Semidefinite Programming and Applications: Lecture Note
Exploiting symmetry in semidefinite programming

Fernando Mário de Oliveira Filho
Institut für Mathematik, FU Berlin
fmario@math.fu-berlin.de

1. Invariant semidefinite programs. Let $C, A_1, \ldots, A_m \in \mathbb{C}^{V\times V}$ be Hermitian matrices, where V is a finite set. Consider the complex semidefinite programming problem

$$\begin{array}{ll}\max & \langle C, X\rangle \\ & \langle A_i, X\rangle = b_i, \quad \text{for } i = 1, \ldots, m, \\ & X \in \mathbb{C}^{n\times n}, \quad X \succeq 0.\end{array} \tag{1}$$

Let G be a finite group acting on V. We denote the action of $g \in G$ on an element $v \in V$ by $g \cdot v$. If $A \in \mathbb{C}^{V\times V}$ is a matrix, then for $g \in G$ we write $g \cdot A$ for the matrix such that $(g \cdot A)(u, v) = A(g \cdot u, g \cdot v)$ for all u, $v \in V$. We say that matrix A is *G-invariant* if $g \cdot A = A$ for all $g \in G$.

We say that (1) is *G-invariant* if, for every feasible solution $X \in \mathbb{C}^{V\times V}$ and every $g \in G$ we have that $g \cdot X$ is also a feasible solution and $\langle C, g \cdot X\rangle = \langle C, X\rangle$. In particular, notice that if the matrices C and $A_1, \ldots, A_m$ are G-invariant, then also (1) is G-invariant.

Suppose problem (1) is G-invariant. Then when solving it, one may restrict oneself to G-invariant solutions. Indeed, if $X \in \mathbb{C}^{V\times V}$ is any feasible solution of (1), then

$$\overline{X} = \frac{1}{|G|}\sum_{g\in G} g \cdot X$$

is G-invariant and feasible, and its objective value is the same as that of X.

Consider the vector space $\mathcal{W}$ of all G-invariant matrices. When solving (1), we may restrict ourselves to matrices in this vector space. Our aim is to use this fact to simplify our problem.

Notice that G acts on $V\times V$ by $g\cdot(u, v) = (g\cdot u, g\cdot v)$ for all $(u, v) \in V\times V$. Let $O_1, \ldots, O_N$ be the orbits of this action, that is, for (u, v), $(u', v') \in V\times V$ we write $(u, v) \sim (u', v')$ if there is $g \in G$ such that $(u, v) = g \cdot (u', v')$. Note $\sim$ gives an equivalence relation, and $O_1, \ldots, O_N$ are the equivalence classes of this relation.

With this, matrices $M_1, \ldots, M_N \in \mathbb{C}^{V\times V}$ such that

$$M_k(u, v) = \begin{cases} 1 & \text{if } (u, v) \in O_k; \\ 0 & \text{otherwise,}\end{cases}$$

form an orthogonal basis of $\mathcal{W}$.

So, $X \in \mathbb{C}^{V\times V}$ is G-invariant if and only if

$$X = \alpha_1 M_1 + \cdots + \alpha_N M_N$$

for some numbers $\alpha_1, \ldots, \alpha_N$. This means we may rewrite problem (1) as:

$$\begin{array}{lll}\max & \sum_{k=1}^N \alpha_k \langle C, M_k\rangle & \\ & \sum_{k=1}^N \alpha_k \langle A_i, M_k\rangle = b_i & \text{for } i = 1, \ldots, m, \\ & \alpha_k = \overline{\alpha_{k'}} & \text{if } M_k = M_{k'}^{\mathrm{T}}, \\ & \sum_{k=1}^N \alpha_k M_k \succeq 0. & \end{array}$$

Above, constraint $\alpha_k = \overline{\alpha_{k'}}$ when $M_k = M_{k'}^{\mathrm{T}}$ ensures that matrix $\alpha_1 M_1 + \cdots + \alpha_N M_N$ will be Hermitian. Our main job is to rewrite the constraint

$$\sum_{k=1}^N \alpha_k M_k \succeq 0 \tag{2}$$

in a simpler form.

---

* *Date:* 11/06/2012.

2. Matrix $*$-algebras and the regular representation. We say that a set $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ is a *matrix $*$-algebra* if (i) $\mathcal{A}$ is a complex vector space; (ii) $\mathcal{A}$ is closed under taking the conjugate transpose, i.e., if $A \in \mathcal{A}$ then also $A^* \in \mathcal{A}$; and (iii) $\mathcal{A}$ is closed under multiplication, i.e., if A, $B \in \mathcal{A}$ then $AB \in \mathcal{A}$.

