A Crash Course on Semidefinite Programming

MCS 521, Fall 2017
LCD-grad 38317,
Tu&Th 4–5:15, Lincoln Hall 201
Instructor: Shmuel Friedland
Office: 715 SEO, phone: (312) 413-2176, *e:mail*: friedlan@uic.edu,
web: http://www.math.uic.edu/∼friedlan

Last update December 4, 2017

1 Symmetric matrices

1.1 General matrices

For a positive integer n let $[n] = \{1, \ldots, n\}$. Denote by $\mathbb{R}^n$ the n-dimensional space of real vectors $\mathbf{x} = (x_1, \ldots, x_n)^\top$. On $\mathbb{R}^n$ we have the standard inner product $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^\top \mathbf{y}$. Denote by $\mathbb{R}^{m\times n}$ the vector space of $m \times n$ matrices. A matrix $A \in \mathbb{R}^{m\times n}$ has entry a_{ij} in the row i and column j. It would be convenient to denote sometime the (i,j) entry of A as $(A)_{ij} = a_{ij}$. So we abbreviate is as $A = [a_{ij}]_{i,j=1}^{m,n}$ or simply $A = [a_{ij}]$. Recall that $\dim \mathbb{R}^{m\times n} = mn$. A standard basis in $\mathbb{R}^{m\times n}$ is the set of matrices E_{pq} , for $p \in [m], q \in [n]$, whose $(i,j) - th$ entry is $\delta_{pi}\delta_{pj}, i \in [m], j \in [n]$, where δ_{st} is the Kronecker δ. Recall that $A^\top \in \mathbb{R}^{n\times m}$ and $(A^\top)_{ij} = (A)_{ji}$.

Assume that $A = [a_{ij}] \in \mathbb{R}^{n\times n}$. A has n-complex eigenvalues $\lambda_1(A), \ldots, \lambda_n(A)$, which are all the n-complex roots, counting with their multiplicities, of $\det(zI_n - A)$. (Here $I_n = [\delta_{ij}] \in \mathbb{R}^{n\times n}$ is the identity matrix of order n.) Then the trace of A, denoted as $\operatorname{tr} A$, is $\sum_{i=1}^n a_{ii}$. Recall that $\operatorname{tr} A = \sum_{i=1}^n \lambda_i(A)$. Clearly $\operatorname{tr} A = \operatorname{tr} A^\top$.

The space $\mathbb{R}^{m\times n}$ has a standard inner product, when one identifies $\mathbb{R}^{m\times n}$ with $\mathbb{R}^{mn}$. Namely, if $A = [a_{ij}], B = [b_{ij}] \in \mathbb{R}^{m\times n}$, then $\langle A, B\rangle = \sum_{i,j=1}^{m,n} a_{ij}b_{ij}$. Note that the standard basis $E_{pq}, p \in [m], q \in [n]$ is an orthonormal basis for this inner product. It is straightforward to show that

$$\langle A, B\rangle = \operatorname{tr} AB^\top = \operatorname{tr} B^\top A = \operatorname{tr} BA^\top.$$

The induced Euclidean norm $\|A\| = \sqrt{\operatorname{tr} AA^\top} = \sqrt{\sum_{i,j=1}^{m,n} a_{ij}^2}$ is called the Frobenius norm on $\mathbb{R}^{m\times n}$.

1.2 Space of symmetric matrice

A matrix $A \in \mathbb{R}^{n\times n}$ is called symmetric if $A = A^\top$. Denote by $\mathrm{S}_n \subset \mathbb{R}^{n\times n}$ the subspace of symmetric matrices of order n. Recall that $\dim \mathrm{S}_n = \frac{n(n+1)}{2} = \binom{n+1}{2}$. Then the induced inner product on S_n is $\langle A, B\rangle = \operatorname{tr} AB$. An orthogonal basis in S_n is $\frac{1}{2}(E_{pq} + E_{qp})$ for $1 \le p \le q \le n$.

A system of linear equations in S_n is

$$\langle A_i, X\rangle = b_i, \quad X, A_i \in \mathrm{S}_n, \quad i \in [m]. \tag{1.1}$$

Here, we view X as an unknown vector, and $A_1, \ldots, A_m \in \mathrm{S}_n$ are given. Geometrically, (1.1) is a hyperplane in S_n. Recall the necessary and sufficient conditions of solvability of (1.1). For each nontrivial linear combination of $A_1, \ldots, A_m$ which vanish the corresponding linear combination of $b_1, \ldots, b_m$ also vanish:

$$\sum_{i=1}^{m} a_i A_i = 0 \Rightarrow \sum_{i=1}^{m} a_i b_i = 0.$$

Assume that (1.1) is solvable. Perform the Gram-Schmidt process on $A_1, \ldots, A_m$ to obtain an orthonormal basis in $\mathrm{span}(A_1, \ldots, A_m)$: $A'_1, \ldots, A'_{m'}$. The the system (1.1)is equivalent to

$$\langle A'_i, X\rangle = b'_i, \quad X, A'_i \in \mathrm{S}_n, \quad \langle A'_i, A'_j\rangle = \delta_{ij}, i, j \in [m']. \tag{1.2}$$

For simplicity of notation we will assume sometimes that the system (1.1) is already in the form (1.2). That is, in addition to (1.1) we have the condition

$$\langle A_i, A_j\rangle = \delta_{ij}, \quad i, j \in [m]. \tag{1.3}$$

Next recall that $A \in \mathrm{S}_n$ has n real eigenvalues with corresponding set of orthonormal eigenvectors:

$$A\mathbf{x}_i = \lambda_i(A)\mathbf{x}_i,\ \mathbf{x}_i \in \mathbb{R}^n, \quad \mathbf{x}_j^\top \mathbf{x}_i = \delta_{ij}, i, j \in [n], \tag{1.4}$$

$$\lambda_{\max}(A) = \lambda_1(A) \ge \cdots \ge \lambda_n(A) = \lambda_{\min}(A). \tag{1.5}$$

