MATHEMATICAL ENGINEERING
TECHNICAL REPORTS

On the Number of Matrices to Generate a Matrix $*$-Algebra over the Real Field

Daishi AIURA, Naonori KAKIMURA, and
Kazuo MUROTA

METR 2012–06 March 2012

DEPARTMENT OF MATHEMATICAL INFORMATICS
GRADUATE SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY
THE UNIVERSITY OF TOKYO
BUNKYO-KU, TOKYO 113-8656, JAPAN

WWW page: http://www.keisu.t.u-tokyo.ac.jp/research/techrep/index.html

On the Number of Matrices to Generate a Matrix $*$-Algebra over the Real Field

Daishi AIURA[*] Naonori KAKIMURA[*] Kazuo MUROTA[*]

March 2012

Abstract

In this paper, we discuss generating a matrix $*$-algebra over the real field with a set of symmetric matrices. This is motivated by an application in structural engineering. We show that any matrix $*$-algebra can be generated with at most four randomly-chosen symmetric matrices. The proof relies on the structure theorem for matrix $*$-algebras and the notion of genericity in eigenvalue structure.

1 Introduction

Let $\mathcal{M}_n$ be the set of matrices of order n over the real field. We say that $\mathcal{T} \subseteq \mathcal{M}_n$ is a *matrix $*$-algebra* if it contains the identity matrix and it is closed under linear combination, multiplication, and transposition. Matrix $*$-algebras have been studied extensively in engineering fields such as semidefinite programming [2, 4, 12, 15], signal processing [13], and structural engineering [1]. In these applications, we can reduce the computational effort by exploiting the Artin-Wedderburn type structure theorem for matrix $*$-algebras: A matrix $*$-algebra can be decomposed uniquely into irreducible components with a single orthogonal matrix. Recently, a numerical algorithm for finding such decomposition was proposed by Murota, Kanno, Kojima, and Kojima [15] and Maehara and Murota [12]. A variant of this algorithm was designed by de Klerk, Dobre, and Pasechnik [4]. Maehara and Murota [14] further developed a simpler decomposition algorithm, which allows us to control numerical errors.

In this paper, we consider a situation that we do not know an explicit representation of a matrix $*$-algebra $\mathcal{T}$, but instead, we can obtain a symmetric matrix from $\mathcal{T}$ randomly. In this setting, we discuss how many symmetric matrices in $\mathcal{T}$ are required to generate $\mathcal{T}$. Here, a set of matrices *generates* $\mathcal{T}$ if the minimum matrix $*$-algebra containing these matrices coincides with $\mathcal{T}$. It should be emphasized that $\mathcal{T}$ is a subalgebra over the real field, which is not algebraically closed, and that generators are restricted to be symmetric. This is in contrast to other related problems, e.g., generating simple groups [6], Lie algebras [3, 9], and matrix algebras over algebraically closed fields [11].

This problem is motivated by an application in structural engineering. When we investigate the deformation of structures, we repeatedly solve a system of governing nonlinear equations, say, for different loadings. It is noteworthy that the Jacobian matrix is always a symmetric matrix, which is a consequence of reciprocity of structural systems. Sometimes, structures are endowed with (geometric) symmetry. In such a case we can make use of the symmetry in various ways to enhance the computational efficiency of the numerical analysis. For example, the symmetry implies that all the Jacobian matrices at symmetric deformations are contained

[*] Department of Mathematical Informatics, Graduate School of Information Science and Technology, University of Tokyo, Tokyo 113-8656, Japan. {daishi_aiura, kakimura, murota}@mist.i.u-tokyo.ac.jp

in some nontrivial matrix $*$-algebra $\mathcal{T}$. This means that the Jacobian matrices can be block-diagonalized simultaneously with a single orthogonal matrix P. If $\mathcal{T}$ is explicitly given in advance, e.g., represented by group symmetry, then we can compute P with the aid of group representation theory [7, 8]. It should be noted, however, that we often do not know an explicit representation of $\mathcal{T}$, for example, when we deal with large complex structures. In such a situation, it is natural to pick several Jacobian matrices randomly, and to substitute for P an orthogonal matrix $\hat{P}$ that diagonalizes the matrix $*$-subalgebra $\hat{\mathcal{T}}$ generated by these Jacobian matrices. In fact, this idea was recently introduced in [1] to develop a numerical algorithm for computing the deformation of symmetric structures. A motivation of this paper is to analyze this approach theoretically, that is, to estimate the number of Jacobian matrices, which are symmetric, necessary to generate $\mathcal{T}$. This is indeed the problem which this paper deals with.

In this paper, we show that any matrix $*$-algebra over the real field can be generated with at most four randomly-chosen symmetric matrices (Theorem 3.1). This is optimal in the sense that some matrix $*$-algebra cannot be generated with any three symmetric matrices. The proof relies on the structure theorem for matrix $*$-algebras. Since a matrix $*$-algebra can be decomposed into irreducible components, it suffices to discuss irreducible cases. By providing the explicit minimum number of matrices that are necessary to generate each irreducible case, we obtain Theorem 3.1 for general matrix $*$-algebras. We remark that large complex structures with group symmetry, such as dihedral or tetrahedral symmetry, yield matrix $*$-algebras with special irreducible components, which can be generated with only two symmetric matrices.

This paper is organized as follows. Section 2 provides some notation and basic results in the theory of matrix $*$-algebras. Section 3 is devoted to the proof of our main results. Finally, concluding remarks are presented in Section 4.

2 Matrix $*$-algebras

2.1 Structure theorem

Throughout this paper, we denote by $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$ the real field, the complex field, and the quaternion field, respectively. Let $\mathcal{M}_n$ be the set of matrices of order n over the real field $\mathbb{R}$, and $\mathcal{S}_n$ be the set of symmetric matrices in $\mathcal{M}_n$. We say that $\mathcal{T} \subseteq \mathcal{M}_n$ is a *matrix $*$-algebra* if it satisfies (i) $I_n \in \mathcal{T}$, and (ii) $A, B \in \mathcal{T}; \alpha, \beta \in \mathbb{R} \Rightarrow \alpha A + \beta B, AB, A^\top \in \mathcal{T}$, where I_n is the identity matrix of order n. The value n is called the *order of $\mathcal{T}$*. Obviously, $\mathcal{M}_n$ itself is a matrix $*$-algebra. There are two other basic matrix $*$-algebras: the real representation of complex matrices $\mathcal{C}_n \subset \mathcal{M}_{2n}$ and the real representation[1] of quaternion matrices $\mathcal{H}_n \subset \mathcal{M}_{4n}$, which are respectively defined by

$$\mathcal{C}_n = \left\{ C(Z) := \begin{pmatrix} C(z_{11}) & \cdots & C(z_{1n}) \\ \vdots & \ddots & \vdots \\ C(z_{n1}) & \cdots & C(z_{nn}) \end{pmatrix} \middle| \; Z = (z_{ij}) \in \mathbb{C}^{n \times n} \right\} \text{ and}$$

$$\mathcal{H}_n = \left\{ H(Y) := \begin{pmatrix} H(h_{11}) & \cdots & H(h_{1n}) \\ \vdots & \ddots & \vdots \\ H(h_{n1}) & \cdots & H(h_{nn}) \end{pmatrix} \middle| \; Y = (h_{ij}) \in \mathbb{H}^{n \times n} \right\}$$

[1] Our definition of $\mathcal{H}_n$ is slightly different in signs of the entries from those in [12, 15], but these two are equivalent.

with

$$C(a+ib) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \text{ and } H(a+ib+jc+kd) = \begin{pmatrix} a & -b & -c & d \\ b & a & -d & -c \\ c & d & a & b \\ -d & c & -b & a \end{pmatrix},$$

where $a+ib \in \mathbb{C}$ and $a+ib+jc+kd \in \mathbb{H}$.

