambda),(0;\lambda')\rangle = 1$.

Since the field trace is surjective (see Exercise V.7.2 of [8]), there exists $\gamma \in \mathbb{F}_{p^m}$ such that $Tr_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\gamma) = 1$. Thus, we can choose $\lambda = \gamma(\lambda'(\alpha' - \alpha))^{-1}$ for (i) and choose $\lambda = (\lambda')^{-1}$ for (ii). Now, for any $\alpha \in \mathbb{F}_{p^m}$ and $A \in N_{\mathfrak{sl}_{p^m}(R)}(H_\alpha)$,

$$A = \sum_{\lambda' \in \mathbb{F}_q^\times} \Big(\sum_{\alpha' \in \mathbb{F}_q} a_{(\lambda',\alpha')}\mathcal{J}_{(\lambda',\alpha'\lambda')} + b_{\lambda'}\mathcal{J}_{(0,\lambda')} \Big).$$

For any basis element $\mathcal{J}_{(\lambda,\alpha\lambda)} \in H_\alpha$, we have

$$\sum_{\lambda' \in \mathbb{F}_q^\times} \Big(\sum_{\substack{\alpha' \in \mathbb{F}_q \\ \alpha' \neq \alpha}} a_{(\lambda',\alpha')}[\mathcal{J}_{(\lambda',\alpha'\lambda')}, \mathcal{J}_{(\lambda,\alpha\lambda)}] + b_{\lambda'}[\mathcal{J}_{(0,\lambda')}, \mathcal{J}_{(\lambda,\alpha\lambda)}] \Big) \in H_\alpha. \tag{3.14}$$

Note that

$$[\mathcal{J}_{(\lambda',\alpha'\lambda')}, \mathcal{J}_{(\lambda,\alpha\lambda)}] = u^{-\mathfrak{B}((\lambda,\alpha\lambda),(\lambda',\alpha'\lambda'))}(u^{\langle(\lambda',\alpha'\lambda'),(\lambda,\alpha\lambda)\rangle} - 1)\mathcal{J}_{(\lambda'+\lambda,\alpha'\lambda'+\alpha\lambda)},$$
$$[\mathcal{J}_{(0,\lambda')}, \mathcal{J}_{(\lambda,\alpha\lambda)}] = u^{-\mathfrak{B}((\lambda,\alpha\lambda),(0,\lambda'))}(u^{\langle(0,\lambda'),(\lambda,\alpha\lambda)\rangle} - 1)\mathcal{J}_{(\lambda,\lambda'+\alpha\lambda)}.$$

The summation in (3.14) is also in $\sum_{i\neq\alpha} H_i$. For any (λ', α'), by (i), we can choose a suitable λ for which $u^{\langle(\lambda';\alpha'\lambda'),(\lambda;\alpha\lambda)\rangle} - 1 = u - 1$ is a unit in R. This implies $a_{(\lambda',\alpha')}$ is zero because the sums in (3.13) are direct. By (ii), we can show that any $b_{\lambda'}$ is also zero. Thus, $A \in H_\alpha$ and so, $N_{\mathfrak{sl}_{p^m}(R)}(H_k) = H_k$. By using similar arguments, we can show $N_{\mathfrak{sl}_{p^m}(R)}(H_\infty) = H_\infty$. □

Example 3.2.2. Assume that $2 \nmid \mathrm{char}(R)$. We will construct an ODAC of $\mathfrak{sl}_4(R)$. Recall from Example 2.1.3 that

$$\mathfrak{sl}_2(R) = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_R \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle_R \oplus \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle_R$$

and we have

$$J_{(0,0)} = I_2, J_{(1,0)} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, J_{(0,1)} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } J_{(1,1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $f(x) = x^2 + x + 1$. This polynomial is irreducible over $\mathbb{Z}_2$. Thus, we can assume

$$\mathbb{F}_4 = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle = \{0, 1, x, 1 + x\}.$$

Let $W = \mathbb{F}_4 \oplus \mathbb{F}_4$ and a symplectic form $\langle \cdot, \cdot \rangle : W \times W \to \mathbb{Z}_2$ be defined by

$$\langle \vec{w}, \vec{w}' \rangle = \mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\alpha\beta' - \alpha'\beta).$$

for any elements $\vec{w} = (\alpha, \beta), \vec{w}' = (\alpha', \beta') \in W$. For convenience in this example, we use Tr to denote $\mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}$. Then $\mathrm{Tr}(0) = 0, \mathrm{Tr}(1) = 0, \mathrm{Tr}(x) = 1$ and $\mathrm{Tr}(1 + x) = 1$. Consider the basis

$$\mathcal{B} = \{(1, 0), (1 + x, 0), (0, x), (0, 1)\}.$$

It is clear that the equation (3.10) holds. By the construction in Theorem 3.2.1,

$$\begin{aligned}
H_\infty &= \left\langle \mathcal{J}_{(0,\lambda)} | \lambda \in \mathbb{F}_4^\times \right\rangle \\
&= \left\langle \mathcal{J}_{(0,1)}, \mathcal{J}_{(0,x)}, \mathcal{J}_{(0,1+x)} \right\rangle \\
&= \left\langle \mathcal{J}_{(0,0;0,1)}, \mathcal{J}_{(0,0;1,0)}, \mathcal{J}_{(0,0;1,1)} \right\rangle \\
&= \left\langle J_{(0,0)} \otimes J_{(0,1)}, J_{(0,1)} \otimes J_{(0,0)}, J_{(0,1)} \otimes J_{(0,1)} \right\rangle \\
&= \mathrm{Span}_R \left\{ \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{bmatrix}, \begin{bmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{bmatrix}, \begin{bmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{bmatrix} \right\}, \\
H_0 &= \left\langle \mathcal{J}_{(\lambda,0)} | \lambda \in \mathbb{F}_4^\times \right\rangle \\
&= \left\langle \mathcal{J}_{(1,0)}, \mathcal{J}_{(x,0)}, \mathcal{J}_{(1+x,0)} \right\rangle \\
&= \left\langle \mathcal{J}_{(1,0;0,0)}, \mathcal{J}_{(1,1;0,0)}, \mathcal{J}_{(0,1;0,0)} \right\rangle \\
&= \left\langle J_{(1,0)} \otimes J_{(0,0)}, J_{(1,0)} \otimes J_{(1,0)}, J_{(0,0)} \otimes J_{(1,0)} \right\rangle \\
&= \mathrm{Span}_R \left\{ \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix} \right\}, \\
H_1 &= \left\langle \mathcal{J}_{(\lambda,\lambda)} | \lambda \in \mathbb{F}_4^\times \right\rangle \\
&= \left\langle \mathcal{J}_{(1,1)}, \mathcal{J}_{(x,x)}, \mathcal{J}_{(1+x,1+x)} \right\rangle \\
&= \left\langle \mathcal{J}_{(1,0;0,1)}, \mathcal{J}_{(1,1;1,0)}, \mathcal{J}_{(0,1;1,1)} \right\rangle
\end{aligned}$$

$$
\begin{aligned}
&= \left\langle J_{(1,0)} \otimes J_{(0,1)}, J_{(1,1)} \otimes J_{(1,0)}, J_{(0,1)} \otimes J_{(1,1)} \right\rangle \\
&= \mathrm{Span}_R \left\{ \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & -1 \\ & & -1 & \end{bmatrix}, \begin{bmatrix} & & 1 & \\ & & & -1 \\ -1 & & & \\ & 1 & & \end{bmatrix}, \begin{bmatrix} & & & 1 \\ & & -1 & \\ & 1 & & \\ -1 & & & \end{bmatrix} \right\}, \\
H_x &= \left\langle \mathcal{J}_{(\lambda, x\lambda)} | \lambda \in \mathbb{F}_4^\times \right\rangle \\
&= \left\langle \mathcal{J}_{(1,x)}, \mathcal{J}_{(x,1+x)}, \mathcal{J}_{(1+x,1)} \right\rangle \\
&= \left\langle \mathcal{J}_{(1,0;1,0)}, \mathcal{J}_{(1,1;1,1)}, \mathcal{J}_{(0,1;0,1)} \right\rangle \\
&= \left\langle J_{(1,1)} \otimes J_{(0,0)}, J_{(1,1)} \otimes J_{(1,1)}, J_{(0,0)} \otimes J_{(1,1)} \right\rangle \\
&= \mathrm{Span}_R \left\{ \begin{bmatrix} & & 1 & \\ & & & 1 \\ -1 & & & \\ & -1 & & \end{bmatrix}, \begin{bmatrix} & & & 1 \\ & & -1 & \\ & -1 & & \\ 1 & & & \end{bmatrix}, \begin{bmatrix} & 1 & & \\ -1 & & & \\ & & & 1 \\ & & -1 & \end{bmatrix} \right\}, \\
H_{1+x} &= \left\langle \mathcal{J}_{(\lambda, (1+x)\lambda)} | \lambda \in \mathbb{F}_4^\times \right\rangle \\
&= \left\langle \mathcal{J}_{(1,1+x)}, \mathcal{J}_{(x,1)}, \mathcal{J}_{(1+x,x)} \right\rangle \\
&= \left\langle \mathcal{J}_{(1,0;1,1)}, \mathcal{J}_{(1,1;0,1)}, \mathcal{J}_{(0,1;1,0)} \right\rangle \\
&= \left\langle J_{(1,1)} \otimes J_{(0,1)}, J_{(1,0)} \otimes J_{(1,1)}, J_{(0,1)} \otimes J_{(1,0)} \right\rangle \\
&= \mathrm{Span}_R \left\{ \begin{bmatrix} & & & 1 \\ & & 1 & \\ & -1 & & \\ -1 & & & \end{bmatrix}, \begin{bmatrix} & 1 & & \\ -1 & & & \\ & & & -1 \\ & & 1 & \end{bmatrix}, \begin{bmatrix} & & 1 & \\ & & & -1 \\ 1 & & & \\ & -1 & & \end{bmatrix} \right\}
\end{aligned}
$$

and an ODAC of $\mathfrak{sl}_4(R)$ is

$$\mathfrak{sl}_4(R) = H_\infty \oplus H_1 \oplus H_x \oplus H_{1+x}.$$

Example 3.2.3. Here, we give an example of an algebra that does not have an ODAC, when all the conditions of Theorem 3.2.1 hold except the condition that $u - 1$ being a unit. Consider $\mathfrak{sl}_3(\mathbb{Z}_9)$. There are two primitive cube roots of unity 4 and 7 in $\mathbb{Z}_9$, but 3 and 6 are nonunits. Moreover, $3I_3$ is contained in $\mathfrak{sl}_3(\mathbb{Z}_9)$ and also in every abelian Cartan subalgebras. Therefore, each pair of abelian Cartan subalgebras has a non-trivial intersection and thus

$\mathfrak{sl}_3(\mathbb{Z}_9)$ does not have an ODAC since it is nonabelian.

We note that Theorem 3.2.1 relies on the existence of a primitive pth root of unity u such that $u-1$ is a unit. If R is local, i.e. it has the unique maximal ideal, we can give a sufficient condition for the existence of such a primitive root of unity by the help of Cauchy's theorem for a finite group.

Theorem 3.2.4. *[8](Cauchy) If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Thus, we have:

Theorem 3.2.5. *Let R be a finite local ring with a maximal ideal M and the residue field $k = R/M$. For a prime power $n = p^m$, if $p||k^\times|$, then $\mathfrak{sl}_n(R)$ has an* ODAC

$$\mathfrak{sl}_n(R) = H_\infty \oplus H_0 \oplus H_1 \oplus \cdots \oplus H_{n-1}.$$

Proof. By Theorem 1.4.6,

$$R^\times \cong (1+M) \times k^\times.$$

Thus $p||R^\times|$ too, so by Theorem 3.2.4, there exists $u \in R^\times$ of order p. Moreover, it follows that p is relatively prime to the characteristic of R. Thus, $p \cdot 1$ is a unit in R. Next, we show that $u-1$ is also a unit in R. Suppose that $u-1$ is not a unit. Then $u = 1+x$ for some nonzero $x \in M$. Then $1 = u^p = 1 + px +$ (higher power terms of x), so $px +$ (higher power terms of x) $= 0$. Let $d > 1$ be the smallest integer such that $x^d = 0$ and multiply the equation by x^{d-2}, we have $px^{d-1} = 0$, so $x^{d-1} = 0$ since p is a unit in R. A contradiction to the choice of d. □

Note that a finite field $\mathbb{F}_q$ is a finite local ring with maximal ideal $\{0\}$ and $|\mathbb{F}_q^\times| = q-1$, so by the above theorem, we have:

Corollary 3.2.6. *Let q be a prime power and let $\mathbb{F}_q$ be a finite field of q elements. For another prime power $n = p^m$, if $p|(q-1)$, then $\mathfrak{sl}_n(\mathbb{F}_q)$ has an ODAC*

$$\mathfrak{sl}_n(\mathbb{F}_q) = H_\infty \oplus H_0 \oplus H_1 \oplus \cdots \oplus H_{n-1}.$$

Theorem 3.2.7. *Let $R = R_1 \times R_2 \times \cdots \times R_t$ be a finite direct product of finite local rings and let k_i be the residue field of R_i for all $i \in \{1, 2, \ldots, t\}$. For a prime power $n = p^m$, if $p||k_i^\times|$ for all $i \in \{1, 2, \ldots, t\}$, then $\mathfrak{sl}_n(R)$ has an ODAC*

$$\mathfrak{sl}_n(R) = H_\infty \oplus H_0 \oplus H_1 \oplus \cdots \oplus H_{n-1}.$$

Proof. By the proof of Theorem 3.2.5, there exists a primitive pth root of unity $u_i \in R_i^\times$ such that $u_i - 1_{R_i} \in R_i^\times$ for all i. Then $u = (u_1, u_2, \ldots, u_t)$ is a primitive pth root of unity in R such that

$$\begin{aligned} u - 1 &= (u_1, u_2, \ldots, u_t) - (1_{R_1}, 1_{R_2}, \ldots, 1_{R_t}) \\ &= (u_1 - 1_{R_1}, u_2 - 1_{R_2}, \ldots, u_t - 1_{R_t}) \in R^\times \end{aligned}$$

because $R_1^\times \times R_2^\times \times \ldots \times R_t^\times = R^\times$ (Theorem 1.4.7). Thus Theorem 3.2.1 implies that $\mathfrak{sl}_n(R)$ admits an ODAC. □

By the above theorem, we have the following examples.