The eigenvalues max and min of A have the Rayleigh characterization [2]

$$\lambda_{\max}(A) = \max_{\mathbf{x}\neq\mathbf{0}} \frac{\mathbf{x}^\top A\mathbf{x}}{\mathbf{x}^\top\mathbf{x}}, \quad \lambda_{\min}(A) = \min_{\mathbf{x}\neq\mathbf{0}} \frac{\mathbf{x}^\top A\mathbf{x}}{\mathbf{x}^\top\mathbf{x}}.$$

1.3 The cone of positive semidefinite matrices

$A \in \mathrm{S}_n$ is called positive definite or positive semidefinite,(nonnegative definite), denoted as $A \succ 0$ or $A \succeq 0$, if $\lambda_{\min}(A) > 0$ or $\lambda_{\min}(A) \ge 0$. This is equivalent to $\mathbf{x}^\top A\mathbf{x} > 0$ or $\mathbf{x}^\top A\mathbf{x} \ge 0$ for all $\mathbf{x} \neq 0$.

The following results are well known [2]. $A \succ 0$ if and only if all leading principal minors are positive:

$$\det([a_{ij}]_{i,j=1}^k) > 0, \quad k \in [n].$$

$A \succeq 0$ if and only if all principal minors of A are nonnegative.

Deciding if $A \succ 0$ or $A \succeq 0$ is polynomial if $A \in \mathrm{S}_n(\mathbb{Q})$, where $\mathrm{S}_n(\mathbb{Q}) = \mathrm{S}_n \cap \mathbb{Q}^{n\times n}$.

Algorithm 1.1 *Let $A = [a_{ij}] \in \mathrm{S}_n$.*

1. *If $a_{11} < 0$ then A is not positive semidefinite.*

2. *If $a_{11} = 0$ then A is not positive semidefinite if $\sum_{i=2}^n a_{1i}^2 + a_{i1}^2 > 0$. (This is implied by the fact that all 2×2 principal minors are nonnegative.)*

3. *Assume that* $a_{1i} = a_{i1} = 0$ *for* $i \in [n]$. *Thus* $A = [0] \oplus A_1$, *where* $A_1 \in \mathrm{S}_{n-1}$. *Then* $A \succeq 0 \iff A_1 \succeq 0$.

4. *Assume* $a_{11} > 0$. *Perform the following Gauss eliminations: For* $i = 2, \ldots, n$ *subtract from row* i $\frac{a_{i1}}{a_{11}}$ *times row one, and from column* i $\frac{a_{1i}}{a_{11}}$ *times column one. Call the resulting matrix* $A' \in \mathrm{S}_n$. *So* $A' = [a_{11}] \oplus A_1$. *Then*

$$A \succ 0 \iff A_1 \succ 0, \quad A \succeq 0 \iff A_1 \succeq 0.$$

Denote by $\mathrm{S}_{n,+} = \{A \in \mathrm{S}_n, A \succeq 0\}$. Note that $\mathrm{S}_{n,+}$ is a closed set, with the interior $\mathrm{S}^o_{n,+} = \{A \in \mathrm{S}_n, A \succ 0\}$. So $\mathrm{S}_{n,+}$ is a *cone*: $A, B \in \mathrm{S}_{n,+} \Rightarrow aA + bB \in \mathrm{S}_{n,+}$ for $a, b \geq 0$. It is a pointed cone: $\mathrm{S}_{n,+} \cap (-\mathrm{S}_{n,+}) = \{0\}$. (Here $-\mathrm{S}_{n,+} = \{A, -A \in \mathrm{S}_{n,+}\}$.) It is a generating cone: $\mathrm{S}_n = \mathrm{S}_{n,+} - \mathrm{S}_{n,+}$.

Indeed, for $x \in \mathbb{R}$ let $x_+ = \max(x, 0), x_- = \max(-x, 0)$. So $x = x_+ - x_-$. Recall that the spectral decomposition of A induced by (1.4) is

$$A = Q\Lambda Q^\top,\ Q = [\mathbf{x}_1, \ldots, \mathbf{x}_n], \Lambda = \mathrm{diag}(\lambda_1(A), \ldots, \lambda_n(A)).$$

So Q is an orthogonal matrix, i.e., $Q^\top Q = I_n$. Here $D = \mathrm{diag}(d_1, \ldots, d_n)$ denotes the diagonal matrix with the diagonal entries $d_1, \ldots, d_n$. For a diagonal matrix D as above set

$$D_+ = \mathrm{diag}((d_1)_+, \ldots, (d_n)_+),\ D_- = (\mathrm{diag}((d_1)_-, \ldots, (d_n)_-).$$

So $D_+, D_- \in \mathrm{S}_{n,+}$, and $D = D_+ - D_-$ and $A = Q\Lambda_+ Q^\top - Q\Lambda_- Q^\top$ are the decompositions of D and A to a difference of two positive semidefinite matrices.

Recall that any linear functional $\phi : \mathrm{S}_n \to \mathbb{R}$ is of the form $\phi(X) = \langle X, C\rangle$ for some $C \in \mathrm{S}_n$.

Lemma 1.2 *Denote by* $\mathrm{S}^\vee_{n,+}$ *the dual cone of all linear functionals on* S_n *which are nonnegative on* $\mathrm{S}_{n,+}$. *Then* $\mathrm{S}^\vee_{n,+} = \mathrm{S}_{n,+}$.

