Orthogonal decomposition for a modular Lie algebra $\mathfrak{sl}_n$

Songpon Sriwongsa

King Mongkut's University of Technology Thonburi

Conference on Recent Trends in Algebra and Related Topics 2023

January 19th, 2023

Outline

Orthogonal decomposition problem of Lie algebras over $\mathbb{C}$ has many applications and relations to other areas of Mathematics and Sciences.

- We define a suitable type of orthogonal decomposition of a modular Lie algebra and construct it for Lie algebra $\mathfrak{sl}_n$ under some sufficient conditions.
- A necessary condition is also discussed of this type of Lie algebra.
- We analyze the problem over finite fields by using some important facts of modular Lie algebras over fields of positive characteristic.

References I

A. Bondal, I. Zhdanovskiy, Orthogonal pairs for Lie algebra $sl(6)$, Preprint of IPMU, (2014) IPMU14-0296

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

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.

D. L. Donoho, X. Huo, Uncertainty principles and ideal atomic decomposition, *IEEE Trans. on Information Theory.*, 47 No. 7 (2001) 2845–2862.

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.

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, *Mat. Issled.*, 74 (1983) 80–105.

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

References II

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

S. Sriwongsa and Y. M. Zou, Orthogonal Cartan subalgebra decomposition of sln over a finite commutative ring, *Linear Multilinear Algebra* 67 (2020) 817829.

J. Thompson, A conjugacy theorem for E_8, *J. Algebra*, 38 No. 2 (1976) 525–530.

Modular Lie algebras

Let R be a commutative ring with 1. A **Lie algebra** over R is an R-module L equipped with a bilinear form $[\cdot, \cdot]$ (called Lie bracket) satisfying

1. $[x, x] = 0$ for all $x \in L$.
2. $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$.

Modular Lie algebras

Let R be a commutative ring with 1. A **Lie algebra** over R is an R-module L equipped with a bilinear form $[\cdot,\cdot]$ (called Lie bracket) satisfying

1. $[x,x] = 0$ for all $x \in L$.
2. $[[x,y],z] + [[y,z],x] + [[z,x],y] = 0$.

Example

$M_n(R) = \{\text{all } n \times n \text{ matrices over } R\}$ is a Lie algebra with $[x,y] = xy - yx$.

Modular Lie algebras

Define $[L, L] := \{\sum[x_i, y_i] : x_i, y_i \in L\}$.

Modular Lie algebras

Define $[L, L] := \{\sum [x_i, y_i] : x_i, y_i \in L\}$.

Define $L^0 = L, L^1 = [L, L], L^2 = [L, L^1], \dots, L^i = [L, L^{i-1}]$.

Modular Lie algebras

Define $[L, L] := \{\sum [x_i, y_i] : x_i, y_i \in L\}$.

Define $L^0 = L, L^1 = [L, L], L^2 = [L, L^1], \ldots, L^i = [L, L^{i-1}]$.

L is called **nilpotent** if $L^n = 0$ for some n.

Modular Lie algebras

Define $[L, L] := \{\sum [x_i, y_i] : x_i, y_i \in L\}$.

Define $L^0 = L, L^1 = [L, L], L^2 = [L, L^1], \ldots, L^i = [L, L^{i-1}]$.

L is called **nilpotent** if $L^n = 0$ for some n.

Let H be a subalgebra of L. The set $N_L(H) := \{x \in L : [x, H] \subset H\}$ is called the **normalizer** of H in L.

Modular Lie algebras

Define $[L, L] := \{\sum[x_i, y_i] : x_i, y_i \in L\}$.

Define $L^0 = L, L^1 = [L, L], L^2 = [L, L^1], \dots, L^i = [L, L^{i-1}]$.

L is called **nilpotent** if $L^n = 0$ for some n.

Let H be a subalgebra of L. The set $N_L(H) := \{x \in L : [x, H] \subset H\}$ is called the **normalizer** of H in L.

Modular Lie algebras

Definition

A subalgebra H of L is a *Cartan subalgebra* if it is a nilpotent subalgebra which is its own normalizer.

Modular Lie algebras

Definition

A subalgebra H of L is a *Cartan subalgebra* if it is a nilpotent subalgebra which is its own normalizer.