Example 3.2.8. Let q be an odd positive integer and m a positive integer. Then all prime factors of q are odd and $\mathfrak{sl}_{2^m}(\mathbb{Z}_q)$ has an ODAC.

Example 3.2.9. For any positive integers s, t and m, $\mathfrak{sl}_{3^m}(\mathbb{Z}_{7^s 31^t})$ has an ODAC.

3.3 Necessary conditions on rings

As mentioned, the OD problem for $\mathfrak{sl}_6(\mathbb{C})$ is still unsolved. This motivates the following problem: searching for some necessary conditions on finite commutative rings with identity for which $\mathfrak{sl}_n$ over these rings have an ODAC, in particular, when $n = 6$. We will be able to find a necessary condition on the characteristics of the rings by using the ingredients from Section 2.2.

Let $R = R_1 \times R_2 \times \ldots \times R_t$ be a finite direct product of finite local rings. By Corollary 2.2.4,

$$\mathfrak{sl}_n(R) \cong \mathrm{Proj}_1(\phi(\mathfrak{sl}_n(R))) \oplus \mathrm{Proj}_2(\phi(\mathfrak{sl}_n(R))) \oplus \cdots \oplus \mathrm{Proj}_t(\phi(\mathfrak{sl}_n(R))).$$

Lemma 3.3.1. *Under the above setting,* $\mathfrak{sl}_n(R)$ *has an* ODAC *if and only if* $\mathfrak{sl}_n(R_i)$ *has an* ODAC *for all* $i = 1, 2, \ldots, t$.

Proof. Let $i \in \{1, 2, \ldots, t\}$. We show that $\mathrm{Proj}_i(\phi(\mathfrak{sl}_n(R))) = \mathfrak{sl}_n(R_i)$. Then the result follows from Corollary 2.2.4 directly. It suffices to prove the case $i = 1$. Let $x \in \mathrm{Proj}_1(\phi(\mathfrak{sl}_n(R)))$. Then $(x, 0, \ldots, 0) \in \phi(\mathfrak{sl}_n(R))$. By the definition of the map ϕ (see the proof of Corollary 2.2.4), $\mathrm{Tr}(x) = 0$. Conversely, if $x \in \mathfrak{sl}_n(R_1)$, then $(x, 0, \ldots, 0) \in \phi(\mathfrak{sl}_n(R))$, i.e. $x \in \mathrm{Proj}_1(\phi(\mathfrak{sl}_n(R)))$. □

Using the above lemma, we can derive a necessary condition on the characteristic of R and n for the existence of ODAC.

Theorem 3.3.2. *Let* R *be a finite commutative ring with identity. If* $\mathfrak{sl}_n(R)$ *admits an* ODAC*, then* $\mathrm{char}(R)$ *is relatively prime to* n.

Proof. Suppose that $\mathrm{char}(R)$ is not relatively prime to n. Then $\mathrm{char}(R) = p^a p_1^{s_1} p_2^{s_2} \cdots p_l^{s_l}$ and $n = p^b p_1^{t_1} p_2^{t_2} \cdots p_{l'}^{t_{l'}}$ where p and p_i's are all distinct prime integers and $a, s_1, \ldots, s_t, b, t_1, \ldots, t_{l'}$ are non negative integers. Let $R = R_1 \times R_2 \times \ldots \times R_t$. Then there exists $i_0 \in \{1, 2, \ldots, t\}$ such that $\mathrm{char}(R_{i_0}) = p^a$. Consider $\mathfrak{sl}_n(R_{i_0})$ and we have two different cases.

Case 1: $b \geq a$. Then n is divisible by p^a and so the trace of the identity matrix I_n is 0. Thus, $\mathfrak{sl}_n(R_{i_0})$ contains I_n and so does every abelian Cartan subalgebra. Thus, any two abelian Cartan subalgebras have a nontrivial intersection. Since $\mathfrak{sl}_n(R_{i_0})$ is not abelian, it does not have an ODAC.

Case 2: $b < a$. Then $p^{a-b}I_n$ is in $\mathfrak{sl}_n(R_{i_0})$. By the similar reason to case 1, there is no ODAC for $\mathfrak{sl}_n(R_{i_0})$.

Hence, by Lemma 3.3.1, $\mathfrak{sl}_n(R)$ does not have an ODAC. □

We next provide some nonexistence examples of ODAC of $\mathfrak{sl}_6$.

Example 3.3.3. When $R = \mathbb{Z}_{2k}, \mathbb{Z}_{3l}, k, l \in \mathbb{Z}_+$, $\mathfrak{sl}_6(R)$ does not have an ODAC.

3.4 Maximum number of classical components

Consider the classical ODAC of $\mathfrak{sl}_n(\mathbb{F}_q)$, $n = 2, 3$ again, we will build Magma codes to determine characteristic of $\mathbb{F}_q$ for which $\mathfrak{sl}_n(\mathbb{F}_q)$ has a classical ODAC. If not, we will look for the maximum number of classical Cartan subalgebras that are pairwise orthogonal with respect to the killing form.

Let $\mathbb{F}_q$ be a finite field of characteristic $p \neq 2, 3$. Assume further that the characteristic p does not divide n. By Chapter III §6 in [17], $\mathfrak{sl}_n(\mathbb{F}_q)$ is classical and so, all classical Cartan subalgebras are conjugate under the matrix conjugation provided by the special linear group $\mathrm{SL}_n(\mathbb{F}_q)$, the set of all $n \times n$ matrices over $\mathbb{F}_q$ having determinant 1.

Now, we describe how to build our codes in Magma. We will do this for $\mathfrak{sl}_3(\mathbb{F}_q)$ because the same process can be applied for $\mathfrak{sl}_2(\mathbb{F}_q)$. Since all classical Cartan subalgebras are conjugate, we can choose the first classical Cartan subalgebra H_0, so it consists of diagonal matrices

$$H_0 = \langle \mathrm{diag}\{1, -1, 0\}, \mathrm{diag}\{0, 1, -1\} \rangle_{\mathbb{F}_q}.$$

Let $X_1 = \mathrm{diag}\{1, -1, 0\}$ and $X_2 = \mathrm{diag}\{0, 1, -1\}$. The fact that the Killing form is non-

degenerate on any classical Cartan subalgebra implies that a sum of orthogonal Cartan subalgebras is always direct. To find the next classical Cartan subalgebra that is orthogonal to H_0, it suffices to find a matrix $M_1 \in SL_n(\mathbb{F}_q)$ such that $\mathrm{Tr}(X_i M_1 X_j M_1^{-1}) = 0$ for $i, j = 1, 2$. If there exists such a matrix M_1, we will then try to find another matrix M_2 that satisfies $\mathrm{Tr}(X_i M_2 X_j M_2^{-1}) = \mathrm{Tr}(M_1 X_i M_1^{-1} M_2 X_j M_2^{-1}) = 0$ for $i, j = 1, 2$. We will present the Magma codes in Appendix B. Results for the maximum number of classical components for some cases are exhibited in the following table.

	$n = 5$	$n = 7$	$n = 11$	$n = 13$	$n = 17$
$\mathfrak{sl}_2(\mathbb{Z}_n)$	3	2	2	3	3
$\mathfrak{sl}_3(\mathbb{Z}_n)$	1	4	1	4	1

Remark 3.4.1. From the above table, we conclude that $\mathfrak{sl}_2(\mathbb{Z}_n)$ has a classical ODAC when $n = 5, 13, 17$ while $\mathfrak{sl}_2(\mathbb{Z}_n), n = 7, 11$, does not. Moreover, $\mathfrak{sl}_3(\mathbb{Z}_n)$ has a classical ODAC when $n = 7, 13$ while $\mathfrak{sl}_3(\mathbb{Z}_n), n = 5, 11, 17$, does not.

3.5 Enumeration of $\mathbb{J}$-decompositions of $\mathfrak{sl}_n, n = 2, 3$ over finite fields

In Section 3.1 and Section 3.2, we gave some sufficient conditions for the existence of ODAC under the assumptions there. One may ask about the following question.

Question 1. If $\mathfrak{sl}_n(R)$ possesses an ODAC, how many are there up to $\mathrm{Aut}(\mathfrak{sl}_n(R))$-conjugacy?

In the complex case, it is known there exists a unique OD for $\mathfrak{sl}_n(\mathbb{C})$ for all $n \leq 5$ up to conjugacy [12]. Consider the case $\mathfrak{sl}_2(R)$. If $R = \mathbb{C}$, then all Cartan subalgebras are conjugate [7]. Thus, we can assume that an OD of $\mathfrak{sl}_2(\mathbb{C})$ has the Cartan subalgebra consisting of diagonal matrices as a component, so up to conjugacy, the OD looks as follows

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{C}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right\rangle_{\mathbb{C}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \right\rangle_{\mathbb{C}}$$

for some $a, b \neq 0$. By using orthogonality with respect to the Killing form, we derive $b = -a$. Note that conjugation by

$$\begin{pmatrix} \sqrt{a} & 0 \\ 0 & 1 \end{pmatrix}$$

stabilizes the first component and maps

$$\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \longmapsto \sqrt{a} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Therefore, $\mathfrak{sl}_2(\mathbb{C})$ has a unique OD up to conjugacy. For a comparison, consider $R = \mathbb{F}_{p^m}$, where $p \neq 2$ and the following ODAC of $\mathfrak{sl}_2(\mathbb{F}_{p^m})$

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \tag{3.15}$$

for some $a \neq 0$. In contrast to the complex case, the element $a \in \mathbb{F}_{p^m}$ may not have a square root in $\mathbb{F}_{p^m}$. Consequently, we may not have an automorphism of $\mathrm{Aut}(\mathfrak{sl}_2(\mathbb{F}_{p^m}))$ mapping this decompostion to

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}}.$$

For example, $\mathfrak{sl}_2(\mathbb{Z}_7)$ has an ODAC

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{Z}_7} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}_7} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -3 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}_7}.$$

Since 3 and -3 are non square units in $\mathbb{Z}_7$, we can show that this ODAC is not conjugate to the ODAC

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{Z}_7} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}_7} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}_7}.$$

The verification of this example is similar to the detailed computation in the proof of Theorem 3.5.4 below.

For this section, we will consider a weaker version of Question 1 as follows. For $n = 2, 3$, we will consider the collection of ODCAs described in (3.2) and (3.3). An element in such collections is called a $\mathbb{J}$**-decomposition.** This is the generalization of the $\mathbb{J}$-decomposition in the complex numbers case when $n = 2, 3$. Note that $\mathbb{J}$-decompositions play an important role in the OD theory over the complex number case [13]. As examples, we will find the number of $\mathbb{J}$-decompositions of $\mathfrak{sl}_2(\mathbb{F}_{p^m})$ if p is odd prime and of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ if $3|(p^m - 1)$.

Definition 3.5.1. (1) Assume that p is an odd prime integer. For $a \neq 0$, a $\mathbb{J}$-decomposition

$$\mathfrak{sl}_2(\mathbb{F}_{p^m}) = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}}$$

is said to be a $\mathbb{J}_{\mathbf{2}}(\boldsymbol{a})$**-decomposition** ($\mathbb{J}_{\mathbf{2}}(\boldsymbol{a})$ for short).

(2) Assume that $3|(p^m - 1)$. For $a, b \neq 0$ and a primitive root of unity $u \in \mathbb{F}_{p^m}$, a $\mathbb{J}$-decomposition

$$\mathfrak{sl}_3(\mathbb{F}_{p^m}) = H_0 \oplus H_1 \oplus H_2 \oplus H_3,$$

where

$$H_1 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & a \\ ab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ ab & 0 & 0 \\ 0 & b & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}},$$

$$H_2 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & ua \\ u^2ab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ u^2ab & 0 & 0 \\ 0 & ub & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}},$$

$$H_3 = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & u^2a \\ uab & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ uab & 0 & 0 \\ 0 & u^2b & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}},$$

is said to be a $\mathbb{J}_{\mathbf{3}}(\boldsymbol{a}, \boldsymbol{b})$**-decomposition** ($\mathbb{J}_{\mathbf{3}}(\boldsymbol{a}, \boldsymbol{b})$ for short).

Remark 3.5.2. For (2) in this definition, if $3|(p^m - 1)$, then $\mathbb{J}_3(a, b)$ is independent from the choice of a primitive root of unity because there are only two such roots, namely u and

u^2, in $\mathbb{F}_{p^m}$, moreover, H_2 and H_3 are interchangeable.

We begin with $n = 2$. There are two scenarios to be considered for $\mathfrak{sl}_2(\mathbb{F}_{p^m})$ depending on the congruency of p modulo 4. We first observe that:

Lemma 3.5.3. *Let p be an odd prime integer and m a positive integer. Then -1 is a square in $\mathbb{F}_{p^m}$ if and only if $p^m \equiv 1 \pmod 4$.*

Proof. Recall that the unit group of $\mathbb{F}_{p^m}$ is cyclic of order $p^m - 1$. Let a be its generator. Since $(a^{\frac{p^m-1}{2}})^2 = 1$, $a^{\frac{p^m-1}{2}} = 1$ or -1. But a has order $p^m - 1$. Then $a^{\frac{p^m-1}{2}} = -1$. Now, -1 is the square of a unit in $\mathbb{F}_{p^m}$ if and only if it is an even power of a. Finally, we note that the later condition is equivalent to $p^m \equiv 1 \pmod 4$. □

We will see in the next theorem that there are at most two $\mathbb{J}$-decompositions of $\mathfrak{sl}_2(\mathbb{F}_{p^m})$: one is represented by $\mathbb{J}_2(1)$ and the other one is represented by $\mathbb{J}_2(a)$, where a is a non square unit in $\mathbb{F}_{p^m}$.

Theorem 3.5.4. *Let p be an odd prime integer and m a positive integer. Suppose that a is a non square unit in $\mathbb{F}_{p^m}$.*

(1) If $p^m \equiv 3 \pmod 4$, then $\mathbb{J}_2(1)$ and $\mathbb{J}_2(a)$ are conjugate and $\mathfrak{sl}_2(\mathbb{F}_{p^m})$ has a unique $\mathbb{J}$-decomposition up to conjugacy.