Proof. Assume that $C = Q\Lambda(C)Q^\top$ is the spectral decomposition of C. Then $\langle X, C\rangle = \mathrm{tr}(XC) = \mathrm{tr}((Q^\top XQ)\Lambda(C))$. Clearly $Q^\top \mathrm{S}_{n,+} Q = \mathrm{S}_{n,+}$. So it is enough to show that $\mathrm{tr}(YD) \geq 0$ for a diagonal D for each $Y \in \mathrm{S}_{n,+}$ if and only if the diagonal entries of $D = \mathrm{diag}(d_1, \ldots, d_n)$ are nonnegative. Clearly, a diagonal Y is positive semidefinite if and only if the diagonal entries are nonnegative. Hence if $\mathrm{tr}(E_{ii}D) \geq 0$ for $i \in [n]$ then D has nonnegative diagonal entries. Suppose now that $Y = [y_{ij}] \succeq 0$. Hence $y_{ii} \geq 0$ for $i \in [n]$. Now $\mathrm{tr}(YD) = \sum_{i=1}^n y_{ii} d_i \geq 0$ if all the diagonal entries of D are nonnegative. $\square$

The cone $\mathrm{S}_{n,+}$ induces the partial order $A \succeq B$ and $A \succ B$ which is equivalent to $A - B \succeq 0$ and $A - B \succ 0$ respectively.

Corollary 1.3 *Let* $A, B, X \in \mathrm{S}_n$. *Suppose that* $A \succeq B$ *and* $X \succeq 0$. *Then* $\langle A, X\rangle \geq \langle B, X\rangle$. *Suppose furthermore that* $A \succ B$ *and* $X \neq 0$. *Then* $\langle A, X\rangle > \langle B, X\rangle$.

2 Semidefinite programming

2.1 The duality theorem of linear programming

Let $A \in \mathbb{R}^{m\times n}, \mathbf{c} \in \mathbb{R}^n, \mathbf{b} \in \mathbb{R}^m$. Then one has the following two linear programming problems, (LP problems):

$$\inf\{\mathbf{c}^\top \mathbf{x}, \quad \mathbf{x} \geq \mathbf{0}, A\mathbf{x} = \mathbf{b}\}, \tag{2.1}$$

$$\sup\{\mathbf{b}^\top \mathbf{y}, \quad A^\top \mathbf{y} \leq \mathbf{c}\}. \tag{2.2}$$

These two LP problems are called dual LP problems. It is understood that if the set $\mathbf{x} \geq \mathbf{0}, A\mathbf{x} = \mathbf{b}$ is empty then the infimum in (2.1) is ∞, and if the set $A^\top \mathbf{y} \leq \mathbf{c}$ is empty the the supremum in (2.2) is $-\infty$.

Proposition 2.1 *(Weak duality) Assume that* $A\mathbf{x}_0 = \mathbf{b}, \mathbf{x}_0 \geq \mathbf{0}$ *and* $A^\top \mathbf{y}_0 \leq \mathbf{c}$. *Then* $\mathbf{b}^\top \mathbf{y}_0 \leq \mathbf{c}^\top \mathbf{x}_0$.

Proof. The above conditions imply straightforward

$$\mathbf{b}^\top \mathbf{y}_0 = (A\mathbf{x}_0)^\top \mathbf{y}_0 = \mathbf{x}_0^\top (A^\top \mathbf{y}_0) \leq \mathbf{x}_0^\top \mathbf{c} = \mathbf{c}^\top \mathbf{x}_0.$$

Theorem 2.2 *Assume that at least one of the sets in* (2.1) *and* (2.2) *is feasible. Then the infimum in* (2.1) *is equal to the supremum in* (2.2). *Suppose furthermore that the assumption of Proposition 2.1 holds. Then the infimum in* (2.1) *is* min *and the supremum in* (2.2) *are* max, *i.e., they are both attained and equal.*

See for example [1, Appendix A].

2.2 The weak duality theorem of semidefinite programming

Let $C \in \mathrm{S}_n, \mathbf{b} = (b_1, \ldots, b_m)^\top \in \mathbb{R}^m, \mathbf{y} = (y_1, \ldots, y_m)^\top \in \mathbb{R}^m$. The dual semidefinite programming problems are

$$\inf\{\langle C, X\rangle, X \succeq 0, \langle A_i, X\rangle = b_i, i \in [m]\}, \tag{2.3}$$

$$\sup\{\mathbf{b}^\top \mathbf{y}, \mathbf{y} = (y_1, \ldots, y_m)^\top \in \mathbb{R}^m, \sum_{i=1}^m y_i A_i \preceq C\}. \tag{2.4}$$

Again, we have the same convention as in the LP case. If the set in (2.3) is empty then the inf $= \infty$, and if the set in (2.4) is empty then the sup $= -\infty$.

Proposition 2.3 *Assume that the system* (1.1) *is solvable. Then the problem* (2.4) *can be stated as a following supremum problem*

$$\sup\{\langle F, Y\rangle, Y \succeq 0, \langle B_i, Y\rangle = e_i, i \in [\ell]\}, \tag{2.5}$$

plus a constant, for some $Y, B_1, \ldots, B_\ell \in \mathrm{S}_{n,+}$.