Definition

The Killing form $K(A, B) := \mathrm{Tr}(adA \cdot adB)$ for $A, B \in L$ where $adA : X \mapsto [A, X]$.

$\mathrm{Tr}(\cdot)$ is the trace of the matrix.

Special Linear Lie algebras: $\mathfrak{sl}_n(R) = \{X \in M_n(R) : \mathrm{Tr}(X) = 0\}$.

Modular Lie algebras

Special Linear Lie algebras: $\mathfrak{sl}_n(R) = \{X \in M_n(R) : \mathrm{Tr}(X) = 0\}$.

Type A: $K(A, B) = 2n\,\mathrm{Tr}(AB)$ for $A, B \in \mathfrak{sl}_n(R)$.

Definition of OD

Definition

Let $\mathfrak{L}$ be a Lie algebra over $\mathbb{C}$. An *orthogonal decomposition* (OD) of $\mathfrak{L}$ is the decomposition (as a vector space) of $\mathfrak{L}$ into a direct sum of Cartan subalgebras which are pairwise orthogonal with respect to the Killing form.

History I

- In 1976, J.G.Thompson used OD of E_8 for the construction of a special finite simple group.

Figure : J. G. Thompson

History II

- In 1981, Kostrikin and his collaborators developed the theory of such decompositions of simple Lie algebras of types A, B, C, D over $\mathbb{C}$.

Figure : Aleksei Ivanovich Kostrikin (1929-2000)

Related topic to OD

- The OD problem for $\mathfrak{sl}_n(\mathbb{C})$ has applications in Quantum information theory, e.g., mutually unbiased bases.

Related topic to OD

- The OD problem for $\mathfrak{sl}_n(\mathbb{C})$ has applications in Quantum information theory, e.g., mutually unbiased bases.
- MUBs have applications in physics and engineering, such as in quantum information and signal processing. The construction of mutually unbiased bases has a strong combinatorial and algebraic flavor.

MUBs

Let Φ_1 and Φ_2 be two orthonormal bases in $\mathbb{R}^n$ (or $\mathbb{C}^n$).

MUBs

Let Φ_1 and Φ_2 be two orthonormal bases in $\mathbb{R}^n$ (or $\mathbb{C}^n$).
Let

$$M = M(\Phi_1, \Phi_2) := \sup\{| < \Phi_1, \Phi_2 > | : \phi_i \in \Phi_i, i = 1, 2\},$$

MUBs

Let Φ_1 and Φ_2 be two orthonormal bases in $\mathbb{R}^n$ (or $\mathbb{C}^n$).
Let

$$M = M(\Phi_1, \Phi_2) := \sup\{| < \Phi_1, \Phi_2 > | : \phi_i \in \Phi_i, i = 1, 2\},$$

and let $A = (\Phi_1, \Phi_2)$ be the $n \times (2n)$ matrix with the columns given by the Φ_i.

MUBs

Let Φ_1 and Φ_2 be two orthonormal bases in $\mathbb{R}^n$ (or $\mathbb{C}^n$).
Let

$$M = M(\Phi_1, \Phi_2) := \sup\{| < \Phi_1, \Phi_2 > | : \phi_i \in \Phi_i, i = 1, 2\},$$

and let $A = (\Phi_1, \Phi_2)$ be the $n \times (2n)$ matrix with the columns given by the Φ_i.

Consider the system of linear equations

$$AX = B, X = (x_1, \ldots, x_{2n})^t, B = (b_1, \ldots, b_n)^t.$$

MUBs

Let Φ_1 and Φ_2 be two orthonormal bases in $\mathbb{R}^n$ (or $\mathbb{C}^n$).
Let

$$M = M(\Phi_1, \Phi_2) := \sup\{| < \Phi_1, \Phi_2 > | : \phi_i \in \Phi_i, i = 1, 2\},$$

and let $A = (\Phi_1, \Phi_2)$ be the $n \times (2n)$ matrix with the columns given by the Φ_i.

Consider the system of linear equations

$$AX = B, X = (x_1, \ldots, x_{2n})^t, B = (b_1, \ldots, b_n)^t.$$

Since $\mathrm{rank}(A) = \mathrm{rank}(A|B)$, the system has infinitely many solutions.