For two matrix $*$-algebras $\mathcal{T}_1$ and $\mathcal{T}_2$, their *direct sum*, denoted by $\mathcal{T}_1 \oplus \mathcal{T}_2$, is defined as

$$\mathcal{T}_1 \oplus \mathcal{T}_2 = \{A \oplus B \mid A \in \mathcal{T}_1, B \in \mathcal{T}_2\},$$

where

$$A \oplus B = \begin{pmatrix} A & O \\ O & B \end{pmatrix},$$

and their *tensor product*, denoted by $\mathcal{T}_1 \otimes \mathcal{T}_2$, is

$$\mathcal{T}_1 \otimes \mathcal{T}_2 = \left\{ \sum_{i=1}^{t} (A_i \otimes B_i) \;\middle|\; t \in \mathbb{N}, A_i \in \mathcal{T}_1, B_i \in \mathcal{T}_2 \, (i = 1, \ldots, t) \right\},$$

where

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix}.$$

Note that both $\mathcal{T}_1 \oplus \mathcal{T}_2$ and $\mathcal{T}_1 \otimes \mathcal{T}_2$ are matrix $*$-algebras. For notational convenience, we sometimes identify the identity matrix I_n with the matrix $*$-algebra $\{aI_n \mid a \in \mathbb{R}\}$. For example, we denote

$$I_n \otimes \mathcal{T} = \left\{ \begin{pmatrix} A & & O \\ & \ddots & \\ O & & A \end{pmatrix} \;\middle|\; A \in \mathcal{T} \right\} \text{ and } \mathcal{T} \otimes I_m = \left\{ \begin{pmatrix} a_{11}I_m & \cdots & a_{1n}I_m \\ \vdots & \ddots & \vdots \\ a_{n1}I_m & \cdots & a_{nn}I_m \end{pmatrix} \;\middle|\; A = (a_{ij}) \in \mathcal{T} \right\}.$$

A matrix $*$-algebra $\mathcal{T}$ is called *simple* if it has no ideal other than $\{O\}$ and $\mathcal{T}$ itself, where an *ideal* of $\mathcal{T}$ means a submodule $\mathcal{I}$ of $\mathcal{T}$ such that $[A \in \mathcal{T}, B \in \mathcal{I} \Rightarrow AB, BA \in \mathcal{I}]$. We say that $\mathcal{T}$ is *irreducible* if no $\mathcal{T}$-invariant subspace other than $\{0\}$ and $\mathbb{R}^n$ exists, where a linear subspace W of $\mathbb{R}^n$ is *$\mathcal{T}$-invariant* if $AW \subseteq W$ for every $A \in \mathcal{T}$. The matrix $*$-algebras $\mathcal{M}_n$, $\mathcal{C}_n$, and $\mathcal{H}_n$ are typical examples of irreducible matrix $*$-algebras.

We say that two matrix $*$-algebras $\mathcal{T}_1$ and $\mathcal{T}_2$ are *equivalent* if there exists an orthogonal matrix P such that

$$\mathcal{T}_2 = P^\top \mathcal{T}_1 P, \quad \text{where } P^\top \mathcal{T}_1 P = \{P^\top A P \mid A \in \mathcal{T}_1\}.$$

We denote the equivalence by $\mathcal{T}_1 \simeq \mathcal{T}_2$.

From a standard result of the theory of matrix $*$-algebras [16, 17], we obtain the following structure theorem for a matrix $*$-algebra over the real field $\mathbb{R}$. The proof can be found, e.g., in [10, 15].

Theorem 2.1. *A matrix $*$-algebra $\mathcal{T}$ is equivalent to the direct sum of simple matrix $*$-algebras. A simple matrix $*$-algebra is equivalent to the direct sum of equivalent irreducible matrix $*$-algebras. Moreover, an irreducible matrix $*$-algebra of order p is equivalent to one of $\mathcal{M}_p$, $\mathcal{C}_{p/2}$, and $\mathcal{H}_{p/4}$. In other words, it holds that*

$$\mathcal{T} \simeq \bigoplus_{j=1}^{\ell} (I_{m_j} \otimes \mathcal{T}_j),$$

where $\mathcal{T}_j$ is one of $\mathcal{M}_{p_j}$, $\mathcal{C}_{p_j/2}$, and $\mathcal{H}_{p_j/4}$ and p_j is the order of $\mathcal{T}_j$ for $j = 1, \ldots, \ell$.

Note that the decomposition in Theorem 2.1 is uniquely determined by a matrix $*$-algebra $\mathcal{T}$.

It then follows that, with a single orthogonal matrix P, every matrix X in $\mathcal{T}$ can be transformed simultaneously to a block-diagonal form as

$$P^\top XP = \bigoplus_{j=1}^{\ell}(I_{m_j} \otimes B_j) \tag{1}$$

for some $B_j \in \mathcal{T}_j$ for $j = 1, \dots, \ell$.

2.2 Commutant algebra

For a matrix $*$-algebra $\mathcal{T}$, the *commutant algebra*, denoted by $\mathcal{T}'$, is defined to be

$$\mathcal{T}' = \{X \mid AX = XA, \forall A \in \mathcal{T}\}.$$

Note that $\mathcal{T}'$ also forms a matrix $*$-algebra, and that $(\mathcal{T}')' = \mathcal{T}$ holds.

The following lemma is not difficult to see.

Lemma 2.2.

(i) $\mathcal{M}_n' = \{aI_n \mid a \in \mathbb{R}\}$.

(ii) $\mathcal{C}_n' = I_n \otimes \mathcal{C}_1$.

(iii) $\mathcal{H}_n' = I_n \otimes \mathcal{W}$, *where*

$$\mathcal{W} = \left\{ \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R} \right\}.$$

Note that $\mathcal{W}$ is equivalent to $\mathcal{H}_1$, because $\mathrm{diag}(1, 1, 1, -1)\mathcal{W}\mathrm{diag}(1, 1, 1, -1) = \mathcal{H}_1$, where $\mathrm{diag}(\cdots)$ is a (block)-diagonal matrix whose diagonal blocks are in the parentheses.

For two matrix $*$-algebras $\mathcal{T}_1$ and $\mathcal{T}_2$, it follows from the definition that

$$\mathcal{T}_1 \subseteq \mathcal{T}_2 \Longleftrightarrow \mathcal{T}_1' \supseteq \mathcal{T}_2'.$$

Moreover, it can be shown by using Theorem 2.1 and Lemma 2.2 that

$$(\mathcal{T}_1 \otimes \mathcal{T}_2)' = \mathcal{T}_1' \otimes \mathcal{T}_2'. \tag{2}$$

3 Main theorem

Assume that a matrix $*$-algebra $\mathcal{T}$ is generated by symmetric matrices $A_1, \dots, A_N$. Note that, in our setting, we do not have any information of $A_1, \dots, A_N$ in advance. For a real vector $r = (r^{(1)}, \dots, r^{(N)})$, put

$$A(r) = r^{(1)}A_1 + \cdots + r^{(N)}A_N.$$

We denote by $\mathrm{span}\{\cdots\}$ the set of linear combinations of the matrices in the braces, and by $\langle\cdots\rangle$ the matrix $*$-algebra generated by the matrices in the brackets.

The main result of this section is the following.

Table 1: Minimum number of symmetric matrices to generate irreducible matrix $*$-algebras

	$n = 1$	$n = 2$	$n = 3$	$n \geq 4$
$\mathcal{M}_n$	1	2		
$\mathcal{C}_n$	—	3	2	
$\mathcal{H}_n$	—	4	3	2

Theorem 3.1. *Assume that* $\mathrm{span}\{I_n, A_1, \dots, A_N\} = \mathcal{T} \cap \mathcal{S}_n$*. Then there exists an open dense subset* $R \subseteq \mathbb{R}^{4N}$ *such that for any* $(r_1, r_2, r_3, r_4) \in R$ *with* $r_i \in \mathbb{R}^N$ *for* $i = 1, \dots, 4$*, it holds that*

$$\langle A(r_1), A(r_2), A(r_3), A(r_4)\rangle = \mathcal{T}.$$

We may assume that the coefficient vector (r_1, r_2, r_3, r_4) is normalized, for example, to $\|r_i\| = 1$ for $i = 1, \dots, 4$. Then, by the proof of this theorem, we can show that $A(r_1), \dots, A(r_4)$ generate $\mathcal{T}$ for almost all values of (r_1, r_2, r_3, r_4), or with probability one if (r_1, r_2, r_3, r_4) is chosen at random. See also remarks for simpler cases after Lemmas 3.4 and 3.9.