Proof. Since the system (1.1) is solvable, it is equivalent to the system (1.2). We first show that (2.4) is equivalent to the set of dual problems:

$$\inf\{\langle C, X\rangle, X \succeq 0, \langle A_i', X\rangle = b_i', i \in [m']\}, \tag{2.6}$$

$$\sup\{(\mathbf{b}')^\top \mathbf{y}', \mathbf{b}' = (b_1', \ldots, b_{m'}')^\top, \mathbf{y}' = (y_1', \ldots, y_m')^\top \in \mathbb{R}^{m'}, \sum_{i=1}^{m'} y_i' A_i' \preceq C\}. \tag{2.7}$$

Indeed, since (1.1) and (1.2) gives the same hyperplane in S_n we obtain that the problems (2.3) is equal to the problem of (2.6). To show that (2.4) and (2.7) are equivalent problems, it is enough to recall

$$A_i = \sum_{j=1}^{m'} t_{ij} A'_j,\ b_i = \sum_{j=1}^{m'} t_{ij} b'_j.$$

Then

$$\sum_{i=1}^{m} y_i A_i = \sum_{j=1}^{m'} y'_j A'_j, \quad y'_j = \sum_{i=1}^{m} y_i t_{ij}.$$

Hence $\mathbf{b}^\top \mathbf{y} = (\mathbf{b}')^\top \mathbf{y}'$.

By abusing the notation, we can assume that $\langle A_i, A_j\rangle = \delta_{ij}$ for $i, j \in [m]$. Let $A_1, \ldots, A_m, A_{m+1}, \ldots, A_{\frac{n(n+1)}{2}}$ be an orthonormal basis in S_n. Observe next that the inequality $\sum_{i=1}^m y_i A_i \preceq C$ is equivalent to

$$Y + \sum_{i=1}^{m} y_i A_i = C, \quad Y \succeq 0. \tag{2.8}$$

Let

$$\ell = \frac{n(n+1)}{2} - m, B_i = A_{m+i}, e_i = \langle B_i, C\rangle \text{ for } i \in [\ell].$$

Assume that $Y \succeq 0$ and $\langle B_i, Y\rangle = e_i$ for $i \in [\ell]$. Hence $C - Y \in \mathrm{span}(A_1, \ldots, A_m)$, i.e. (2.8) holds. Set $F = -\sum_{i=1}^m b_i A_i$. Then

$$\sum_{i=1}^{m} b_i y_i = \langle -F, \sum_{i=1}^{m} y_i A_i\rangle = \langle F, Y\rangle - \langle F, C\rangle.$$

Hence the supremum in (2.4) is equal to the supremum in (2.7) plus the constant $-\langle F, C\rangle$. □

Proposition 2.4 *(Weak duality) Assume that* $X_0 \succeq 0$ *satisfies* (1.1), *and* $Y_0 \succeq 0, \mathbf{y}_0 = (y_{1,0}, \ldots, y_{m,0})^\top$ *satisfies* (2.8). *Then* $\mathbf{b}^\top \mathbf{y}_0 \le \langle C, X_0\rangle$.

Proof. As $\langle Y_0, X_0\rangle \ge 0$ it follows that

$$\langle C, X_0\rangle = \langle Y_0 + \sum_{i=1}^{m} y_{i,0} A_i, X_0\rangle = \langle Y_0, X_0\rangle + \sum_{i=1}^{m} y_{i,0}\langle A_i, X_0\rangle \ge \sum_{i=1}^{m} y_{i,0} b_i = \mathbf{b}^\top \mathbf{y}_0.$$

□

Corollary 2.5 *The infimum in* (2.3) *is not less than the supremum in* (2.4).

Note that when the both sets in (2.3) and in (2.4) are not feasible we have the trivial gap $-\infty < \infty$. Same situation holds for the LP programs. However, it is possible that at least one of the sets in (2.3) and in (2.4) are feasible and the infimum in (2.3) is strictly bigger than the supremum in (2.4). This strict inequality is called the *gap* of SDP. Also the analog of Theorem 2.2 can fail as we see in the following simple examples in the next subsection.

2.3 Examples

Example 2.6 *Let*

$$X = \begin{bmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{bmatrix}, \ C = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \ A_1 = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \ b_1 = 1.$$

Then the infimum in (2.3) *is* 0 *but not attainable. The supremum in* (2.4) *is* 0 *and is attainable.*

Proof. Observe that $\langle A_1, X\rangle = 1$ yields that $x_{12} = 1$. As $X \succeq 0$ it follows that $x_{11}, x_{22} \geq 0$ and $x_{11}x_{22} - 1 \geq 0$. Hence $x_{11} > 0$. Next, $\langle C, X\rangle = x_{12}$. Note that $X_\varepsilon = \begin{bmatrix} \varepsilon & 1 \\ 1 & \frac{1}{\varepsilon} \end{bmatrix}$ is a feasible solution for any $\varepsilon > 0$. Hence the infimum in (2.3) is 0 but is not achievable.

The dual SDP problem (2.4) is $y_1 A_1 \leq C$, i.e., $C - y_1 A_1 \succeq 0$. In particular $0 \leq \det(C - y_1 A_1) = -\frac{y_1^2}{4}$. So $y_1 = 0$ gives a unique feasible solution. Hence $b_1 y_1 = y_1 = 0$. So the supremum is attainable and is equal to 0. $\square$

In this example we do not have a gap.