MUBs

Example

The system of equations:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The general solutions of this system is

$$\begin{aligned} x_1 &= 1 - x_3 - x_4, \\ x_2 &= -x_3 + x_4, \end{aligned}$$

where x_3 and x_4 are free variables.

MUBs

Example

The system of equations:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The general solutions of this system is

$$x_1 = 1 - x_3 - x_4,$$
$$x_2 = -x_3 + x_4,$$

where x_3 and x_4 are free variables.

Remark: if we impose (ex of condition) the condition $||X||_0 =$ number of nonzero $x_i = 1$, then the solution is unique.

MUBs

Theorem

(Donoho and Huo, 2001) Suppose that $\alpha \in \mathbb{R}^{2n}$ *satisfies*

$$A\alpha = B, \text{ and } ||\alpha||_0 < \frac{1}{2}(1 + M^{-1}),$$

where $B \in \mathbb{R}^n$*. Then* α *is the unique solution of the* ℓ_1*-optimization problem*

$$\min ||\alpha||_1 \text{ such that } A\alpha = B.$$

($||X||_1 = \sum |x_i|$*).*

MUBs

Theorem

(Donoho and Huo, 2001) Suppose that $\alpha \in \mathbb{R}^{2n}$ *satisfies*

$$A\alpha = B, \text{ and } ||\alpha||_0 < \frac{1}{2}(1 + M^{-1}),$$

where $B \in \mathbb{R}^n$*. Then* α *is the unique solution of the* ℓ_1*-optimization problem*

$$\min ||\alpha||_1 \text{ such that } A\alpha = B.$$

$(||X||_1 = \sum |x_i|)$.

Note that the smaller the $M = M(\Phi_1, \Phi_2)$, the wider range of vectors α we can recover. How small can M be?

MUBs

It can be proved that $M = M(\Phi_1, \Phi_2) \geq \frac{1}{\sqrt{n}}$.

Definition

Two orthonormal bases Φ_1 and Φ_2 are *mutually unbiased* if $M = M(\Phi_1, \Phi_2) = \frac{1}{\sqrt{n}}$.

OD of $\mathfrak{sl}_n(\mathbb{C})$ and MUBs

The $*$-operation on $\mathfrak{sl}_n(\mathbb{C})$ is defined by $A* = \bar{A}^t$. The following theorem is due to Boykin et al. (2007)

Theorem

- *Any collection of k MUB in $\mathbb{C}^n$ gives rise to k orthogonal Cartan subalgebras of $\mathfrak{sl}_n(\mathbb{C})$ with respect to the Killing form. Thus, if there exists a collection of $n+1$ MUB in $\mathbb{C}^n$, then there is an OD in $\mathfrak{sl}_n(\mathbb{C})$.*
- *Conversely, any OD of $\mathfrak{sl}_n(\mathbb{C})$ into a direct sum of Cartan subalgebras which are stable with respect to the $*$-operation gives rise to a collection of $n+1$ MUB in $\mathfrak{sl}_n(\mathbb{C})$.*

OD of $\mathfrak{sl}_n(\mathbb{C})$

- The following theorem is due to Kostrikin et al. (1981).

Theorem

For $n = p^m$, where p is a prime integer and m is a positive integer, $\mathfrak{sl}_n(\mathbb{C})$ has an OD

$$\mathfrak{sl}_n(\mathbb{C}) = H_0 \oplus H_1 \oplus \cdots \oplus H_n$$

where H_i's are all Cartan subalgebras.

Winnie-the-Pooh conjecture

Conjecture (Winnie-the-Pooh conjecture)

$\mathfrak{sl}_n(\mathbb{C})$ *has an OD if and only if n is a prime power integer.*

Winnie-the-Pooh conjecture

Conjecture (Winnie-the-Pooh conjecture)

$\mathfrak{sl}_n(\mathbb{C})$ *has an OD if and only if* n *is a prime power integer.*

The name is due to a play on words found in Zahoder's translation of Milne's famous childrens book Winnie-the-Pooh into Russian. Zahoder's play on words can be interpreted as the sequence of Cartan types A_5-corresponding to the smallest open case $\mathfrak{sl}_6$-then A_6, A_7 and A_8.