(2) If $p^m \equiv 1 \pmod 4$, then $\mathbb{J}_2(1)$ and $\mathbb{J}_2(a)$ are not conjugate and $\mathfrak{sl}_2(\mathbb{F}_{p^m})$ has two $\mathbb{J}$-decompositions up to conjugacy.

Proof. Let x be a square unit in $\mathbb{F}_{p^m}$. Conjugating by

$$\begin{pmatrix} \sqrt{x} & 0 \\ 0 & 1 \end{pmatrix}$$

leads to the conjugation between $\mathbb{J}_2(x)$ and $\mathbb{J}_2(1)$. Now, let y, z be two non square units in $\mathbb{F}_{p^m}$. Then $y = zx$ for some square unit x. Using the same matrix, we have conjugation between $\mathbb{J}_2(y)$ and $\mathbb{J}_2(z)$.

To prove (1), assume that $p^m \equiv 3 \pmod 4$. By Lemma 3.5.3, -1 is not a square. Thus, $-a$ is a square unit. Again conjugating by

$$\begin{pmatrix} \sqrt{-a} & 0 \\ 0 & 1 \end{pmatrix},$$

we obtain a conjugation between $\mathbb{J}_2(1)$ and $\mathbb{J}_2(a)$.

Next, we assume that $p^m \equiv 1 \pmod 4$. By Lemma 3.5.3, -1 is a square. Thus, $-a$ is a non square unit. We will show that $\mathbb{J}_2(1)$ and $\mathbb{J}_2(a)$ are not conjugate. Suppose, to the contrary, that there exists an automorphism $\phi \in \mathrm{Aut}(\mathfrak{sl}_2(\mathbb{F}_{p^m}))$ sending each component of $\mathbb{J}_2(a)$ to a component of $\mathbb{J}_2(1)$. Since $\mathbb{J}_2(a)$ is

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}}$$

and $\mathbb{J}_2(1)$ is

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}} \oplus \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_{p^m}},$$

we have the following cases.

Case 1: $\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}$ and $\phi \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} = \begin{pmatrix} 0 & y \\ y & 0 \end{pmatrix}$ for some $x, y \neq 0$. Then

$$\begin{aligned} 2\phi \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} &= \phi \left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right] \\ &= \left[\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \phi \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right] \\ &= \left[\begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}, \begin{pmatrix} 0 & y \\ y & 0 \end{pmatrix} \right] \end{aligned}$$

$$= 2xy \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

So,

$$\phi \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} = xy \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus,

$$\begin{aligned} -2ax \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} &= -2a\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \phi \left[\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} \right] \\ &= \left[\phi \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \phi \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} \right] \\ &= \left[\begin{pmatrix} 0 & y \\ y & 0 \end{pmatrix}, \begin{pmatrix} 0 & xy \\ -xy & 0 \end{pmatrix} \right] \\ &= -2xy^2 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

This implies that $a = y^2$, which is a contradiction.

Case 2: $\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}$ and $\phi \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} 0 & y \\ y & 0 \end{pmatrix}$ for some $x, y \neq 0$. Let $b = -a$. Then b is a non square unit and we can use the argument in Case 1 to obtain a contradiction.

Case 3: $\phi\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}0 & y\\ y & 0\end{pmatrix}$ and $\phi\begin{pmatrix}0 & 1\\ a & 0\end{pmatrix} = \begin{pmatrix}x & 0\\ 0 & -x\end{pmatrix}$ for some $x, y \neq 0$. Then

$$\begin{aligned}
2\phi\begin{pmatrix}0 & 1\\ -a & 0\end{pmatrix} &= \phi\left[\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}0 & 1\\ a & 0\end{pmatrix}\right] \\
&= \left[\phi\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \phi\begin{pmatrix}0 & 1\\ a & 0\end{pmatrix}\right] \\
&= \left[\begin{pmatrix}0 & y\\ y & 0\end{pmatrix}, \begin{pmatrix}x & 0\\ 0 & -x\end{pmatrix}\right] \\
&= -2xy\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.
\end{aligned}$$

So,

$$\phi\begin{pmatrix}0 & 1\\ -a & 0\end{pmatrix} = -xy\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.$$

Thus,

$$\begin{aligned}
-2ay\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} &= -2a\phi\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \\
&= \phi\left[\begin{pmatrix}0 & 1\\ a & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ -a & 0\end{pmatrix}\right] \\
&= \left[\phi\begin{pmatrix}0 & 1\\ a & 0\end{pmatrix}, \phi\begin{pmatrix}0 & 1\\ -a & 0\end{pmatrix}\right] \\
&= \left[\begin{pmatrix}x & 0\\ 0 & -x\end{pmatrix}, \begin{pmatrix}0 & -xy\\ xy & 0\end{pmatrix}\right]
\end{aligned}$$

$$= -2x^2y \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This implies that $a = x^2$, which is a contradiction.

Case 4: $\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & y \\ y & 0 \end{pmatrix}$ and $\phi \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}$ for some $x, y \neq 0$. Let $b = -a$. Then b is a non square unit and we can use the same argument in Case 3 to obtain a contradiction.

Case 5: $\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix}$ and $\phi \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}$ for some $x, y \neq 0$. Then

$$\begin{aligned} 2\phi \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} &= \phi \left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right] \\ &= \left[\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \phi \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix} \right] \\ &= \left[\begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix}, \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix} \right] \\ &= -2xy \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

So,

$$\phi \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} = -xy \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus,

$$-2ay \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -2a\phi \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$
\begin{aligned}
&= \phi\left[\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix}\right] \\
&= \left[\phi\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \phi\begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix}\right] \\
&= \left[\begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}, \begin{pmatrix} 0 & -xy \\ -xy & 0 \end{pmatrix}\right] \\
&= -2x^2y \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.
\end{aligned}
$$

This implies that $a = x^2$, which is a contradiction.

Case 6: $\phi\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix}$ and $\phi\begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & -x \end{pmatrix}$ for some $x, y \neq 0$. Let $b = -a$. Then b is a non square unit and we can use the argument in Case 5 to obtain a contradiction. □

We now consider the case $n = 3$. If $3|(p^m - 1)$, then a $\mathbb{J}$-decomposition exists for $\mathfrak{sl}_3(\mathbb{F}_{p^m})$. With this condition, we will have three certain cosets derived as follows. Assume that $3|(p^m - 1)$. Then $p^m - 1 = 3l$ for some $l \in \mathbb{Z}_{>0}$. Let x be a generator of $\mathbb{F}_{p^m}^{\times}$. Then $|\langle x^3 \rangle| = l$ and the index $[\mathbb{F}_{p^m}^{\times} : \langle x^3 \rangle] = 3$. Let $z \in \mathbb{F}_{p^m}^{\times} \setminus \langle x^3 \rangle$. We are focusing on these three distinct cosets: $\langle x^3 \rangle, z\langle x^3 \rangle$ and $z^2\langle x^3 \rangle$. We will use them to find the number of $\mathbb{J}$-decompositions of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$. For $n = 2$, there was a case with multiple $\mathbb{J}$-decompositions. So, one may expect that we have more than one $\mathbb{J}$-decompositions up to conjugacy for $n = 3$ at least in some cases as well.

Our goal is to show that there are exactly two $\mathbb{J}$-decompositions of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$, where $3|(p^m - 1)$. For the sake of convenience, we define a relation

$$\mathbb{J}_3(a, b) \approx \mathbb{J}_3(c, d) \iff \mathbb{J}_3(a, b) \text{ is conjugate to } \mathbb{J}_3(c, d)$$

for all $a, b, c, d \neq 0$. Obviously, this is an equivalence relation.

The following lemma provides a sufficient condition for two $\mathbb{J}$-decompositions to be conjugate to one another.

Lemma 3.5.5. *Suppose that* $3|(p^m - 1)$. *For nonzero* $a, b, c, d \in \mathbb{F}_{p^m}$, *if* $a^{-1}c$ *and* $b^{-1}d$ *are in the same left coset defined by* $\langle x^3 \rangle$, *then* $\mathbb{J}_3(a, b) \approx \mathbb{J}_3(c, d)$.

Proof. Assume that $a^{-1}c$ and $b^{-1}d$ are in the same coset. Then $(a^{-1}c)^2 b^{-1}d$ and $a^{-1}c(b^{-1}d)^2$ have the cube roots. Thus, we can use the matrix conjugation defined by

$$\begin{pmatrix} 1 & & \\ & \sqrt[3]{(a^{-1}c)^2 b^{-1}d} & \\ & & \sqrt[3]{a^{-1}c(b^{-1}d)^2} \end{pmatrix}$$

to map $\mathbb{J}_3(a, b)$ to $\mathbb{J}_3(c, d)$. □

Similarly to the case $n = 2$, we will use the $\mathbb{J}_3(1, 1)$ to represent one of $\mathbb{J}$-decompositions for this case. From the above lemma, it follows that if a and b are in the same coset defined by $\langle x^3 \rangle$, then $\mathbb{J}_3(a, b) \approx \mathbb{J}_3(1, 1)$. On the other hand, if they are in different cosets, we will show that $\mathbb{J}_3(a, b)$ is conjugate to either $\mathbb{J}_3(1, z)$ or $\mathbb{J}_3(1, z^2)$. As a result, we will have at most three $\mathbb{J}$-decompositions of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ up to conjugacy where $3|(p^m - 1)$.

Proposition 3.5.6. *Under the above setting, we have:*

(1) If a *and* b *are in the same coset, then* $\mathbb{J}_3(a, b) \approx \mathbb{J}_3(1, 1)$.

(2) If a *and* b *are in the different cosets, then* $\mathbb{J}_3(a, b) \approx \mathbb{J}_3(1, z)$ *or* $\mathbb{J}_3(a, b) \approx \mathbb{J}_3(1, z^2)$.

Proof. We only need to prove (2). Since $\mathbb{F}_{p^m}^\times / \langle x^3 \rangle \simeq \mathbb{Z}_3$, let $\varphi : \mathbb{F}_{p^m}^\times \to (\mathbb{Z}_3, +)$ be the isomorphism that sends $z^i \langle x^3 \rangle$ to i. For $i = 0, 1, 2$, let $\overline{z}^i$ denote the coset $z^i (\mathbb{F}_{p^m}^\times)^3$. Now, assume that a and b are in two distinct cosets, say $a \in \overline{z}^i$ and $b \in \overline{z}^j$, we write $(a, b) \in (\overline{z}^i, \overline{z}^j)$. Thus, if $(c, d) \in (\overline{z}^s, \overline{z}^t)$, then $(a + c, b + d) \in (\overline{z}^{i+s}, \overline{z}^{j+t})$. Note that $(1, z) \in (\overline{z}^0, \overline{z}^1)$

and so $(1, z^{-1}) \in (\overline{z}^0, \overline{z}^2)$. By Lemma 3.5.5, for any (a, b) in $(\overline{z}^0, \overline{z}^1), (\overline{z}^2, \overline{z}^0)$ and $(\overline{z}^1, \overline{z}^2)$, $\mathbb{J}_3(a, b) \approx \mathbb{J}_3(1, z)$. Finally, $(1, z^2) \in (\overline{z}^0, \overline{z}^2)$ and so $(1, z^{-2}) \in (\overline{z}^0, \overline{z}^1)$. By Lemma 3.5.5 again, for any (a, b) in $(\overline{z}^1, \overline{z}^0), (\overline{z}^0, \overline{z}^2)$ and $(\overline{z}^2, \overline{z}^1)$, $\mathbb{J}_3(a, b) \approx \mathbb{J}_3(1, z^2)$. □

To conclude that there are exactly two $\mathbb{J}$-decompositions of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ up to conjugacy when $3|(p^m - 1)$, we will prove that $\mathbb{J}_3(1, z)$ is conjugate to $\mathbb{J}_3(1, z^2)$ but not to $\mathbb{J}_3(1, 1)$.

Theorem 3.5.7. *Let p be an odd prime integer and m a positive integer such that $3|(p^m - 1)$. Then $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ has two $\mathbb{J}$-decompositions up to conjugacy, which are represented by $\mathbb{J}_3(1, 1)$ and $\mathbb{J}_3(1, z)$.*

Proof. The $\mathbb{J}_3(1, 1)$ of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ is

$$\mathfrak{sl}_3(\mathbb{F}_{p^m}) = \langle J_{(1,0)}, J_{(2,0)} \rangle \oplus \langle J_{(0,1)}, J_{(0,2)} \rangle \oplus \langle J_{(1,1)}, J_{(2,2)} \rangle \oplus \langle J_{(2,1)}, J_{(1,2)} \rangle ,$$

where $J_{(a,b)} = D^a P^b$ and

$$D = \operatorname{diag}\{1, u, u^2\}, P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Note that $[J_{(a,b)}, J_{(c,d)}] = (u^{-bc} - u^{-ad}) J_{(a+c,b+d)}$ for all $a, b \in \{0, 1, 2\}$ (cf. eq. (3.7)).

The following description is for $\mathbb{J}_3(1, z)$. Let

$$P_0 = I_3, P_1 = \begin{pmatrix} 0 & 0 & 1 \\ z & 0 & 0 \\ 0 & z & 0 \end{pmatrix} \text{ and } P_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ z & 0 & 0 \end{pmatrix}.$$

Define $J'_{(a,b)} = D^a P_b$ for $a, b \in \{0, 1, 2\}$. Let $m_{bd} = \min\{b, d\} \pmod 2$. Then

$$[J'_{(a,b)}, J'_{(c,d)}] = z^{m_{bd}} (u^{-bc} - u^{-ad}) J'_{(a+c,b+d)}. \tag{3.16}$$

The $\mathbb{J}_3(1,z)$ of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ is

$$\mathfrak{sl}_3(\mathbb{F}_{p^m}) = \langle J'_{(1,0)}, J'_{(2,0)} \rangle \oplus \langle J'_{(0,1)}, J'_{(0,2)} \rangle \oplus \langle J'_{(1,1)}, J'_{(2,2)} \rangle \oplus \langle J'_{(2,1)}, J'_{(1,2)} \rangle .$$

Suppose that $\mathbb{J}_3(1,z) \approx \mathbb{J}_3(1,1)$ by an automorphism φ. We will show that this leads to a contradiction. Since φ sends one component of $\mathbb{J}_3(1,z)$ to exactly one component of $\mathbb{J}_3(1,1)$, for each (a,b), by (3.16) there exists a unique (a',b') such that $\varphi(J'_{(a,b)}) = \alpha_{a,b} J_{(a',b')}$ where $\alpha_{a,b} \in \mathbb{F}_{p^m}^{\times}$. We will consider all possible cases. Here, we provide the details of two cases. For the remaining cases, we refer the reader to Appendix C.1 for Mathematica code to verify that z would be a cube unit in $\mathbb{F}_{p^m}$ and thus have a contradiction.