To prove Theorem 3.1, it suffices, by Theorem 2.1, to discuss each case of irreducible matrix $*$-algebras, i.e., $\mathcal{M}_n$, $\mathcal{C}_n$, and $\mathcal{H}_n$. The main part of the proof is to provide the minimum number of symmetric matrices to generate each irreducible matrix $*$-algebra, which is summarized in Table 1. Note that $\mathcal{C}_1$ and $\mathcal{H}_1$ cannot be generated by any set of symmetric matrices.

1. $\mathcal{M}_n$ $(n \geq 2)$ can be generated with *two* randomly-chosen symmetric matrices (Lemma 3.4).
2. $\mathcal{C}_2$ *cannot* be generated with any *two* symmetric matrices (Lemma 3.7), but can be done with *three* randomly-chosen symmetric matrices (Lemma 3.9).
3. $\mathcal{C}_n$ $(n \geq 3)$ can be generated with *two* randomly-chosen symmetric matrices (Lemma 3.11).
4. $\mathcal{H}_2$ cannot be generated with any *three* symmetric matrices (Lemma 3.16), but can be done with *four* randomly-chosen symmetric matrices (Lemma 3.18).
5. $\mathcal{H}_3$ cannot be generated with any *two* symmetric matrices (Lemma 3.19), but can be done with *three* randomly-chosen symmetric matrices (Lemma 3.21).
6. $\mathcal{H}_n$ $(n \geq 4)$ can be generated with *two* randomly-chosen symmetric matrices (Lemma 3.23).

In what follows, we will prove 1–6 above in turn.

3.1 Genericity in eigenvalue structure

To obtain our main theorem, we make use of the notion of genericity introduced in [12, 15]. Let X be a symmetric matrix in $\mathcal{T}$. We say that X is *generic* (more precisely, *generic in eigenvalue structure*) if the matrices $B_1, \dots, B_\ell$ appearing in the decomposition in (1) do not share a common eigenvalue, and in addition, for each $j = 1, \dots, \ell$, it holds that

- If $\mathcal{T}_j = \mathcal{M}_{p_j}$, then all the eigenvalues of B_j are simple.
- If $\mathcal{T}_j = \mathcal{C}_{p_j/2}$, then all the eigenvalues of B_j have multiplicity two.
- If $\mathcal{T}_j = \mathcal{H}_{p_j/4}$, then all the eigenvalues of B_j have multiplicity four.

The following lemma can be proved in a similar way to [12, 15].

Lemma 3.2. *Assume that* $\mathrm{span}\{I_n, A_1, \dots, A_N\} = \mathcal{T} \cap \mathcal{S}_n$*. Then there exists an open dense subset* $R_{\mathrm{g}} \subseteq \mathbb{R}^N$ *such that for any* $r \in R_{\mathrm{g}}$*, the matrix* $A(r)$ *is generic.*

3.2 Case of $\mathcal{M}_n$

In this section, we deal with generating the irreducible matrix $*$-algebra $\mathcal{M}_n$. Note that if $n = 1$ one nonzero matrix generates $\mathcal{M}_n = \mathcal{M}_1$.

The following lemma asserts that if two symmetric matrices satisfy the genericity with some condition, they generate $\mathcal{M}_n$. We remark that a single symmetric matrix $X \in \mathcal{M}_n$ does not generate $\mathcal{M}_n$ if $n \geq 2$. Indeed, since X is diagonalized by some orthogonal matrix P, we see $\langle P^\top X P \rangle \subseteq \bigoplus_{j=1}^n \mathcal{M}_1 \subsetneq \mathcal{M}_n$. Hence $\langle X \rangle \subsetneq P\mathcal{M}_n P^\top = \mathcal{M}_n$ holds.

Lemma 3.3. *Let X_1, X_2 be two symmetric matrices in $\mathcal{M}_n$ with $n \geq 2$. If X_1 is generic and there exists an orthogonal matrix Q such that* (a) *it diagonalizes X_1 and* (b) $(Q^\top X_2 Q)_{1j} \neq 0$ *for every $j = 2, \ldots, n$, then it holds that $\langle X_1, X_2 \rangle = \mathcal{M}_n$.*

Proof. It suffices to show that $\langle X_1, X_2 \rangle' \subseteq I_n$. Indeed, if so, then we have $\langle X_1, X_2 \rangle \supseteq I_n' = \mathcal{M}_n$ by Lemma 2.2 and (2). This, together with $\langle X_1, X_2 \rangle \subseteq \mathcal{M}_n$, implies that $\langle X_1, X_2 \rangle = \mathcal{M}_n$.

Let $Y_\ell = Q^\top X_\ell Q$ for $\ell = 1, 2$. Then Y_1 is a diagonal matrix whose diagonal entries are its eigenvalues, denoted by $\lambda_1, \ldots, \lambda_n$. Assume that $A = (a_{ij})$ is a matrix in $\langle Y_1, Y_2 \rangle'$. By $AY_1 = Y_1 A$, we have

$$a_{ij}\lambda_j = \lambda_i a_{ij} \text{ for any } i, j.$$

Hence if $i \neq j$ then $a_{ij} = 0$ holds since $\lambda_i \neq \lambda_j$ by the genericity of X_1. Moreover, by $AY_2 = Y_2 A$, it holds that

$$a_{ii}(Y_2)_{ij} = (Y_2)_{ij} a_{jj} \text{ for any } i, j,$$

where $(Y_2)_{ij}$ is the (i, j)-entry of Y_2. Since $(Y_2)_{1j} \neq 0$ by the assumption, we see that $a_{11} = a_{jj}$ for every j, and hence $A = \alpha I$ for some $\alpha \in \mathbb{R}$. Therefore, $\langle Y_1, Y_2 \rangle' \subseteq I_n$ holds. Hence we have $\langle X_1, X_2 \rangle' = Q \langle Y_1, Y_2 \rangle' Q^\top \subseteq Q I_n Q^\top = I_n$, which proves the statement. □

By Lemma 3.3, together with Lemma 3.2, we have the following lemma, which says that almost all pairs of symmetric matrices generate $\mathcal{M}_n$.

Lemma 3.4. *Assume that* $\operatorname{span}\{I_n, A_1, \ldots, A_N\} = \mathcal{M}_n \cap \mathcal{S}_n$ *with $n \geq 2$. Then there exists an open dense subset $R \subseteq \mathbb{R}^{2N}$ such that for any $(r_1, r_2) \in R$ with $r_i \in \mathbb{R}^N$ for $i = 1, 2$, it holds that $\langle A(r_1), A(r_2) \rangle = \mathcal{M}_n$.*

Proof. Let $(r_1, r_2) \in \mathbb{R}^{2N}$ with $r_1, r_2 \in \mathbb{R}^N$, and $X_i = A(r_i)$ for $i = 1, 2$. It follows from Lemma 3.3 that if (a) X_1 is generic and (b) there exists an orthogonal matrix Q such that it diagonalizes X_1 and $(Q^\top X_2 Q)_{1j} \neq 0$ for every $j = 2, \ldots, n$, then it holds that $\langle X_1, X_2 \rangle = \mathcal{M}_n$. It is not difficult to see from Lemma 3.2 that these conditions are satisfied for any parameter value (r_1, r_2) in some open dense subset R of $\mathbb{R}^{2N}$. Thus the statement holds. □

We may assume that the vectors r_1 and r_2 are both normalized to unit vectors in Lemma 3.4. If r_1 is chosen at random, then $A(r_1)$ is generic with probability one by Lemma 3.2. Under this condition, $A(r_1)$ and $A(r_2)$ generate $\mathcal{M}_n$ with probability one if r_2 is chosen at random, because $A(r_2)$ satisfies for almost all values of r_2 that $(Q^\top A(r_2) Q)_{1j} \neq 0$ for $j = 2, \ldots, n$ for an orthogonal matrix Q that diagonalizes X_1. Therefore, $A(r_1)$ and $A(r_2)$ generate $\mathcal{M}_n$ with probability one if r_1 and r_2 are chosen at random, respectively.

