数理解析研究所講究録
1004 巻 1997 年 1-23

Linear Algebra for Semidefinite Programming

Graduate School of Information Science and Engineering
Tokyo Institute of Technology, Masakazu Kojima
Graduate School of Information Science and Engineering
Tokyo Institute of Technology, Sadayoshi Kojima
Interdisciplinary Graduate School of Science and Engineering
Tokyo Institute of Technology, Shinji Hara

1. Introduction.

There are numerous variations and extensions of primal-dual interior-point algorithms for linear programs, convex quadratic programs, linear complementarity problems, convex programs and nonlinear complementarity problems ([8, 9, 10, 11, 13, 14, 17, 18, 19, 20, 24, 26, 29], etc.). A common basic idea behind the algorithms in this class is "moving in a Newton direction for approximating a point on the central trajectory at each iteration." Among others, primal-dual infeasible-interior-point algorithms are known to solve large scale practical linear programs very efficiently ([14, 15, 16],etc.). In their recent paper [12], Kojima, Shindoh and Hara extended primal-dual interior-point algorithms to SDPs (semidefinite programs) and monotone SDLCPs (semidefinite linear complementarity problems) in real symmetric matrices. See also [2]. This paper is motivated by

(a) further extensions of interior-point algorithms to more general SDPs and SDLCPs in real symmetric matrices, complex Hermitian matrices and quaternion Hermitian matrices, and
(b) a unified treatment of those possible extensions.

There is another important class of interior-point algorithms which are founded on the theory of self-concordance [21]. From the papers [6, 22], we know that algorithms in this class cover SDPs not only in real symmetric matrices but also in complex Hermitian matrices and quaternion Hermitian matrices. Hence the two issues (a) and (b) above have been settled there. The class of primal-dual interior-point algorithms which we are concerned with is closely related to the class of interior-point algorithms founded on the theory of self-concordance. For example, the central trajectory which has been playing an essential role in the former class can be characterized as the set of minimizers of the primal-dual logarithmic barrier function = a special case of self-concordant barrier functions (see [9, 17]), and primal-dual potential reduction algorithms ([8, 11, 18], etc.) utilize the logarithmic potential function = a special case of self-concordant potential functions. Such close relationships support the issue (a) in the class of primal-dual interior-point algorithms. A substantial difference, however, lies in their search directions. Roughly speaking, we employ as a search direction in the former class of interior-point algorithms "a Newton direction toward the central trajectory represented in terms of a system of equations," while we apply Newton's method to the minimization of "the objective function of the problem to be solved (or the duality gap) + a self-concordant barrier function" over the interior of the feasible region to get a search direction in the latter class of interior-point algorithms. When we deal with SDPs, this difference in search directions is critical; the minimization problem used in the latter class always yields a consistent search direction, but we need an essential modification in a usual Newton direction toward the central trajectory in the former class because it does not necessarily exist (see [2, 12]). Therefore it seems difficult to rely on the theory of self-concordance to settle the issues (a) and (b) in the class of primal-dual interior point algorithms.

Let $\mathcal{M}_n(\mathbb{K})$ denote the set of $n \times n$ matrices with elements in $\mathbb{K}$, where $\mathbb{K}$ represents the field $\mathbb{R}$ of real numbers, the field $\mathbb{C}$ of complex numbers or the (noncommutative) field $\mathbb{H}$ of quaternion numbers.

Let $n_1, n_2, \ldots n_\ell$ be positive integers such that $n = n_1 + n_2 + \cdots + n_\ell$. Consider the set $\mathcal{T}$ of $n \times n$ block diagonal real matrices

$$\boldsymbol{A} = \text{diag}\ (\boldsymbol{A}_{11}, \boldsymbol{A}_{22}, \ldots, \boldsymbol{A}_{\ell\ell}) = \begin{pmatrix} \boldsymbol{A}_{11} & \boldsymbol{O} & \cdots & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{A}_{22} & \cdots & \boldsymbol{O} \\ \cdot & \cdot & \cdots & \cdot \\ \boldsymbol{O} & \boldsymbol{O} & \cdots & \boldsymbol{A}_{\ell\ell} \end{pmatrix} \in \mathcal{M}_n(\mathbb{R}),$$

where $\boldsymbol{A}_{ii} \in \mathcal{M}_{n_i}(\mathbb{R})$ $(i = 1, 2, \ldots, \ell)$. We may identify the set $\mathcal{T}$ of $n \times n$ block diagonal real matrices with the direct sum of $\mathcal{M}_{n_i}(\mathbb{R})$ $(i = 1, 2, \ldots, \ell)$;

$$\mathcal{M}_{n_1}(\mathbb{R}) \oplus \mathcal{M}_{n_2}(\mathbb{R}) \oplus \cdots \oplus \mathcal{M}_{n_\ell}(\mathbb{R}).$$

Specifically, if $\ell = n$ and $n_i = 1$ $(i = 1, 2, \ldots, n)$ then $\mathcal{T}$ turns out to be the n-dimensional Euclidean space $\mathbb{R}^n$.

Apparently the set $\mathcal{T}$ of block diagonal real matrices satisfies the conditions below if we take $\mathbb{K} = \mathbb{R}$.

(i) $\mathcal{T}$ forms a subring of $\mathcal{M}_n(\mathbb{K})$ with the usual addition $\boldsymbol{A} + \boldsymbol{B}$ and multiplication $\boldsymbol{AB}$ of matrices $\boldsymbol{A},\ \boldsymbol{B} \in \mathcal{M}_n(\mathbb{K})$; specifically the zero matrix $\boldsymbol{O}$ and the identity matrix $\boldsymbol{I}$ belong to $\mathcal{T}$.

(ii) $\mathcal{T}$ is an $\mathbb{R}$-module, *i.e.*, a vector space over the field $\mathbb{R}$; $\alpha\boldsymbol{A} + \beta\boldsymbol{B} \in \mathcal{T}$ for every $\alpha,\ \beta \in \mathbb{R}$ and $\boldsymbol{A},\ \boldsymbol{B} \in \mathcal{T}$,

(iii) $\boldsymbol{A}^* \in \mathcal{T}$ if $\boldsymbol{A} \in \mathcal{T}$, where $\boldsymbol{A}^*$ denotes the conjugate transpose of $\boldsymbol{A} \in \mathcal{M}_n(\mathbb{K})$.

It is a subset $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K})$ satisfying these conditions that we will focus our attention in this paper. We call $\mathcal{T}$ *a subalgebra of* $\mathcal{M}_n(\mathbb{K})$ *over the field* $\mathbb{R}$ if it satisfies the conditions (i) and (ii), and simply *a subalgebra* if it is a subalgebra of $\mathcal{M}_n(\mathbb{K})$ for $\mathbb{K} = \mathbb{R},\ \mathbb{C}$ or $\mathbb{H}$ and for some n. We call $\mathcal{T}$ *a *-subalgebra* if it satisfies the conditions (i), (ii) and (iii). For example, the set of $n \times n$ lower triangular real matrices forms a subalgebra of $\mathcal{M}_n(\mathbb{R})$ but it is not a *-subalgebra. Obviously $\mathcal{M}_n(\mathbb{K})$ is a *-subalgebra. It should be noted that we always employ a real number $\alpha \in \mathbb{R}$ with which we perform the scalar multiple $\alpha\boldsymbol{A}$ of $\boldsymbol{A} \in \mathcal{M}_n(\mathbb{K})$ in the condition (ii) even when $\mathbb{K} = \mathbb{C}$ or $\mathbb{K} = \mathbb{H}$. To make this feature clear, we write $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$ instead of $\mathcal{M}_n(\mathbb{K})$, and we call it *a *-algebra* (over the field $\mathbb{R}$). Thus the dimension of $\mathcal{M}_n(\mathbb{C}, \mathbb{R})$ and $\mathcal{M}_n(\mathbb{H}, \mathbb{R})$ are $2n^2$ and $4n^2$, respectively.

For every *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$, we use the notation $\mathcal{T}^h$ to denote the set of all Hermitian matrices in $\mathcal{T}$; *i.e.*, $\mathcal{T}^h = \{\boldsymbol{A} \in \mathcal{T} : \boldsymbol{A}^* = \boldsymbol{A}\}$. Obviously $\mathcal{T}^h$ forms a sub $\mathbb{R}$-module of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$ but it is not a subalgebra in general. Assume that $\boldsymbol{A} \in \mathcal{M}_n(\mathbb{K}, \mathbb{R})^h$. The notation $\boldsymbol{A} \succeq \boldsymbol{O}$ (resp., $\boldsymbol{A} \succ \boldsymbol{O}$) means that $\boldsymbol{A}$ is positive semi-definite, *i.e.*, $\boldsymbol{x}^*\boldsymbol{A}\boldsymbol{x} \geq 0$ for every $\boldsymbol{x} \in \mathbb{K}^n$ (resp., positive definite, *i.e.*, $\boldsymbol{x}^*\boldsymbol{A}\boldsymbol{x} > 0$ for every nonzero $\boldsymbol{x} \in \mathbb{K}^n$).

Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$, and let $A_i \in \mathcal{T}^h$ and $b_i \in \mathbb{R}$ $(i = 0,1,2,\ldots,m)$. We are concerned with an SDP (semidefinite program) in $\mathcal{T}$ and its dual

$$\left.\begin{array}{lll} (P) & \text{minimize} & A_0 \bullet X \\ & \text{subject to} & A_i \bullet X = b_i \ (i = 1,2,\ldots,m) \\ & & X \succeq O, \ X \in \mathcal{T}^h. \end{array}\right\}$$

$$\left.\begin{array}{lll} (D) & \text{maximize} & \sum_{i=1}^m b_i z_i \\ & \text{subject to} & \sum_{i=1}^m A_i z_i + Y = A_0, \\ & & Y \succeq O, \ Y \in \mathcal{T}^h. \end{array}\right\}$$

Here $A \bullet B$ stands for the inner product of matrices A and B in the $\mathbb{R}$-module $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ whose definition will be given in the next section. Specifically, the inner product of matrices A and B in $\mathcal{M}_n(\mathbb{R}) = \mathcal{M}_n(\mathbb{R},\mathbb{R})$ turns out to be the standard one, *i.e.*, the trace of $A^T B$. The formulation of the primal-dual pair of SDPs above covers an equality standard form LP (linear program) and its dual in the Euclidean space $\mathbb{R}^n$ when

$$\mathcal{T} = \mathcal{M}_1(\mathbb{R}) \oplus \mathcal{M}_1(\mathbb{R}) \oplus \cdots \oplus \mathcal{M}_1(\mathbb{R}),$$

and a usual SDP and its dual in the entire matrix-algebra $\mathcal{M}_n(\mathbb{R})$ of $n \times n$ real matrices when $\mathcal{T} = \mathcal{M}_n(\mathbb{R})$ ([1, 2, 4, 22, 21, 27],etc.).

We show a simple example of an SDP in a *-subalgebra. Let

$$N(z) = N_0 + \sum_{j=1}^m z_j N_j \quad \text{for every } z = (z_1, z_2, \ldots, z_m)^T \in \mathbb{R}^m,$$

where N_j $(j = 0,1,\ldots,m)$ are given $k \times \ell$ complex matrices. Consider the problem

$$\begin{array}{l} \text{minimize } \|N(z)\| \\ \text{subject to } \|z\| \leq 1. \end{array}$$

Here $\|\cdot\|$ denotes the 2-norm of vectors and matrices;

$$\begin{aligned} \|u\| &= \left(\sum_{j=1}^p u_j \bar{u}_j\right)^{1/2} \quad \text{for every } u = (u_1, u_2, \ldots, u_p)^T \in \mathbb{C}^p, \\ \|N\| &= \max\left\{\|Nu\| : \|u\| = 1, \ u \in \mathbb{C}^\ell\right\} \text{ for every } k \times \ell \text{ matrix } N. \end{aligned}$$

If we define

$$H(z, z_{m+1}) = \operatorname{diag}\left(\begin{pmatrix} z_{m+1} I & N(z) \\ N(z)^* & z_{m+1} I \end{pmatrix}, \begin{pmatrix} I & z \\ z^T & 1 \end{pmatrix}\right) \text{ for every } (z, z_{m+1})^T \in \mathbb{R}^{m+1},$$

we can reformulate the problem above as

$$\begin{array}{ll} \text{maximize} & -z_{m+1} \\ \text{subject to} & Y = H(z, z_{m+1}), \\ & Y \succeq O, \ Y \in \mathcal{T}^h. \end{array}$$

Here

$$\mathcal{T} = \mathcal{M}_{k+\ell}(\mathbb{C},\mathbb{R}) \oplus \mathcal{M}_{m+1}(\mathbb{R}).$$

Thus we obtain a dual form SDP in a *-subalgebra $\mathcal{T}$. See [1, 2, 4, 23], etc. for various applications of SDPs.

We are also concerned with a monotone SDLCP (semidefinite linear complementarity problem) in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$. Let q denote the dimension of the $\mathbb{R}$-module $\mathcal{T}^h$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$. The monotone SDLCP in $\mathcal{T}$ is defined as the problem of finding an $(\boldsymbol{X},\boldsymbol{Y}) \in \mathcal{T}^h \times \mathcal{T}^h$ such that

$$(\boldsymbol{X},\boldsymbol{Y}) \in \mathcal{F} \equiv \mathcal{F}_0 + (\boldsymbol{X}_0,\boldsymbol{Y}_0), \ \boldsymbol{X} \succeq \boldsymbol{O}, \ \boldsymbol{Y} \succeq \boldsymbol{O} \ \text{ and } \boldsymbol{X} \bullet \boldsymbol{Y} = 0, \tag{1}$$

where $(\boldsymbol{X}_0,\boldsymbol{Y}_0) \in \mathcal{T}^h \times \mathcal{T}^h$, and $\mathcal{F}_0 \subset \mathcal{T}^h \times \mathcal{T}^h$ is a q-dimensional sub $\mathbb{R}$-module of $\mathcal{M}_n(\mathbb{K},\mathbb{R}) \times \mathcal{M}_n(\mathbb{K},\mathbb{R})$ satisfying the monotonicity

$$d\boldsymbol{X} \bullet d\boldsymbol{Y} \geq 0 \ \text{ if } \ (d\boldsymbol{X}, d\boldsymbol{Y}) \in \mathcal{F}_0. \tag{2}$$

The monotone SDLCP in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ simultaneously covers monotone LCPs in $\mathbb{R}^n$ (see, for example, [5, 8]), and monotone SDLCPs in $\mathcal{M}_n(\mathbb{R})$, $\mathcal{M}_n(\mathbb{C},\mathbb{R})$ and $\mathcal{M}_n(\mathbb{H},\mathbb{R})$. The monotone SDLCP in $\mathcal{M}_n(\mathbb{R})$ was first introduced by Kojima, Shindoh and Hara [12].