Case 1

$$\begin{aligned} \varphi : J'_{(1,0)} &\mapsto aJ_{(1,0)}, J'_{(0,1)} \mapsto cJ_{(0,1)} \\ J'_{(2,0)} &\mapsto bJ_{(2,0)}, J'_{(0,2)} \mapsto dJ_{(0,2)} \end{aligned}$$

for some $a, b, c, d \in \mathbb{F}_{p^m}^{\times}$. Using (3.16), we obtain

(i) $\varphi(J'_{(1,1)}) = acJ_{(1,1)}$,

(ii) $\varphi(J'_{(2,2)}) = bdJ_{(2,2)}$,

(iii) $\varphi(J'_{(1,2)}) = adJ_{(1,2)}$.

Since $\varphi([J'_{(0,1)}, J'_{(1,1)}]) = [\varphi(J'_{(0,1)}), \varphi(J'_{(1,1)})]$ and $\varphi([J'_{(0,1)}, J'_{(2,2)}]) = [\varphi(J'_{(0,1)}), \varphi(J'_{(2,2)})]$, by (i), (ii) and (iii), we have $zd = c^2$ and $z = cd$, accordingly. This forces $z = d^3$ which contradicts the choice of z.

Case 2

$$\begin{aligned} \varphi : J'_{(2,0)} &\mapsto aJ_{(1,0)}, J'_{(0,1)} \mapsto cJ_{(0,1)} \\ J'_{(1,0)} &\mapsto bJ_{(2,0)}, J'_{(0,2)} \mapsto dJ_{(0,2)} \end{aligned}$$

for some $a, b, c, d \in \mathbb{F}_{p^m}^{\times}$. Using (3.16), we obtain

(i) $\varphi(J'_{(1,1)}) = (\frac{bc}{1+u})J_{(2,1)}$,

(ii) $\varphi(J'_{(2,2)}) = (\frac{ad}{1+u})J_{(1,2)}$,

(iii) $\varphi(J'_{(1,2)}) = bd(1+u)J_{(2,2)}$.

Since $\varphi([J'_{(0,1)}, J'_{(1,1)}]) = [\varphi(J'_{(0,1)}), \varphi(J'_{(1,1)})]$ and $\varphi([J'_{(0,1)}, J'_{(2,2)}]) = [\varphi(J'_{(0,1)}), \varphi(J'_{(2,2)})]$, by (i), (ii) and (iii), we have $zd(1+u)^3 = c^2$ and $z = cd$, accordingly. This forces $z = d^3(1+u)^3$ which contradicts the choice of z.

Finally, let

$$Q_0 = I_3, Q_1 = \begin{pmatrix} 0 & 0 & 1 \\ z^2 & 0 & 0 \\ 0 & z^2 & 0 \end{pmatrix} \text{ and } Q_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ z^2 & 0 & 0 \end{pmatrix}.$$

Define $J''_{(a,b)} = D^a P_b$ for $a, b \in \{0, 1, 2\}$. Let $m_{bd} = \min\{b, d\} \pmod 2$. Then

$$[J''_{(a,b)}, J''_{(c,d)}] = z^{2m_{bd}}(u^{-bc} - u^{-ad})J''_{(a+c,b+d)}. \tag{3.17}$$

The $\mathbb{J}_3(1, z^2)$ of $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ is

$$\mathfrak{sl}_3(\mathbb{F}_{p^m}) = \langle J''_{(1,0)}, J''_{(2,0)} \rangle \oplus \langle J''_{(0,1)}, J''_{(0,2)} \rangle \oplus \langle J''_{(1,1)}, J''_{(2,2)} \rangle \oplus \langle J''_{(2,1)}, J''_{(1,2)} \rangle .$$

We will find an automorphism in $\mathfrak{sl}_3(\mathbb{F}_{p^m})$ that maps $\mathbb{J}_3(1, z^2)$ to $\mathbb{J}_3(1, z)$. To construct such an automorphism, we define a map ψ on the basis of $\mathbb{J}_3(1, z^2)$ as follows:

$$\begin{aligned}
&J''(1,0) \mapsto -J'(1,0), && J''(2,0) \mapsto -J'(2,0), \\
&J''(0,1) \mapsto -zJ'(0,2), && J''(0,2) \mapsto -J'(0,1), \\
&J''(1,1) \mapsto \frac{z}{1+u}J'(1,2), && J''(2,2) \mapsto \frac{1}{1+u}J'(2,1) \\
&J''(1,2) \mapsto (1+u)J'(1,1) && J''(2,1) \mapsto z(1+u)J'(2,2).
\end{aligned}$$

We extend ψ linearly to the entire $\mathbb{J}_3(1, z^2)$. Then by using the fact that u is a primitive cube root of unity together with (3.16) and (3.17), we see that ψ is an automorphism in $\mathfrak{sl}_3(\mathbb{F}_{p^m})$. For the details of this part, we refer the reader to Appendix C.2. $\square$

Chapter 4

Orthogonal decompositions of Lie algebras of type C

In this chapter, we will consider the ODAC problem of the symplectic Lie algebra $\mathfrak{sp}_n$ over a finite commutative ring R with identity. Since $\mathfrak{sp}_n(R)$ is a subalgebra of $\mathfrak{sl}_n(R)$, the construction in Chapter 3 will be used throughout this chapter. As we see in the complex case [13], the OD problem of Lie algebra type C has the same difficulty as type A. However, in the special case of a Lie algebra of type C_{2^m}, it is manageable because C_{2^m} is a subalgebra of the Lie algebra of type $A_{2^{m+1}}$ and we know that there is an OD for $A_{2^{m+1}}$. We will consider the problem when the characteristic of R is odd and show that this Lie algebra has an ODAC obtained by restricting an ODAC of Lie algebra $\mathfrak{sl}_{2^{m+1}}(R)$ constructed in Section 3.2.

We assume that R has odd characteristic in this chapter.

4.1 Special basis elements of $\mathfrak{sp}_{2^{m+1}}$

We recall that

$$\mathfrak{sp}_{2^{m+1}}(R) = \{X \in M_{2^{m+1}}(R) : XK + KX^T = 0\},$$

where $K = \begin{pmatrix} 0 & I_{2^m} \\ -I_{2^m} & 0 \end{pmatrix}$. Let

$$D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

From the proof of Theorem 3.2.1, we can fix a suitable basis $\{\vec{e}_1, \ldots, \vec{e}_m, \vec{f}_1, \ldots, \vec{f}_m\}$ in the space $W = \mathbb{F}_{2^{m+1}} \oplus \mathbb{F}_{2^{m+1}}$, and set

$$\mathcal{J}_{\vec{w}} = J_{(a_1,b_1)} \otimes J_{(a_2,b_2)} \otimes \cdots \otimes J_{(a_{m+1},b_{m+1})}$$

for $\vec{w} = (a_1, \ldots, a_{m+1}; b_1, \ldots, b_{m+1}) \in W$, where $J(a,b) = D^a P^b$. Moreover, we define

$$q(\vec{w}) = \sum_{i=1}^{m+1} a_i b_i + (a_1 + b_1).$$

Then the symplectic form (3.9) is equal to

$$\langle \vec{w}, \vec{w}' \rangle = q(\vec{w}) + q(\vec{w}') + q(\vec{w} + \vec{w}')$$

for all $\vec{w}, \vec{w}' \in W$ and (W, q) is a nondegenerate quadratic space with Witt index m (Proposition 1.5.42 in [5]). To be used later in this section, we note that $(W, \langle \cdot, \cdot \rangle)$, which is defined in Theorem 3.2.1, is a symplectic space with maximum totally isotropic subspaces of dimension $m+1$.

Let $Q = \{\vec{w} \in W : q(\vec{w}) = 1\}$. We will describe a special basis of $\mathfrak{sp}_{2^{m+1}}(R)$ by using Q in the next theorem. This special basis will be used for the construction of an ODAC of $\mathfrak{sp}_{2^{m+1}}(R)$.

Theorem 4.1.1. *The Lie algebra $\mathfrak{sp}_{2^{m+1}}(R)$ has $\{\mathcal{J}_{\vec{w}} : \vec{w} \in Q\}$ as a basis.*

Proof. Write $\mathcal{J}_{\vec{w}} = J_{(a_1,b_1)} \otimes \mathcal{J}_{\vec{v}}$, where $\vec{v} = (a_2, \ldots, a_{m+1}; b_1, \ldots, b_{m+1})$. Note that $K =$

$DP \otimes I_{2^m}$. We show that if $\vec{w} \in Q$, then $\mathcal{J}_{\vec{w}} \in \mathfrak{sp}_{2^{m+1}}(R)$. Recall the notation

$$\mathfrak{B}(\vec{w}, \vec{w}) = \sum_{i=1}^{m+1} a_i b_i.$$

Now, consider

$$\begin{aligned}
K\mathcal{J}_{\vec{w}}^T &= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})} K\mathcal{J}_{\vec{w}} \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})} (DP \otimes I_{2^m})(J_{(a_1,b_1)} \otimes \mathcal{J}_{\vec{v}}) \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})} (DPJ_{(a_1,b_1)}) \otimes \mathcal{J}_{\vec{v}} \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})} (DPD^{a_1}P^{b_1}) \otimes \mathcal{J}_{\vec{v}} \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})+a_1+b_1} (D^{a_1}P^{b_1}DP) \otimes \mathcal{J}_{\vec{v}} \quad \text{(by (3.5))} \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})+a_1+b_1} (J_{(a_1,b_1)}DP) \otimes \mathcal{J}_{\vec{v}} \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})+a_1+b_1} (J_{(a_1,b_1)}DP) \otimes \mathcal{J}_{\vec{v}} I_{2^m} \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})+a_1+b_1} (J_{(a_1,b_1)} \otimes \mathcal{J}_{\vec{v}})(DP \otimes I_{2^m}) \\
&= (-1)^{-\mathfrak{B}(\vec{w},\vec{w})+a_1+b_1} \mathcal{J}_{\vec{w}} K \\
&= (-1)^{q(\vec{w})} \mathcal{J}_{\vec{w}} K \quad \text{(because } W \text{ is over } \mathbb{Z}_2) \ .
\end{aligned}$$

Since $\vec{w} \in Q$, $K\mathcal{J}_{\vec{w}}^T = -\mathcal{J}_{\vec{w}}K$, i.e. $\mathcal{J}_{\vec{w}} \in \mathfrak{sp}_{2^{m+1}}(R)$.

It is clear from the definition that all $\mathcal{J}_{\vec{w}}, \vec{w} \in Q$ are linearly independent. To complete the proof, we show that $|Q| = 2^m(2^{m+1}+1)$ which is the rank of $\mathfrak{sp}_{2^{m+1}}(R)$ as a free R-module. Then $\mathrm{Span}_R(\{\mathcal{J}_{\vec{w}} : \vec{w} \in Q\}) = \mathfrak{sp}_{2^{m+1}}(R)$ since R is finite. Let $\vec{w} = (a_1, \ldots, a_{m+1}; b_1, \ldots, b_{m+1}) \in Q$. Then

$$a_1b_1 + a_1 + b_1 = 1 + \sum_{i=2}^{m+1} a_i b_i.$$

Case 1: $a_1 = 0$. Then $b_1 = 1 + \sum_{i=2}^{m+1} a_i b_i$. Hence,

$$\Omega_0 = \{\vec{w} \in Q : \vec{w} = (0, a_2, \ldots, a_{m+1}; b_1, \ldots, b_{m+1})\}$$

has 2^{2m} elements.

Case 2: $a_1 = 1$. Then $\sum_{i=2}^{m+1} a_i b_i = 0$ and b_1 is 0 or 1. Let

$$\Omega_j = \begin{cases} \{\vec{w} \in Q : \vec{w} = (1, 0, \ldots, 0; b_1, \ldots, b_{m+1})\} & \text{if } j = 1, \\ \{\vec{w} \in Q : \vec{w} = (1, 0, \ldots, 0, 1, a_{j+1}, \ldots, a_{m+1}; b_1, \ldots, b_{m+1})\} & \text{if } 2 \leq j \leq m+1. \end{cases}$$

Then $|\Omega_1| = 2^{m+1}$. For $2 \leq j \leq m+1$, if $a_2 = \ldots = a_{j-1} = 0$ and $a_j = 1$, then $b_2, \ldots, b_{j-1}$ are 0 or 1 and $b_j = \sum_{i=j+1}^{m+1} a_i b_i$. Thus, $|\Omega_j| = 2^{2m-j+1}$. If $a_2 = \ldots = a_m = 0$ and $a_{m+1} = 1$, then $b_2, \ldots, b_m$ are 0 or 1 and $a_{m+1} = b_{m+1} = 1$. Thus, $|\Omega_{m+1}| = 2^m$.