Conjecture (Winnie-the-Pooh conjecture)

$\mathfrak{sl}_n(\mathbb{C})$ *has an OD if and only if* n *is a prime power integer.*

The name is due to a play on words found in Zahoder's translation of Milne's famous childrens book Winnie-the-Pooh into Russian. Zahoder's play on words can be interpreted as the sequence of Cartan types A_5-corresponding to the smallest open case $\mathfrak{sl}_6$-then A_6, A_7 and A_8.

- The only if part is still open, even $n = 6$.

Winnie-the-Pooh conjecture

Conjecture (Winnie-the-Pooh conjecture)

$\mathfrak{sl}_n(\mathbb{C})$ has an OD if and only if n is a prime power integer.

The name is due to a play on words found in Zahoder's translation of Milne's famous childrens book Winnie-the-Pooh into Russian. Zahoder's play on words can be interpreted as the sequence of Cartan types A_5-corresponding to the smallest open case $\mathfrak{sl}_6$-then A_6, A_7 and A_8.

- The only if part is still open, even $n = 6$.
- For $n = 6$, Bondal et. al. proved the existence of four collection of pairwise orthogonal Cartan subalgebras of $\mathfrak{sl}_6(\mathbb{C})$ [1, 2].

OD over finite commutative rings

Goal: To generalize OD problem to ring cases.

OD over finite commutative rings

Goal: To generalize OD problem to ring cases.

Let $\mathfrak{L}$ be a Lie algebra over a field of prime characteristic.

OD over finite commutative rings

- Unlike Lie algebras over $\mathbb{C}$, not all Cartan subalgebras of $\mathfrak{L}$ are abelian.

OD over finite commutative rings

- Unlike Lie algebras over $\mathbb{C}$, not all Cartan subalgebras of $\mathfrak{L}$ are abelian.
- We consider the orthogonal decomposition of $\mathfrak{L}$ into abelian Cartan subalgebras (abbreviated ODAC). An ODAC of $\mathfrak{L}$ is

$$\mathfrak{L} = H_0 \oplus H_1 \oplus \ldots \oplus H_k$$

where the H_i's are pairwise orthogonal abelian Cartan subalgebra of $\mathfrak{L}$.

Classical Lie algebra over finite fields

Let $\mathbb{F}$ be a field with characteristic $\neq 2, 3$.

Classical Lie algebra over finite fields

Let $\mathbb{F}$ be a field with characteristic $\neq 2, 3$.
A Lie algebra $\mathfrak{L}$ over $\mathbb{F}$ is called *classical* if :

(i) the center of $\mathfrak{L}$ is zero;

(ii) $[\mathfrak{L}, \mathfrak{L}] = \mathfrak{L}$;

(iii) $\mathfrak{L}$ has an abelian Cartan subalgebra H, relative to which:

  (a) $\mathfrak{L} = \oplus \mathfrak{L}_\alpha$, where $[x, h] = \alpha(h)x$ for all $x \in \mathfrak{L}_\alpha, h \in H$;
  (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 $1 \leq k \leq p - 1$.

We call this H a **classical** Cartan subalgebra.

COD

- Let's consider an OD whose components are classical Cartan subalgebras. We call a **classical OD** and denote by (COD).

COD

- Let's consider an OD whose components are classical Cartan subalgebras. We call a **classical OD** and denote by (COD).
- All classical Cartan subalgebras are conjugate.

COD

Example

If $2 \nmid \mathrm{char}(\mathbb{F})$ and -1 is a square in $\mathbb{F}$, then $\mathfrak{sl}_2(\mathbb{F})$ is the Lie algebra with a COD

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

COD

- In general cases of $\mathfrak{sl}_n(\mathbb{F})$, we would like to find sufficient conditions to construct a COD.

Main Theorem

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a field of positive characteristic and let $n = p^m$ be a prime power. Assume that $\mathrm{char}(\mathbb{F}) \neq 2, 3$ and p. If

1. *$p = 2$ and -1 is a square in $\mathbb{F}$ or*
2. *$p > 2$ and $\mathbb{F}$ contains a primitive pth root of unity,*

then $\mathfrak{sl}_n(\mathbb{F})$ has a COD.