Example 2.7 *Let*

$$X = \begin{bmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{bmatrix}, \ C = \begin{bmatrix} 0 & -\frac{1}{2} \\ -\frac{1}{2} & -1 \end{bmatrix}, \ A_1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \ b_1 = 0.$$

Then the infimum in (2.3) *is* 0 *and is attainable. The equality* (2.8) *is not feasible. Hence the supremum* (2.4) *is* $-\infty$*.*

Proof. Note that $\langle A_1, X\rangle = \mathbf{1}^\top X \mathbf{1}, \mathbf{1} = (1,1)^\top$. As $X \succeq 0$ it follows that $\mathbf{1}$ is an eigenvector of X corresponding to the eigenvalue 0. So $x_{11} + x_{12} = x_{12} + x_{22} = 0$. Hence $x_{11} = x_{22} = -x_{12} = a \geq 0$. Now $\langle C, X\rangle = -x_{12} - x_{22} = 0$. So the infimum is 0 and is achieved. The dual set is $y_1 A \preceq C \iff 0 \preceq C - y_1 A = D$. First the diagonal elements of D are nonnegative. This condition yields that $y_1 \leq -1$. The determinant condition is

$$0 \leq -y_1(-1 - y_1) - (\frac{1}{2} + y_1)^2 = -\frac{1}{4},$$

which is impossible. Hence the supremum in (2.4) is $-\infty$. $\square$

In this example we do have a gap. This situation can not happen for the linear programming problem. Another situation that can not happen in LP is that not all SDP are polynomially solvable with given precision $\varepsilon > 0$. See
https://cstheory.stackexchange.com/questions/14548/solving-semidefinite-programs-in-polynomial-time/14550

2.4 Strong SDP duality

Theorem 2.8 *(Strong duality first version) Assume that* (2.8) *solvable with* $Y \succ 0$*. Denote by* β *the supremum in* (2.4)*. Then the infimum in* (2.3) *is equal to* β*. Furthermore,* $\beta < \infty$ *if and only if the infimum in* (2.3) *is attainable.*

To prove the theorem we need the following results.

Theorem 2.9 *(Separation theorem.) Let $\Sigma_1, \Sigma_2 \subset \mathbb{R}^p$ be two convex closed sets, such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Suppose furthermore that Σ_1 is compact and Σ_2 is a cone. Then there exists a linear functional $\phi : \mathbb{R}^p \to \mathbb{R}$ such that $\phi(\mathbf{u}) \geq 0$ for each $\mathbf{u} \in \Sigma_2$ and $\phi(\mathbf{v}) < 0$ for each $\mathbf{v} \in \Sigma_1$.*

See for example [9].

Lemma 2.10 *Let $F_1, \ldots, F_p \in \mathrm{S}_n$. Consider the linear map $L : \mathrm{S}_n \to \mathbb{R}^p$ given by $X \mapsto (\langle F_1, X\rangle, \ldots, \langle F_p, X\rangle)^\top$. Assume that $\mathrm{span}(F_1, \ldots, F_p)$ contains a positive definite matrix $Z \succ 0$. Then $L(\mathrm{S}_{n,+})$ is closed. That is if $X_i \succeq 0$ for $i \in \mathbb{N}$, and $\lim_{i\to\infty} L(X_i) = \mathbf{x} = (x_1, \ldots, x_p)^\top \in \mathbb{R}^p$, then there exists a convergent subsequence $X_{i_j}, 1 \leq i_1 < \cdots$ such that $lim_{j\to\infty} X_{i_j} = X \geq 0$.*

Proof. Assume that $Z = \sum_{k=1}^p z_i F_i \succ 0$. We claim that

$$\limsup_{i\to\infty} \lambda_{\max}(X_i) \leq \frac{\sum_{k=1}^p x_i z_i}{\lambda_{\min}(Z)}. \tag{2.9}$$

First recall the spectral decomposition of $A \in \mathrm{S}_n$ given by (1.4): $A = \sum_{l=1}^n \lambda_i(A)\mathbf{x}_i\mathbf{x}_i^\top$. As $I_n = \sum_{l=1}^n \mathbf{x}_i\mathbf{x}_i^\top$ it follows that $A - \lambda_{\min}(A)I_n = \sum_{l=1}^{n-1}(\lambda_i(A) - \lambda_{\min})(A)\mathbf{x}_i\mathbf{x}_i^\top \succeq 0$. Recall that $Z \succ 0 \iff \lambda_{\min}(Z) > 0$. So $Z \succeq \lambda_{\min}(Z)I_n \succ 0$.

Next consider the spectral decomposition of X_i:

$$X_i = \sum_{l=1}^n \lambda_l(X_i)\mathbf{x}_{l,i}\mathbf{x}_{l,i}^\top, \lambda_1(X_i) \geq \ldots \geq \lambda_n(X_i) \geq 0, \mathbf{x}_{p,i}^\top\mathbf{x}_{q,i} = \delta_{p,q}, p, q \in [n], i \in \mathbb{N}.$$

Hence $X_i \succeq \lambda_{\max}\mathbf{x}_{1,i}\mathbf{x}_{1,i}^\top$. Therefore:

$$\sum_{k=1}^p z_k\langle B_k, X_i\rangle = \langle Z, X_i\rangle = \langle Z, X_i\rangle \geq \langle Z, \lambda_{\max}(X_i)\mathbf{x}_{1,i}\mathbf{x}_{1,i}^\top\rangle \geq$$
$$\langle \lambda_{\min}(Z)I_n, \lambda_{\max}(X_i)\mathbf{x}_{1,i}\mathbf{x}_{1,i}^\top\rangle = \lambda_{\min}(Z)\lambda_{max}(X_i)\,\mathrm{tr}(I_n\mathbf{x}_{1,i}\mathbf{x}_{1,i}^\top) = \lambda_{\min}(Z)\lambda_{max}(X_i).$$

Let $i \to \infty$ and recall the assumption that $\lim_{i\to\infty} L(X_i) = \mathbf{x} = (x_1, \ldots, x_p)^\top$. Combine that with the above inequality to deduce (2.9).