In Section 2, we present a common fundamental algebraic structure of $\mathcal{M}_n(\mathbb{R})$, $\mathcal{M}_n(\mathbb{C},\mathbb{R})$ and $\mathcal{M}_n(\mathbb{H},\mathbb{R})$.

In Section 3, we state (without proof) the weak and the strong duality on the SDPs (P) and (D) in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ (Theorem 3.1), and derive a monotone SDLCP in $\mathcal{T}$ from them.

Section 4 is devoted to brief discussions on adaptation of interior-point methods given for the monotone SDLCP in $\mathcal{M}_n(\mathbb{R})$ by Kojima, Shindoh and Hara [12] to the monotone SDLCP in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$. The theoretical results, interior-point methods and their complexity analysis presented in the paper Kojima-Shindoh-Hara [12] remain valid if we replace $\mathcal{M}_n(\mathbb{R})$ by $\mathcal{T}$ and make appropriate minor modifications. Specifically, we state the existence of the central trajectory in the SDLCP in $\mathcal{T}$ (without proof), the existence of the Newton direction towards the central trajectory (with proof) and the Generic IP Method for the monotone SDLCP in $\mathcal{T}$. Their interior-point methods are based on the primal-dual interior point method [9, 17, 19, 26] for linear programs in the Euclidean space $\mathbb{R}^n$. Strictly speaking, however, their methods are not extensions of the primal-dual interior point method simply because the monotone SDLCP in $\mathcal{M}_n(\mathbb{R})$ covers neither the standard monotone LCP in $\mathbb{R}^n$ nor linear programs in $\mathbb{R}^n$. Now, using *-subalgebras of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$, we can handle the monotone SDLCP and interior-point methods for solving it in $\mathbb{R}^n$, $\mathcal{M}_n(\mathbb{R})$, $\mathcal{M}_n(\mathbb{C},\mathbb{R})$ and $\mathcal{M}_n(\mathbb{H},\mathbb{R})$ simultaneously.

Section 5 studies theoretical characterization of *-subalgebras of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$.

In Section 5.1, we introduce "a faithful *-representation $(\tilde{\boldsymbol{\rho}},\mathbb{R}^{dn})$" of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ where $d = 1$, 2 and 4 if $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$, respectively. The mapping $\tilde{\boldsymbol{\rho}}$ is a homomorphism from $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ into $\mathcal{M}_{dn}(\mathbb{R})$ that transforms each *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ into a *-subalgebra $\mathcal{T}' = \tilde{\boldsymbol{\rho}}(\mathcal{T})$ of $\mathcal{M}_{dn}(\mathbb{R})$ having the same algebraic structure as $\mathcal{T}$, so that we may restrict ourselves to *-subalgebras of $\mathcal{M}_n(\mathbb{R})$ when we classify all *-subalgebras in Section 5.2. Furthermore the faithful *-representation $(\tilde{\boldsymbol{\rho}},\mathbb{R}^{dn})$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ makes it possible to convert any SDP and any monotone SDLCP in a *-subalgebra of $\mathcal{M}_n(\mathbb{C},\mathbb{R})$ (or $\mathcal{M}_n(\mathbb{H},\mathbb{R})$) into some SDP and some monotone SDLCP in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_{2n}(\mathbb{R})$ (or $\mathcal{M}_{4n}(\mathbb{R})$), respectively. The homomorphism $\tilde{\boldsymbol{\rho}}$ from $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ into $\mathcal{M}_{dn}(\mathbb{R})$ was utilized in the paper [3] where duality of general linear programs with real, complex and quaternion matrix variables was discussed.

In Section 5.2, we present a classification of *-subalgebras of $\mathcal{M}_n(\mathbb{R})$. The main results are roughly summarized as follows:

- There are exactly three types of "irreducible" *-subalgebras of $\mathcal{M}_n(\mathbb{R})$

$$\tilde{\boldsymbol{\rho}}(\mathcal{M}_n(\mathbb{R})) = \mathcal{M}_n(\mathbb{R}), \ \tilde{\boldsymbol{\rho}}(\mathcal{M}_{n/2}(\mathbb{C},\mathbb{R})) \ \text{ and } \tilde{\boldsymbol{\rho}}(\mathcal{M}_{n/4}(\mathbb{H},\mathbb{R})),$$

  where $(\tilde{\boldsymbol{\rho}},\mathbb{R}^n)$ is a faithful *-representation of $\mathcal{M}_{n/d}(\mathbb{K},\mathbb{R})$ given in Section 5.1 and $d =$ 1, 2, 4 when $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, respectively.

- Any *-subalgebra of $\mathcal{M}_n(\mathbb{R})$ is isomorphic to a direct sum of some $\mathcal{T}_i$ $(i = 1, 2, \ldots, \ell)$ such that each $\mathcal{T}_i$ belongs to one of the three types of irreducible *-subalgebras of $\mathcal{M}_m(\mathbb{R})$ for some m.

2. Fundamental Algebraic Structures of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$.

Let $\mathbb{K}$ represent the field $\mathbb{R}$ of real numbers, the field $\mathbb{C}$ of complex numbers or the (noncommutative) field $\mathbb{H}$ of quaternion numbers. We will regard $\mathbb{K}$ an $\mathbb{R}$-module, *i.e.*, a linear space over the field $\mathbb{R}$. To clarify this aspect, we write $\mathbb{K}(\mathbb{R})$. Apparently

$$\dim \mathbb{K}(\mathbb{R}) = \begin{cases} 1 & \text{if } \mathbb{K} = \mathbb{R}, \\ 2 & \text{if } \mathbb{K} = \mathbb{C}, \\ 4 & \text{if } \mathbb{K} = \mathbb{H}. \end{cases} \tag{3}$$

We endow the $\mathbb{R}$-module $\mathbb{K}(\mathbb{R})$ with an inner product

$$z^1 \cdot z^2 = \frac{\overline{z^1} z^2 + \overline{(\overline{z^1} z^2)}}{2} \in \mathbb{R}$$

of z^1 and z^2 in $\mathbb{K}(\mathbb{R})$. Here $\overline{z}$ denotes the conjugate of $z \in \mathbb{K}(\mathbb{R})$. More specifically,

$$\begin{aligned} \overline{z} &= z \ \text{ if } z \in \mathbb{R}, \\ \overline{z} &= v - iw \ \text{ if } z = v + iw \in \mathbb{C}, \\ \overline{z} &= v - iw - jx - ky \ \text{ if } z = v + iw + jx + ky \in \mathbb{H}, \\ z^1 \cdot z^2 &= z^1 z^2 \in \mathbb{R} \ \text{ if } z^1,\ z^2 \in \mathbb{R}, \\ z^1 \cdot z^2 &= v^1 v^2 + w^1 w^2 \in \mathbb{R} \ \text{ if } z^1 = v^1 + iw^1,\ z^2 = v^2 + iw^2 \in \mathbb{C}, \\ z^1 \cdot z^2 &= v^1 v^2 + w^1 w^2 + x^1 x^2 + y^1 y^2 \in \mathbb{R} \\ & \quad \text{if } z^1 = v^1 + iw^1 + jx^1 + ky^1,\ z^2 = v^2 + iw^2 + jx^2 + ky^2 \in \mathbb{H}. \end{aligned}$$

Here i, j and k satisfy

$$ii = jj = kk = -1,\ i = jk = -kj,\ j = ki = -ik,\ k = ij = -ji.$$

The definitions above naturally lead to the $\mathbb{R}$-module $\mathbb{K}(\mathbb{R})^n$ with the inner product

$$\boldsymbol{z}^1 \cdot \boldsymbol{z}^2 = \sum_{\ell=1}^{n} z^1_\ell \cdot z^2_\ell \in \mathbb{R} \tag{4}$$

for every $\boldsymbol{z}^1 = (z^1_1, \ldots, z^1_n)^T$, $\boldsymbol{z}^2 = (z^2_1, \ldots, z^2_n)^T \in \mathbb{K}(\mathbb{R})^n$. It follows from (3) that

$$\dim \mathbb{K}(\mathbb{R})^n = \begin{cases} n & \text{if } \mathbb{K} = \mathbb{R}, \\ 2n & \text{if } \mathbb{K} = \mathbb{C}, \\ 4n & \text{if } \mathbb{K} = \mathbb{H}. \end{cases}$$

Note that $\mathbb{R}(\mathbb{R})^n$ coincides with the n-dimensional Euclidean space $\mathbb{R}^n$ with the standard inner product $\boldsymbol{z}^1 \cdot \boldsymbol{z}^2 = (\boldsymbol{z}^1)^T \boldsymbol{z}^2$ of $\boldsymbol{z}^1$, $\boldsymbol{z}^2 \in \mathbb{R}^n$.

Each element $a \in \mathbb{K}$ induces a linear transformation in $\mathbb{K}(\mathbb{R})$ such that

$$z \in \mathbb{K}(\mathbb{R}) \to az \in \mathbb{K}(\mathbb{R}).$$

Thus we may regard the set of such linear transformations in $\mathbb{K}(\mathbb{R})$ as an $\mathbb{R}$-module, which we will denote by $\mathcal{M}_1(\mathbb{K},\mathbb{R})$. We define the inner product of a^1 and a^2 in the $\mathbb{R}$-module $\mathcal{M}_1(\mathbb{K},\mathbb{R})$ by

$$a^1 \bullet a^2 = \frac{(\dim \mathbb{K}(\mathbb{R}))\left(\overline{a^1}a^2 + \overline{(\overline{a^1}a^2)}\right)}{2} \tag{5}$$

or

$$\begin{aligned}
a^1 \bullet a^2 &= a^1a^2 \in \mathbb{R} \text{ if } a^1,\ a^2 \in \mathbb{R}, \\
a^1 \bullet a^2 &= 2(v^1v^2 + w^1w^2) \in \mathbb{R} \text{ if } a^1 = v^1 + iw^1,\ a^2 = v^2 + iw^2 \in \mathbb{C}, \\
a^1 \bullet a^2 &= 4(v^1w^2 + w^1w^2 + x^1x^2 + y^1y^2) \in \mathbb{R} \\
&\quad \text{if } a^1 = v^1 + iw^1 + jx^1 + ky^1,\ a^2 = v^2 + iw^2 + jx^2 + ky^2 \in \mathbb{H}.
\end{aligned}$$

It should be noted that elements in $\mathbb{K}$ have two distinct inner products "$\cdot$" (see (4)) and "$\bullet$" (see (5)); the former is used when we regard z^1, $z^2 \in \mathbb{K}$ as elements of $\mathbb{K}(\mathbb{R})$ while the latter is used when we regard a^1, $a^2 \in \mathbb{K}$ as elements of $\mathcal{M}_1(\mathbb{K},\mathbb{R})$. But the difference in values of the former and the latter inner products of two elements e^1, e^2 in $\mathbb{K}$ is a constant multiple;

$$e^1 \bullet e^2 = \dim \mathbb{K}(\mathbb{R}) e^1 \cdot e^2.$$

The use of these two distinct inner products will be necessary in Section 5.1 where we present a faithful *-representation $(\tilde{\rho}, \mathbb{R}^{dn})$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ which preserves the values of inner products in both $\mathbb{R}$-modules $\mathbb{K}^n$ and $\mathcal{M}_n(\mathbb{K},\mathbb{R})$. See the conditions (f) and (g) in Section 5.1.

Now we define $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ as the set of all matrices with elements in $\mathcal{M}_1(\mathbb{K},\mathbb{R})$. Then $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ forms *a *-algebra*, and each $\boldsymbol{A} \in \mathcal{M}_n(\mathbb{K},\mathbb{R})$ induces a linear transformation

$$\boldsymbol{z} \in \mathbb{K}(\mathbb{R})^n \to \boldsymbol{A}\boldsymbol{z} \in \mathbb{K}(\mathbb{R})^n$$

in the $\mathbb{R}$-module $\mathbb{K}(\mathbb{R})^n$. The inner product of two matrices $\boldsymbol{A}^1$ and $\boldsymbol{A}^2$ in $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ is given by

$$\boldsymbol{A}^1 \bullet \boldsymbol{A}^2 = \sum_{\ell=1}^{n}\sum_{p=1}^{n} a^1_{\ell p} \bullet a^2_{\ell p},$$

and the norm $\|\boldsymbol{A}\|$ of a matrix $\boldsymbol{A}$ in $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ by

$$\|\boldsymbol{A}\| = (\boldsymbol{A} \bullet \boldsymbol{A})^{1/2}.$$

Here $a_{\ell p}$ denotes the (ℓ,p)th element of a matrix $\boldsymbol{A} \in \mathcal{M}_n(\mathbb{K},\mathbb{R})$.