Main Theorem

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a field of positive characteristic and let $n = p^m$ be a prime power. Assume that $\mathrm{char}(\mathbb{F}) \neq 2, 3$ and p. If

1. *$p = 2$ and -1 is a square in $\mathbb{F}$ or*
2. *$p > 2$ and $\mathbb{F}$ contains a primitive pth root of unity,*

then $\mathfrak{sl}_n(\mathbb{F})$ has a COD.

Note that the sufficient conditions 1 and 2 provide the existence of a primitive pth root of unity $u \in \mathbb{F}$.

Main Theorem

Corollary

Let $\mathbb{F}$ be an algebraically closed field of positive characteristic and let $n = p^m$ be a prime power. If $\mathrm{char}(\mathbb{F}) \neq 2, 3$ and p, then $\mathfrak{sl}_n(\mathbb{F})$ has a COD.

Main Theorem

For the finite field $\mathbb{F}_q$, it is known that -1 is a square if and only if $q \equiv 1 \pmod 4$ and, by Cauchy theorem of a finite group, $\mathbb{F}_q$ has a primitive pth root of unity if and only if $p \mid (q-1)$. Thus, we have:

Main Theorem

For the finite field $\mathbb{F}_q$, it is known that -1 is a square if and only if $q \equiv 1 \pmod 4$ and, by Cauchy theorem of a finite group, $\mathbb{F}_q$ has a primitive pth root of unity if and only if $p \mid (q-1)$. Thus, we have:

Corollary

Let $\mathbb{F}_q$ be the finite field of q elements and let $n = p^m$ be a prime power. Assume that $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$ and p. If

1. $p = 2$ *and* $q \equiv 1 \pmod 4$, *or*
2. $p > 2$ *and* $p \mid (q-1)$,

then $\mathfrak{sl}_n(\mathbb{F}_q)$ has a COD.

When $n = 2, 3$

The following discussion is about the characterization of fields for COD of $\mathfrak{sl}_n$, $n = 2, 3$.

When $n = 2, 3$

The following discussion is about the characterization of fields for COD of $\mathfrak{sl}_n, n = 2, 3$.

Let H_0 be the classical Cartan subalgebra of $\mathfrak{sl}_n(\mathbb{F})$ consisting of the diagonal matrices.

When $n = 2, 3$

Lemma

Every classical Cartan subalgebra orthogonal to H_0 has a basis of the form indicated below.

(1) *If $n = 2$, then*

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

for some $a \in \mathbb{F} \setminus \{0\}$.

(2) *If $n = 3$, then*

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

for some $a, b \in \mathbb{F} \setminus \{0\}$.

When $n = 2, 3$

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a any field such that $\mathrm{char}(\mathbb{F}) > 3$. Then $\mathfrak{sl}_2(\mathbb{F})$ has a unique (up to conjugacy) COD if and only if $\mathbb{F}$ contains a primitive fourth root of unity.

When $n = 2, 3$

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a any field such that $\mathrm{char}(\mathbb{F}) > 3$. Then $\mathfrak{sl}_2(\mathbb{F})$ has a unique (up to conjugacy) COD if and only if $\mathbb{F}$ contains a primitive fourth root of unity.

Corollary

Let $\mathbb{F}_q$ be the finite field of $q = p^m$ elements with $p > 3$. Then $\mathfrak{sl}_2(\mathbb{F}_q)$ has a unique (up to conjugacy) COD if and only if $q \equiv 1 \pmod 4$.

When $n = 2, 3$

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a any field such that $\mathrm{char}(\mathbb{F}) > 3$. Then $\mathfrak{sl}_2(\mathbb{F})$ has a unique (up to conjugacy) COD if and only if $\mathbb{F}$ contains a primitive fourth root of unity.

Corollary

Let $\mathbb{F}_q$ be the finite field of $q = p^m$ elements with $p > 3$. Then $\mathfrak{sl}_2(\mathbb{F}_q)$ has a unique (up to conjugacy) COD if and only if $q \equiv 1 \pmod 4$.