An example of a matrix $*$-algebra is the space $\mathbb{C}^{n\times n}$ of all $n \times n$ complex matrices. Another example is the space $\mathcal{W}$ of matrices invariant under the action of some group. Indeed, suppose G is a finite group acting on the finite set V. Then, if $\mathcal{W}$ is the space of G-invariant matrices we have

$$\mathcal{W} = \{\, A \in \mathbb{C}^{V\times V} : P_g^{\mathrm{T}} A P_g = A \text{ for } g \in G \,\},$$

where $P_g \in \mathbb{C}^{V\times V}$ is the permutation matrix associated with element $g \in G$. From this identity one may easily show that $\mathcal{W}$ is a matrix $*$-algebra.

Let $\mathcal{A}$, $\mathcal{B}$ be matrix $*$-algebras. A *$*$-homomorphism* is a linear function $\phi\colon \mathcal{A} \to \mathcal{B}$ such that (i) $\phi(A^*) = \phi(A)^*$ for all $A \in \mathcal{A}$ and (ii) $\phi(AB) = \phi(A)\phi(B)$ for all A, $B \in \mathcal{A}$. If, moreover, $\mathcal{A}$ contains the identity matrix $I_{\mathcal{A}}$, then we require that $\phi(I_{\mathcal{A}}) = I_{\mathcal{B}}$.

It follows from the Cayley-Hamilton theorem that, if $\mathcal{A}$ is a matrix $*$-algebra containing the identity matrix, then whenever $A \in \mathcal{A}$ is invertible, then also $A^{-1} \in \mathcal{A}$. This implies that, if $\mathcal{A}$ and $\mathcal{B}$ are both matrix $*$-algebras containing the identity, and if $\phi\colon \mathcal{A} \to \mathcal{B}$ is an *injective* $*$-homomorphism, then one has that $A \in \mathcal{A}$ is singular if and only if $\phi(A)$ is singular. This implies in particular that A and $\phi(A)$ have the same eigenvalues, and so we have:

Theorem 1. *Let $\mathcal{A}$ and $\mathcal{B}$ be matrix $*$-algebras containing the identity. Suppose $\phi\colon \mathcal{A} \to \mathcal{B}$ is an injective $*$-homomorphism. Then $A \in \mathcal{A}$ is positive semidefinite if and only if $\phi(A)$ is positive semidefinite.*

Now, since $\mathcal{W}$ is a matrix $*$-algebra, if we find another matrix $*$-algebra $\mathcal{V}$ and an injective $*$-homomorphism $\phi\colon \mathcal{W} \to \mathcal{V}$, we may rewrite condition (2) equivalently as

$$\sum_{k=1}^{N} \alpha_k \phi(M_k) \succeq 0.$$

If the matrices in $\mathcal{V}$ are smaller than the ones in $\mathcal{W}$, then we have a computationally simpler constraint to work with.

The main result behind this approach is the following powerful theorem known as the Wedderburn-Artin theorem:

Theorem 2. *Let $\mathcal{A}$ be a matrix $*$-algebra containing the identity matrix. Then $\mathcal{A}$ is isomorphic to the algebra*

$$\bigoplus_{k=1}^{d} \mathbb{C}^{n_k\times n_k}$$

for some numbers d and n_k. Notice we then have $\sum_{k=1}^{d} n_k^2 = \dim \mathcal{A}$.

We say that a matrix $*$-algebra $\mathcal{A}$ is *commutative* if $AB = BA$ for all A, $B \in \mathcal{A}$. A special case of the above theorem is the following classical result:

Theorem 3. *A commutative matrix $*$-algebra $\mathcal{A} \subseteq \mathbb{C}^{n\times n}$ can be diagonalized, that is, there is a unitary matrix $U \in \mathbb{C}^{n\times n}$ such that the matrix U^*AU is diagonal for each $A \in \mathcal{A}$.*

Proof. Let $A_1, \ldots, A_r$ be a basis of $\mathcal{A}$. We claim that $A_1, \ldots, A_r$ have a common eigenvector. To show this, we proceed by induction in r.