3.3 Case of $\mathcal{C}_n$

In this section, we provide the explicit number of symmetric matrices to generate the irreducible matrix $*$-algebra $\mathcal{C}_n$. For a matrix $A \in \mathcal{C}_n$, there exists a matrix B in $\mathbb{C}^{n \times n}$ such that $C(B) = A$. For $1 \leq p, q \leq n$, the $[p, q]$-*block of* A, denoted by $A_{[p,q]}$, means the submatrix $C(B_{pq})$ of order two, where B_{pq} is the (p, q)-entry of B.

We say that an orthogonal matrix P is $\mathbb{C}$-*compatible* if $P = C(U)$ for some unitary matrix U over the complex field. Note that a $\mathbb{C}$-compatible orthogonal matrix P preserves the form of a matrix in $\mathcal{C}_n$, that is, $P^\top \mathcal{C}_n P = \mathcal{C}_n$.

We first show the following lemma.

Lemma 3.5. *For a symmetric matrix X in $\mathcal{C}_n$, there exists a $\mathbb{C}$-compatible orthogonal matrix P that diagonalizes X.*

Proof. Since $X \in \mathcal{C}_n \cap \mathcal{S}_{2n}$, there exists a Hermitian matrix $Y \in \mathbb{C}^{n\times n}$ such that $X = C(Y)$. Then there exists a unitary matrix U that diagonalizes Y, i.e., U^*YU is a diagonal matrix whose diagonal entries are its eigenvalues. Note that all the eigenvalues of Y are real. Define $P = C(U)$. Then, since the mapping C from $\mathbb{C}^{n\times n}$ to $\mathcal{C}_n$ is isomorphic, we see that $P^\top P = C(U^*)C(U) = C(U^*U) = I_{2n}$, i.e., P is orthogonal. Moreover, it holds that $P^\top XP = C(U^*)C(Y)C(U) = C(U^*YU)$, which is a diagonal matrix all of whose diagonal entries have multiplicity two. □

Observe that for any nonzero matrix $C(a+ib) \in \mathcal{C}_1$, the matrix $\mu^{-1}C(a+ib)$ is orthogonal, where $\mu = \sqrt{a^2+b^2}$. This fact gives the following lemma.

Lemma 3.6. *Let X_1, X_2 be two symmetric matrices in $\mathcal{C}_n$. Then the following two statements hold.*

(i) *There exists a $\mathbb{C}$-compatible orthogonal matrix Q_1 such that* (a) *it diagonalizes X_1 and* (b) $(Q_1^\top X_2 Q_1)_{[1,j]} = \mu_j I_2$ *for some $\mu_j \in \mathbb{R}$ for every $j = 2, \dots, n$.*

(ii) *If X_1 is generic and there exists a $\mathbb{C}$-compatible orthogonal matrix Q_1 satisfying* (a), (b), *and* (c) *$\mu_j \neq 0$ for every $j = 2, \dots, n$, then it holds that $Q_1^\top \langle X_1, X_2\rangle Q_1 \supseteq \mathcal{M}_n \otimes I_2$.*

Proof. **(i)** By Lemma 3.5, there exists a $\mathbb{C}$-compatible orthogonal matrix Q_0 diagonalizing X_1. We denote $Q_0^\top X_1 Q_0 = \mathrm{diag}(x_1 I_2, x_2 I_2, \dots, x_n I_2)$, and the $[p,q]$-block of $Q_0^\top X_2 Q_0$ by $C_{pq} = C(a_{pq} + ib_{pq})$ for $p, q = 1, \dots, n$. Define $D_1 = I_2$, and, for $j = 2, \dots, n$, define D_j to be $D_j = \mu_j^{-1} C_{1j}$ if $C_{1j} \neq O$ and $D_j = I_2$ otherwise, where $\mu_j = \sqrt{a_{1j}^2 + b_{1j}^2}$. Then D_j is orthogonal for $j = 1, \dots, n$.

Let $Q_1' = \mathrm{diag}(D_1^\top, D_2^\top, \dots, D_n^\top)$. Then $Q_1 = Q_0 Q_1'$ is orthogonal and $\mathbb{C}$-compatible, and $Q_1^\top X_1 Q_1 = \mathrm{diag}(x_1 I_2, x_2 I_2, \dots, x_n I_2)$ holds. Moreover, the $[p,q]$-block of $Q_1^\top X_2 Q_1$ is equal to $D_p C_{pq} D_q^\top$, and in particular, the $[1,j]$-block is equal to $\mu_j I_2$ if $C_{1j} \neq O$ and to O otherwise for every $j = 2, \dots, n$. Thus the statement holds.

(ii) Define $Y_h = Q_1^\top X_h Q_1$ for $h = 1, 2$. We will show that

$$\langle Y_1, Y_2\rangle' \subseteq I_n \otimes \mathcal{M}_2.$$

Indeed, let A be a matrix such that $Y_h A = AY_h$ for $h = 1, 2$. Since A is commutative with Y_1, the matrix A has the form of $A = \mathrm{diag}(A_1, A_2, \dots, A_n)$, where A_j's are matrices of order two. This is because $x_p \neq x_q$ holds for distinct p, q by the genericity of X_1. Moreover, since A is commutative with Y_2, comparing the $[1,j]$-blocks of $Y_1 A$ and AY_1 leads to $\mu_j A_1 = A_j \mu_j$ for $j = 2, \dots, n$, and hence $A_1 = A_j$ holds since $\mu_j \neq 0$. Hence A is contained in $I_n \otimes \mathcal{M}_2$. Therefore, since $(I_n \otimes \mathcal{M}_2)' = \mathcal{M}_n \otimes I_2$ by Lemma 2.2, it holds that $\langle Y_1, Y_2\rangle \supseteq \mathcal{M}_n \otimes I_2$. □

Subcase: $n = 2$

We first discuss the case of $\mathcal{C}_2$. The following lemma asserts that $\mathcal{C}_2$ cannot be generated with any two symmetric matrices.

Lemma 3.7. *Let X_1, X_2 be two symmetric matrices in $\mathcal{C}_2$. Then it holds that $\langle X_1, X_2\rangle \subsetneq \mathcal{C}_2$.*

Proof. By Lemma 3.6 (i), there exists a $\mathbb{C}$-compatible orthogonal matrix Q_1 satisfying (a) and (b). Then $Y_h = Q_1^\top X_h Q_1$ for $h = 1, 2$ have the forms of

$$Y_1 = \begin{pmatrix} x_1 I_2 & O \\ O & y_1 I_2 \end{pmatrix} \text{ and } Y_2 = \begin{pmatrix} x_2 I_2 & \mu I_2 \\ \mu I_2 & y_2 I_2 \end{pmatrix} \tag{3}$$

for some real numbers x_j, y_j $(j = 1, 2)$ and μ. This means that $\langle Y_1, Y_2 \rangle \subseteq \mathcal{M}_2 \otimes I_2 \subsetneq \mathcal{C}_2$. Thus $\langle X_1, X_2 \rangle \subsetneq \mathcal{C}_2$ holds. □

On the other hand, if we have three symmetric matrices with some condition, they generate $\mathcal{C}_2$.