Note that $\{\Omega_0, \Omega_1, \ldots, \Omega_{m+1}\}$ is a partition of Q. Therefore,

$$|Q| = \sum_{j=0}^{m+1} |\Omega_j| = 2^{2m} + 2^{m+1} + \sum_{j=2}^{m+1} 2^{2m-j+1} = 2^m(2^{m+1} + 1)$$

as desired. □

4.2 Orthogonal decomposition of $\mathfrak{sp}_{2^{m+1}}$

In this section, we will present the construction of an ODAC of $\mathfrak{sp}_{2^{m+1}}(R)$ by using the basis in Theorem 4.1.1. Note that $\mathfrak{sp}_{2^{m+1}}(R)$ is a Lie supalgebra of $\mathfrak{sl}_{2^{m+1}}(R)$ and we saw that an ODAC of $\mathfrak{sl}_{2^{m+1}}(R)$ is

$$\mathfrak{sl}_{2^{m+1}}(R) = H_\infty \oplus (\oplus_{\alpha \in \mathbb{F}_{2^{m+1}}} H_\alpha),$$

where $H_\infty = \langle \mathcal{J}_{(0;\lambda)} | \lambda \in \mathbb{F}_{2^{m+1}}^\times \rangle_{\mathbb{F}_{2^{m+1}}}$ and $H_\alpha = \langle \mathcal{J}_{(\alpha;\lambda\alpha)} | \lambda \in \mathbb{F}_{2^{m+1}}^\times \rangle_{\mathbb{F}_{2^{m+1}}}$ for all $\alpha \in \mathbb{F}_{2^{m+1}}$. The basis in Theorem 4.1.1 is the union of some subsets of these H_j's. We will see that the components of an ODAC of $\mathfrak{sp}_{2^{m+1}}(R)$ can be obtained from the H_i's by picking up the

elements whose index belongs to Q. We will use the following lemma to verify the constructed decomposition is an ODAC.

Lemma 4.2.1. *For each $\alpha \in \mathbb{F}_{2^{m+1}}$, let $W_\alpha = \{(\lambda, \alpha\lambda) \in W : \lambda \in \mathbb{F}_{2^{m+1}}^\times\}$, and let $W_\infty = \{(0,\lambda) \in W : \lambda \in \mathbb{F}_{2^{m+1}}^\times\}$. Then*

(1) $W = \left(\bigcup_{\alpha\in\mathbb{F}_{2^{m+1}}} \dot{W}_\alpha\right) \cup \dot{W}_\infty$ where $\dot{W}_\alpha = W_\alpha \cup \{(0,0)\}$, $\dot{W}_\infty = W_\infty \cup \{(0,0)\}$ are subspaces of W.

(2) For $\alpha \in \mathbb{F}_{2^{m+1}} \cup \{\infty\}$, if $Q_\alpha = W_\alpha \cap Q$, then $\dot{W}_\alpha = \langle Q_\alpha \rangle_{\mathbb{Z}_2}$.

Proof. It is clear that the $\dot{W}_\alpha$'s are subspaces of W and (1) holds. To prove (2), we first note that $Q^c = W \setminus Q = \{\vec{w} \in W : q(\vec{w}) = 0\}$ and

$$\begin{aligned} |Q^c \setminus \{(0,0)\}| &= |W| - |Q| \\ &= (2^{2(m+1)} - 1) - 2^m(2^{m+1} + 1) \\ &= (2^m - 1)(2^{m+1} - 1). \end{aligned} \tag{4.1}$$

We show that for all $\alpha \in \mathbb{F}_{2^{m+1}} \cup \{\infty\}, |W_\alpha \cap (Q^c \setminus \{(0,0)\})| \geq 2^m - 1$. Suppose, to the contrary, that there exists an α such that $|W_\alpha \cap (Q^c \setminus \{(0,0)\})| < 2^m - 1$. Then by (4.1), there exists an α' such that $|W_{\alpha'} \cap (Q^c \setminus \{(0,0)\})| \geq 2^m$. So $|\dot{W}_{\alpha'} \cap Q^c| \geq 2^m + 1$. But $\dot{W}_{\alpha'} \cap Q^c$ is a totally isotopic subspace of (W, q). Indeed, if $\vec{w}_1, \vec{w}_2 \in \dot{W}_{\alpha'} \cap Q^c$, then $q(\vec{w}_1 + \vec{w}_2) = q(\vec{w}_1) + q(\vec{w}_2) + \langle \vec{w}_1, \vec{w}_2 \rangle = 0$. Thus, $\dim(\dot{W}_{\alpha'} \cap Q^c) \leq m$ and as a subspace over $\mathbb{Z}_2$, $|\dot{W}_{\alpha'} \cap Q^c| \leq 2^m$. This is a contradiction.

Now, for each $\alpha \in \mathbb{F}_{2^{m+1}} \cup \{\infty\}$, by (4.1), $|W_\alpha \cap (Q^c \setminus \{(0,0)\})| = 2^m - 1$, and hence,

$$|W_\alpha \cap Q| = (2^{m+1} - 1) - (2^m - 1) = 2^m.$$

Let $Q_\alpha = W_\alpha \cap Q$. Then $\langle Q_\alpha \rangle_{\mathbb{Z}_2}$ is a totally isotopic subspace of $(W, \langle \cdot, \cdot \rangle)$ and $W_\alpha \supseteq \langle Q_\alpha \rangle_{\mathbb{Z}_2}$. We have $\dim(\langle Q_\alpha \rangle_{\mathbb{Z}_2}) \leq m+1$. But since $|\langle Q_\alpha \rangle_{\mathbb{Z}_2}| \geq |Q_\alpha| + 1 = 2^m + 1$, $\dim(\langle Q_\alpha \rangle_{\mathbb{Z}_2}) \geq m+1$ which forces $\dim(\langle Q_\alpha \rangle_{\mathbb{Z}_2}) = m+1$. Thus, $|\langle Q_\alpha \rangle_{\mathbb{Z}_2}| = 2^{m+1} = |\dot{W}_\alpha|$, and so $\dot{W}_\alpha = \langle Q_\alpha \rangle_{\mathbb{Z}_2}$. □

Using the above lemma and Theorem 4.1.1, we have the following theorem.

Theorem 4.2.2. *For a positive integer m, $\mathfrak{sp}_{2^{m+1}}(R)$ has an* ODAC *obtained by restricting an* ODAC *of $\mathfrak{sl}_{2^{m+1}}(R)$ constructed in Theorem 3.2.1.*

Proof. For each $\alpha \in \mathbb{F}_{2^{m+1}}$, let

$$H'_\alpha = \langle \mathcal{J}_{(\lambda,\alpha\lambda)} | \lambda \in \mathbb{F}^\times_{2^{m+1}} \text{ and } (\lambda, \alpha\lambda) \in Q \rangle_R ,$$

and let

$$H'_\infty = \langle \mathcal{J}_{(0,\lambda)} | \lambda \in \mathbb{F}^\times_{2^{m+1}} \text{ and } (0, \lambda) \in Q \rangle_R .$$

It follows from the proof of Theorem 3.2.1 and Theorem 4.1.1 that all H'_α's, $\alpha \in \mathbb{F}_{2^{m+1}} \cup \{\infty\}$ are orthogonal abelian subalgebras of $\mathfrak{sp}_{2^{m+1}}(R)$ and the sum of all these H'_α's is direct. Thus,

$$\mathfrak{sp}_{m+1}(R) = H'_\infty \oplus (\oplus_{\alpha \in \mathbb{F}_{2^{m+1}}} H'_\alpha).$$

To show that each H'_α is a self-normalizer, let $\alpha \in \mathbb{F}_{2^{m+1}}$ and $A \in N_{\mathfrak{sp}_{2^{m+1}}(R)}(H'_\alpha)$. Then

$$A = \sum_{\beta' \in \mathbb{F}_q} \left(\sum_{\substack{\lambda' \in \mathbb{F}_q^\times \\ (\lambda', \beta'\lambda') \in Q}} a_{(\lambda',\beta')} \mathcal{J}_{(\lambda',\beta'\lambda')} \right) + \sum_{\substack{\lambda' \in \mathbb{F}_q^\times \\ (0,\lambda') \in Q}} b_{\lambda'} \mathcal{J}_{(0,\lambda')}$$

where $a_{(\lambda',\beta')}$ and $b_{\lambda'}$ are elements in R. For any $\mathcal{J}_{(\lambda,\alpha\lambda)} \in H'_\alpha$,

$$[A, \mathcal{J}_{(\lambda,\alpha\lambda)}] = \sum_{\beta' \in \mathbb{F}_q} \left(\sum_{\substack{\lambda' \in \mathbb{F}_q^\times \\ (\lambda', \beta'\lambda') \in Q}} a_{(\lambda',\beta')} [\mathcal{J}_{(\lambda',\beta'\lambda')}, \mathcal{J}_{(\lambda,\alpha\lambda)}] \right) + \sum_{\substack{\lambda' \in \mathbb{F}_q^\times \\ (0,\lambda') \in Q}} b_{\lambda'} [\mathcal{J}_{(0,\lambda')}, \mathcal{J}_{(\lambda,\alpha\lambda)}] \in H'_\alpha.$$

This implies

$$\sum_{\substack{\beta'\in\mathbb{F}_q\\ \beta'\neq\alpha}}\left(\sum_{\substack{\lambda'\in\mathbb{F}_q^\times\\ (\lambda',\beta'\lambda')\in Q}} a_{(\lambda',\beta')}[\mathcal{J}_{(\lambda',\beta'\lambda')},\mathcal{J}_{(\lambda,\alpha\lambda)}]\right)+\sum_{\substack{\lambda'\in\mathbb{F}_q^\times\\ (0,\lambda')\in Q}} b_{\lambda'}[\mathcal{J}_{(0,\lambda')},\mathcal{J}_{(\lambda,\alpha\lambda)}]\in H'_\alpha.$$

For each (λ',β'), if for all $(\lambda,\alpha\lambda)\in Q$, $\langle(\lambda,\alpha\lambda),(\lambda',\beta'\lambda')\rangle=0$, then by Lemma 4.2.1, $\mathcal{J}_{(\lambda',\beta'\lambda')}$ would be in $N_{\mathfrak{sl}_{2^{m+1}}(R)}(H_\alpha)=H_\alpha$. So, we may assume that we can choose $(\lambda,\alpha\lambda)\in Q$ such that $\langle(\lambda,\alpha\lambda),(\lambda',\beta'\lambda')\rangle=1$. Argue as in the proof of Theorem 3.2.1, we obtain $a_{(\lambda',\beta')}=0$. Similarly, $b_{\lambda'}=0$. Thus, $A\in H'_\alpha$, and so $N_{\mathfrak{sp}_{2^{m+1}}(R)}(H'_\alpha)=H'_\alpha$. By analogous arguments, we also have $N_{\mathfrak{sp}_{2^{m+1}}(R)}(H'_\infty)=H'_\infty$. Hence, $\mathfrak{sp}_{2^{m+1}}(R)$ has an ODAC. □

Example 4.2.3. We will present an ODAC of $\mathfrak{sp}_4(R)$ which is obtained by restricting the ODAC in Example 3.2.2 as described in the proof of the theorem above. Consider the basis

$$\mathcal{B}=\{(1,0),(1+x,0),(0,x),(0,1)\}$$

of the symplectic space W. We have

$$\begin{aligned}
H'_\infty &= \left\langle \mathcal{J}_{(0,\lambda)} | \lambda\in\mathbb{F}_4^\times \text{ and } (0,\lambda)\in Q\right\rangle_R\\
&= \left\langle \mathcal{J}_{(0,x)},\mathcal{J}_{(0,1+x)}\right\rangle_R\\
&= \left\langle \mathcal{J}_{(0,0;1,0)},\mathcal{J}_{(0,0;1,1)}\right\rangle_R\\
&= \left\langle J_{(0,1)}\otimes J_{(0,0)}, J_{(0,1)}\otimes J_{(0,1)}\right\rangle_R\\
&= \mathrm{Span}_R\left\{\begin{bmatrix} & 1 & & \\ & & & 1\\ 1 & & & \\ & 1 & & \end{bmatrix},\begin{bmatrix} & & & 1\\ & & 1 & \\ & 1 & & \\ 1 & & & \end{bmatrix}\right\},\\
H'_0 &= \left\langle \mathcal{J}_{(\lambda,0)} | \lambda\in\mathbb{F}_4^\times \text{ and } (\lambda,0)\in Q\right\rangle_R\\
&= \left\langle \mathcal{J}_{(1,0)},\mathcal{J}_{(x,0)}\right\rangle_R\\
&= \left\langle \mathcal{J}_{(1,0;0,0)},\mathcal{J}_{(1,1;0,0)}\right\rangle_R\\
&= \left\langle J_{(1,0)}\otimes J_{(0,0)}, J_{(1,0)}\otimes J_{(1,0)}\right\rangle_R
\end{aligned}$$

$$= \mathrm{Span}_R \left\{ \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix} \right\},$$

$$H_1' = \left\langle \mathcal{J}_{(\lambda,\lambda)} | \lambda \in \mathbb{F}_4^\times \text{ and } (\lambda, x\lambda) \in Q \right\rangle_R$$

$$= \left\langle \mathcal{J}_{(1,1)}, \mathcal{J}_{(x,x)} \right\rangle_R$$

$$= \left\langle \mathcal{J}_{(1,0;0,1)}, \mathcal{J}_{(1,1;1,0)} \right\rangle_R$$

$$= \left\langle J_{(1,0)} \otimes J_{(0,1)}, J_{(1,1)} \otimes J_{(1,0)} \right\rangle_R$$

$$= \mathrm{Span}_R \left\{ \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & -1 \\ & & -1 & \end{bmatrix}, \begin{bmatrix} & & 1 & \\ & & & -1 \\ -1 & & & \\ & 1 & & \end{bmatrix} \right\},$$

$$H_x' = \left\langle \mathcal{J}_{(\lambda,x\lambda)} | \lambda \in \mathbb{F}_4^\times \text{ and } (\lambda, x\lambda) \in Q \right\rangle_R$$

$$= \left\langle \mathcal{J}_{(1,x)}, \mathcal{J}_{(1+x,1)} \right\rangle_R$$

$$= \left\langle \mathcal{J}_{(1,0;1,0)}, \mathcal{J}_{(0,1;0,1)} \right\rangle_R$$

$$= \left\langle J_{(1,1)} \otimes J_{(0,0)}, J_{(0,0)} \otimes J_{(1,1)} \right\rangle_R$$

$$= \mathrm{Span}_R \left\{ \begin{bmatrix} & & 1 & \\ & & & 1 \\ -1 & & & \\ & -1 & & \end{bmatrix}, \begin{bmatrix} & 1 & & \\ -1 & & & \\ & & & 1 \\ & & -1 & \end{bmatrix} \right\},$$

$$H_{1+x}' = \left\langle \mathcal{J}_{(\lambda,(1+x)\lambda)} | \lambda \in \mathbb{F}_4^\times \text{ and } (\lambda, (1+x)\lambda) \in Q \right\rangle_R$$

$$= \left\langle \mathcal{J}_{(1,1+x)}, \mathcal{J}_{(1+x,x)} \right\rangle_R$$

$$= \left\langle \mathcal{J}_{(1,0;1,1)}, \mathcal{J}_{(0,1;1,0)} \right\rangle_R$$

$$= \left\langle J_{(1,1)} \otimes J_{(0,1)}, J_{(0,1)} \otimes J_{(1,0)} \right\rangle_R$$

$$= \mathrm{Span}_R \left\{ \begin{bmatrix} & & & 1 \\ & & 1 & \\ & -1 & & \\ -1 & & & \end{bmatrix}, \begin{bmatrix} & & 1 & \\ & & & -1 \\ 1 & & & \\ & -1 & & \end{bmatrix} \right\}.$$

We conclude that $\mathfrak{sp}_4(R)$ has an ODAC:

$$\mathfrak{sp}_4(R) = H_\infty' \oplus H_0' \oplus H_1' \oplus H_x' \oplus H_{1+x}'.$$

Chapter 5

Orthogonal decompositions of Lie algebras of types B and D

In this chapter, we again assume that R has odd characteristic.