If $\boldsymbol{A} = [a_{\ell p}]$ is a matrix in $\mathcal{M}_n(\mathbb{K},\mathbb{R})$, its conjugate $\boldsymbol{A}^*$ is defined as

$$\boldsymbol{A} = \left(\overline{\boldsymbol{A}}\right)^T = \begin{pmatrix} \overline{a}_{11} & \overline{a}_{21} & \cdots & \overline{a}_{n1} \\ \overline{a}_{12} & \overline{a}_{22} & \cdots & \overline{a}_{n2} \\ \cdot & \cdot & \cdots & \cdot \\ \overline{a}_{1n} & \overline{a}_{2n} & \cdots & \overline{a}_{nn} \end{pmatrix}.$$

For each subset $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$, we use the notation $\mathcal{T}^h$ for the set of Hermitian matrices in $\mathcal{M}_n(\mathbb{K},\mathbb{R})$;

$$\mathcal{T}^h = \{\boldsymbol{A} \in \mathcal{T} : \boldsymbol{A}^* = \boldsymbol{A}\}.$$

Let $\boldsymbol{A} \in \mathcal{M}_n(\mathbb{K},\mathbb{R})^h$. Then we can easily verify that

$$\boldsymbol{z} \cdot \boldsymbol{A}\boldsymbol{z} = \boldsymbol{z}^*\boldsymbol{A}\boldsymbol{z} \text{ for every } \boldsymbol{z} \in \mathbb{K}(\mathbb{R})^n.$$

Therefore a Hermitian matrix $\boldsymbol{A} \in \mathcal{M}_n(I\!\!K, I\!\!R)^h$ is positive semi-definite or positive definite if and only if

$$\boldsymbol{z} \cdot \boldsymbol{A}\boldsymbol{z} \geq 0 \ \text{ for every } \boldsymbol{z} \in I\!\!K(I\!\!R)^n$$

or

$$\boldsymbol{z} \cdot \boldsymbol{A}\boldsymbol{z} > 0 \ \text{ for every nonzero } \boldsymbol{z} \in I\!\!K(I\!\!R)^n,$$

respectively.

3. Duality in SDPs.

This section presents a duality theorem on the SDPs (P) and (D) in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(I\!\!K, I\!\!R)$. We call an $\boldsymbol{X} \in \mathcal{M}_n(I\!\!K, I\!\!R)$ (resp., $(\boldsymbol{Y}, \boldsymbol{z}) \in \mathcal{M}_n(I\!\!K, I\!\!R) \times I\!\!R^m$) a feasible solution if it satisfies the constraints of (P) (resp., the constraints of (D)), and an interior feasible solution if in addition $\boldsymbol{X} \succ \boldsymbol{O}$ (resp., $\boldsymbol{Y} \succ \boldsymbol{O}$). We have the following duality theorem between the primal-dual pair of SDPs (P) and (D).

Theorem 3.1. *Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(I\!\!K, I\!\!R)$.*

(a) (Weak Duality) Let $\boldsymbol{X}$ and $(\boldsymbol{Y}, \boldsymbol{z})$ be feasible solutions of (P) and (D), respectively. Then

$$\boldsymbol{A}_0 \bullet \boldsymbol{X} - \sum_{i=1}^{m} b_i z_i = \boldsymbol{X} \bullet \boldsymbol{Y} \geq 0.$$

If $\boldsymbol{X} \bullet \boldsymbol{Y} = 0$ then $\boldsymbol{X}$ and $(\boldsymbol{Y}, \boldsymbol{z})$ are optimal solutions of (P) and (D), respectively.

(b) (Strong Duality) Suppose that there exist interior feasible solutions of (P) and (D). Then there exist optimal solutions $\boldsymbol{X}$ of (P) and $(\boldsymbol{Y}, \boldsymbol{z})$ of (D) such that

$$\boldsymbol{A}_0 \bullet \boldsymbol{X} - \sum_{i=1}^{m} b_i z_i = \boldsymbol{X} \bullet \boldsymbol{Y} = 0.$$

The assertion (a) (Weak Duality) can be verified easily. The assertion (b) (Strong Duality) follows from a more general result (Theorem 4.1), given in the next section, on the monotone SDLCP in a *-subalgebra of $\mathcal{M}_n(I\!\!K, I\!\!R)$. These results (a) and (b) are well-known when $\mathcal{T}$ is the real full matrix-algebra, *i.e.*, $\mathcal{T} = \mathcal{M}_n(I\!\!R)$. See, for example, [1, 4, 27].

Let $q = \dim \mathcal{T}^h$. Suppose that there exist interior feasible solutions $\boldsymbol{X}_0$ of (P) and $(\boldsymbol{Y}_0, \boldsymbol{z}_0)$ of (D) as assumed in (b) of Theorem 3.1. Define

$$\begin{aligned} \mathcal{F}_0 &\equiv \left\{ (d\boldsymbol{X}, d\boldsymbol{Y}) \in \mathcal{T}^h \times \mathcal{T}^h : \begin{array}{l} \boldsymbol{A}_i \bullet d\boldsymbol{X} = 0 \ (i = 1, 2, \ldots, m), \\ d\boldsymbol{Y} = -\sum_{i=1}^{m} \boldsymbol{A}_i z_i \ \text{ for some } \boldsymbol{z} \in I\!\!R^m \end{array} \right\}, \\ \mathcal{F} &\equiv \mathcal{F}_0 + (\boldsymbol{X}_0, \boldsymbol{Y}_0). \end{aligned}$$

Note that $\mathcal{F}$ can be rewritten as

$$\mathcal{F} = \left\{ (\boldsymbol{X}, \boldsymbol{Y}) \in \mathcal{T}^h \times \mathcal{T}^h : \begin{array}{l} \boldsymbol{A}_i \bullet \boldsymbol{X} = b_i \ (i = 1, 2, \ldots, m), \\ \boldsymbol{Y} = \boldsymbol{A}_0 - \sum_{i=1}^{m} \boldsymbol{A}_i z_i \ \text{ for some } \boldsymbol{z} \in I\!\!R^m \end{array} \right\}.$$

It is easily verified that $\mathcal{F}_0$ forms a q-dimensional sub $I\!\!R$-module of the $2q$-dimensional $I\!\!R$-module $\mathcal{T}^h \times \mathcal{T}^h$ such that

$$d\boldsymbol{X} \bullet d\boldsymbol{Y} = 0 \ \text{ for every } (d\boldsymbol{X}, d\boldsymbol{Y}) \in \mathcal{F}_0. \qquad (6)$$

This implies that $\mathcal{F}_0$ is monotone (see (2)). Obviously $\boldsymbol{X}$ and $(\boldsymbol{Y}, \boldsymbol{z})$ are feasible solutions of (P) and (D) if and only if

$$(\boldsymbol{X}, \boldsymbol{Y}) \in \mathcal{F} \equiv \mathcal{F}_0 + (\boldsymbol{X}_0, \boldsymbol{Y}_0), \ \boldsymbol{X} \succeq \boldsymbol{O} \ \text{ and } \boldsymbol{Y} \succeq \boldsymbol{O}.$$

Hence we see by Theorem 3.1 that $\boldsymbol{X}$ and $(\boldsymbol{Y}, \boldsymbol{z})$ are optimal solutions of SDPs (P) and (D) if and only if $(\boldsymbol{X}, \boldsymbol{Y})$ is a solution of the monotone SDLCP (1) in $\mathcal{T}$. Thus we have derived a monotone SDLCP in $\mathcal{T}^h$, which we will discuss in the next section, from the primal-dual pair of SDPs (P) and (D).

4. Monotone SDLCPs and Interior-Point Methods.

Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$, and let p and q denote the dimensions of $\mathcal{T}$ and $\mathcal{T}^h$, respectively. Recall that the monotone SDLCP in $\mathcal{T}$ has been defined as the problem of finding an $(\boldsymbol{X}, \boldsymbol{Y}) \in \mathcal{T}^h \times \mathcal{T}^h$ satisfying (1) and that $\mathcal{F}_0$ is a q-dimensional sub $\mathbb{R}$-module of the $2q$-dimensional $\mathbb{R}$-module $\mathcal{T}^h \times \mathcal{T}^h$ satisfying the monotonicity (2).

Let

$$\begin{aligned} \mathcal{F}_+ &= \{(\boldsymbol{X}, \boldsymbol{Y}) \in \mathcal{F} : \boldsymbol{X} \succeq \boldsymbol{O}, \ \boldsymbol{Y} \succeq \boldsymbol{O}\}, \\ \mathcal{F}_{++} &= \{(\boldsymbol{X}, \boldsymbol{Y}) \in \mathcal{F} : \boldsymbol{X} \succ \boldsymbol{O}, \ \boldsymbol{Y} \succ \boldsymbol{O}\}. \end{aligned}$$

We call $(\boldsymbol{X}, \boldsymbol{Y}) \in \mathcal{F}_+$ a feasible solution of the monotone SDLCP (1), and $(\boldsymbol{X}, \boldsymbol{Y}) \in \mathcal{F}_{++}$ an interior feasible solution of the monotone SDLCP (1).

The theorem below states the existence of the central trajectory under the assumption that $\mathcal{F}_{++} \neq \emptyset$. The theorem was established by Kojima, Shindoh and Hara for the case $\mathcal{T} = \mathcal{M}_n(\mathbb{R})$ in their paper [12]. The generalized theorem can be proved in a similar way as the original theorem, Theorem 3.1 of [12], and the proof is omitted here.

Theorem 4.1. *Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$ and $q = \dim \mathcal{T}^h$. Assume that the q-dimensional sub $\mathbb{R}$-module $\mathcal{F}_0$ is monotone and that $\mathcal{F}_{++} \neq \emptyset$.*

(i) *For every $\mu > 0$, there exists a unique $(\boldsymbol{X}(\mu), \boldsymbol{Y}(\mu)) \in \mathcal{F}_{++}$ such that $\boldsymbol{X}(\mu)\boldsymbol{Y}(\mu) = \mu \boldsymbol{I}$.*

(ii) *The set $\Gamma = \{(\boldsymbol{X}(\mu), \boldsymbol{Y}(\mu)) : \mu > 0\}$ forms a smooth trajectory. (We call Γ the central trajectory.)*

(iii) *$(\boldsymbol{X}(\mu), \boldsymbol{Y}(\mu))$ converges to a solution $(\boldsymbol{X}^*, \boldsymbol{Y}^*)$ of the SDLCP (1) as $\mu > 0$ tends to zero.*

Theorem 4.1 ensures that the monotone SDLCP (1) has a solution whenever $\mathcal{F}_{++} \neq \emptyset$, and we can derive (b) (Strong Duality) of Theorem 3.1 from Theorem 4.1.

Let $\mathcal{T}^{skew}$ denote the class of skew symmetric matrices contained in $\mathcal{T}$;

$$\mathcal{T}^{skew} = \{\boldsymbol{W} \in \mathcal{T} : \boldsymbol{W}^* = -\boldsymbol{W}\} = \{\boldsymbol{X} - \boldsymbol{X}^* : \boldsymbol{X} \in \mathcal{T}\}.$$

Obviously $\mathcal{T}^h$ and $\mathcal{T}^{skew}$ are sub $\mathbb{R}$-modules of $\mathcal{T}$ such that either of them is the orthogonal complement of the other in $\mathcal{T}$. That is,

- $\boldsymbol{V} \bullet \boldsymbol{W} = 0$ if $\boldsymbol{V} \in \mathcal{T}^h$ and $\boldsymbol{W} \in \mathcal{T}^{skew}$,
- every $\boldsymbol{X} \in \mathcal{T}$ can be represented as the sum $\boldsymbol{V} + \boldsymbol{W}$ of a unique pair of $\boldsymbol{V} \in \mathcal{T}^h$ and $\boldsymbol{W} \in \mathcal{T}^{skew}$.

Let $\tilde{\mathcal{F}}_0$ be a $(p-q)-$dimensional sub $\mathbb{R}$-module of the $2(p-q)-$dimensional $\mathbb{R}$-module $\mathcal{T}^{skew} \times \mathcal{T}^{skew}$. We impose $\tilde{\mathcal{F}}_0$ on the condition below:

Condition 4.2. $\tilde{\mathcal{F}}_0$ *is monotone, i.e.,*

$$\tilde{dX} \bullet \tilde{dY} \geq 0 \ \ \textit{for every} \ (\tilde{dX}, \tilde{dY}) \ \in \tilde{\mathcal{F}}_0.$$

For example, we can take

$$\tilde{\mathcal{F}}_0 = \{(t\boldsymbol{W}, (1-t)\boldsymbol{W}) : \boldsymbol{W} \in \mathcal{T}^{skew}\},$$

where $t \in [0,1]$ is an arbitrary constant. Let

$$\mathcal{T}^h_{++} = \{\boldsymbol{X} \in \mathcal{T}^h : \boldsymbol{X} \succ \boldsymbol{O}\}.$$

We now consider the Newton equation at $(\boldsymbol{X},\boldsymbol{Y}) \in \mathcal{T}^h_{++} \times \mathcal{T}^h_{++}$ for approximating a point $(\boldsymbol{X}',\boldsymbol{Y}') = (\boldsymbol{X}+d\boldsymbol{X}, \boldsymbol{Y}+d\boldsymbol{Y})$ on the central trajectory Γ:

$$\left.\begin{array}{l} (\boldsymbol{X}+d\boldsymbol{X}, \boldsymbol{Y}+d\boldsymbol{Y}) \in \mathcal{F}, \ (\tilde{dX}, \tilde{dY}) \in \tilde{\mathcal{F}}_0 \ \text{ and} \\ \boldsymbol{X}(d\boldsymbol{Y}+\tilde{dY}) + (d\boldsymbol{X}+\tilde{dX})\boldsymbol{Y} = \beta\mu\boldsymbol{I} - \boldsymbol{X}\boldsymbol{Y}. \end{array}\right\} \tag{7}$$

Here $\mu = \boldsymbol{X} \bullet \boldsymbol{Y}/n$ and $\beta \in [0,1]$ denotes *a search direction parameter.* We will see later that the Newton equation (7) has a unique solution $(d\boldsymbol{X}, d\boldsymbol{Y}, \tilde{dX}, \tilde{dY})$ for every $(\boldsymbol{X},\boldsymbol{Y}) \in \mathcal{T}^h_{++} \times \mathcal{T}^h_{++}$ and every $\beta \in [0,1]$.

Generic IP Method.

Step 0: Choose $(\boldsymbol{X}^0, \boldsymbol{Y}^0) \in \mathcal{T}^h_{++} \times \mathcal{T}^h_{++}$. Let $r = 0$.