Lemma 3.8. *Let X_1, X_2, X_3 be three symmetric matrices in $\mathcal{C}_2$. If X_1 is generic and there exists a $\mathbb{C}$-compatible orthogonal matrix Q_1 satisfying* (a), (b), *and* (c) *in Lemma* 3.6 *with an additional condition* (d) $(Q_1^\top X_3 Q_1)_{1,4} \neq 0$, *then it holds that $\langle X_1, X_2, X_3 \rangle = \mathcal{C}_2$.*

Proof. Define $Y_h = Q_1^\top X_h Q_1$ for $h = 1, 2, 3$. Then Y_1 and Y_2 take the forms of (3), and Y_3 has the form of

$$Y_3 = \begin{pmatrix} x_3 I_2 & C(a+ib) \\ C(a+ib)^\top & y_3 I_2 \end{pmatrix}.$$

By (d), $b \neq 0$ holds. We will show that

$$\langle Y_1, Y_2, Y_3 \rangle' \subseteq I_2 \otimes \mathcal{C}_1.$$

To see this, let A be a matrix such that $Y_h A = A Y_h$ for $h = 1, 2, 3$. Since $A \in \langle Y_1, Y_2 \rangle'$, Lemma 3.6 (ii) implies that $A \in (\mathcal{M}_2 \otimes I_2)' = I_2 \otimes \mathcal{M}_2$, that is, $A = I_2 \otimes A_1$ for some matrix A_1 of order two. Moreover, since A is commutative with Y_3, we have $C(a+ib)A_1 = A_1 C(a+ib)$. By $b \neq 0$, we obtain $A_1 \in \mathcal{C}_1$. Hence $A \in I_2 \otimes \mathcal{C}_1$, and therefore, since $(I_2 \otimes \mathcal{C}_1)' = \mathcal{C}_2$ by Lemma 2.2, we have $\langle Y_1, Y_2, Y_3 \rangle \supseteq \mathcal{C}_2$. Thus $\langle X_1, X_2, X_3 \rangle \supseteq Q_1 \mathcal{C}_2 Q_1^\top = \mathcal{C}_2$, and moreover the equality holds since $\langle X_1, X_2, X_3 \rangle \subseteq \mathcal{C}_2$ obviously holds. □

It follows from Lemma 3.8 that almost all triples of symmetric matrices in $\mathcal{C}_2$ generate $\mathcal{C}_2$.

Lemma 3.9. *Assume that* $\operatorname{span}\{I_n, A_1, \ldots, A_N\} = \mathcal{C}_2 \cap \mathcal{S}_4$. *Then there exists an open dense subset $R \subseteq \mathbb{R}^{3N}$ such that for any $(r_1, r_2, r_3) \in R$ with $r_i \in \mathbb{R}^N$ for $i = 1, 2, 3$, it holds that $\langle A(r_1), A(r_2), A(r_3) \rangle = \mathcal{C}_2$.*

Proof. Let $(r_1, r_2, r_3) \in \mathbb{R}^{3N}$ with $r_i \in \mathbb{R}^N$ for $i = 1, 2, 3$, and denote $X_i = A(r_i)$. Suppose that the condition of Lemma 3.8 is satisfied, that is, X_1 is generic and there exists a $\mathbb{C}$-compatible orthogonal matrix Q_1 satisfying (a), (b), (c) in Lemma 3.6, and (d) $(Q_1^\top X_3 Q_1)_{1,4} \neq 0$. Then it follows from Lemma 3.8 that $\langle X_1, X_2, X_3 \rangle = \mathcal{C}_2$. By Lemma 3.2, such Q_1 exists for any parameter value (r_1, r_2, r_3) in some open dense subset R of $\mathbb{R}^{3N}$. Thus the statement holds. □

In a similar way to Lemma 3.4, $A(r_1)$, $A(r_2)$, and $A(r_3)$ generate $\mathcal{C}_2$ with probability one if r_1, r_2, and r_3 are chosen at random from normalized vectors. Indeed, if r_1 is chosen at random, then $A(r_1)$ is generic for almost all values of r_1 by Lemma 3.2. Under this condition, a $\mathbb{C}$-compatible orthogonal matrix Q_1 with the two conditions (a) and (b) also satisfies (c) for almost all values of r_2, and, in addition, Q_1 satisfies $(Q_1^\top X_3 Q_1)_{1,4} \neq 0$ for almost all values of r_3. Thus $A(r_1)$, $A(r_2)$, and $A(r_3)$ generate $\mathcal{C}_2$ for almost all values of (r_1, r_2, r_3). We remark that we can apply a similar argument for all the other cases in the rest of this section.

Subcase: $n \geq 3$

We next discuss the case where $n \geq 3$. The following lemmas correspond to Lemmas 3.8 and 3.9 for $n = 2$.

Lemma 3.10. *Let X_1, X_2 be two symmetric matrices in $\mathcal{C}_n$ with $n \geq 3$. If there exists a $\mathbb{C}$-compatible orthogonal matrix Q_1 satisfying* (a)*,* (b)*,* (c) *in Lemma* 3.6 *with an additional condition* (d) $(Q_1^\top X_2 Q_1)_{3,6} \neq 0$*, then it holds that $\langle X_1, X_2 \rangle = \mathcal{C}_n$.*

Proof. Define $Y_h = Q_1^\top X_h Q_1$ for $h = 1, 2$. We will show that

$$\langle Y_1, Y_2 \rangle' \subseteq I_n \otimes \mathcal{C}_1.$$

Let A be a matrix such that $Y_h A = A Y_h$ for $h = 1, 2$. By Lemma 3.6 (ii), $A = I_n \otimes A_1$ for some matrix A_1 of order two. Let $C = (Y_2)_{[2,3]} \in \mathcal{C}_1$. Since A is commutative with Y_2, comparing the $[2,3]$-blocks of $Y_2 A$ and $A Y_2$ leads to $C A_1 = A_1 C$. Since the off-diagonal entries of C are nonzero by (d), we obtain $A_1 \in \mathcal{C}_1$. Therefore, A is contained in $I_n \otimes \mathcal{C}_1$. Since $(I_n \otimes \mathcal{C}_1)' = \mathcal{C}_n$ by Lemma 2.2, $\langle Y_1, Y_2 \rangle \supseteq \mathcal{C}_n$ holds. Thus $\langle X_1, X_2 \rangle \supseteq Q_1 \mathcal{C}_n Q_1^\top = \mathcal{C}_n$, and the equality holds since $\langle X_1, X_2 \rangle \subseteq \mathcal{C}_n$. □

Lemma 3.11. *Assume that* $\operatorname{span}\{I_n, A_1, \ldots, A_N\} = \mathcal{C}_n \cap \mathcal{S}_{2n}$ *with $n \geq 3$. Then there exists an open dense subset $R \subseteq \mathbb{R}^{2N}$ such that for any $(r_1, r_2) \in R$ with $r_i \in \mathbb{R}^N$ for $i = 1, 2$, it holds that $\langle A(r_1), A(r_2) \rangle = \mathcal{C}_n$.*

Proof. This follows in a similar way to the proof of Lemma 3.9. □

3.4 Case of $\mathcal{H}_n$

In this section, we discuss the number of symmetric matrices to generate the irreducible matrix $*$-algebra $\mathcal{H}_n$. The outline of this section is essentially similar to, but more complex than, the case of $\mathcal{C}_n$.

We say that an orthogonal matrix P is $\mathbb{H}$-*compatible* if $P = H(U)$ for some quaternion unitary matrix U; recall that a matrix U over the quaternion field $\mathbb{H}$ is *unitary* if $U^* U = I$, where U^* denotes the conjugate transpose of U with respect to $\mathbb{H}$, i.e., the (q,p)-entry of U^* is $a - ib - jc - kd$ if the (p,q)-entry of U is $a + ib + jc + kd$. Note that an $\mathbb{H}$-compatible orthogonal matrix P preserves the form of a matrix X in $\mathcal{H}_n$, that is, $P^\top \mathcal{H}_n P = \mathcal{H}_n$. In a similar way to the case of $\mathcal{C}_n$, we have the following lemma.

Lemma 3.12. *For a symmetric matrix X in $\mathcal{H}_n$, there exists an $\mathbb{H}$-compatible orthogonal matrix P that diagonalizes X.*

Proof. Since $X \in \mathcal{H}_n$ is symmetric, we have $X = H(Y)$ for some quaternion Hermitian matrix $Y \in \mathbb{H}^{n \times n}$, where Y being Hermitian means $Y^* = Y$. There exists a quaternion unitary matrix U such that $U^* Y U$ is a diagonal matrix whose diagonal entries are real. Then $P = H(U)$ is orthogonal and $P^\top X P = H(U^*) H(Y) H(U) = H(U^* Y U)$, which is a diagonal matrix. □

For $A \in \mathcal{H}_n$ and $B \in \mathbb{H}^{n \times n}$ with $H(B) = A$, the $[p,q]$-*block of* A, denoted by $A_{[p,q]}$, is the matrix $H(B_{pq})$ of order four for $1 \leq p, q \leq n$, where B_{pq} is the (p,q)-entry of B.