The Lie algebras of skew symmetric $n \times n$ matrices $\mathfrak{so}_n(R)$ are of type B or type D. When n is even, they are of type D. Otherwise, they are of type B. We will construct ODACs in both cases.

5.1 Orthogonal decomposition of $\mathfrak{so}_{2n}$

Recall that

$$\mathfrak{so}_{2n}(R) = \langle X_{(i,j)} | 1 \leq i \neq j \leq 2n \rangle_R ,$$

where $X_{(i,j)} = e_{ij} - e_{ji}$ and e_{ij} is the matrix having 1 in the (i,j) position and 0 elsewhere. We will utilize these basis elements to construct an ODAC of this Lie algebra. The matrices $X_{(i,j)}$'s satisfy the following properties:

Lemma 5.1.1. *With the above notations and denoted by $\{\cdot,\cdot\}$ an unordered pair, we have*

(1) $X_{(i,j)} = -X_{(j,i)}$.

(2) If $\{i,j\} \neq \{k,l\}$, *then* $\mathrm{Tr}(X_{(i,j)}X_{(k,l)}) = 0$.

(3) $[X_{(i,j)}, X_{(k,l)}] = \begin{cases} X_{(i,l)} & \text{if } j = k, \\ 0 & \text{if } \{i,j\} \cap \{k,l\} = \emptyset. \end{cases}$

Proof. The first property is clear from the definition. To prove (2), we first compute

$$\begin{aligned} X_{(i,j)}X_{(k,l)} &= (e_{ij} - e_{ji})(e_{kl} - e_{lk}) \\ &= e_{ij}e_{kl} - e_{ij}e_{lk} - e_{ji}e_{kl} + e_{ji}e_{lk}. \end{aligned}$$

Assume that $\{i,j\} \neq \{k,l\}$. We consider two distinct cases.

Case 1: $i \neq k$ and l. We have $X_{(i,j)}X_{(k,l)} = e_{ij}e_{kl} - e_{ij}e_{lk}$. Then $\mathrm{Tr}(X_{(i,j)}X_{(k,l)}) = 0$.

Case 2: $j \neq k$ and l. We have $X_{(i,j)}X_{(k,l)} = -e_{ji}e_{kl} + e_{ji}e_{lk}$. Then $\mathrm{Tr}(X_{(i,j)}X_{(k,l)}) = 0$.

Finally,

$$\begin{aligned} [X_{(i,j)}, X_{(k,l)}] &= X_{(i,j)}X_{(k,l)} - X_{(k,l)}X_{(i,j)} \\ &= (e_{ij}e_{kl} - e_{ij}e_{lk} - e_{ji}e_{kl} + e_{ji}e_{lk}) - (e_{kl}e_{ij} - e_{kl}e_{ji} - e_{lk}e_{ij} + e_{lk}e_{ji}) \\ &= \begin{cases} X_{(i,l)} & \text{if } j = k, \\ 0 & \text{if } \{i,j\} \cap \{k,l\} = \emptyset, \end{cases} \end{aligned}$$

as claimed. □

We will use the relations in the above lemma to construct an ODAC of $\mathfrak{so}_{2n}(R)$. To do that, we introduce the following set of unordered pairs and its partition. Let

$$X = \{\{i,j\} : 1 \leq i \neq j \leq 2n\}$$

and let

$$\mathcal{P} = \{M_k : 1 \leq k \leq 2n-1\}$$

be a partition of X, where $|M_k| = n$ and $\alpha \cap \beta = \emptyset$ for any $\alpha, \beta \in M_k$ such that $\alpha \neq \beta$.

This partition $\mathcal{P}$ can be viewed as a partition of the complete graph with vertex set $\{1, 2, \ldots, 2n\}$ and edge set X, it is also called 1-factorization of the graph. Thus, the partition is constructible. Note that $|X| = n(2n-1)$ which is equal to the rank of $\mathfrak{so}_{2n}(R)$ as an R-module.

Example 5.1.2. For $n = 4$, we have

$$\begin{aligned} X = \{&\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{1,7\},\{1,8\} \\ &\{2,3\},\{2,4\},\{2,5\},\{2,6\},\{2,7\},\{2,8\},\{3,4\} \\ &\{3,5\},\{3,6\},\{3,7\},\{3,8\},\{4,5\},\{4,6\},\{4,7\} \\ &\{4,8\},\{5,6\},\{5,7\},\{5,8\},\{6,7\},\{6,8\},\{7,8\}\}. \end{aligned}$$

Then we can choose

$$\begin{aligned} M_1 &= \{\{1,8\},\{2,5\},\{3,6\},\{4,7\}\}, \\ M_2 &= \{\{1,7\},\{2,8\},\{3,4\},\{5,6\}\}, \\ M_3 &= \{\{1,6\},\{2,7\},\{3,8\},\{4,5\}\}, \\ M_4 &= \{\{1,5\},\{2,6\},\{3,7\},\{4,8\}\}, \\ M_5 &= \{\{1,4\},\{2,3\},\{5,8\},\{6,7\}\}, \\ M_6 &= \{\{1,3\},\{2,4\},\{5,7\},\{6,8\}\}, \\ M_7 &= \{\{1,2\},\{3,5\},\{4,6\},\{7,8\}\}. \end{aligned}$$

Theorem 5.1.3. *For a positive integer n, $\mathfrak{so}_{2n}(R)$ has an ODAC*

$$\mathfrak{so}_{2n}(R) = H_1 \oplus H_2 \oplus \cdots \oplus H_{2n-1},$$

where $H_k = \langle X_{(i,j)} | \{i,j\} \in M_k \rangle_R$.

Proof. By Lemma 5.1.1 (2) and (3), we have the orthogonality and the commutativity of H_k's. Next, we show that $N_{\mathfrak{so}_{2n}(R)}(H_k) = H_k$. Let $A \in N_{\mathfrak{so}_{2n}(R)}(H_k)$ and write it as a linear combination of the elements $X_{(i,j)}$

$$A = \sum_{i \neq j} \alpha_{ij} X_{(i,j)}.$$

For any $X_{(s,t)} \in H_k$,

$$[A, X_{(s,t)}] = \sum_{i \neq j} \alpha_{ij} [X_{(i,j)}, X_{(s,t)}] \in H_k,$$

and so

$$\sum_{\substack{i \neq j \\ \{i,j\} \notin M_k}} \alpha_{ij} [X_{(i,j)}, X_{(s,t)}] \in H_k.$$

For each pair (i, j), since the M_k's form a partition of X, there exists $X_{(j,t)} \in H_k$ such that $t \neq i$ and $[X_{(i,j)}, X_{(j,t)}] = X_{(i,t)} \neq 0$ by Lemma 5.1.1. Therefore, $\alpha_{ij} = 0$, and so $A \in H_k$. $\square$

Example 5.1.4. Using the decomposition in Example 5.1.2, we obtain an ODAC of $\mathfrak{so}_8(R)$

$$\mathfrak{so}_8(R) = H_1 \oplus H_2 \oplus \cdots \oplus H_7,$$

where

$$H_1 = \mathrm{Span}_R\{X_{(1,8)}, X_{(2,5)}, X_{(3,6)}, X_{(4,7)}\},$$

$$H_2 = \mathrm{Span}_R\{X_{(1,7)}, X_{(2,8)}, X_{(3,4)}, X_{(5,6)}\},$$

$$H_3 = \mathrm{Span}_R\{X_{(1,6)}, X_{(2,7)}, X_{(3,8)}, X_{(4,5)}\},$$

$$H_4 = \mathrm{Span}_R\{X_{(1,5)}, X_{(2,6)}, X_{(3,7)}, X_{(4,8)}\},$$

$$H_5 = \mathrm{Span}_R\{X_{(1,4)}, X_{(2,3)}, X_{(5,8)}, X_{(6,7)}\},$$

$$H_6 = \mathrm{Span}_R\{X_{(1,3)}, X_{(2,4)}, X_{(5,7)}, X_{(6,8)}\},$$

$$H_7 = \mathrm{Span}_R\{X_{(1,2)}, X_{(3,5)}, X_{(4,6)}, X_{(7,8)}\}.$$

5.2 Orthogonal decomposition of $\mathfrak{so}_{2n-1}$

In this section, we will discuss the existence of ODAC of the Lie algebra

$$\mathfrak{so}_{2n-1}(R) = \langle X_{(i,j)} | 1 \leq i \neq j \leq 2n-1 \rangle_R .$$

Similar to Section 5.1, we let

$$X' = \{\{i,j\} : 1 \leq i \neq j \leq 2n-1\}.$$

In the next step, we will construct a partition of this set into subsets M'_k satisfying

$$|M'_k| = n-1 \text{ and } \alpha \cap \beta = \emptyset \text{ for all } \alpha, \beta \in M'_k, \alpha \neq \beta.$$

The construction can be obtained from all M_k's of the construction of an ODAC of $\mathfrak{so}_{2n}(R)$ in the previous section. Without loss of generality, we assume that each M_k contains the pair $\{k, 2n\}$. Let $M'_k = M_k \setminus \{k, 2n\}$.

Theorem 5.2.1. *For a positive integer $n \geq 2$, $\mathfrak{so}_{2n-1}(R)$ has an* ODAC

$$\mathfrak{so}_{2n-1}(R) = H'_1 \oplus H'_2 \oplus \cdots \oplus H'_{2n-1},$$

where $H'_k = \langle X_{(i,j)} | \{i,j\} \in M'_k \rangle_R$.

Proof. We only need to show that each H'_k is a self-normalizer because analogous arguments from the proof of Theorem 5.1.3 can be used to prove the rest. Let $A \in N_{\mathfrak{so}_{2n-1}(R)}(H_k)$ and write it as a linear combination of the elements $X_{(i,j)}$

$$A = \sum_{i \neq j} \alpha_{ij} X_{(i,j)}.$$

For any $X_{(s,t)} \in H_k$,

$$[A, X_{(s,t)}] = \sum_{i \neq j} \alpha_{ij}[X_{(i,j)}, X_{(s,t)}] \in H_k,$$

and so

$$\sum_{\substack{i \neq j \\ \{i,j\} \notin M'_k}} \alpha_{ij}[X_{(i,j)}, X_{(s,t)}] \in H_k.$$

For each pair (i, j), if $j \neq k$, we can use the argument provided in Theorem 5.1.3 to prove $\alpha_{ij} = 0$. If $j = k$, we use the relation (1) of Lemma 5.1.1 to interchange i and j. This completes the proof. □

Example 5.2.2. The Lie algebra $\mathfrak{so}_7(R)$ has an ODAC

$$\mathfrak{so}_7(R) = H_1 \oplus H_2 \oplus \cdots \oplus H_7,$$

where

$$H_1 = \mathrm{Span}_R\{X_{(2,5)}, X_{(3,6)}, X_{(4,7)}\},$$
$$H_2 = \mathrm{Span}_R\{X_{(1,7)}, X_{(3,4)}, X_{(5,6)}\},$$
$$H_3 = \mathrm{Span}_R\{X_{(1,6)}, X_{(2,7)}, X_{(4,5)}\},$$
$$H_4 = \mathrm{Span}_R\{X_{(1,5)}, X_{(2,6)}, X_{(3,7)}\},$$
$$H_5 = \mathrm{Span}_R\{X_{(1,4)}, X_{(2,3)}, X_{(6,7)}\},$$
$$H_6 = \mathrm{Span}_R\{X_{(1,3)}, X_{(2,4)}, X_{(5,7)}\},$$
$$H_7 = \mathrm{Span}_R\{X_{(1,2)}, X_{(3,5)}, X_{(4,6)}\}.$$

Chapter 6

Further developments

In Theorem 3.2.5, 3.2.6 and Corollary 3.2.7, we provided some sufficient conditions for the existence of an ODAC of $\mathfrak{sl}_n(R)$. On the other hand, a necessary condition of this ODAC is given in Theorem 3.3.2. These conditions are from the structure of the ring R and n, and can be checked readily. As a result, we can provide a collection of the rings R such that $\mathfrak{sl}_n(R)$ has an ODAC and another collection of the rings R for nonexistence of ODAC of $\mathfrak{sl}_n(R)$. However, the complete description of the rings R for which $\mathfrak{sl}_n(R)$ has an ODAC requires further attention.

The orthogonal decomposition problem of $\mathfrak{sl}_6(R)$ should be more focused on. We would like to answer the following question:

Question 2. Is there any commutative ring R with identity for which $\mathfrak{sl}_6(R)$ has an ODAC?

The first step that may be manageable is to study a classical ODAC of $\mathfrak{sl}_6(\mathbb{Z}_5)$ because the structure of $\mathrm{Aut}(\mathfrak{sl}_6(\mathbb{Z}_5))$ and some useful properties of this modular Lie algebra are known. Moreover, we may be able to use the concept of Gröbner bases and use Magma for the computation to answer this question. If there is no any ODAC of $\mathfrak{sl}_6(\mathbb{Z}_5)$, then we will find the maximum number of pairwise orthogonal classical Cartan subalgebras.

Appendix A

Gröbner bases

The following Sage code and Magma code are used to complete the proof in Lemma 3.1.6.The output for both code should be "True".