We claim that the sequence $X_i, i \in \mathbb{N}$ is bounded. Assume that $X = [x_{ij}] \in \mathrm{S}_{n,+}$. The the maximal characterization and the minimal characterization of $\lambda_{\max}(X)$ and $\lambda_{\min}(X)$ yield that $0 \leq x_{ii} \leq \lambda_{max}(X)$ for $i \in [n]$. As all 2×2 principal minors of X are nonnegative we deduce that $|x_{ij}| \leq \sqrt{x_{ii}x_{jj}} \leq \lambda_{\max}(X)$ for $i, j \in [n]$. The inequality (2.9) yields that all the entries of $X_i, i \in \mathbb{N}$ are uniformly bounded. Hence there exists a subsequence $X_{i_j}, j \in \mathbb{N}$ that converges to $X \in \mathrm{S}_{n,+}$. □

Proof of Theorem 2.8. Assume first that $\beta = \infty$. The weak duality theorem yields that there is no $X \succeq 0$ which satisfies (1.1). Hence the the infimum in (2.3) is β by definition.

Assume now that the infimum in (2.3) is attainable. The weak duality theorem yields that $\beta < \infty$.

Assume now that $\beta < \infty$. We will show that there exists $X \succeq 0$ satisfying the equalities (1.1), such that $\langle C, X\rangle = \beta$. Let $L : \mathrm{S}_n \to \mathbb{R}^{m+1}$ be given by $L(X) =$

$(\langle C,X\rangle,\langle A_1,X\rangle,\ldots,\langle A_m,X\rangle)^\top$. Clearly $L(\mathrm{S}_{n,+})\subset\mathbb{R}^{m+1}$ is a cone. The assumption that (2.8) solvable with $Y\succ 0$ implies that $Y\in\mathrm{span}(C,A_1,\ldots,A_m)$. Lemma (2.10) implies that $L(\mathrm{S}_{n,+})$ is a closed convex set in $\mathbb{R}^{m+1}$. Let $\mathbf{x}=(\beta,b_1,\ldots,b_m)^\top$. Suppose first $\mathbf{x}\in L(\mathrm{S}_{n,+})$. This is equivalent to the existence of $X\succeq 0$ satisfying the equalities (1.1), such that $\langle C,X\rangle=\beta$.

It is left to show that we can't have the possibility $\mathbf{x}\notin L(\mathrm{S}_{n,+})$. Assume to the contrary that $\mathbf{x}\notin L(\mathrm{S}_{n,+})$. Theorem 2.9 yields that there exists a linear functional $\phi:\mathbb{R}^{m+1}\to\mathbb{R}$ such that $\phi(\mathbf{y})\ge 0$ for $\mathbf{y}\in L(\mathrm{S}_{n,+})$ and $\phi(\mathbf{x})<0$. Let $\phi((y_0,y_1,\ldots,y_{m+1})^\top)=\sum_{l=0}^m f_iy_i$ for $\mathbf{y}\in\mathbb{R}^{m+1}$. Hence

$$f_0\langle C,X\rangle+\sum_{i=1}^m f_i\langle A_i,X\rangle=\langle f_0C+\sum_{l=1}^m f_iA_i,X\rangle\ge 0 \text{ if } X\succeq 0.$$

Lemma (1.2) yields that $f_0C+\sum_{l=1}^m f_iA_i\succeq 0$. The assumption that $\phi(\mathbf{x})<0$ is $f_0\beta+\sum_{i=1}^m f_ib_i<0$.

Suppose first that $f_0>0$. by dividing by f_0 we can assume that $f_0=1$. That is $C+\sum_{i=1}^m f_iA_i=Z\succeq 0$. Equivalently, $C\succeq\sum_{i=1}^m(-f_i)A_i$. The maximal characterization of β yields that $\beta\ge\sum_{i=1}^n b_i(-f_i)$. This contradicts the assumption that $\phi(\mathbf{x})<0$.

Assume second that $f_0=0$. Then $\sum_{i=1}^m f_ib_i<0$ and $\sum_{i=1}^m f_iA_i\succeq 0$. Recall that we assumed that (2.8) solvable with $Y\succ 0$. Let $t>0$. Then $\sum_{i=1}^m(y_i-tf_i)A_i\prec C$. Hence $\beta\ge\sum_{i=1}^m b_i(y_i-tf_i)=-t\sum_{i=1}^m b_if_i+\sum_{i=1}^m b_iy_i$. Letting $t\to\infty$ we we will obtain a contradiction.

Assume now that $f_0<0$. By dividing by $-f_0$ we can assume that $f_0=-1$. Hence $\beta>\sum_{i=1} f_ib_i$. Furthermore $-C+\sum_{i=1}^m f_iA_i\succeq 0$. Let us choose an admissible point $\mathbf{z}=(z_1,\ldots,z_m)^\top$ such $\sum_{i=1}^m z_iA_i\preceq C$ and $\sum_{i=1}^m b_if_i<\sum_{i=1}^m b_iz_i<\beta$. Let $t>0$. Then

$$\sum_{i=1}^m(y_i+t(z_i-f_i))A_i=(\sum_{i=1}^m y_iA_i)+t\sum_{i=1}^m z_iA_i+t\sum_{i=1}^m(-f_iA_i)\prec(C+tC+t(-C))=C.$$

As β is the supremum of (2.4) it follows that

$$\beta\ge t((\sum_{i=1}^m b_iz_i)-(\sum_{i=1}^m b_if_i))+\sum_{i=1}^m f_iy_i.$$

Letting $t\to\infty$ we obtain a contradiction. $\square$

Theorem 2.11 *(Strong duality second version) Assume that there exists $X\succ 0$ satisfying* (1.1)*. Let α be the infimum in* (2.3)*. Then the supremum in* (2.4) *is equal to α. Furthermore, $\alpha>-\infty$ if and only if the supremum in* (2.4) *is attainable.*