If $r = 1$, the claim is obvious. Suppose $r > 1$. Let λ be an eigenvalue of A_r and write

$$E_\lambda = \{\, v \in \mathbb{C}^n : A_r v = \lambda v \,\}.$$

Then for $i = 1, \ldots, r-1$ and $v \in E_\lambda$ we have that $A_r(A_i v) = A_i A_r v = \lambda A_i v$, and so we see that $A_i v \in E_\lambda$. So, the restriction of each A_i to E_λ is a linear transformation, and they commute. This means that $A_1, \ldots, A_{r-1}$ have a common eigenvector (by induction hypothesis), and since this eigenvector belongs to E_λ it is also an eigenvector of A_r. So $A_1, \ldots, A_r$, and therefore all matrices in $\mathcal{A}$, have a common eigenvector, say $e \in \mathbb{C}^n$, proving the claim.

Let V be the space of vectors orthogonal to e. Then for $A \in \mathcal{A}$ and $x \in V$ we have

$$e^*(Ax) = (A^*e)^*x = \mu e^*x = 0$$

for some number μ, since e is also an eigenvector of $A^* \in \mathcal{A}$. So we see that $Ax \in V$. With this we may restrict the linear transformations $A_1, \ldots, A_r$ to the space V and proceed by induction again, finding at the end an orthogonal basis of $\mathbb{C}^{n\times n}$ of common eigenvectors of $A_1, \ldots, A_r$. ■

It is not always easy to compute the isomorphism that the Wedderburn-Artin theorem asserts to exist. There is however a simpler, mechanical way to, given a $*$-algebra $\mathcal{A}$, obtain a $*$-algebra $\mathcal{B}$ with rather small matrices and an injective $*$-homomorphism $\phi\colon \mathcal{A} \to \mathcal{B}$.

Let $\mathcal{A}$ be a $*$-algebra and let $M_1, \ldots, M_N$ be a basis of $\mathcal{A}$. To a matrix $A \in \mathcal{A}$ we may assign a linear transformation $A_{\mathrm{L}}\colon \mathcal{A} \to \mathcal{A}$ which is such that

$$A_{\mathrm{L}}(X) = AX$$

for all $X \in \mathcal{A}$, that is, A_{L} is the left multiplication by A.

Each transformation A_{L} for $A \in \mathcal{A}$ has a matrix representation in the basis $M_1, \ldots, M_N$, which we denote by $M(A) \in \mathbb{C}^{N\times N}$. The *regular $*$-representation* of $\mathcal{A}$ is then the function $\mathcal{R}\colon \mathcal{A} \to \mathbb{C}^{N\times N}$ which assigns to each matrix $A \in \mathcal{A}$ the matrix $M(A)$.

It is easy to show that $\mathcal{R}$ gives a $*$-homomorphism between $\mathcal{A}$ and $\mathbb{C}^{N\times N}$. Moreover, if $\mathcal{A}$ contains the identity matrix, then this homomorphism is injective. Notice moreover that, whatever the sizes of the matrices M_k might be, their images under the homomorphism $\mathcal{R}$ are $N \times N$ matrices, where N is the dimension of $\mathcal{A}$.

Matrices $\mathcal{R}(M_k)$ may be explicitly computed. Indeed, one has that

$$(M_k)_{\mathrm{L}} M_j = M_k M_j = \sum_{i=1}^{N} \alpha_{ij}^k M_i$$

for some numbers α_{ij}^k, and so the entries of $\mathcal{R}(M_k)$ are given as $\mathcal{R}(M_k)_{ij} = \alpha_{ij}^k$, for $i, j = 1, \ldots, N$. Notice that, in particular, if the matrices $M_1, \ldots, M_N \in \mathcal{A}$ are all real (as is the case for the space $\mathcal{W}$ of G-invariant matrices), then all the matrices $\mathcal{R}(M_k)$ will be real. This means that, if we have a real semidefinite programming problem from the beginning, then by using the regular $*$-representation we do not need to consider complex numbers at any point. Notice that this is not necessarily the case with the Wedderburn-Artin theorem.

So the regular $*$-representation is a simple way to obtain potentially smaller matrices from our original matrices without having to work hard for it. In practical applications, like for instance for computing bounds for binary codes, the matrices M_k can be quite big, but one may find closed formulas for the numbers α_{ij}^k, so that it is not necessary to use the computer to compute these numbers, or at any point to work explicitly with the matrices M_k.

3. References.

[1] C. Bachoc, D.C. Gijswijt, A. Schrijver, and F. Vallentin, Invariant semidefinite programs, in: *Handbook on Semidefinite, Conic, and Polynomial Optimization* (M.F. Anjos and J.B. Lasserre, eds.), Springer-Verlag, Berlin, 2012.