Sage code:

```
R.<a, b, c, d, x, y, z, u, v, w > = ZZ[]
A = matrix([[0, 0, 0], [a, 0, b], [c, d, 0]])
B = matrix([[0, x, y], [u, 0, z], [v, w, 0]])
C = A*B - B*A
detkilling = (A*A).trace()*(B*B).trace() - ((A*B).trace())^ 2
J = ideal (list (C[0]) + list (C[1]) + list (C[2]) + [a*b*c*d])
detkilling in J
```

Magma code:

```
P<a,b,c,d,x, y,z,u,v,w> := PolynomialRing(IntegerRing(),10);
A := Matrix(3, [0,0,0, a,0,b, c,d,0]);
B := Matrix(3, [0,x,y, u,0,z, v,w,0]);
C := A*B - B*A;
detkilling := Trace(A*A)*Trace(B*B) - Trace(A*B)^ 2;
S := { C[i,j]: i,j in [1, 2, 3] } join { a*b*c*d };
```

J := Ideal(S);

detKilling in J;

Appendix B

Maximum number of classical components

For $\mathfrak{sl}_2$, we input the value of a prime power integer k into the code below to represent the cardinality of a needed finite field. The conclusion can be drawn from Max 2 and Max 3. If both are assigned, then the maximum number of pairwise orthogonal classical Cartan subalgebras is three. If only Max 2 is assigned, then the maximum number of pairwise orthogonal classical Cartan subalgebras is two. Otherwise, the maximum number is one.

The code for $\mathfrak{sl}_2$:

```
k := ...;
K:=FiniteField(k);
X1 := DiagonalMatrix(K, [1, -1]);
H := {X1};
SL := SpecialLinearGroup(2,K);
for M1 in SL do
if Trace(X1*M1*X1*M1^(-1)) eq 0 then
Max2 := 2;
for M2 in SL do
```

```
if M1 ne M2 then
if Trace(X1*M2*X1*M2^(-1)) eq 0 then
if Trace(M1*X1*M1^(-1)*M2*X1*M2^(-1)) eq 0 then
Max3 := 3;
break M1;
end if;
end if;
end if;
end for;
end if;
end for;
Max2;
Max3;
```

For $\mathfrak{sl}_3$, we proceed analogously with the code:

```
k := ...;
K := FiniteField(k);
X1 := DiagonalMatrix(K, [1, -1, 0]);
X2 := DiagonalMatrix(K, [0, 1, -1]);
H := {X1, X2};
SL := SpecialLinearGroup(3,K);
for M1 in SL do
if forall{ <X,Y> : X, Y in H — Trace(X*M1*Y*M1^(-1)) eq 0} then
Max2 := 2;
for M2 in SL do
if M1 ne M2 then
if forall{ <X,Y> : X, Y in H — Trace(X*M2*Y*M2^(-1)) eq 0} then
if forall{ <X,Y> : X, Y in H — Trace(M1*X*M1^(-1)*M2*Y*M2^(-1)) eq 0} then
```

```
Max3 := 3;
for M3 in SL do
if M1 ne M3 then
if M2 ne M3 then
if forall{ <X,Y> : X, Y in H — Trace(X*M3*Y*M3^(-1)) eq 0} then
if forall{ <X,Y> : X, Y in H — Trace(M1*X*M1^(-1)*M3*Y*M3^(-1)) eq 0 and
Trace(M2*X*M2^(-1)*M3*Y*M3^(-1)) eq 0} then
Max4 := 4;
break M1;
end if;
end if;
end if;
end if;
end for;
end if;
end if;
end if;
end for;
end if;
end for;
Max2;
Max3;
Max4;
```

Appendix C

$\mathbb{J}$-decompositions of $\mathfrak{sl}_3$ over finite fields

C.1 Mathematica code for checking $\mathbb{J}_3(1,z)$ and $\mathbb{J}_3(1,1)$

Recalling the setting of the proof of Theorem 3.5.7, we need to consider the following $\mathbb{J}$-decompositions.

(1) $\mathbb{J}_3(1,1)$:

$$\mathfrak{sl}_3(\mathbb{F}_{p^m}) = \langle J_{(1,0)}, J_{(2,0)} \rangle \oplus \langle J_{(0,1)}, J_{(0,2)} \rangle \oplus \langle J_{(1,1)}, J_{(2,2)} \rangle \oplus \langle J_{(2,1)}, J_{(1,2)} \rangle ,$$

where $J_{(a,b)} = D^a P^b$ and

$$D = \mathrm{diag}\{1, u, u^2\}, P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

(2) $\mathbb{J}_3(1,z)$:

$$\mathfrak{sl}_3(\mathbb{F}_{p^m}) = \langle J'_{(1,0)}, J'_{(2,0)} \rangle \oplus \langle J'_{(0,1)}, J'_{(0,2)} \rangle \oplus \langle J'_{(1,1)}, J_{(2,2)} \rangle \oplus \langle J'_{(2,1)}, J'_{(1,2)} \rangle ,$$

where $J'_{(a,b)} = D^a P_b$ and

$$D = \mathrm{diag}\{1, u, u^2\}, P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

The inputs of the above matrices is:

$P = \{\{0,0,1\},\{1,0,0\},\{0,1,0\}\};$

$p[0] = \mathrm{IdentityMatrix}[3];$

$p[1] = P;$

$p[2] = P.P;$

$p'[0] = \mathrm{IdentityMatrix}[3];$

$p'[1] = \{\{0,0,1\},\{z,0,0\},\{0,z,0\}\};$

$p'[2] = \{\{0,1,0\},\{0,0,1\},\{z,0,0\}\};$

$p''[0] = \mathrm{IdentityMatrix}[3];$

$p''[1] = \{\{0,0,1\},\{z^2,0,0\},\{0,z^2,0\}\};$

$p''[2] = \{\{0,1,0\},\{0,0,1\},\{z^2,0,0\}\};$

$d[0] = \mathrm{IdentityMatrix}[3];$

$d[i\_]:=\mathrm{DiagonalMatrix}[\{1, u^{\mathrm{Mod}[i,3]}, u^{\mathrm{Mod}[2i,3]}\}];$

$f[A\_, B\_]:=A.B - B.A$

$J[\mathrm{a}\_, \mathrm{b}\_]:=d[\mathrm{Mod}[a,3]].p[\mathrm{Mod}[b,3]]$

$$J'[\mathrm{a\_}, \mathrm{b\_}]{:=}d[\mathrm{Mod}[a,3]].p'[\mathrm{Mod}[b,3]]$$

$$J''[\mathrm{a\_}, \mathrm{b\_}]{:=}d[\mathrm{Mod}[a,3]].p''[\mathrm{Mod}[b,3]]$$

Suppose that $\mathbb{J}_3(1,1) \approx \mathbb{J}_3(1,z)$ by the map φ. Then we consider:

$$\varphi(J'[1,0]) = \alpha J[m[i], n[i]];$$

$$\varphi(J'[2,0]) = \beta J[k[i], l[i]];$$

$$\varphi(J'[0,1]) = \gamma J[s[i], t[i]];$$

$$\varphi(J'[0,2]) = \delta J[x[i], y[i]];$$

$$\varphi(J'[1,1]) = \text{Simplify}\left[\frac{f\left[\varphi(J'[1,0]), \varphi(J'[0,1])\right]}{1-u^2}\right];$$

$$\varphi(J'[2,2]) = \text{Simplify}\left[\frac{f\left[\varphi(J'[2,0]), \varphi(J'[0,2])\right]}{1-u^2}\right];$$

$$\varphi(J'[1,2]) = \text{Simplify}\left[\frac{f\left[\varphi(J'[1,0]), \varphi(J'[0,2])\right]}{1-u}\right];$$

and check all of the following cases:

$$m[1]=1; n[1]=0; k[1]=2; l[1]=0; s[1]=0; t[1]=1; x[1]=0; y[1]=2;$$

$$m[2]=1; n[2]=0; k[2]=2; l[2]=0; s[2]=0; t[2]=2; x[2]=0; y[2]=1;$$

$$m[3]=1; n[3]=0; k[3]=2; l[3]=0; s[3]=1; t[3]=1; x[3]=2; y[3]=2;$$

$$m[4]=1; n[4]=0; k[4]=2; l[4]=0; s[4]=2; t[4]=2; x[4]=1; y[4]=1;$$

$$m[5]=1; n[5]=0; k[5]=2; l[5]=0; s[5]=2; t[5]=1; x[5]=1; y[5]=2;$$

$$m[6]=1; n[6]=0; k[6]=2; l[6]=0; s[6]=1; t[6]=2; x[6]=2; y[6]=1;$$

$$m[7]=2; n[7]=0; k[7]=1; l[7]=0; s[7]=0; t[7]=1; x[7]=0; y[7]=2;$$

$$m[8]=2; n[8]=0; k[8]=1; l[8]=0; s[8]=0; t[8]=2; x[8]=0; y[8]=1;$$

$$m[9]=2; n[9]=0; k[9]=1; l[9]=0; s[9]=1; t[9]=1; x[9]=2; y[9]=2;$$

$$m[10]=2; n[10]=0; k[10]=1; l[10]=0; s[10]=2; t[10]=2; x[10]=1; y[10]=1;$$

$m[11] = 2; n[11] = 0; k[11] = 1; l[11] = 0; s[11] = 2; t[11] = 1; x[11] = 1; y[11] = 2;$

$m[12] = 2; n[12] = 0; k[12] = 1; l[12] = 0; s[12] = 1; t[12] = 2; x[12] = 2; y[12] = 1;$

$m[13] = 0; n[13] = 1; k[13] = 0; l[13] = 2; s[13] = 1; t[13] = 0; x[13] = 2; y[13] = 0;$

$m[14] = 0; n[14] = 1; k[14] = 0; l[14] = 2; s[14] = 2; t[14] = 0; x[14] = 1; y[14] = 0;$

$m[15] = 0; n[15] = 1; k[15] = 0; l[15] = 2; s[15] = 1; t[15] = 1; x[15] = 2; y[15] = 2;$

$m[16] = 0; n[16] = 1; k[16] = 0; l[16] = 2; s[16] = 2; t[16] = 2; x[16] = 1; y[16] = 1;$

$m[17] = 0; n[17] = 1; k[17] = 0; l[17] = 2; s[17] = 2; t[17] = 1; x[17] = 1; y[17] = 2;$

$m[18] = 0; n[18] = 1; k[18] = 0; l[18] = 2; s[18] = 1; t[18] = 2; x[18] = 2; y[18] = 1;$

$m[19] = 0; n[19] = 2; k[19] = 0; l[19] = 1; s[19] = 1; t[19] = 0; x[19] = 2; y[19] = 0;$

$m[20] = 0; n[20] = 2; k[20] = 0; l[20] = 1; s[20] = 2; t[20] = 0; x[20] = 1; y[20] = 0;$

$m[21] = 0; n[21] = 2; k[21] = 0; l[21] = 1; s[21] = 1; t[21] = 1; x[21] = 2; y[21] = 2;$

$m[22] = 0; n[22] = 2; k[22] = 0; l[22] = 1; s[22] = 2; t[22] = 2; x[22] = 1; y[22] = 1;$

$m[23] = 0; n[23] = 2; k[23] = 0; l[23] = 1; s[23] = 2; t[23] = 1; x[23] = 1; y[23] = 2;$

$m[24] = 0; n[24] = 2; k[24] = 0; l[24] = 1; s[24] = 1; t[24] = 2; x[24] = 2; y[24] = 1;$

$m[25] = 1; n[25] = 1; k[25] = 2; l[25] = 2; s[25] = 1; t[25] = 0; x[25] = 2; y[25] = 0;$

$m[26] = 1; n[26] = 1; k[26] = 2; l[26] = 2; s[26] = 2; t[26] = 0; x[26] = 1; y[26] = 0;$

$m[27] = 1; n[27] = 1; k[27] = 2; l[27] = 2; s[27] = 0; t[27] = 1; x[27] = 0; y[27] = 2;$

$m[28] = 1; n[28] = 1; k[28] = 2; l[28] = 2; s[28] = 0; t[28] = 2; x[28] = 0; y[28] = 1;$

$m[29] = 1; n[29] = 1; k[29] = 2; l[29] = 2; s[29] = 2; t[29] = 1; x[29] = 1; y[29] = 2;$

$m[30] = 1; n[30] = 1; k[30] = 2; l[30] = 2; s[30] = 1; t[30] = 2; x[30] = 2; y[30] = 1;$

$m[31] = 2; n[31] = 2; k[31] = 1; l[31] = 1; s[31] = 1; t[31] = 0; x[31] = 2; y[31] = 0;$

$m[32] = 2; n[32] = 2; k[32] = 1; l[32] = 1; s[32] = 2; t[32] = 0; x[32] = 1; y[32] = 0;$

$m[33] = 2; n[33] = 2; k[33] = 1; l[33] = 1; s[33] = 0; t[33] = 1; x[33] = 0; y[33] = 2;$