Proof. The assumption that there exists $X\succ 0$ satisfying (1.1), implies that the system (1.1) is solvable. We now use Proposition 2.3 and the arguments of its proof. For simplicity of notation we can assume that $A_1,\ldots,A_{\frac{n(n+1)}{2}}$ is an orthonormal basis in $\mathrm{S}_{n,+}$. Hence the problem (2.4) is equivalent to the problem (2.7). Clearly, (2.7) is equal to

$$-\inf\{\langle -F,Y\rangle,Y\succeq 0,\langle B_i,Y\rangle=e_i,i\in[\ell]\},\tag{2.10}$$

Recall that

$$-F=\sum_{i=1}^{m} b_iA_i,\ B_i=A_{m+i}, e_i=\langle B_i, C\rangle, i\in[\ell],\ \ell=\frac{n(n+1)}{2}-m.$$

Note that the system $\langle B_i, Y\rangle = e_i, i\in[\ell]$ is solvable in S_n. We claim that the dual to (2.10) is (2.3) plus a constant. To show that we apply the arguments of the proof of Proposition 2.3. Thus the dual to (2.10) is

$$-\sup\{\langle G, X\rangle, X\succeq 0,\ \langle A_i, X\rangle=\langle A_i, -F\rangle,\ i\in[m].$$

Here $G=-\sum_{j=1}^{\ell} e_iB_i$. Recall that $\langle A_i, -F\rangle = b_i$ for $i\in[m]$. Recall next $C=\sum_{k=1}^{\frac{n(n+1)}{2}}\langle A_k, C\rangle A_k$. Hence $-G=C-\sum_{i=1}^{m}\langle A_i, C\rangle A_i$. If $\langle A_i, X\rangle = b_i, i\in[m]$ we obtain

$$\langle -G, X\rangle=\langle C, X\rangle-\sum_{i=1}^{m}\langle A_i, C\rangle b_i.$$

Thus the dual to (2.10) is (2.3) plus a constant. Now use Theorem 2.8 to deduce the theorem. □

2.5 Flexibility of SDP

We first observe that the problems of linear programming can be stated as an SDP problem. Consider first the system $A\mathbf{x}=\mathbf{b}, \mathbf{x}\ge 0$, where $\mathbf{x}\in\mathbb{R}^n$ and $A\in\mathbb{R}^{m\times n}$. For $\mathbf{x}=(x_1,\ldots,x_n)^\top\in\mathbb{R}^n$ denote by $D(\mathbf{x})=\mathrm{diag}(x_1,\ldots,x_n)\in\mathrm{S}_n$. Let $X=[x_{ij}]\in\mathrm{S}_n$. Then the set of all diagonal matrices in S_n is given by the $\frac{n(n-1)}{2}$ linear conditions

$$\langle E_{pq}+E_{qp}, X\rangle = 0 \text{ for } 1\le p<q\le n.$$

Furthermore $\mathbf{x}\ge\mathbf{0}$ if and only if $D(\mathbf{x})\succeq 0$. Let $\mathbf{a}_i$ be the i-th row of A for $i\in[m]$. Then the system $A\mathbf{x}=\mathbf{b}$ is equivalent to

$$\langle D(\mathbf{a}_i), D(\mathbf{x})\rangle = b_i,\quad i\in[m].$$

Hence the LP (2.1) can be stated as (2.3).

Suppose we have an SDP problem with k matrices $X_1,\ldots,X_k\in\mathrm{S}_{n,+}$:

$$\inf\{\sum_{i=1}^{k}\langle C_k, X_k\rangle,\ X_j\in\mathrm{S}_{n,+},\ \langle A_{ij}, X_j\rangle=b_{ij}, i\in[m_j], j\in[k]\}. \tag{2.11}$$

Then it is possible convert this problem to the problem (2.3) for $X\in\mathrm{S}_{kn,+}$. Consider the block diagonal symmetric matrix $X=\mathrm{diag}(X_1,\ldots,X_k)\in\mathrm{S}_{kn}$. The subspace of such matrices $X\in\mathrm{S}_{kn}$ is given by a corresponding number homogeneous linear conditions. Then $X_1,\ldots X_k\in\mathrm{S}_{n,+}\iff X=\mathrm{diag}(X_1,\ldots,X_k)\in\mathrm{S}_{kn,+}$. Let $C=\mathrm{diag}(C_1,\ldots,C_k)$. Then $\langle C, X\rangle=\sum_{i=1}^{k}\langle C_i, X_i\rangle$.

3 Applications of SDP to combinatorial optimization

A good reference to this topic is [5].

3.1 Max and min boolean problems

Let
$$\{-1,1\}^n = \{\mathbf{x} = (x_1,\ldots,x_n)^\top \in \mathbb{R}^n, x_1^2 = \cdots = x_n^2 = 1\}.$$

A vector $\mathbf{x} \in \{-1,1\}^n$ is called a boolean vector. (Note that $\mathbf{x}$ is boolean if and only if $\mathbf{x} = 2\mathbf{y} - \mathbf{1}_n$, where $\mathbf{y} = (y_1,\ldots,y_n)^\top$ and $y_i \in \{1,0\}, i \in [n]$.) For a symmetric matrix $B \in \mathrm{S}_n$ denote

$$\nu_{\max}(B) = \max_{\mathbf{x}\in\{-1,1\}^n} \mathbf{x}^\top B\mathbf{x}, \quad \nu_{\min}(B) = \min_{\mathbf{x}\in\{-1,1\}^n} \mathbf{x}^\top B\mathbf{x} \tag{3.1}$$

The above two quantities are called the boolean (binary) optimizations. Clearly

$$\nu_{\max}(B) = -\nu_{\min}(-B). \tag{3.2}$$

It is straightforward to show that

$$n\lambda_n(A) = n\lambda_{\min}(B) \le \nu_{\min}(B) \le \nu_{\max}(B) \le n\lambda_{\max}(B) = n\lambda_1(B). \tag{3.3}$$

Actually, we have better bounds. We state these bounds for $\nu_{\max}(B)$.