Step 1: Let $(\boldsymbol{X},\boldsymbol{Y}) = (\boldsymbol{X}^r, \boldsymbol{Y}^r)$ and $\mu = \boldsymbol{X} \bullet \boldsymbol{Y}/n$.

Step 2: Choose *a direction parameter* $\beta \in [0,1]$.

Step 3: Compute a solution $(d\boldsymbol{X}, d\boldsymbol{Y}, \tilde{dX}, \tilde{dY})$ of the system (7) of equations.

Step 4: Choose *a step size parameter* $\alpha \geq 0$ such that

$$(\boldsymbol{X}^{r+1}, \boldsymbol{Y}^{r+1}) = (\boldsymbol{X},\boldsymbol{Y}) + \alpha(d\boldsymbol{X}, d\boldsymbol{Y}) \in \mathcal{T}^h_{++} \times \mathcal{T}^h_{++}.$$

Step 5: Replace $r+1$ by r, and go to Step 1.

The Newton equation (7) and the Generic IP Method above are essentially the same as the original ones proposed by Kojima, Shindoh and Hara in their paper [12] except that we have replaced the real full matrix-algebra $\mathcal{M}_n(\mathbb{R})$ by a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K},\mathbb{R})$ (or $\mathcal{M}_n(\mathbb{R})^h$ by $\mathcal{T}^h$). As special cases of the Generic IP Method, Kojima, Shindoh and Hara [12] presented a central trajectory following method, a potential reduction method and an infeasible-interior-point potential-reduction method. These three methods are based on the interior-point methods given in the papers [10], [11] and [18] for the monotone LCP in $\mathbb{R}^n$, respectively. Once we establish the existence of the Newton direction towards the central trajectory, all the methods and their convergence analysis remain valid for the monotone SDLCP in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K}.\mathbb{R})$ without any substantial change. The details are omitted here.

In the remainder of the section, we give a proof of the existence of the Newton direction towards the central trajectory, *i.e.*, a solution $(d\boldsymbol{X}, d\boldsymbol{Y}, \tilde{dX}, \tilde{dY})$ of the system (7) of equations. We are concerned with a little more general system of equations than (7):

$$\left.\begin{array}{l}(\boldsymbol{X}+d\boldsymbol{X},\boldsymbol{Y}+d\boldsymbol{Y})\in\mathcal{F},\ (\tilde{d\boldsymbol{X}},\tilde{d\boldsymbol{Y}})\in\tilde{\mathcal{F}}_0\ \text{ and}\\ \boldsymbol{X}(d\boldsymbol{Y}+\tilde{d\boldsymbol{Y}})+(d\boldsymbol{X}+\tilde{d\boldsymbol{X}})\boldsymbol{Y}=\boldsymbol{Q},\end{array}\right\} \qquad (7)'$$

where $\boldsymbol{Q}$ is an arbitrary constant matrix in $\mathcal{T}$. If we take $\boldsymbol{Q}=\beta\boldsymbol{I}-\boldsymbol{X}\boldsymbol{Y}\in\mathcal{T}$, (7)' coincides with (7). The theorem below is an extension of Theorem 4.2 of [12].

Theorem 4.3. *For every $(\boldsymbol{X},\boldsymbol{Y})\in\mathcal{T}^h_{++}\times\mathcal{T}^h_{++}$, the system (7)' of equations has a unique solution $(d\boldsymbol{X},d\boldsymbol{Y},\tilde{d\boldsymbol{X}},\tilde{d\boldsymbol{Y}})$.*

Proof: Let $\tilde{q}=p-q$. Let $\{(\boldsymbol{M}^i,\boldsymbol{N}^i)\in\mathcal{T}^h\times\mathcal{T}^h\ (i=1,2,\ldots,q)\}$ be a basis of the q-dimensional $I\!R$-module $\mathcal{F}_0$, $\{(\tilde{\boldsymbol{M}}^j,\tilde{\boldsymbol{N}}^j)\in\mathcal{T}^{skew}\times\mathcal{T}^{skew}\ (j=1,2,\ldots,\tilde{q})\}$ a basis of the $\tilde{q}$-dimensional $I\!R$-module $\tilde{\mathcal{F}}_0$, and $(\boldsymbol{X}^0,\boldsymbol{Y}^0)\in\mathcal{F}$. Then the first relation of the Newton equation (7)' can be written as

$$(\boldsymbol{X}+d\boldsymbol{X},\boldsymbol{Y}+d\boldsymbol{Y}) = (\boldsymbol{X}^0,\boldsymbol{Y}^0)+\sum_{i=1}^{q}c_i(\boldsymbol{M}^i,\boldsymbol{N}^i),$$

hence

$$d\boldsymbol{X} = \boldsymbol{X}^0-\boldsymbol{X}+\sum_{i=1}^{q}c_i\boldsymbol{M}^i,$$

$$d\boldsymbol{Y} = \boldsymbol{Y}^0-\boldsymbol{Y}+\sum_{i=1}^{q}c_i\boldsymbol{N}^i,$$

where c_i $(i=1,2,\ldots,q)$ are real variables. With new variables $\tilde{c}_j$ $(j=1,2,\ldots,\tilde{q})$, we also rewrite the second relation of (7)' as

$$(\tilde{d\boldsymbol{X}},\tilde{d\boldsymbol{Y}}) = \sum_{j=1}^{\tilde{q}}\tilde{c}_j(\tilde{\boldsymbol{M}}^j,\tilde{\boldsymbol{N}}^j).$$

Now the last equation in (7)' is reduced to

$$\sum_{i=1}^{q}c_i(\boldsymbol{X}\boldsymbol{N}^i+\boldsymbol{M}^i\boldsymbol{Y})+\sum_{j=1}^{\tilde{q}}\tilde{c}_j(\boldsymbol{X}\tilde{\boldsymbol{N}}^j+\tilde{\boldsymbol{M}}^j\boldsymbol{Y})=\boldsymbol{Q}-\boldsymbol{X}(\boldsymbol{Y}^0-\boldsymbol{Y})-(\boldsymbol{X}^0-\boldsymbol{X})\boldsymbol{Y}.$$

Thus we have only to show that the system of linear equations above in $p=q+\tilde{q}$ variables c_i $(i=1,2,\ldots,q)$ and $\tilde{c}_j$ $(j=1,2,\ldots,\tilde{q})$ has a unique solution. We note that all the p coefficient matrices

$$(\boldsymbol{X}\boldsymbol{N}^i+\boldsymbol{M}^i\boldsymbol{Y})\ \ (i=1,2,\ldots,q)\quad\text{and}\quad(\boldsymbol{X}\tilde{\boldsymbol{N}}^j+\tilde{\boldsymbol{M}}^j\boldsymbol{Y})\ \ (j=1,2,\ldots,\tilde{q}) \qquad (8)$$

appearing on the left hand side of the system of equations above are in the p-dimensional sub $I\!R$-module $\mathcal{T}$ of $\mathcal{M}_n(I\!K,I\!R)$, and that the constant matrix

$$\boldsymbol{Q}-\boldsymbol{X}(\boldsymbol{Y}^0-\boldsymbol{Y})-(\boldsymbol{X}^0-\boldsymbol{X})\boldsymbol{Y}$$

on the right hand side also belongs to $\mathcal{T}$. Therefore it suffices to show that the set of p matrices given in (8) forms a basis of the p-dimensional sub $I\!R$-module $\mathcal{T}$ of $\mathcal{M}_n(I\!K,I\!R)$. Assuming that

$$\sum_{i=1}^{q}c'_i(\boldsymbol{X}\boldsymbol{N}^i+\boldsymbol{M}^i\boldsymbol{Y})+\sum_{j=1}^{\tilde{q}}\tilde{c}'_j(\boldsymbol{X}\tilde{\boldsymbol{N}}^j+\tilde{\boldsymbol{M}}^j\boldsymbol{Y})=\boldsymbol{O}, \qquad (9)$$

we will show that all the c'_i $(i = 1, 2, \ldots, q)$ and $\tilde{c}'_j$ $(j = 1, 2, \ldots, \tilde{q})$ vanish. Let

$$d\boldsymbol{X}' = \sum_{i=1}^{q} c'_i \boldsymbol{M}^i, \ d\boldsymbol{Y}' = \sum_{i=1}^{q} c'_i \boldsymbol{N}^i, \ d\tilde{\boldsymbol{X}}' = \sum_{j=1}^{\tilde{q}} \tilde{c}'_j \tilde{\boldsymbol{M}}^j \text{ and } d\tilde{\boldsymbol{Y}}' = \sum_{j=1}^{\tilde{q}} \tilde{c}'_j \tilde{\boldsymbol{N}}^j.$$

Then $(d\boldsymbol{X}', d\boldsymbol{Y}') \in \mathcal{F}_0 \subset \mathcal{T}^h \times \mathcal{T}^h$ and $(d\tilde{\boldsymbol{X}}', d\tilde{\boldsymbol{Y}}') \in \tilde{\mathcal{F}}_0 \subset \mathcal{T}^{skew} \times \mathcal{T}^{skew}$. We also see from (9) that

$$\boldsymbol{O} = \boldsymbol{X}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}') + (d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\boldsymbol{Y}. \tag{10}$$

Since $\boldsymbol{X} \in \mathcal{T} \subset \mathcal{M}_n(I\!\!K, I\!\!R)$ and $\boldsymbol{Y} \in \mathcal{T} \subset \mathcal{M}_n(I\!\!K, I\!\!R)$ are positive definite, there exist nonsingular $\sqrt{\boldsymbol{X}} \in \mathcal{M}_n(I\!\!K, I\!\!R)$ and $\sqrt{\boldsymbol{Y}} \in \mathcal{M}_n(I\!\!K, I\!\!R)$ such that $\boldsymbol{X} = \sqrt{\boldsymbol{X}}\sqrt{\boldsymbol{X}}$ and $\boldsymbol{Y} = \sqrt{\boldsymbol{Y}}\sqrt{\boldsymbol{Y}}$. It follows from (10) that

$$\boldsymbol{O} \ = \ \sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1} + \sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}.$$

From the above equality, we obtain that

$$\begin{aligned}
0 \ &= \ \left(\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1} + \sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}\right) \\
&\quad \bullet \left(\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1} + \sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}\right) \\
&= \ \|\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1}\|^2 \ + \ \|\sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}\|^2 \\
&\quad + \sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1} \bullet \sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}} \\
&\quad + \sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}} \bullet \sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1} \\
&= \ \|\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1}\|^2 \ + \ \|\sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}\|^2 \\
&\quad + (d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}') \bullet (d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}') \ + \ (d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}') \bullet (d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}') \\
&= \ \|\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1}\|^2 \ + \ \|\sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}\|^2 \\
&\quad + 2d\boldsymbol{Y}' \bullet d\boldsymbol{X}' + 2d\tilde{\boldsymbol{X}}' \bullet d\tilde{\boldsymbol{Y}}' \\
&\quad (\text{since } d\boldsymbol{Y}' \bullet d\tilde{\boldsymbol{X}}' = d\tilde{\boldsymbol{Y}}' \bullet d\boldsymbol{X}' = 0\ ) \\
&\geq \ \|\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1}\|^2 \ + \ \|\sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}\|^2. \\
&\quad (\text{since } d\boldsymbol{Y}' \bullet d\boldsymbol{X}' \geq 0 \text{ and } d\tilde{\boldsymbol{X}}' \bullet d\tilde{\boldsymbol{Y}}' \geq 0)
\end{aligned}$$

Hence we see that

$$\|\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1}\| = 0 \ \text{ and } \|\sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}}\| = 0.$$

This implies that

$$\sqrt{\boldsymbol{X}}(d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}')\sqrt{\boldsymbol{Y}}^{-1} = \boldsymbol{O} \ \text{ and } \ \sqrt{\boldsymbol{X}}^{-1}(d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}')\sqrt{\boldsymbol{Y}} = \boldsymbol{O}.$$

By the nonsingularity of $\sqrt{\boldsymbol{X}}$ and $\sqrt{\boldsymbol{Y}}$, we obtain

$$d\boldsymbol{Y}' + d\tilde{\boldsymbol{Y}}' = \boldsymbol{O} \ \text{ and } \ d\boldsymbol{X}' + d\tilde{\boldsymbol{X}}' = \boldsymbol{O}.$$

Since $d\boldsymbol{X}' \in \mathcal{T}^h$, $d\tilde{\boldsymbol{X}}' \in \mathcal{T}^{skew}$, $d\boldsymbol{Y}' \in \mathcal{T}^h$ and $d\tilde{\boldsymbol{Y}}' \in \mathcal{T}^{skew}$, we see that $d\boldsymbol{X}' \bullet d\tilde{\boldsymbol{X}}' = d\boldsymbol{Y}' \bullet d\tilde{\boldsymbol{Y}}' = 0$. Hence the equalities above imply that

$$(\boldsymbol{O}, \boldsymbol{O}) = (d\boldsymbol{X}', d\boldsymbol{Y}') = \sum_{i=1}^{q} c'_i(\boldsymbol{M}^i, \boldsymbol{N}^i) \ \text{ and } (\boldsymbol{O}, \boldsymbol{O}) = (d\tilde{\boldsymbol{X}}', d\tilde{\boldsymbol{Y}}') = \sum_{j=1}^{\tilde{q}} \tilde{c}'_j(\tilde{\boldsymbol{M}}^j, \tilde{\boldsymbol{N}}^j).$$

Recall that $\{(M^i, N^i) \in \mathcal{T}^h \times \mathcal{T}^h \ (i = 1, 2, \ldots, q)\}$ and $\{(\tilde{M}^j, \tilde{N}^j) \in \mathcal{T}^{skew} \times \mathcal{T}^{skew} \ (j = 1, 2, \ldots, \tilde{q})\}$ are bases of the q-dimensional sub $I\!R$-module $\mathcal{F}_0$ of $\mathcal{T}^h \times \mathcal{T}^h$ and the $\tilde{q}$-dimensional sub $I\!R$-module $\tilde{\mathcal{F}}_0$ of $\mathcal{T}^{skew} \times \mathcal{T}^{skew}$, respectively. Hence $c'_i = 0 \ (i = 1, 2, \ldots, q)$ and $\tilde{c}'_j = 0 \ (j = 1, 2, \ldots, \tilde{q})$. This means that the set of p matrices given in (8) is linearly independent, and forms a basis of the p-dimensional sub $I\!R$-module $\mathcal{T}$ of $\mathcal{M}_n(I\!K, I\!R)$. This completes the proof of Theorem 4.3. ∎

5. Characterization of *-Subalgebras of $\mathcal{M}_n(I\!K, I\!R)$.

5.1. A *-Representation of $\mathcal{M}_n(I\!K, I\!R)$.

In the latter part of this section, we construct "a one-to-one *-homomorphism" $\tilde{\rho}$ that transforms the algebraic structure of $\mathcal{M}_n(I\!K, I\!R)$ into $\mathcal{M}_{dn}(I\!R)$. The *-homomorphism $\tilde{\rho}$ then makes it possible for us to convert any SDP and any monotone SDLCP in $\mathcal{M}_n(I\!K, I\!R)$ into an SDP and a monotone SDLCP in $\mathcal{M}_{dn}(I\!K, I\!R)$, respectively. Here $d = \dim I\!K(I\!R)$. We need several definitions. Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are subalgebras. A mapping $\rho : \mathcal{T} \to \mathcal{T}'$ is *a homomorphism* if it satisfies:

(a) $\rho(A + B) = \rho(A) + \rho(B)$ and $\rho(AB) = \rho(A)\rho(B)$ for every $A, \ B \in \mathcal{T}$.