$m[34] = 2; n[34] = 2; k[34] = 1; l[34] = 1; s[34] = 0; t[34] = 2; x[34] = 0; y[34] = 1;$

$$m[35]=2; n[35]=2; k[35]=1; l[35]=1; s[35]=2; t[35]=1; x[35]=1; y[35]=2;$$

$$m[36]=2; n[36]=2; k[36]=1; l[36]=1; s[36]=1; t[36]=2; x[36]=2; y[36]=1;$$

$$m[37]=2; n[37]=1; k[37]=1; l[37]=2; s[37]=1; t[37]=0; x[37]=2; y[37]=0;$$

$$m[38]=2; n[38]=1; k[38]=1; l[38]=2; s[38]=2; t[38]=0; x[38]=1; y[38]=0;$$

$$m[39]=2; n[39]=1; k[39]=1; l[39]=2; s[39]=0; t[39]=1; x[39]=0; y[39]=2;$$

$$m[40]=2; n[40]=1; k[40]=1; l[40]=2; s[40]=0; t[40]=2; x[40]=0; y[40]=1;$$

$$m[41]=2; n[41]=1; k[41]=1; l[41]=2; s[41]=1; t[41]=1; x[41]=2; y[41]=2;$$

$$m[42]=2; n[42]=1; k[42]=1; l[42]=2; s[42]=2; t[42]=2; x[42]=1; y[42]=1;$$

$$m[43]=1; n[43]=2; k[43]=2; l[43]=1; s[43]=1; t[43]=0; x[43]=2; y[43]=0;$$

$$m[44]=1; n[44]=2; k[44]=2; l[44]=1; s[44]=2; t[44]=0; x[44]=1; y[44]=0;$$

$$m[45]=1; n[45]=2; k[45]=2; l[45]=1; s[45]=0; t[45]=1; x[45]=0; y[45]=2;$$

$$m[46]=1; n[46]=2; k[46]=2; l[46]=1; s[46]=0; t[46]=2; x[46]=0; y[46]=1;$$

$$m[47]=1; n[47]=2; k[47]=2; l[47]=1; s[47]=1; t[47]=1; x[47]=2; y[47]=2;$$

$$m[48]=1; n[48]=2; k[48]=2; l[48]=1; s[48]=2; t[48]=2; x[48]=1; y[48]=1;$$

We use a "for loop" to reduce z symbolically:

$$\text{For}[i=1, i<49, i{+}{+}, \text{Print}[i]; \text{Print}[\text{Reduce}[\{zt(u^2-1)\varphi J'[1,2] == f[\varphi J'[0,1], \varphi J'[1,1]],$$
$$z(u-1)\varphi J'[2,0] == f[\varphi J'[0,1], \varphi J'[2,2]], u\neq 0, \alpha\neq 0, \beta\neq 0, \gamma\neq 0, \delta\neq 0\}, z]]]$$

C.2 Verifying the automorphism ψ

The map ψ was defined on the basis of $\mathbb{J}_3(1, z^2)$ as follows:

$$J''(1,0)\mapsto -J'(1,0), \qquad J''(2,0)\mapsto -J'(2,0),$$

$$J''(0,1)\mapsto -zJ'(0,2), \qquad J''(0,2)\mapsto -J'(0,1),$$

$$J''(1,1) \mapsto \frac{z}{1+u}J'(1,2), \qquad J''(2,2) \mapsto \frac{1}{1+u}J'(2,1)$$
$$J''(1,2) \mapsto (1+u)J'(1,1) \qquad J''(2,1) \mapsto z(1+u)J'(2,2).$$

Then

(1) $\psi([J''(1,0), J''(0,1)]) = z(1-u)J'(1,2) = [\psi(J''(1,0)), \psi(J''(0,1))]$,

(2) $\psi([J''(1,0), J''(0,2)]) = (1-u^2)J'(1,1) = [\psi(J''(1,0)), \psi(J''(0,2))]$,

(3) $\psi([J''(1,0), J''(1,1)]) = z(1-u^2)(1+u)J'(2,2) = [\psi(J''(1,0)), \psi(J''(1,1))]$,

(4) $\psi([J''(1,0), J''(2,2)]) = -(1-u)J'(0,2) = [\psi(J''(1,0)), \psi(J''(2,2))]$,

(5) $\psi([J''(1,0), J''(1,2)]) = -(1+u)(1-u^2)J'(2,1) = [\psi(J''(1,0)), \psi(J''(1,2))]$,

(6) $\psi([J''(1,0), J''(2,1)]) = -z(1-u^2)J'(0,2) = [\psi(J''(1,0)), \psi(J''(2,1))]$,

(7) $\psi([J''(2,0), J''(0,1)]) = z(1-u^2)J'(2,2) = [\psi(J''(2,0)), \psi(J''(0,1))]$,

(8) $\psi([J''(2,0), J''(0,2)]) = (1-u)J'(2,1) = [\psi(J''(2,0)), \psi(J''(0,2))]$,

(9) $\psi([J''(2,0), J''(1,1)]) = -z(1-u)J'(0,2) = [\psi(J''(2,0)), \psi(J''(1,1))]$,

(10) $\psi([J''(2,0), J''(2,2)]) = (1-u^2)(1+u)J'(1,1) = [\psi(J''(2,0)), \psi(J''(2,2))]$,

(11) $\psi([J''(2,0), J''(1,2)]) = -(1-u^2)J'(0,1) = [\psi(J''(2,0)), \psi(J''(1,2))]$,

(12) $\psi([J''(2,0), J''(2,1)]) = -z(1+u)(1-u^2)J'(1,2) = [\psi(J''(2,0)), \psi(J''(2,1))]$,

(13) $\psi([J''(0,1), J''(1,1)]) = -z^2(u-1)J'(2,0) = [\psi(J''(0,1)), \psi(J''(1,1))]$,

(14) $\psi([J''(0,1), J''(1,2)]) = -z^2(u^2-1)J'(2,0) = [\psi(J''(0,1)), \psi(J''(1,2))]$,

(15) $\psi([J''(0,1), J''(2,1)]) = -z^2(u^2-1)(1+u)J'(2,1) = [\psi(J''(0,1)), \psi(J''(2,1))]$,

(16) $\psi([J''(0,2), J''(1,1)]) = -z^2(u-1)J'(1,0) = [\psi(J''(0,2)), \psi(J''(1,1))]$,

(17) $\psi([J''(0,2),J''(2,2)]) = z(1+u)(u^2-1)J'(2,2) = [\psi(J''(0,2)),\psi(J''(2,2))]$,

(18) $\psi([J''(0,2),J''(1,2)]) = -z(1+u)(u^2-1)J'(1,2) = [\psi(J''(0,2)),\psi(J''(1,2))]$,

(19) $\psi([J''(0,2),J''(2,1)]) = -z^2(u^2-1)J'(2,0) = [\psi(J''(0,2)),\psi(J''(2,1))]$,

(20) $\psi([J''(1,1),J''(1,2)]) = z^2(u-u^2)J'(2,0) = [\psi(J''(1,1)),\psi(J''(1,2))]$,

(21) $\psi([J''(1,1),J''(2,1)]) = -z^2(u-u^2)J'(0,1) = [\psi(J''(1,1)),\psi(J''(2,1))]$,

(22) $\psi([J''(2,2),J''(1,2)]) = z(u^2-u)J'(0,2) = [\psi(J''(2,2)),\psi(J''(1,2))]$,

(23) $\psi([J''(2,2),J''(2,1)]) = -z^2(u^2-u)J'(1,0) = [\psi(J''(2,2)),\psi(J''(2,2))]$.

Bibliography

[1] G. Bini, F. Flamini, *Finite Commutative Rings and Their Applications*, Springer New York, 2002.

[2] A. Bondal, I. Zhdanovskiy, Orthogonal pairs and mutually unbiased bases, *J. Math. Sci. (N.Y.)*, **216** (2016), no. 1, 23–40.

[3] P. O. Boykin, M. Sitharam, P. H. Tiep, P. Wocjan, Mutually unbiased bases and orthogonal decompositions of Lie algebras, *Quantum Inf. Comput.*, **7** (2007) 371–382.

[4] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.

[5] J. N. Bray, D. F. Holt and C. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, LMS Lecture Notes Ser. 407, Cambridge UP, 2013.

[6] T. Durt, B. G. Englert, I. Bengtsson, K. Zyczkowski, On mutually unbiased bases, *Int. J. Quantum Inform.*, **8** (2010) 535–640.

[7] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Grad. Texts in Math., vol. 9, Springer-Verlag New York Inc., 1972.

[8] T. W. Hungerford, *Algebra*, Grad. Texts in Math, vol. 73, Springer, 1974.

[9] N. Jacobson, *Lie algebras*, Interscience Tracts on Pure and Applied Mathematics, vol. 10, John Wiley and Sons, New York, 1962.

[10] D. N. Ivanov, Homogeneous commutative orthogonal decompositions of semisimple algebras, (Russian) *Uspekhi Mat. Nauk.*, **62** (2007), no. 6 (378), 173–174; translation in *Russian Math. Surveys.*, **62** (2007), no. 6, 1204–1206.

[11] A. I. Kostrikin, I. A. Kostrikin, V. A. Ufnarovskii, Orthogonal decompositions of simple Lie algebras (type A_n), *Trudy Mat. Inst. Steklov.*, **158** (1981) 105–120.

[12] A. I. Kostrikin, I. A. Kostrikin, V. A. Ufnarovskii, On the uniqueness of orthogonal decompositions of Lie algebras of type A_n and C_n, (Russian) *Mat. Issled.*, **74** (1983) 80–105.

[13] A. I. Kostrikin, P. H. Tiep, *Orthogonal Decompositions and Integral Lattices*, Walter de Gruyter, 1994.

[14] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.

[15] M. B. Ruskai, Some connections between frames, mutually unbiased bases, and POVM's in quantum information theory, *Acta Appl. Math.*, **108** (2009), no. 3, 709–719.

[16] SageMath, the Sage Mathematics Software System (Version 8.1), The Sage Developers, 2017, http://www.sagemath.org.

[17] G. B. Seligman, *Modular Lie Algebras*, Springer-Verlag, New York, 1967.

[18] R. Steinberg, Automorphisms of classical Lie algebras, *Pac. J. Math*, **11** (1961), 1119 – 1129.

[19] J. G. Thompson, A conjugacy theorem for E_8, *J. Algebra*, **38** (1976), no. 2, 525–530.

[20] A. Torstensson, On the existence of orthogonal decompositions of the simple Lie algebra of type C_3, *Comput. Sci. J. Moldova*, **8** (2000), no. 1(22), 16–41.

[21] Z. Wan, *Geometry of Classical Groups over Finite Fields*, 2nd Edition, Science Press, Beijing/New York, 2002.

[22] Wolfram Research, Inc., Mathematica, Version 7.0, Champaign, IL (2008).

Curriculum Vitae

EDUCATION

- 2015-2018 PhD in Mathematics, University of Wisconsin-Milwaukee, USA

  Dissertation Title: Orthogonal abelian Cartan subalgebra decomposition of classical Lie algebrs over finite commutative rings

  Advisor: Professor Yi Ming Zou

- 2013-2015 MS in Mathematics, Chulalongkorn University, Thailand

  Thesis Title: Orthogonal graphs over finite commutative rings of odd characteristic

  Advisor: Professor Yotsanan Meemark

- 2009-2013 BA in Mathematics, Chulalongkorn University, Thailand

  Senior Project: Perfect state transfer in unitary Cayley graphs over local rings

  Advisor: Professor Yotsanan Meemark

PUBLICATIONS

- **Papers in peer reviewed journals**

  1. Sriwongsa S. and Zou Y. M., Orthogonal abelian Cartan subalgebra decomposition of $\mathfrak{sl}_n$ over a finite commutative ring, *Linear Multilinear Algebra.* 2018, to appear
  2. Meemark Y. and Sriwongsa S., Antiderivatives and linear differential equations using matrix, *Involve, a Journal of Mathematics.* 2017, to appear
  3. Sriwongsa S., Congruence of symmetric inner products over finite commutative rings of odd characteristic, *Bull. Aust. Math. Soc.*, **96** (2017), 389–397
  4. Meemark Y. and Sriwongsa S., Orthogonal graphs over finite commutative rings of odd characteristic, *Finite Fields Appl.*, **40** (2016), 26–45

5. Meemark Y. and Sriwongsa S., Perfect state transfer in unitary Cayley graphs over local rings, *Trans. Comb.* **3** (2014) no.4, 43–54

- **Papers submitted to journals**

1. Sriwongsa S., Orthogonal decompositions of classical Lie algebras over finite commutative rings
2. Sriwongsa S., A note on symplectic graphs over finite commutative rings
3. Sriwongsa S., Orthogonal graphs modulo power of 2

EMPLOYMENT

- Graduate Teaching Assistant, Department of Mathematical sciences, University of Wisconsin-Milwaukee, USA (2015-2018)
- Summer Maths tutor, Nakprasith high school, Thailand (2009-present)

SELECTED TALKS

- *Orthogonal classical Cartan subalgebra decomposition of* $\mathfrak{sl}_n$ *over a finite commutative ring*, AMS Spring Western Sectional Meeting, Portland State University, USA (2018)
- *Orthogonal graphs modulo power of* 2, Graduate Student Combinatorics Conference (GSCC), University of Texas at Dallas, USA (2018)
- *Congruence of symmetric inner products over finite commutative rings of odd characteristic*, MAA WI section meeting, University of Wisconsin-Milwaukee, USA (2017)
- *Orthogonal graphs over finite commutative rings of odd characteristic*, The 12th international conference on Finite Fields and Their Applications, Skidmore College, New York, USA (2015)
- *Cogredient standard forms of orthogonal matrices over finite local rings of odd characteristic*, Annual pure and applied Mathematics conference, Chulalongkorn University, Thailand (2015)

- *Perfect state transfer in unitary Cayley graphs over local rings*, The 8th Conference on Science and Technology for Youths, Thailand (2013)

TEACHING EXPERIENCE

- Calculus and Analytic Geometry I: Instructor (Spring 2018) at University of Wisconsin-Milwaukee, USA
- Intermediate Algebra: Instructor (Fall 2017) at University of Wisconsin-Milwaukee, USA
- Survey in Calculus and Analytic Geometry: Discussion Leader (Fall 2016 - Spring 2017) at University of Wisconsin-Milwaukee, USA
- Foundations of Elementary Mathematics: Discussion Leader (Spring 2016) at University of Wisconsin-Milwaukee, USA
- Mathematical Literacy for College Students II: Discussion Leader (Fall 2015) at University of Wisconsin-Milwaukee, USA

HONORS AND AWARDS

- Summer Research Excellence Award, Department of Mathematical Sciences, University of Wisconsin-Milwaukee, USA (Summer 2017)
- Morris and Miriam Marden Award in Mathematics (High quality paper in Math), Department of Mathematical Sciences, University of Wisconsin-Milwaukee, USA (2017)
- Chancellor's award and Excellent Research award, Department of Mathematical Sciences, University of Wisconsin-Milwaukee, USA (2015-2018)
- Excellent outstanding academic performance (GPA 4.00), Professor Tab Neelaneti, Ph.D., Chulalongkorn University, Thailand (2015)

- The 2nd place from Mathematics competition, MCSC Math Science Day, Bethany College, USA (2008)
- The 2nd place from Physics competition, Physics Olympics, Youngtown State University, USA (2008)

RESEARCH INTERESTS

Algebraic graph theory, Commutative ring theory, Lie algebra and Lie superalgebra and their representation theories, as well as the applications of these theories.