Remark: If $q \equiv 3 \pmod 4$, then $\mathfrak{sl}_2(\mathbb{F}_q)$ has only two classical orthogonal components which are $\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle_{\mathbb{F}_q}$ and $\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle_{\mathbb{F}_q}$.

When $n = 2, 3$

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a field such that $\mathrm{char}(\mathbb{F}) > 3$. Then $\mathfrak{sl}_3(\mathbb{F})$ has a COD if and only if $\mathbb{F}$ contains a primitive cube root of unity.

When $n = 2, 3$

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a field such that $\mathrm{char}(\mathbb{F}) > 3$. Then $\mathfrak{sl}_3(\mathbb{F})$ has a COD if and only if $\mathbb{F}$ contains a primitive cube root of unity.

Corollary

Let $\mathbb{F}_q$ be the finite field of $q = p^m$ elements with $p > 3$. Then $\mathfrak{sl}_3(\mathbb{F}_q)$ has a COD if and only if $3 \mid (q - 1)$.

When $n = 2, 3$

Theorem (Meemark, S. 2022?)

Let $\mathbb{F}$ be a field such that $\mathrm{char}(\mathbb{F}) > 3$. Then $\mathfrak{sl}_3(\mathbb{F})$ has a COD if and only if $\mathbb{F}$ contains a primitive cube root of unity.

Corollary

Let $\mathbb{F}_q$ be the finite field of $q = p^m$ elements with $p > 3$. Then $\mathfrak{sl}_3(\mathbb{F}_q)$ has a COD if and only if $3 \mid (q-1)$.

Remark: If $3 \nmid (q-1)$, then lack of primitive cube root of unity implies that $\mathfrak{sl}_3(\mathbb{F}_q)$ does not have an orthogonal pair of classical Cartan subalgebras.

A finite commutative ring case

ODAC of $\mathfrak{sl}_n(R)$

- 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 prescribed in the previous page is of the form $D^a P^b$ for some $a, b \in \{0, 1, 2\}$.

ODAC of $\mathfrak{sl}_n(R)$

- 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 prescribed in the previous page is of the form $D^a P^b$ for some $a, b \in \{0, 1, 2\}$.
- 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.

ODAC of $\mathfrak{sl}_n(R)$

Theorem (S. and Yi Ming Zou 2020)

Let R be a finite commutative ring with 1. 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.

Local rings case

- If R is local,i.e. it is has the unique maximal ideal, then we have a sufficient condition for $\mathfrak{sl}_n(R)$ to satisfy the hypothesis of Main theorem. Then $\mathfrak{sl}_n(R)$ admits an ODAC in the next theorem.

Local rings case

- If R is local,i.e. it is has the unique maximal ideal, then we have a sufficient condition for $\mathfrak{sl}_n(R)$ to satisfy the hypothesis of Main theorem. Then $\mathfrak{sl}_n(R)$ admits an ODAC in the next theorem.

Theorem (S. and Yi Ming Zou 2020)

Let R be a finite local ring with the 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.

Local rings case

- If R is local,i.e. it is has the unique maximal ideal, then we have a sufficient condition for $\mathfrak{sl}_n(R)$ to satisfy the hypothesis of Main theorem. Then $\mathfrak{sl}_n(R)$ admits an ODAC in the next theorem.

Theorem (S. and Yi Ming Zou 2020)

Let R be a finite local ring with the 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.

- The proof use the fact that $R^\times \cong (1 + M) \times k^\times$ and that every element of M is nilpotent.

Finite fields case

- Since a finite field $\mathbb{F}_q$ is a finite local ring, we have an immediate corollary.

Corollary (S. and Yi Ming Zou 2020)

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

General case

- A finite commutative ring R with identity can be decomposed into a finite direct product of finite local rings.

Theorem (S. and Yi Ming Zou 2020)

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.*

General case

- A finite commutative ring R with identity can be decomposed into a finite direct product of finite local rings.

Theorem (S. and Yi Ming Zou 2020)

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.

- The proof use the fact $R^\times \cong R_1^\times \times R_2^\times \times \ldots \times R_t^\times$.

Thank you