(b) ρ is linear on $\mathcal{T}$; $\rho(\alpha A + \beta B) = \alpha\rho(A) + \beta\rho(B)$ for every $\alpha, \ \beta \in R$ and $A, \ B \in \mathcal{T}$.

If in addition $\rho : \mathcal{T} \to \mathcal{T}'$ is one-to-one and onto, ρ is *an isomorphism* from $\mathcal{T}$ onto $\mathcal{T}'$. When $\mathcal{T}$ and $\mathcal{T}'$ are *-subalgebras, $\rho : \mathcal{T} \to \mathcal{T}'$ is *a *-homomorphism* (or *a *-isomorphism*) if it satisfies

(c) $\rho(A^*) = \rho(A)^*$ for every $A \in \mathcal{T}$

For example, if $S \in \mathcal{M}_n(I\!R)$ is a nonsingular matrix and $P \in \mathcal{M}_n(I\!R)$ an orthogonal matrix then

$$\rho^1 : A \in \mathcal{M}_n(I\!R) \to SAS^{-1} \in \mathcal{M}_n(I\!R) \tag{11}$$

is an isomorphism from $\mathcal{M}_n(I\!R)$ onto $\mathcal{M}_n(I\!R)$, and

$$\rho^2 : A \in \mathcal{M}_n(I\!R) \to \begin{pmatrix} P^T A P & O \\ O & A \end{pmatrix} \in \mathcal{M}_{2n}(I\!R) \tag{12}$$

is a *-homomorphism from $\mathcal{M}_n(I\!R)$ into $\mathcal{M}_{2n}(I\!R)$. If there exists an isomorphism (or *-isomorphism) ρ from $\mathcal{T}$ onto $\mathcal{T}'$, $\mathcal{T}$ and $\mathcal{T}'$ are *isomorphic* (or **-isomorphic*).

Let $\mathcal{T}$ be a subalgebra (or a *-subalgebra) of $\mathcal{M}_m(I\!K, I\!R)$. If a homomorphism (or a *-homomorphism) ρ from $\mathcal{T}$ into $\mathcal{M}_n(I\!R)$ satisfies

(d) $\rho(I) = I \in \mathcal{M}_n(I\!R)$,

$(\rho, I\!R^n)$ is *a representation* (or *a *-representation*) of $\mathcal{T}$. In this case $\rho(\mathcal{T})$ forms a subalgebra (or a *-subalgebra) of $\mathcal{M}_n(I\!R)$. A representation (or a *-representation) $(\rho, I\!R^n)$ of $\mathcal{T}$ is *faithful* if

(e) ρ is one-to-one on $\mathcal{T}$.

$(\rho^1, I\!R^n)$ in the example (11) is a faithful representation of $\mathcal{M}_n(I\!R)$ but it is not a *-representation in general. $(\rho^2, I\!R^{2n})$ in the example (12) is a faithful *-representation of $\mathcal{M}_n(I\!R)$.

We will construct below a faithful *-representation $(\rho, I\!R^{dn})$ of $\mathcal{T} = \mathcal{M}_n(I\!K, I\!R)$ that satisfies the following additional conditions.

(f) There is an isomorphism (*i.e.*, a one-to-one linear mapping) ϕ from the dn-dimensional $\mathbb{R}$-module $\mathbb{K}^n$ onto the dn-dimensional Euclidean space $\mathbb{R}^{dn}$ such that

$$\begin{aligned} \phi(\boldsymbol{A}\boldsymbol{z}) &= \rho(\boldsymbol{A})\phi(\boldsymbol{z}) \text{ for every } \boldsymbol{A} \in \mathcal{T} \text{ and } \boldsymbol{z} \in \mathbb{K}^n, \\ \phi(\boldsymbol{z}^1) \cdot \phi(\boldsymbol{z}^2) &= \boldsymbol{z}^1 \cdot \boldsymbol{z}^2 \text{ for every } \boldsymbol{z}^1, \ \boldsymbol{z}^2 \in \mathbb{K}^n. \end{aligned}$$

(g) $\rho(\boldsymbol{A}) \bullet \rho(\boldsymbol{B}) = \boldsymbol{A} \bullet \boldsymbol{B}$ for every $\boldsymbol{A}, \ \boldsymbol{B} \in \mathcal{T}$.

Here $d = \dim \mathbb{K}(\mathbb{R})$. Such a faithful *-representation $(\rho, \mathbb{R}^{dn})$ of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$ preserves the algebraic structure which is necessary to study SDPs and monotone SDLCPs. It is easily seen that if $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$ is an $n \times n$ orthogonal matrix and

$$\rho : \boldsymbol{A} \in \mathcal{M}_n(\mathbb{R}) \rightarrow \boldsymbol{P}^T\boldsymbol{A}\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$$

then $(\rho, \mathbb{R}^n)$ is a faithful *-representation of $\mathcal{M}_n(\mathbb{R})$ that satisfies the conditions (f) and (g) with $\phi(\boldsymbol{z}) = \boldsymbol{P}^T\boldsymbol{z}$ ($\boldsymbol{z} \in \mathbb{R}^n$).

Theorem 5.1. *Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_m(\mathbb{K}, \mathbb{R})$ and $(\rho, \mathbb{R}^n)$ be a faithful *-representation of $\mathcal{T}$ satisfying the conditions (f) and (g). Then the following (h), (i) and (j) hold.*

*(h) $\rho(\mathcal{T})$ is a *-subalgebra of $\mathcal{M}_{dn}(\mathbb{R})$ with $\dim \rho(\mathcal{T}) = \dim \mathcal{T}$.*
*(Specifically $\rho(\mathcal{M}_n(\mathbb{K}, \mathbb{R}))$ is a *-subalgebra of $\mathcal{M}_{dn}(\mathbb{R})$.)*

(i) $\rho(\mathcal{T}^h) = \rho(\mathcal{T})^h$.

(j) $\rho(\boldsymbol{A}) \in \rho(\mathcal{T})^h$ is positive semi-definite (or positive definite) if and only if $\boldsymbol{A} \in \mathcal{T}^h$ is positive semi-definite (or positive definite).

Proof: By the assumption, all the conditions (a) through (g) are satisfied. We can easily derive the assertion (h) and (i) from these conditions, so that we will only prove the assertion (j). Let $\boldsymbol{A} \in \mathcal{T}^h$. By the condition (f),

$$\phi(\boldsymbol{z}) \cdot \rho(\boldsymbol{A})\phi(\boldsymbol{z}) = \phi(\boldsymbol{z}) \cdot \phi(\boldsymbol{A}\boldsymbol{z}) = \boldsymbol{z} \cdot \boldsymbol{A}\boldsymbol{z}$$

holds for every $\boldsymbol{z} \in \mathbb{K}(\mathbb{R})^n$. Since ϕ is an isomorphism from $\mathbb{K}(\mathbb{R})^n$ onto $\mathbb{R}^{dn}$, we know that $\phi(\mathbb{K}(\mathbb{R})^n) = \mathbb{R}^{dn}$ and $\phi(\boldsymbol{z}) = \boldsymbol{0}$ if and only if $\boldsymbol{z} = \boldsymbol{0}$. Hence $\boldsymbol{u} \cdot \rho(\boldsymbol{A})\boldsymbol{u}$ is nonnegative for every $\boldsymbol{u} \in \mathbb{R}^{dn}$ (or positive for every nonzero $\boldsymbol{u} \in \mathbb{R}^{dn}$) if and only if $\boldsymbol{z} \cdot \boldsymbol{A}\boldsymbol{z}$ is nonnegative for every $\boldsymbol{z} \in \mathbb{K}(\mathbb{R})^n$ (or positive for every nonzero $\boldsymbol{z} \in \mathbb{K}(\mathbb{R})^n$). This implies the assertion (j). ∎

Using the properties (a) through (j) presented so far, we can convert the primal-dual pair of SDPs (P) and (D) in a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$, which we have stated in Section 1, into a primal-dual pair of SDPs in a *-subalgebra $\mathcal{T}' = \rho(\mathcal{T})$ of $\mathcal{M}_{dn}(\mathbb{R})$:

$$\left. \begin{array}{lll} (P)' & \text{minimize} & \rho(\boldsymbol{A}_0) \bullet \boldsymbol{X}' \\ & \text{subject to} & \rho(\boldsymbol{A}_i) \bullet \boldsymbol{X}' = b_i \ (i = 1, 2, \ldots, m) \\ & & \boldsymbol{X}' \succeq \boldsymbol{O}, \ \boldsymbol{X}' \in \rho(\mathcal{T})^h. \end{array} \right\}$$

$$\left. \begin{array}{lll} (D)' & \text{maximize} & \sum_{i=1}^m b_i z_i \\ & \text{subject to} & \sum_{i=1}^m \rho(\boldsymbol{A}_i) z_i + \boldsymbol{Y}' = \rho(\boldsymbol{A}_0), \\ & & \boldsymbol{Y}' \succeq \boldsymbol{O}, \ \boldsymbol{Y}' \in \rho(\mathcal{T})^h. \end{array} \right\}$$

It is easily verified that $\boldsymbol{X} \in \mathcal{T}$ and $(\boldsymbol{Y}, \boldsymbol{z}) \in \mathcal{T} \times \mathbb{R}^m$ are optimal solutions of (P) and (D) if and only if $\boldsymbol{X}' = \rho(\boldsymbol{X}) \in \rho(\mathcal{T})$ and $(\boldsymbol{Y}, \boldsymbol{z}) = (\rho(\boldsymbol{Y}), \boldsymbol{z}) \in \rho(\mathcal{T}) \times \mathbb{R}^m$ are optimal solutions of (P)' and (D)'.

We now consider the monotone SDLCP (1) in a *-subalgebra $\mathcal{T}$. Recall that $\mathcal{F}_0 \subset \mathcal{T}^h \times \mathcal{T}^h$ appearing in the SDLCP (1) is a q-dimensional sub $I\!R$-module of $\mathcal{M}_n(I\!K, I\!R) \times \mathcal{M}_n(I\!K, I\!R)$ satisfying the monotonicity (2). Define

$$\mathcal{F}'_0 \;=\; \{(\rho(X), \rho(Y)) : (X, Y) \in \mathcal{F}_0\} \subset \rho(\mathcal{T}^h) \times \rho(\mathcal{T}^h) = \rho(\mathcal{T})^h \times \rho(\mathcal{T})^h.$$

Then $\mathcal{F}'_0$ forms a q-dimensional sub $I\!R$-module of the $2q$-dimensional $I\!R$-module $\rho(\mathcal{T})^h \times \rho(\mathcal{T})^h$. We also know that

$$\rho(X) \bullet \rho(Y) = X \bullet Y \quad \text{for every } (X, Y) \in \mathcal{T}^h \times \mathcal{T}^h.$$

This ensures that $\mathcal{F}'_0$ inherits the monotonicity from $\mathcal{F}_0$. Thus we have the monotone SDLCP in $\rho(\mathcal{T}) \subset \mathcal{M}_{dn}(I\!K, I\!R)$: Find an (X', Y') such that

$$(X', Y') \in \mathcal{F}' \equiv \mathcal{F}'_0 + (\rho(X_0), \rho(Y_0)), \; X' \succeq O, \; Y' \succeq O \text{ and } X' \bullet Y' = 0; \tag{13}$$

The monotone SDLCP (13) is equivalent to the monotone SDLCP (1) in the sense that $(X, Y) \in \mathcal{T}^h \times \mathcal{T}^h$ is a solution of the SDLCP (1) if and only if $(X', Y') = (\rho(X), \rho(Y)) \in \rho(\mathcal{T})^h \times \rho(\mathcal{T})^h$ is a solution of the SDLCP (13).