By analogy with Lemma 3.6, we have the following lemma, which follows from the fact that for any nonzero matrix $H(a + ib + jc + kd) \in \mathcal{H}_1$, the matrix $\mu^{-1} H(a + ib + jc + kd)$ is orthogonal, where $\mu = \sqrt{a^2 + b^2 + c^2 + d^2}$.

Lemma 3.13. *Let X_1, X_2 be two symmetric matrices in $\mathcal{H}_n$. Then the following two statements hold.*

(i) *There exists an $\mathbb{H}$-compatible orthogonal matrix Q_1 such that* (a) *it diagonalizes X_1 and* (b) $(Q_1^\top X_2 Q_1)_{[1,h]} = \mu_h I_4$ *for some $\mu_h \in \mathbb{R}$ for every $h = 2, \dots, n$.*

(ii) *If X_1 is generic and there exists an $\mathbb{H}$-compatible orthogonal matrix Q_1 satisfying* (a), (b), *and* (c) $\mu_h \neq 0$ *for every $h = 2, \dots, n$, then it holds that $Q_1^\top \langle X_1, X_2 \rangle Q_1 \supseteq \mathcal{M}_n \otimes I_4$.*

We also make the following observations needed later.

Lemma 3.14. *For a matrix H_1 in $\mathcal{H}_1$, there exists an $\mathbb{H}$-compatible orthogonal matrix P such that*

$$P^\top H_1 P = \begin{pmatrix} aI_2 & -\nu I_2 \\ \nu I_2 & aI_2 \end{pmatrix} \tag{4}$$

for some real numbers a and ν, which implies that $P^\top \langle H_1 \rangle P \subseteq \mathcal{C}_1 \otimes I_2$.

Proof. We denote $H_1 = H(a + ib + jc + kd)$ for some real numbers a, b, c, and d. Note that H_1 has the form of

$$H_1 = \begin{pmatrix} C(a+ib) & C(-c-id) \\ C(c-id) & C(a-ib) \end{pmatrix}.$$

We may assume that $b \neq 0$ or $d \neq 0$, since otherwise H_1 itself has the form of (4). Without loss of generality, suppose that $d \neq 0$, because a similar argument holds for the case of $b \neq 0$ by symmetry. For an $\mathbb{H}$-compatible orthogonal matrix

$$P = \begin{pmatrix} I_2 & \\ & \tau^{-1} C(c-id) \end{pmatrix} \begin{pmatrix} 1 & & \\ & \nu^{-1} C(\tau - ib) & \\ & & 1 \end{pmatrix},$$

where $\tau = \sqrt{c^2 + d^2}$ and $\nu = \sqrt{b^2 + c^2 + d^2}$, we have

$$P^\top H_1 P = \begin{pmatrix} aI_2 & -\nu I_2 \\ \nu I_2 & aI_2 \end{pmatrix}.$$

Thus the statement holds. □

Lemma 3.15. *Let H_1, H_2 be two matrices in $\mathcal{H}_1$. If* (d) *there exists an $\mathbb{H}$-compatible orthogonal matrix P satisfying (4), where $\nu \neq 0$, such that all the off-diagonal entries in $P^\top H_2 P$ are nonzero, then it holds that*

$$\langle H_1, H_2 \rangle = \mathcal{H}_1.$$

Proof. Define $G_h = P^\top H_h P$ for $h = 1, 2$. We will show that

$$\langle G_1, G_2 \rangle' \subseteq \mathcal{W}.$$

To see this, let A be a matrix in $\langle G_1, G_2 \rangle'$. Since $G_1 A = A G_1$ and $\nu \neq 0$, the matrix A has the form of

$$A = \begin{pmatrix} B_1 & -B_2 \\ B_2 & B_1 \end{pmatrix}$$

for some matrices B_1, B_2 of order two. Moreover, since A is commutative with G_2 and all the off-diagonal entries of G_2 are nonzero, we have $A \in \mathcal{W}$, and hence $\langle G_1, G_2 \rangle' \subseteq \mathcal{W}$. Therefore, $\langle G_1, G_2 \rangle \supseteq (\mathcal{W})' = \mathcal{H}_1$ by Lemma 2.2. Hence $\langle H_1, H_2 \rangle = P \langle G_1, G_2 \rangle P^\top \supseteq \mathcal{H}_1$, which proves the statement since $\langle H_1, H_2 \rangle \subseteq \mathcal{H}_1$. □

Subcase: $n = 2$

We first discuss the case where $n = 2$.

Lemma 3.16. *Let X_1, X_2, X_3 be three symmetric matrices in $\mathcal{H}_2$. Then $\langle X_1, X_2, X_3 \rangle \subsetneq \mathcal{H}_2$ holds.*

Proof. By Lemma 3.13 (i), there exists an $\mathbb{H}$-compatible orthogonal matrix Q_1 satisfying (a) and (b). Then $Y_h = Q_1^\top X_h Q_1$ for $h = 1, 2$ have the forms of

$$Y_1 = \begin{pmatrix} x_1 I_4 & O \\ O & y_1 I_4 \end{pmatrix} \text{ and } Y_2 = \begin{pmatrix} x_2 I_4 & \mu I_4 \\ \mu I_4 & y_2 I_4 \end{pmatrix}$$

for some real numbers $x_h, y_h\,(h = 1, 2)$ and μ. This means that $\langle Y_1, Y_2 \rangle \subseteq \mathcal{M}_2 \otimes I_4$.

Let $Y_3 = Q_1^\top X_3 Q_1$ have the form of

$$Y_3 = \begin{pmatrix} x_3 I_4 & H_3 \\ H_3^\top & y_3 I_4 \end{pmatrix},$$

where $H_3 \in \mathcal{H}_1$. It follows from Lemma 3.14 that there exists an $\mathbb{H}$-compatible orthogonal matrix P such that $P^\top H_3 P = C \otimes I_2$ for some $C = C(\alpha + i\beta) \in \mathcal{C}_1$. Letting $Q_2 = \operatorname{diag}(P, P)$, we see that $Q_2^\top Y_h Q_2 = Y_h$ for $h = 1, 2$ and

$$Q_2^\top Y_3 Q_2 = \begin{pmatrix} x_3 I_2 & O & \alpha I_2 & -\beta I_2 \\ O & x_3 I_2 & \beta I_2 & \alpha I_2 \\ \alpha I_2 & \beta I_2 & y_3 I_2 & O \\ -\beta I_2 & \alpha I_2 & O & y_3 I_2 \end{pmatrix}.$$

This means that $Q_2^\top \langle Y_1, Y_2, Y_3 \rangle Q_2 \subseteq \mathcal{C}_2 \otimes I_2 \subsetneq \mathcal{H}_2$. Hence $\langle X_1, X_2, X_3 \rangle \subsetneq Q_1 Q_2 \mathcal{H}_2 Q_2^\top Q_1^\top = \mathcal{H}_2$ holds. □

Lemma 3.17. *Let X_1, X_2, X_3, X_4 be four symmetric matrices in $\mathcal{H}_2$. Assume that X_1 is generic and that there exists an $\mathbb{H}$-compatible orthogonal matrix Q_1 satisfying* (a), (b), *and* (c) *in Lemma* 3.13 *with an additional condition that* (d) *in Lemma* 3.15 *holds for $H_1 = (Q_1^\top X_3 Q_1)_{[1,2]}$ and $H_2 = (Q_1^\top X_4 Q_1)_{[1,2]}$. Then it holds that $\langle X_1, X_2, X_3, X_4 \rangle = \mathcal{H}_2$.*

Proof. We denote $Y_h = Q_1^\top X_h Q_1$ for $h = 1, \dots, 4$. By Lemma 2.2, it suffices to show that

$$\langle X_1, X_2, X_3, X_4 \rangle' \subseteq (\mathcal{H}_2)' = I_2 \otimes \mathcal{W}.$$

To see this, let A be a matrix such that $Y_h A = A Y_h$ for $h = 1, \dots, 4$. By Lemma 3.13 (ii), $A = I_2 \otimes A_1$ for some A_1 of order four. Moreover, since A is commutative with both Y_3 and Y_4, the matrix A_1 is commutative with both $H_1 = (Y_3)_{[1,2]}$ and $H_2 = (Y_4)_{[1,2]}$. Since the pair of H_1 and H_2 satisfy the condition (d) of Lemma 3.15, we have $A_1 \in \langle H_1, H_2 \rangle' = \mathcal{H}_1' = \mathcal{W}$. Therefore, we obtain $\langle Y_1, Y_2, Y_3, Y_4 \rangle' \subseteq I_2 \otimes \mathcal{W}$. This implies that $\langle X_1, X_2, X_3, X_4 \rangle' \subseteq I_2 \otimes \mathcal{W}$, and thus $\langle X_1, X_2, X_3, X_4 \rangle = \mathcal{H}_2$ holds. □

Lemma 3.17, together with Lemma 3.2, implies the following lemma, which corresponds to Lemma 3.9 for $\mathcal{C}_2$.