Now we construct a faithful *-representation $(\rho, I\!R^{dn}) = (\tilde{\rho}, I\!R^{dn})$ of $\mathcal{M}_n(I\!K, I\!R)$ satisfying the conditions (f) and (g) Define

$$\tilde{\rho}(h) \;=\; \begin{cases} h & \text{if } h \in \mathcal{M}_1(I\!R), \\ \begin{pmatrix} v & w \\ -w & v \end{pmatrix} & \text{if } h = v + iw \in \mathcal{M}_1(\mathbb{C}, I\!R), \\ \begin{pmatrix} v & -w & -x & -y \\ w & v & -y & x \\ x & y & v & -w \\ y & -x & w & v \end{pmatrix} & \text{if } h = v + iw + jx + ky \in \mathcal{M}_1(I\!H, I\!R), \end{cases}$$

$$\tilde{\rho}(A) \;=\; \begin{pmatrix} \tilde{\rho}(a_{11}) & \tilde{\rho}(a_{12}) & \cdot & \tilde{\rho}(a_{1n}) \\ \tilde{\rho}(a_{21}) & \tilde{\rho}(a_{22}) & \cdot & \tilde{\rho}(a_{2n}) \\ \cdot & \cdot & \cdots & \cdot \\ \tilde{\rho}(a_{n1}) & \tilde{\rho}(a_{n2}) & \cdot & \tilde{\rho}(a_{nn}) \end{pmatrix} \in \mathcal{M}_{dn}(I\!R) \text{ if } A \in \mathcal{M}_n(I\!K, I\!R). \tag{14}$$

Theorem 5.2. $(\rho, I\!R^{dn}) = (\tilde{\rho}, I\!R^{dn})$ *is a faithful *-representation of* $\mathcal{M}_n(I\!K, I\!R)$ *satisfying the conditions (f) and (g).*

Proof: It is easily seen that $\tilde{\rho}$ satisfies the conditions (a), (b), (c), (d), (e) and (g). We can also verify that the condition (f) holds with the isomorphism $\phi = \tilde{\phi}$ from $I\!K(I\!R)^n$ onto $I\!R^{dn}$ given below:

$$\tilde{\phi}(z) \;=\; \begin{cases} z & \text{if } z \in I\!R, \\ \begin{pmatrix} v \\ w \end{pmatrix} \in I\!R^d = I\!R^2 & \text{if } z = v + iw \in \mathbb{C}(I\!R), \\ \begin{pmatrix} v \\ w \\ x \\ y \end{pmatrix} \in I\!R^d = I\!R^4 & \text{if } z = v + iw + jx + ky \in I\!H(I\!R), \end{cases}$$

$$\tilde{\phi}(z) = \begin{pmatrix} \tilde{\phi}(z_1) \\ \tilde{\phi}(z_2) \\ \cdot \\ \tilde{\phi}(z_n) \end{pmatrix} \in \mathbb{R}^{dn} \ \text{ if } z = (z_1, z_2, \ldots, z_n)^T \in \mathbb{K}(\mathbb{R})^n,.$$

∎

Remark. The observation below relates the faithful *-representation $(\tilde{\rho}, \mathbb{R}^{dn})$ of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$ to the recent paper [6] by Güler. Let $\mathcal{M}_n(\mathbb{K}, \mathbb{R})^h_+$ denote the convex cone consisting of positive semi-definite Hermitian matrices in $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$. Then we know by Theorems 5.1 and 5.2 that

$$\tilde{\rho}(\mathcal{M}_n(\mathbb{K}, \mathbb{R})^h_+) \doteq \mathcal{M}_{dn}(\mathbb{R})^h_+ \bigcap \tilde{\rho}(\mathcal{M}_n(\mathbb{K}, \mathbb{R})).$$

The convex cone $\tilde{\rho}(\mathcal{M}_n(\mathbb{K}, \mathbb{R})^h_+)$ enjoys some nice properties, the irreducibility, the regularity, the homogeneity and the self-duality in the $\mathbb{R}$-module $\tilde{\rho}(\mathcal{M}_n(\mathbb{K}, \mathbb{R}))$. By Theorems 4.1 and 4.3 of [6], we can represent the self-concordant universal barrier function (Nesterov-Nemirovskii [21]) for the cone $\tilde{\rho}(\mathcal{M}_n(\mathbb{K}, \mathbb{R})^h_+)$ in terms of the logarithm of a characteristic function of the cone $\tilde{\rho}(\mathcal{M}_n(\mathbb{K}, \mathbb{R})^h_+)$. See [6] for more details.

The next theorem shows that a *-subalgebra of $\mathcal{M}_n(\mathbb{R})$ is closed under the inversion.

Theorem 5.3. *Let $(\rho, \mathbb{R}^{dn})$ be a faithful *-representation of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$ satisfying the conditions (f) and (g). Then the following (k) and (ℓ) hold.*

(k) $A \in \mathcal{M}_n(\mathbb{K}, \mathbb{R})$ is nonsingular if and only if $\rho(A)$ is, and $\rho(A^{-1}) = \rho(A)^{-1}$ if $A \in \mathcal{M}_n(\mathbb{K}, \mathbb{R})$ is nonsingular.

*(ℓ) Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$. If $A \in \mathcal{M}_n(\mathbb{K}, \mathbb{R})$ is nonsingular then $A^{-1} \in \mathcal{T}$.*

Proof: Recall that $A \in \mathcal{M}_n(\mathbb{K}, \mathbb{R})$ is nonsingular and $B \in \mathcal{M}_n(\mathbb{K}, \mathbb{R})$ is its inverse if

$$BA = AB = I.$$

From the conditions (a) with $\mathcal{T} = \mathcal{M}_n(\mathbb{K}, \mathbb{R})$, (d) and (e), we see that the equalities above hold if and only if

$$\tilde{\rho}(B)\tilde{\rho}(A) = \tilde{\rho}(A)\tilde{\rho}(B) = \tilde{\rho}(I) = I.$$

Thus the assertion (k) follows. To prove the assertion (ℓ), we only need to deal with the case where $\mathcal{T}$ is a *-subalgebra of $\mathcal{M}_n(\mathbb{R})$ in view of Theorem 5.1 and the assertion (k). Suppose that $A \in \mathcal{T}$ is nonsingular. Then we know that $A^T \in \mathcal{T}$. Take a sufficiently small positive number ϵ such that all the eigenvalues of the positive definite matrix $\epsilon A^T A$ are less than 1. Then the inverse $(\epsilon A^T A)^{-1}$ of the matrix $\epsilon A^T A$ can be written as

$$\begin{aligned} (\epsilon A^T A)^{-1} &= \left(I - (I - \epsilon A^T A)\right)^{-1} \\ &= I + (I - \epsilon A^T A) + (I - \epsilon A^T A)^2 + \cdots. \end{aligned}$$

By the conditions (i), (ii) and (iii) imposed on the *-subalgebra $\mathcal{T}$, each term on the right hand side belongs to $\mathcal{T}$. Since $\mathcal{T}$ is topologically closed, the infinite sum of matrices on right hand side belongs to $\mathcal{T}$; hence so does the matrix $(\epsilon A^T A)^{-1}$ on the left hand side. Therefore we obtain by the conditions (i) and (ii) that

$$A^{-1} = \epsilon(\epsilon A^T A)^{-1} A^T \in \mathcal{T}.$$

∎

5.2. Classification of *-Subalgebras of $\mathcal{M}_n(\mathbb{R})$.

In Section 5.1, we have utilized some notions such as "homomorphism " and "isomorphism " from the representation theory of algebras to describe a faithful *-representation $(\tilde{\rho}, \mathbb{R}^{dn})$ of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$. We need to rely more upon the theory in order to derive a complete set of characterizations of *-subalgebras of $\mathcal{M}_n(\mathbb{R})$ in Theorem 5.4. Our discussions here are based on the literature [7] written in Japanese. We also refer to Chapter III of the book [28] written in English although the readers may have some difficulty relating the results presented there to ours. We have been searching for more appropriate sources, but all other literatures we have found so far do not fit well in our discussions. We should also mention that Chapter IV of the book [25] studies *algebras with an involution* and **-algebras* which includes our *-subalgebra as a special case but the main subject of the book is not relevant to our discussions.

Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$. *An ideal* of $\mathcal{T}$ is a sub $\mathbb{R}$-module $\mathcal{I}$ of $\mathcal{T}$ satisfying

$$\boldsymbol{AB} \in \mathcal{I} \text{ if } \boldsymbol{A} \in \mathcal{T} \text{ and } \boldsymbol{B} \in \mathcal{I}.$$

Obviously, $\{\boldsymbol{O}\}$ and $\mathcal{T}$ are ideals of $\mathcal{T}$. If $\mathcal{T}$ contains no ideal other than $\{\boldsymbol{O}\}$ and $\mathcal{T}$, $\mathcal{T}$ is *simple.* A sub $\mathbb{R}$-module V of $\mathbb{K}(\mathbb{R})^n$ is $\mathcal{T}$*-invariant* if

$$\boldsymbol{A}V \subset V \text{ for every } \boldsymbol{A} \in \mathcal{T}.$$

Note that the 0-dimensional sub $\mathbb{R}$-module $\{\boldsymbol{0}\}$ and the entire $\mathbb{R}$-module $\mathbb{K}(\mathbb{R})^n$ are always $\mathcal{T}$-invariant. A *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{K}, \mathbb{R})$ is *reducible* if there is a $\mathcal{T}$-invariant sub $\mathbb{R}$-module of $\mathbb{K}(\mathbb{R})^n$ other than $\{\boldsymbol{0}\}$ and $\mathbb{K}(\mathbb{R})^n$, and *irreducible* otherwise. For example, consider

$$\begin{aligned} \mathcal{T}_1 &= \left\{\text{diag }(\boldsymbol{A}, \boldsymbol{P}^T\boldsymbol{A}\boldsymbol{P}) : \boldsymbol{A} \in \mathcal{M}_n(\mathbb{R})\right\}, \\ \mathcal{T}_2 &= \mathcal{M}_n(\mathbb{R}) \oplus \mathcal{T}_1, \end{aligned}$$

where $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$ is an $n \times n$ orthogonal matrix. Then $\mathcal{T}_1$ is simple but not irreducible, and $\mathcal{T}_2$ is neither simple nor irreducible.

Theorem 5.4.

*(A) Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{R})$. Then there is an orthogonal matrix $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$ and simple *-subalgebras $\mathcal{T}_j$ of $\mathcal{M}_{n_j}(\mathbb{R})$ $(j = 1, 2, \ldots, \ell)$ such that*

$$\begin{aligned} \boldsymbol{P}^T\mathcal{T}\boldsymbol{P} &= \mathcal{T}_1 \oplus \mathcal{T}_2 \oplus \cdots \oplus \mathcal{T}_\ell \\ &= \{\textit{diag }(\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_\ell) : \boldsymbol{A}_j \in \mathcal{T}_j \ (j = 1, 2, \ldots, \ell)\}. \end{aligned}$$

*(B) If a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{R})$ is simple, there is an orthogonal matrix $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$ and an irreducible *-subalgebra $\mathcal{T}'$ of $\mathcal{M}_{n'}(\mathbb{R})$ such that*

$$\boldsymbol{P}^T\mathcal{T}\boldsymbol{P} = \{\textit{diag }(\boldsymbol{B}, \boldsymbol{B}, \ldots, \boldsymbol{B}) : \boldsymbol{B} \in \mathcal{T}'\}.$$

*(C) If a *-subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{R})$ is irreducible then there exists an orthogonal matrix $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$ such that*

$$\boldsymbol{P}^T\mathcal{T}\boldsymbol{P} = \tilde{\rho}(\mathcal{M}).$$

Here

$$\mathcal{M} = \mathcal{M}_n(\mathbb{R}), \ \mathcal{M}_{n/2}(\mathbb{C}, \mathbb{R}) \ \text{ or } \mathcal{M}_{n/4}(\mathbb{H}, \mathbb{R}),$$

*and $(\tilde{\rho}, \mathbb{R}^n)$ denotes the faithful *-representation of $\mathcal{M}$ given in Section 3.*

To prove the theorem, we need a series of lemmas.

Lemma 5.5. *If a subalgebra $\mathcal{T}$ has a faithful representation $(\rho, \mathbb{R}^n)$ such that $\rho(\mathcal{T})$ is irreducible, then $\mathcal{T}$ is simple.*

Proof: See Theorem 1.16 of [7]. ∎

Lemma 5.6. *Let $\mathcal{T}$ be a subalgebra, and let $(\rho, \mathbb{R}^n)$ be a faithful representation of $\mathcal{T}$ such that $\rho(\mathcal{T})$ is irreducible. Let $(\rho', \mathbb{R}^{n'})$ be a representations of $\mathcal{T}$ such that $\rho'(\mathcal{T})$ is irreducible. Then $n = n'$ and there exists a nonsingular matrix $\boldsymbol{S}$ such that $\rho'(\boldsymbol{A}) = \boldsymbol{S}^{-1}\rho(\boldsymbol{A})\boldsymbol{S}$ for every $\boldsymbol{A} \in \mathcal{T}$.*

Proof: See Corollary of Theorem 1.15 of [7], and Theorem (3.3.E) of [28]. ∎

Lemma 5.7. *If a subalgebra $\mathcal{T}$ of $\mathcal{M}_n(\mathbb{R})$ is irreducible then there is a faithful representation $(\rho', \mathbb{R}^n)$ of*

$$\mathcal{M} = \mathcal{M}_n(\mathbb{R}), \ \mathcal{M}_{n/2}(\mathbb{C}, \mathbb{R}) \ \ \text{or}\ \mathcal{M}_{n/4}(\mathbb{H}, \mathbb{R})$$

such that $\rho'(\mathcal{M}) = \mathcal{T}$.

Proof: The lemma follows directly from Wedderburns's Theorem. See Theorem 1.17 of [7], and Chapter III, Section 4 of [28]. ∎

Lemma 5.8. *Let $\mathcal{T}$ be a *-subalgebra, and let $(\rho, \mathbb{R}^n)$ be a faithful *-representation of $\mathcal{T}$ such that $\rho(\mathcal{T})$ is irreducible. Let $(\rho', \mathbb{R}^{n'})$ be a *-representation of $\mathcal{T}$ such that $\rho'(\mathcal{T})$ is irreducible. Then $n = n'$ and there exists an orthogonal matrix $\boldsymbol{P}$ such that $\rho'(\boldsymbol{A}) = \boldsymbol{P}^T\rho(\boldsymbol{A})\boldsymbol{P}$ for every $\boldsymbol{A} \in \mathcal{T}$.*

Proof: By Lemma 5.6, $n = n'$ and there is a nonsingular matrix $\boldsymbol{S} \in \mathcal{M}_n(\mathbb{R})$ such that

$$\rho'(\boldsymbol{A}) = \boldsymbol{S}^{-1}\rho(\boldsymbol{A})\boldsymbol{S} \ \text{ for every } \boldsymbol{A} \in \mathcal{T}.$$

By the assumption $(\rho, \mathbb{R}^n)$ and $(\rho', \mathbb{R}^{n'})$ are *-representations of $\mathcal{T}$, so that the relation

$$\begin{aligned} \boldsymbol{S}^{-1}\rho(\boldsymbol{A})\boldsymbol{S} &= (\rho'(\boldsymbol{A})^*)^* \\ &= (\rho'(\boldsymbol{A}^*))^* \\ &= \left(\boldsymbol{S}^{-1}\rho(\boldsymbol{A}^*)\boldsymbol{S}\right)^* \\ &= \boldsymbol{S}^*\rho(\boldsymbol{A})(\boldsymbol{S}^*)^{-1} \end{aligned}$$

holds for every $\boldsymbol{A} \in \mathcal{T}$; hence

$$(\boldsymbol{S}\boldsymbol{S}^*)\boldsymbol{B}(\boldsymbol{S}\boldsymbol{S}^*)^{-1} = \boldsymbol{B} \ \text{ for every } \boldsymbol{B} \in \rho(\mathcal{T}).$$

In the relation above, $\rho(\mathcal{T})$ is an irreducible subalgebra of $\mathcal{M}_n(\mathbb{R})$ by assumption, and all the eigenvalues of the matrix $\boldsymbol{S}\boldsymbol{S}^*$ are in $\mathbb{R}$ since $\boldsymbol{S}\boldsymbol{S}^*$ is symmetric. By applying Schur's lemma (see Theorem 1.8 of [7], and Lemma (3.1.C) of [28] and their proofs), we know that all the eigenvalues are the same α ($\neq 0$) and $\boldsymbol{S}\boldsymbol{S}^T = \alpha\boldsymbol{I}$. Hence, letting $\boldsymbol{P} = \boldsymbol{S}/\sqrt{\alpha}$, we obtain that

$$\begin{aligned} \boldsymbol{P}^T\boldsymbol{P} &= \boldsymbol{I}, \\ \rho'(\boldsymbol{A}) &= \boldsymbol{S}^{-1}\rho(\boldsymbol{A})\boldsymbol{S} = \boldsymbol{P}^T\rho(\boldsymbol{A})\boldsymbol{P} \ \text{ for every } \boldsymbol{A} \in \mathcal{T}. \end{aligned}$$

∎

Lemma 5.9. *Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{R})$. Then there is an orthogonal matrix $\boldsymbol{P} = (\boldsymbol{Q}_1, \boldsymbol{Q}_2, \ldots, \boldsymbol{Q}_m) \in \mathcal{M}_n(\mathbb{R})$, where $\boldsymbol{Q}_i$ is an $n \times n_i$ matrix $(i = 1, 2, \ldots, m)$ and $n_1 + n_2 + \cdots + n_m = n$, such that*

$$\begin{aligned} \boldsymbol{P}^T \mathcal{T} \boldsymbol{P} &= \left\{ \mathit{diag}\,(\boldsymbol{Q}_1^T \boldsymbol{A} \boldsymbol{Q}_1, \boldsymbol{Q}_2^T \boldsymbol{A} \boldsymbol{Q}_2, \cdots, \boldsymbol{Q}_m^T \boldsymbol{A} \boldsymbol{Q}_m) : \boldsymbol{A} \in \mathcal{T} \right\}, \\ \mathcal{T}_i' &\equiv \left\{ \boldsymbol{Q}_i^T \boldsymbol{A} \boldsymbol{Q}_i : \boldsymbol{A} \in \mathcal{T} \right\} \quad \textit{is an irreducible *-subalgebra of } \mathcal{M}_{n_i}(\mathbb{R}) \\ & \quad (i = 1, 2, \ldots, m). \end{aligned}$$

Proof: (i) If $\mathcal{T}$ is irreducible, the lemma obviously holds with $m = 1$ and $\boldsymbol{P} = \boldsymbol{Q}_1 = \boldsymbol{I}$. If $\mathcal{T}$ is reducible, there is k_1-dimensional $\mathcal{T}$-invariant sub $\mathbb{R}$-module V of $\mathbb{R}^n$ with $1 \leq k_1 < n$. Let $k_2 = n - k_1$. We will show that there is an orthogonal matrix $\boldsymbol{P} = (\boldsymbol{Q}_1, \boldsymbol{Q}_2) \in \mathcal{M}_n(\mathbb{R})$, where $\boldsymbol{Q}_i$ is an $n \times k_i$ matrix $(i = 1, 2)$, such that

$$\boldsymbol{P}^T \mathcal{T} \boldsymbol{P} = \left\{ \text{diag}\,(\boldsymbol{Q}_1^T \boldsymbol{A} \boldsymbol{Q}_1, \boldsymbol{Q}_2^T \boldsymbol{A} \boldsymbol{Q}_2) : \boldsymbol{A} \in \mathcal{T} \right\}, \tag{15}$$

$$\mathcal{T}_i' \equiv \{ \boldsymbol{Q}_i^T \boldsymbol{A} \boldsymbol{Q}_i : \boldsymbol{A} \in \mathcal{T} \} \text{ is a *-subalgebra of } \mathcal{M}_{k_i}(\mathbb{R}) \ (i = 1, 2). \tag{16}$$

Let $\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_{k_1}$ be an orthonormal basis of the k_1-dimensional $\mathcal{T}$-invariant sub $\mathbb{R}$-module V of R^n, and Let $\boldsymbol{p}_{k_1+1}, \boldsymbol{p}_{k_1+2}, \ldots, \boldsymbol{p}_n$ be an orthonormal basis of the orthogonal complement $V^{\perp}$ of V. Define

$$\boldsymbol{Q}_1 \equiv (\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_{k_1}), \ \boldsymbol{Q}_2 \equiv (\boldsymbol{p}_{k_1+1}, \boldsymbol{p}_{k_1+2}, \ldots, \boldsymbol{p}_n), \ \boldsymbol{P} \equiv (\boldsymbol{Q}_1, \boldsymbol{Q}_2) \in \mathcal{M}_n(\mathbb{R}).$$

Since $\mathcal{T}$ is a *-subalgebra of $\mathcal{M}_n(\mathbb{R})$, we see that $\boldsymbol{A}^T \in \mathcal{T}$ for every $\boldsymbol{A} \in \mathcal{T}$. It follows from the $\mathcal{T}$-invariance of the sub $\mathbb{R}$-module V of $\mathbb{R}^n$ that

$$\begin{aligned} \boldsymbol{A}\boldsymbol{p}_j &\in V \ (j = 1, 2, \ldots, k_1) \ \text{ for every } \boldsymbol{A} \in \mathcal{T}, \\ \boldsymbol{A}^T \boldsymbol{p}_j &\in V \ (j = 1, 2, \ldots, k_1) \ \text{ for every } \boldsymbol{A} \in \mathcal{T}. \end{aligned}$$

Hence

$$\begin{aligned} (\boldsymbol{p}_i)^T \boldsymbol{A} \boldsymbol{p}_j &= 0 \ (j = 1, 2, \ldots, k_1, \ i = k_1 + 1, k_2 + 1, \ldots, n) \ \text{ for every } \boldsymbol{A} \in \mathcal{T}, \\ (\boldsymbol{p}_i)^T \boldsymbol{A}^T \boldsymbol{p}_j &= 0 \ (j = 1, 2, \ldots, k_1, \ i = k_1 + 1, k_2 + 1, \ldots, n) \ \text{ for every } \boldsymbol{A} \in \mathcal{T}. \end{aligned}$$

This implies

$$\boldsymbol{Q}_i^T \boldsymbol{A} \boldsymbol{Q}_j = \boldsymbol{O} \ (i \neq j) \ \text{ for every } \boldsymbol{A} \in \mathcal{T}. \tag{17}$$

Thus we obtain (15). The relation (16) follows directly from (15) and the definition of a *-subalgebra.

(ii) As long as the resultant subalgebra $\mathcal{T}_1'$ or $\mathcal{T}_2'$ is reducible, we can repeatedly apply the argument (i) above to either or both of them to obtain the desired result. ∎

Lemma 5.10. *Let $(\rho, \mathbb{R}^n)$ and $(\rho', \mathbb{R}^{n'})$ be faithful representations of a simple subalgebra $\mathcal{M}$ such that both $\rho(\mathcal{M})$ and $\rho'(\mathcal{M})$ are irreducible *-subalgebras. Then $n = n'$ and there exists an orthogonal matrix $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$ such that $\rho'(\mathcal{M}) = \boldsymbol{P}^T \rho(\mathcal{M}) \boldsymbol{P}$.*

Proof: (i) Let $\mathcal{T} = \rho'(\mathcal{M})$. By Lemma 5.6, we can take a nonsingular matrix $\boldsymbol{S} \in \mathcal{M}_n(\mathbb{R})$ such that

$$\mathcal{T} = \boldsymbol{S}^{-1} \rho(\mathcal{M}) \boldsymbol{S}. \tag{18}$$

Since $S^T S$ is a positive definite matrix, we can take an orthogonal matrix $P_1 \in \mathcal{M}_n(\mathbb{R})$ and a diagonal matrix D with positive diagonal entries D_{ii} $(i = 1, 2, \ldots, n)$ such that $P_1^T S^T S P_1 = D^2$. Here each diagonal entry D_{ii}^2 of D^2 corresponds to a positive eigenvalue of $S^T S$. It follows that

$$I = D^{-1} P_1^T S^T S P_1 D^{-1} = (S P_1 D^{-1})^T S P_1 D^{-1}.$$

Letting $P_2 = S P_1 D^{-1} \in \mathcal{M}_n(\mathbb{R})$, we obtain $S = P_2 D P_1^T$, and $P_2^T P_2 = I$ (*i.e.*, $P_2 \in \mathcal{M}_n(\mathbb{R})$ is an orthogonal matrix). Hence it follows from the equality (18) that

$$\mathcal{T} = P_1 D^{-1} P_2^T \rho(\mathcal{M}) P_2 D P_1^T. \tag{19}$$

Since both $\mathcal{T}$ and $\rho(\mathcal{M})$ are *-subalgebras of $\mathcal{M}_n(\mathbb{R})$, we then have

$$P_1 D^{-1} P_2^T \rho(\mathcal{M}) P_2 D P_1^T = \mathcal{T} = \mathcal{T}^T = P_1 D P_2^T \rho(\mathcal{M}) P_2 D^{-1} P_1^T.$$

Thus we obtain that

$$P_2^T \rho(\mathcal{M}) P_2 = D^2 P_2^T \rho(\mathcal{M}) P_2 D^{-2} \tag{20}$$

(ii) Let $\mathcal{V}$ be a sub $\mathbb{R}$-module of $\mathbb{R}^m$ and E be an $m \times m$ nonsingular symmetric matrix. Assume that V is E^2-invariant, *i.e.*, $E^2 V = V$. We will show that V is E-invariant, *i.e.*, $EV = V$. Let $k = \dim V$. Under the assumption we can take a set of k eigenvectors $w_1, w_2, \ldots, w_k$ of the symmetric matrix E^2 which forms a basis of V. Since $w_1, w_2, \ldots, w_k$ are eigenvectors of the matrix E too and the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$ of E associated with them are real and nonzero, we obtain that

$$EV = E\left\{\sum_{j=1}^{k} \alpha_j w_j : \alpha_j \in \mathbb{R}\right\} = \left\{\sum_{j=1}^{k} \alpha_j \lambda_j w_j : \alpha_j \in \mathbb{R}\right\} = V.$$

(iii) Consider the linear transformation ϕ in $\mathcal{M}_n(\mathbb{R})$ such that

$$\phi(A) = DAD^{-1}$$

or component-wisely

$$\phi(A)_{ij} = D_{ii} D_{jj}^{-1} A_{ij} \ (i, j = 1, 2, \ldots, n)$$

for every $A \in \mathcal{M}_n(\mathbb{R})$. Then the equality (20) can be rewritten as

$$P_2^T \rho(\mathcal{M}) P_2 = \phi(\phi(P_2^T \rho(\mathcal{M}) P_2)). \tag{21}$$

If we identify $\mathcal{M}_n(\mathbb{R})$ with the n^2-dimensional Euclidean space $\mathbb{R}^{n^2}$, then the linear transformation ϕ in $\mathcal{M}_n(\mathbb{R})$ corresponds to a linear transformation associated with the $n^2 \times n^2$ diagonal matrix E with positive entries $D_{ii} D_{jj}^{-1}$ $(i, j = 1, 2, \ldots, n)$, and the identity (21) implies that the sub $\mathbb{R}$-module of $\mathbb{R}^{n^2}$ corresponding to the sub $\mathbb{R}$-module $P_2^T \rho(\mathcal{M}) P_2$ of $\mathcal{M}_n(\mathbb{R})$ is E^2-invariant. Hence we see by the result shown in (ii) above that

$$P_2^T \rho(\mathcal{M}) P_2 = \phi(P_2^T \rho(\mathcal{M}) P_2)$$

or

$$P_2^T \rho(\mathcal{M}) P_2 = D P_2^T \rho(\mathcal{M}) P_2 D^{-1}.$$

Finally, substituting the equality above into (19) and letting $P = P_2 P_1^T$, we obtain that

$$\mathcal{T} = P_1 D^{-1} P_2^T \rho(\mathcal{M}) P_2 D P_1^T = P_1 P_2^T \rho(\mathcal{M}) P_2 P_1^T = P^T \rho(\mathcal{M}) P.$$