Lemma 3.18. *Assume that* $\operatorname{span}\{I_n, A_1, \dots, A_N\} = \mathcal{H}_2 \cap \mathcal{S}_8$. *Then there exists an open dense subset $R \subseteq \mathbb{R}^{4N}$ such that for any $(r_1, r_2, r_3, r_4) \in R$ with $r_i \in \mathbb{R}^N$ for $i = 1, \dots, 4$, it holds that $\langle A(r_1), A(r_2), A(r_3), A(r_4) \rangle = \mathcal{H}_2$.*

Subcase: $n = 3$

We next discuss the case where $n = 3$.

Lemma 3.19. *Let X_1, X_2 be two symmetric matrices in $\mathcal{H}_3$. Then we have $\langle X_1, X_2\rangle \subsetneq \mathcal{H}_3$.*

Proof. By Lemma 3.13 (i), there exists an $\mathbb{H}$-compatible orthogonal matrix Q_1 satisfying (a) and (b). Let $H = (Q_1^\top X_2 Q_1)_{[2,3]}$. By Lemma 3.14, there exists an $\mathbb{H}$-compatible orthogonal matrix P such that $P^\top H P = C \otimes I_2$ for some $C \in \mathcal{C}_1$. Then

$$Q_2 = Q_1 \begin{pmatrix} P & O & O \\ O & P & O \\ O & O & P \end{pmatrix}$$

is $\mathbb{H}$-compatible and orthogonal, and we have

$$Q_2^\top X_1 Q_2 = X_1 \text{ and } Q_2^\top X_2 Q_2 = \begin{pmatrix} x_2 I_4 & \mu_1 I_4 & \mu_2 I_4 \\ \mu_1 I_4 & y_2 I_4 & C \otimes I_2 \\ \mu_2 I_4 & C^\top \otimes I_2 & z_2 I_4 \end{pmatrix}$$

for some $x_2, y_2, z_2, \mu_1, \mu_2 \in \mathbb{R}$. This means that $Q_2^\top \langle X_1, X_2\rangle Q_2 \subseteq \mathcal{C}_3 \otimes I_2 \subsetneq \mathcal{H}_3$. Hence $\langle X_1, X_2\rangle \subsetneq \mathcal{H}_3$ holds. □

Lemma 3.20. *Let X_1, X_2, X_3 be three symmetric matrices in $\mathcal{H}_3$. Assume that X_1 is generic and that there exists an $\mathbb{H}$-compatible orthogonal matrix Q_1 satisfying* (a), (b), *and* (c) *in Lemma* 3.13 *with an additional condition that* (d) *in Lemma* 3.15 *holds for $H_1 = (Q_1^\top X_2 Q_1)_{[2,3]}$ and $H_2 = (Q_1^\top X_3 Q_1)_{[2,3]}$. Then it holds that $\langle X_1, X_2, X_3\rangle = \mathcal{H}_3$.*

Proof. Define $Y_h = Q_1^\top X_h Q_1$ for $h = 1, 2, 3$. Let A be a matrix such that $Y_h A = A Y_h$ for $h = 1, 2, 3$. Since $A \in \langle Y_1, Y_2\rangle'$, Lemma 3.13 (ii) implies $A = I_3 \otimes A_1$, where A_1 is a matrix of order four. Since A is commutative with both of Y_2 and Y_3, we see that $A_1 H_1 = H_1 A_1$ and $A_1 H_2 = H_2 A_1$ by comparing the $[2,3]$-blocks. Since the pair of H_1 and H_2 satisfy the condition (d) of Lemma 3.15, we have $A_1 \in \mathcal{W}$. Thus $A \in I_3 \otimes \mathcal{W}$. Therefore, $\langle Y_1, Y_2, Y_3\rangle' \subseteq I_3 \otimes \mathcal{W}$ holds, and hence $\langle Y_1, Y_2, Y_3\rangle \supseteq \mathcal{H}_3$ by Lemma 2.2. Thus the statement holds by $\langle Y_1, Y_2, Y_3\rangle = Q_1^\top \langle X_1, X_2, X_3\rangle Q_1$ and $\langle Y_1, Y_2, Y_3\rangle \subseteq \mathcal{H}_3$. □

Lemma 3.21. *Assume that* $\operatorname{span}\{I_n, A_1, \ldots, A_N\} = \mathcal{H}_3 \cap \mathcal{S}_{12}$. *Then there exists an open dense subset $R \subseteq \mathbb{R}^{3N}$ such that for any $(r_1, r_2, r_3) \in R$ with $r_i \in \mathbb{R}^N$ for $i = 1, 2, 3$, it holds that $\langle A(r_1), A(r_2), A(r_3)\rangle = \mathcal{H}_3$.*

Subcase: $n \geq 4$

The case where $n \geq 4$ is obtained in a similar way.

Lemma 3.22. *Let X_1, X_2 be two symmetric matrices in $\mathcal{H}_n$ with $n \geq 4$. Assume that X_1 is generic and that there exists an $\mathbb{H}$-compatible orthogonal matrix Q_1 satisfying* (a), (b), *and* (c) *in Lemma* 3.13 *with an additional condition that* (d) *in Lemma* 3.15 *holds for $H_1 = (Q_1^\top X_2 Q_1)_{[2,3]}$ and $H_2 = (Q_1^\top X_2 Q_1)_{[2,4]}$. Then it holds that $\langle X_1, X_2\rangle = \mathcal{H}_n$.*

Proof. Define $Y_h = Q_1^\top X_h Q_1$ for $h = 1, 2$. Let A be a matrix such that $Y_h A = A Y_h$ for $h = 1, 2$. By Lemma 3.13 (ii), $A = I_n \otimes A_1$ for some matrix A_1 of order four. By comparing the $[2,3]$-blocks and $[2,4]$-blocks of $Y_2 A$ and $A Y_2$, respectively, we have $H_1 A_1 = A_1 H_1$ and $H_2 A_1 = A_1 H_2$. Since the pair of H_1 and H_2 satisfy the condition (d) of Lemma 3.15, we obtain $A_1 \in \mathcal{W}$. This means that $A \in I_n \otimes \mathcal{W}$, and hence $\langle Y_1, Y_2\rangle' \subseteq I_n \otimes \mathcal{W}$. Thus $\langle X_1, X_2\rangle \supseteq \mathcal{H}_n$ by Lemma 2.2. □

Lemma 3.23. *Assume that* $\operatorname{span}\{I_n, A_1, \ldots, A_N\} = \mathcal{H}_n \cap \mathcal{S}_{4n}$ *with* $n \geq 4$*. Then there exists an open dense subset* $R \subseteq \mathbb{R}^{2N}$ *such that for any* $(r_1, r_2) \in R$ *with* $r_i \in \mathbb{R}^N$ *for* $i = 1, 2$*, it holds that* $\langle A(r_1), A(r_2)\rangle = \mathcal{H}_n$*.*

3.5 Proof of Theorem 3.1

We can prove Theorem 3.1 by combining Theorem 2.1 with Lemma 3.4 for $\mathcal{M}_n$, Lemmas 3.9 and 3.11 for $\mathcal{C}_n$, and Lemmas 3.18, 3.21, and 3.23 for $\mathcal{H}_n$. It follows from Theorem 2.1 that there exists an orthogonal matrix P such that

$$P^\top A_h P = \bigoplus_{j=1}^{\ell} (I_{m_j} \otimes B_j^h)$$

with some $B_j^h \in \mathcal{T}_j$ for $j = 1, \ldots, \ell$ and $h = 1, \ldots, N$. Since $A_1, \ldots, A_N$ are symmetric matrices, $\mathcal{T}_j$ is neither $\mathcal{C}_1$ nor $\mathcal{H}_1$.

Define $A'_h = P^\top A_h P$. For $(r_1, r_2, r_3, r_4) \in \mathbb{R}^{4N}$ with $r_i \in \mathbb{R}^N$ for $i = 1, \ldots, 4$, let $A'(r_i) = P^\top A(r_i) P$. Note that the matrix $*$-algebra generated by $A'(r_1), \ldots, A'(r_4)$ is the direct sum of the matrix $*$-algebras generated by the block matrices of $A'(r_1), \ldots, A'(r_4)$. Therefore, it follows that there exists an open dense subset $R \subseteq \mathbb{R}^{4N}$ such that for any $(r_1, r_2, r_3, r_4) \in R$ with $r_i \in \mathbb{R}^N$ for $i = 1, \ldots, 4$, we have

$$\langle A'(r_1), A'(r_2), A'(r_3), A'(r_4)\rangle = \bigoplus_{j=1}^{\ell} (I_{m_j} \otimes \mathcal{T}_j).$$

This implies that

$$\langle A(r_1), A(r_2), A(r_3), A(r_4)\rangle = \mathcal{T}.$$

Thus the statement of Theorem 3.1 is proved.

4 Concluding Remarks

Remark 4.1. It follows from Theorem 3.1 that a matrix $*$-algebra having no $\mathcal{C}_1$ and $\mathcal{H}_1$ as irreducible components can be generated by symmetric matrices. Thus the following corollary holds.

Corollary 4.1. *A matrix $*$-algebra $\mathcal{T}$ is generated by some symmetric matrices if and only if the decomposition of $\mathcal{T}$ in Theorem 2.1 has neither $\mathcal{C}_1$ nor $\mathcal{H}_1$ as an irreducible component $\mathcal{T}_j$.*

Remark 4.2. For an algebra, the *one and a half generation* property is the property that every non-zero element can be completed to a pair of elements that generate the algebra. It is known that this property holds for simple Lie algebras over the complex field [9] and a certain class of an algebraically closed field of finite characteristic [3]. The proof of Theorem 3.1 implies that matrix $*$-algebras over the real field satisfy such kind of property, i.e., every symmetric matrix (which is not a scalar multiple of the identity matrix) can be completed to a tuple of four symmetric matrices that generate the matrix $*$-algebra. Indeed, assume that a matrix $*$-algebra is $\mathcal{M}_n$ (the other cases follow in a similar way). Then, for a given symmetric matrix X_2, we can take a generic symmetric matrix X_1 diagonalized by an orthogonal matrix satisfying (a) and (b) in Lemma 3.3.

Remark 4.3. The proof of Theorem 3.1 can be adopted to matrix $*$-algebras over the complex field $\mathbb{C}$. It is known that a matrix $*$-algebra over $\mathbb{C}$ can be decomposed into the direct sum of

$I_m \otimes \mathcal{M}_p(\mathbb{C})$ for some m and p, where $\mathcal{M}_p(\mathbb{C})$ is the set of matrices of order p over the complex field. See, e.g., [2, 5] for a detailed proof. Hence we only have to discuss the case of $\mathcal{M}_n(\mathbb{C})$. Since the proof of Lemma 3.4 works even when we replace the transpose "$\top$" by the complex conjugate "$*$" and "orthogonal" by "unitary," we have the following theorem.

Theorem 4.2. *Let $\mathcal{T}$ be a matrix $*$-algebra over the complex field, generated by Hermitian matrices $A_1, \ldots, A_N$. Assume that* $\mathrm{span}\{I_n, A_1, \ldots, A_N\} = \mathcal{T} \cap \mathcal{S}_n(\mathbb{C})$*, where $\mathcal{S}_n(\mathbb{C})$ is the set of Hermitian matrices in $\mathcal{M}_n(\mathbb{C})$. Then there exists an open dense subset $R \subseteq \mathbb{R}^{2N}$ such that for any $(r_1, r_2) \in R$ with $r_i \in \mathbb{R}^N$ for $i = 1, 2$, it holds that*

$$\langle A(r_1), A(r_2) \rangle = \mathcal{T}.$$

Acknowledgement

This research is partially supported by the Aihara Project, the FIRST program from JSPS and by Global COE Program "The research and training center for new development in mathematics" from MEXT.

References

[1] Aiura, D., Kakimura, N., and Murota, K., A bifurcation analysis method using numerical block-diagonalization of matrix $*$-algebras, manuscript.

[2] Bachoc, C., Gijswijt, D., Schrijver, A., and Vallentin, F., Invariant semidefinite programs, *Handbook of Semidefinite, Conic, and Polynomial Optimization*, Anjos, M.F., and Lasserre, J.B., Eds., Springer-Verlag, 2011, 219–270.

[3] Bois, J.-M., Generators of simple Lie algebras in arbitrary characteristics, *Mathematische Zeitschrift*, **262**, 715–741, 2009.

[4] de Klerk, E., Dobre, C., and Pasechnik, D.V., Numerical block diagonalization of matrix $*$-algebras with application to semidefinite programming. *Mathematical Programming*, 2011, to appear.

[5] Gijswijt, D., Matrix Algebras and Semidefinite Programming Techniques for Codes, PhD thesis, University of Amsterdam, the Netherlands, 2005. Available at `http://staff.science.uva.nl/g̃ijswijt/promotie/thesis.pdf`.

[6] Guralnick, R., Kantor, W., Probabilistic generation of finite simple groups. *Journal of Algebra*, **234** (2), 743–792, 2000.

[7] Healey, T.J., A group-theoretic approach to computational bifurcation problems with symmetry. *Computer Methods in Applied Mechanics and Engineering*, **67** (3), 257–295, 1988.

[8] Ikeda, K., and Murota, K., *Imperfect Bifurcation of Structures and Materials — Engineering Use of Group-Theoretic Bifurcation Theory, 2nd ed.*, Springer-Verlag, 2010.

[9] Ionescu, T., On the generators of semi-simple Lie algebras, *Linear Algebra and Its Applications*, **15** (3), 271–292, 1976.

[10] Kojima, M., Kojima, S., and Hara, S., Linear algebra for semidefinite programming. Research Report B-290 (1994), Tokyo Institute of Technology. Also in: RIMS Kokyuroku 1004 (1997), 1–23, Kyoto University.

[11] Laffey, T.J., Simultaneous reduction of sets of matrices under similarity, *Linear Algebra and Its Applications*, **84**, 123–138, 1986.

[12] Maehara, T., and Murota, K., A numerical algorithm for block-diagonal decomposition of matrix $*$-algebras with general irreducible components. *Japan Journal of Industrial and Applied Mathematics*, **27** (2), 263–293, 2010.

[13] Maehara, T., and Murota, K., Error-controlling algorithm for simultaneous block-diagonalization and its application to independent component analysis. *JSIAM Letters*, **2**, 131–134, 2010.

[14] Maehara, T., and Murota, K., Algorithm for error-controlled simultaneous block-diagonalization of matrices. *SIAM Journal on Matrix Analysis and Applications*, **32** (2), 605–620, 2011.

[15] Murota, K., Kanno, Y., Kojima, M., and Kojima, S., A numerical algorithm for block-diagonal decomposition of matrix $*$-algebras with application to semidefinite programming. *Japan Journal of Industrial and Applied Mathematics*, **27** (1), 125–160, 2010.

[16] Wedderburn, J.H.M., On hypercomplex numbers, *Proc. London Math. Soc.*, **6** (1907), 77–118.

[17] Wedderburn, J.H.M., *Lectures on Matrices*, American Mathematical Society, New York, 1934; Dover, Mineola, N.Y., 2005.