∎

Now we are ready to prove Theorem 5.4. Let $\mathcal{T}$ be a *-subalgebra of $\mathcal{M}_n(\mathbb{R})$. Take an orthogonal matrix $\boldsymbol{P} \in \mathcal{M}_n(\mathbb{R})$ as in Lemma 5.9. Let

$$\begin{aligned}
\mathcal{T}_1 &= \left\{\text{diag }(\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1, \boldsymbol{Q}_2^T\boldsymbol{A}\boldsymbol{Q}_2, \ldots, \boldsymbol{Q}_p^T\boldsymbol{A}\boldsymbol{Q}) : \boldsymbol{A} \in \mathcal{T}\right\}, \\
\mathcal{T}_j' &= \left\{\boldsymbol{Q}_j^T\boldsymbol{A}\boldsymbol{Q}_j : \boldsymbol{A} \in \mathcal{T}\right\} \ (j = 1, 2, \ldots, m), \\
\mathcal{I}_j' &= \left\{\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1 : \boldsymbol{Q}_j^T\boldsymbol{A}\boldsymbol{Q}_j = \boldsymbol{O}, \ \boldsymbol{A} \in \mathcal{T}\right\} \ (j = 1, 2, \ldots, m).
\end{aligned}$$

Then each $\mathcal{T}_j'$ is irreducible, so that it is simple by Lemma 5.5. Also we can easily verify that each $\mathcal{I}_j'$ forms an ideal of $\mathcal{T}_1'$. Hence

$$\mathcal{I}_j' = \{\boldsymbol{O}\} \ \text{ or } \mathcal{T}_1' \ (j = 1, 2, \ldots, m).$$

We may assume without loss of generality that

$$\begin{aligned}
\mathcal{I}_j' &= \{\boldsymbol{O}\} \ (j = 1, 2, \ldots, p), \\
\mathcal{I}_j' &= \mathcal{T}_1' \ (j = p, p+1, \ldots, m).
\end{aligned} \tag{22}$$

For every $j = 1, 2 \ldots, p$, the mapping

$$\boldsymbol{\rho}_j : \text{ diag }(\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1, \boldsymbol{Q}_2^T\boldsymbol{A}\boldsymbol{Q}_2, \ldots, \boldsymbol{Q}_p^T\boldsymbol{A}\boldsymbol{Q}_p) \in \mathcal{T}_1 \rightarrow \boldsymbol{Q}_j^T\boldsymbol{A}\boldsymbol{Q}_j \in \mathcal{T}_j'$$

forms a homomorphism from $\mathcal{T}_1$ onto $\mathcal{T}_j'$ such that $\boldsymbol{\rho}_j(\boldsymbol{I}) = \boldsymbol{I}$. This implies that $(\boldsymbol{\rho}_j, \mathbb{R}^{n_j})$ is a representation of $\mathcal{T}_1$ such that $\mathcal{T}_j' = \boldsymbol{\rho}_j(\mathcal{T}_1)$ is irreducible. In particular, $\boldsymbol{\rho}_1 : \mathcal{T}_1 \rightarrow \mathcal{T}_1'$ is faithful. Hence $\mathcal{T}_1$ is simple by Lemma 5.5. Applying Lemma 5.8, we then see that $n_j = n_1$ $(j = 1, 2, \ldots, p)$ and

$$\boldsymbol{Q}_j^T\boldsymbol{A}\boldsymbol{Q}_j = \boldsymbol{R}_j^T\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1\boldsymbol{R}_j \ \text{ for every } \boldsymbol{A} \in \mathcal{T}.$$

for some $n_1 \times n_1$ orthogonal matrix $\boldsymbol{R}_j$ $(j = 1, 2, \ldots, p)$. Therefore we obtain that

$$\begin{aligned}
\mathcal{T}_1 &= \left\{\text{diag }(\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1, \boldsymbol{Q}_2^T\boldsymbol{A}\boldsymbol{Q}_2, \cdots, \boldsymbol{Q}_p^T\boldsymbol{A}\boldsymbol{Q}_p) : \boldsymbol{A} \in \mathcal{T}\right\} \\
&= \left\{\text{diag }(\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1, \boldsymbol{R}_2^T\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1\boldsymbol{R}_2, \cdots, \boldsymbol{R}_p^T\boldsymbol{Q}_1^T\boldsymbol{A}\boldsymbol{Q}_1\boldsymbol{R}_p) : \boldsymbol{A} \in \mathcal{T}\right\} \\
&= \left\{\text{diag }(\boldsymbol{B}, \boldsymbol{R}_2^T\boldsymbol{B}\boldsymbol{R}_2, \cdots, \boldsymbol{R}_p^T\boldsymbol{B}\boldsymbol{R}_p) : \boldsymbol{B} \in \mathcal{T}_1'\right\}
\end{aligned}$$

If $p = m$ then $\mathcal{T} = \mathcal{T}_1$; hence the assertions (A) and (B) follow. Suppose that $p < m$. By (22), there is a matrix $\boldsymbol{A}_j \in \mathcal{T}$ such that

$$\boldsymbol{Q}_1^T\boldsymbol{A}_j\boldsymbol{Q}_1 = \boldsymbol{I} \in \mathcal{T}_1' \subset \mathcal{M}_{n_1}(\mathbb{R}) \ \text{ and } \boldsymbol{Q}_j^T\boldsymbol{A}_j\boldsymbol{Q}_j = \boldsymbol{O} \in \mathcal{T}_j' \subset \mathcal{M}_{n_j}(\mathbb{R})$$

$(j = p+1, p+2, \ldots, m)$. Define

$$\hat{\boldsymbol{A}} = \prod_{j=p+1}^{m} \boldsymbol{A}_j \in \mathcal{T} \subset \mathcal{M}_n(\mathbb{R}) \ \text{ and } \tilde{\boldsymbol{A}} = \boldsymbol{I} - \hat{\boldsymbol{A}} \in \mathcal{T} \subset \mathcal{M}_n(\mathbb{R}).$$

Then

$$\begin{aligned}
\boldsymbol{P}^T\hat{\boldsymbol{A}}\boldsymbol{P} &= \text{diag }(\boldsymbol{I}, \ldots, \boldsymbol{I}, \boldsymbol{O}, \ldots, \boldsymbol{O}) \in \boldsymbol{P}^T\mathcal{T}\boldsymbol{P}, \\
\boldsymbol{P}^T\tilde{\boldsymbol{A}}\boldsymbol{P} &= \text{diag }(\boldsymbol{O}, \ldots, \boldsymbol{O}, \boldsymbol{I}, \ldots, \boldsymbol{I}) \in \boldsymbol{P}^T\mathcal{T}\boldsymbol{P}.
\end{aligned}$$

Hence

$$\begin{aligned} P^T \hat{A} \mathcal{T} P &= \left\{ \text{diag}\ (Q_1^T A Q_1, \ldots, Q_p^T A Q_p, O, \ldots, O) : A \in \mathcal{T} \right\} \subset P^T \mathcal{T} P, \\ P^T \tilde{A} \mathcal{T} P &= \left\{ \text{diag}\ (O, \ldots, O, Q_{p+1}^T A Q_{p+1}, \ldots, Q_m^T A Q_m) : A \in \mathcal{T} \right\} \subset P^T \mathcal{T} P. \end{aligned}$$

It is easily seen that $P^T \hat{A} \mathcal{T} P$ is an ideal of $P^T \mathcal{T} P$; hence $\mathcal{T}$ can not be simple. If we define

$$\tilde{\mathcal{T}} = \left\{ \text{diag}\ (Q_{p+1}^T A Q_{p+1}, \ldots, Q_m^T A Q_m) : A \in \mathcal{T} \right\},$$

then

$$P^T \mathcal{T} P \supset P^T \hat{A} \mathcal{T} P + P^T \tilde{A} \mathcal{T} P = \mathcal{T}_1 \oplus \tilde{\mathcal{T}}.$$

By the construction, we obviously see that

$$P^T \mathcal{T} P \subset \mathcal{T}_1 \oplus \tilde{\mathcal{T}}.$$

Therefore we have shown that

$$P^T \mathcal{T} P = \mathcal{T}_1 \oplus \tilde{\mathcal{T}}.$$

Applying the same argument as above repeatedly to the *-subalgebra $\tilde{\mathcal{T}}$, we obtain the assertion (A).

Now prove the assertion (C). Suppose that $\mathcal{T}$ is an irreducible *-subalgebra of $\mathcal{M}_n(I\!R)$. By Lemma 5.7, there is a faithful representation $(\rho', I\!R^n)$ of $\mathcal{M}$ such that $\rho'(\mathcal{M}) = \mathcal{T}$. Let $(\tilde{\rho}, I\!R^n)$ be the faithful *-representation of $\mathcal{M}$ given in Section 3. Since both $\mathcal{T}$ and $\tilde{\rho}(\mathcal{M})$ are *-subalgebras, we obtain the desired result by Lemma 5.10. This completes the proof of Theorem 5.4.

References

[1] W. F. Alizadeh, "Interior point methods in semidefinite programming with applications to combinatorial optimization," *SIAM Journal on Optimization* **5** (1995) 13–51.

[2] W. F. Alizadeh, J-P. A. Haeberly and M. J. Overton, "Primal-dual interior-point methods for semidefinite programming," Technical paper, Computer Science Department, Rutgers University, August, 1994.

[3] B. D. Craven and B. Mond, "Linear programming with matrix variables," *Linear Algebra and Its Applications* **38** (1981) 73–80.

[4] S. Boyd, L. E. Ghaoui, E. Feron and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory,* (SIAM, Philadelphia, 1994).

[5] R. W.Cottle, J. S. Pang, R. E. Stone, *The Linear Complementarity Problem,* (Academic Press, New York, 1992).

[6] O. Güler, "Barrier functions in interior point methods," Dept. of Mathematics and Statistics, University of Maryland Baltimore County, Baltimore, Maryland 21228, USA, 1994.

[7] N. Iwahori, *Taishougun to ippan senkeigun no hyougenron (The Representation Theory of Symmetric Group and General Linear Group)* in Japanese, Iwanami, Kiso sugaku, Senkei daisu vi (Iwanami shoten, 1978).

[8] M. Kojima, N. Megiddo, T. Noma, A. Yoshise, *A Unified Approach to Interior Point Algorithms for Linear Complementarity Problems,* Lecture Notes in Computer Science 538, (Springer-Verlag, New York, 1991).

[9] M. Kojima, S. Mizuno and A. Yoshise, "A primal-dual interior point algorithm for linear programming," In N. Megiddo, ed., *Progress in Mathematical Programming, Interior-Point and Related Methods* (Springer-Verlag, New York, 1989) 29–47.

[10] M. Kojima, S. Mizuno and A. Yoshise, "A polynomial-time algorithm for a class of linear complementary problems," *Mathematical Programming* **44** (1989) 1–26.

[11] M. Kojima, S. Mizuno and A. Yoshise, "An $O(\sqrt{n}L)$ iteration potential reduction algorithm for linear complementarity problems," *Mathematical Programming* **50** (1991) 331–342.

[12] M. Kojima, S. Shindoh and S. Hara, "Interior-point methods for the monotone semidefinite linear complementarity problems in symmetric matrices," Research Reports B-282, Dept. of Information Sciences, Tokyo Institute of Technology, Oh-Okayama, Meguro, Tokyo 152, April 1994, Revised April 1995, to appear in *SIAM Journal on Optimization.*

[13] K. O. Kortanek and J. Zhu, "A polynomial algorithm for convex programming problems satisfying scaled Lipschitz condition," Working Paper Series 90-17, Dept. of Management Sciences, College of Business Administration, The University of Iowa, Iowa City, Iowa 52242, 1990.

[14] I. J. Lustig, "Feasibility issues in primal-dual interior-point method for linear programming," *Mathematical Programming* **49** (1990/1991) 145–162.

[15] I. J. Lustig, R. E. Marsten and D. F. Shanno, "Computational experience with a primal-dual interior-point method for linear programming," *Linear Algebra and Its Applications* **152** (1991) 191–222.

[16] R. Marsten, R. Subramanian, M. Saltzman, I. Lustig and D. Shanno, "Interior point methods for linear programming: Just call Newton, Lagrange, and Fiacco and McCormick!" *Interface* **20** (1990) 105–116.

[17] N. Megiddo, "Pathways to the optimal set in linear programming," In N. Megiddo, ed., *Progress in Mathematical Programming, Interior-Point and Related Methods* (Springer-Verlag, New York, 1989) 131–158.

[18] S. Mizuno, M. Kojima and M. J. Todd, "Infeasible-interior-point primal-dual potential-reduction algorithms for linear programming," *SIAM Journal on Optimization* **1** (1995) 52–67.

[19] R. D. C. Monteiro and I. Adler, "Interior path following primal-dual algorithms. Part I: Linear programming," *Mathematical Programming* **44** (1989) 27–41.

[20] R. D. C. Monteiro and I. Adler, "Interior path following primal-dual algorithms. Part II: Convex quadratic programming," *Mathematical Programming* **44** (1989) 43–66.

[21] Y. E. Nesterov and A. S.Nemirovskii, *Interior Point Polynomial Methods in Convex Programming: Theory and Applications* (SIAM, Philadelphia, 1993).

[22] Y. E. Nesterov and M. J. Todd, "Self-scaled cones and interior-point methods in nonlinear programming," Catholic University of Louvain, Louvain-la-Neuve, Belgium, 1994.

[23] A. Packard, K. Zhou, P. Pandey and G. Becker, "A collection of robust control problems leading to LMI's," *Proceedings of the 30th Conference on Decision and Control,* Brighton, England, December 1991, pp.1245–1250.

[24] F. A. Potra and Y. Ye, "Interior point methods for nonlinear complementarity problems," Technical report, Dept. of Mathematics, The University of Iowa, Iowa City, Iowa 52242, 1991.

[25] C. E. Rickart, *General Theory of Banach Algebras*, (Van Nostrand Co., 1960).

[26] K. Tanabe, "Centered Newton method for mathematical programming," In M. Iri and K. Yajima, eds., *System Modeling and Optimization* (Springer-Verlag, New York, 1988).

[27] L. Vandenberghe and S. Boyd, "A primal-dual potential reduction method for problems involving matrix inequalities," *Mathematical Programming, Series B* **69** (1995) 205–236.

[28] H. Weyl, *The Classical Groups*, Princeton University Press, Princeton, New Jersey, 1946.

[29] Y. Zhang, "On the convergence of an infeasible interior-point algorithm for linear programming and other problems," *SIAM Journal on Optimization* **4** (1994) 208–227.