Lemma 3.1 *For $B \in \mathrm{S}_n$ let*

$$\omega_{\min}(B) = \min\{n\lambda_{\max}(B + D(\mathbf{u})), \mathbf{u} = (u_1,\ldots,u_n)^\top \in \mathbb{R}^n, \mathbf{1}_n^\top\mathbf{u} = 0\}. \tag{3.4}$$

Then
$$\nu_{\max}(B) \le \omega_{\min}(B). \tag{3.5}$$

Proof. Note that if $\mathbf{x} \in \{-1,1\}^n$ then $\|\mathbf{x}\|^2 = \mathbf{x}^\top\mathbf{x} = n$. The maximum Rayleigh characterization yields that

$$\lambda_{\max}(B) \ge \frac{\mathbf{x}^\top A\mathbf{x}}{\mathbf{x}^\top\mathbf{x}} = \frac{1}{n}\mathbf{x}^\top B\mathbf{x} \text{ for } \mathbf{x} \in \{-1,1\}^n.$$

Hence the right hand side of (3.3) hold. (The minimum characterization of $\lambda_{\min}(B)$ yields the left hand side of (3.3).) Observe that for $\mathbf{u} = (u_1,\ldots,u_n)^\top, \mathbf{x} = (x_1,\ldots,x_n)^\top \in \mathbb{R}^n$ we have the equality $\mathbf{x}^\top D(\mathbf{u})\mathbf{x} = \sum_{i=1}^n x_i^2$. Thus if $\mathbf{1}^\top\mathbf{u} = 0$ and $\mathbf{x} \in \{-1,1\}^n$ we obtain that $\mathbf{x}^\top D(\mathbf{u})\mathbf{x} = 0$. In particular, $\nu_{\max}(B) = \nu_{\max}(B + D(\mathbf{u}))$. Use (3.3) to deduce (3.5). $\square$

For $\mathbf{x}_1,\ldots,\mathbf{x}_n \in \mathbb{R}^m$ denote by $G(\mathbf{x}_1,\ldots,\mathbf{x}_n) = [\langle\mathbf{x}_i,\mathbf{x}_j\rangle] \in \mathrm{S}_n$ the Gramian matrix.

Lemma 3.2 *1. Let $\mathbf{x}_1,\ldots,\mathbf{x}_n \in \mathbb{R}^m$. Then $G(\mathbf{x}_1,\ldots,\mathbf{x}_n) \in \mathrm{S}_{n,+}$. Furthermore, $G(\mathbf{x}_1,\ldots,\mathbf{x}_n) \succ 0$ if and only if $\mathbf{x}_1,\ldots,\mathbf{x}_n$ are linearly independent. Moreover,* $\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_n)$ *is the dimension of* $\operatorname{span}(\mathbf{x}_1,\ldots,\mathbf{x}_n)$.

2. Let $X \in \mathrm{S}_n$ and assume that $\operatorname{rank} X = m \ge 1$. *Then $X \in \mathrm{S}_{n,+}$ if and only if $X = G(\mathbf{x}_1,\ldots,\mathbf{x}_n)$ for some $\mathbf{x}_1,\ldots,\mathbf{x}_n \in \mathbb{R}^m$. Furthermore, the vectors $\mathbf{x}_1,\ldots,\mathbf{x}_n$ are determined uniquely up the action of the orthogonal group on $\mathbb{R}^m$: $\{\mathbf{x}_1,\ldots,\mathbf{x}_n\} \to O\{\mathbf{x}_1,\ldots,\mathbf{x}_n\} = \{O\mathbf{x}_1,\ldots,O\mathbf{x}_n\}$.*

Proof. *1.* Let $\mathbf{x}_1,\ldots,\mathbf{x}_n\in\mathbb{R}^m$ an $\mathbf{y}=(y_1,\ldots,y_n)^\top$. Then $\mathbf{y}^\top G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\mathbf{y}=\langle\sum_{i=1}^n y_i\mathbf{x}_i,\sum_{j=1}^n y_j\mathbf{x}_j\rangle\ge 0$. Hence $G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\succeq 0$. Note that $\mathbf{y}^\top G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\mathbf{y}=0$ if and only if $\sum_{i=1}^n y_i\mathbf{x}_i=\mathbf{0}$. In particular, $G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\succ 0$ if and only if $\mathbf{x}_1,\ldots,\mathbf{x}_n$ are linearly independent.

It is left to show that $\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_n)=\dim\operatorname{span}(\mathbf{x}_1,\ldots,\mathbf{x}_n)$. Let $m=\dim\operatorname{span}(\mathbf{x}_1,\ldots,\mathbf{x}_n)$. Assume that $\dim\operatorname{span}(\mathbf{x}_1,\ldots,\mathbf{x}_n)=m\ge 1$. So $n\ge m$. If $m=n$ then $\mathbf{x}_1,\ldots,\mathbf{x}_n$ are linearly independent. Hence $G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\succ 0$ and $\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_n)=n$. Vice versa, if $\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_n)=n$ then $G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\succ 0$ and $\mathbf{x}_1,\ldots,\mathbf{x}_n$ are linearly independent.

Let us assume that $n>m\ge 1$ and $1\le\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_n)<n$. By renaming the $\mathbf{x}_1,\ldots,\mathbf{x}_n$ we can assume that $\mathbf{x}_1,\ldots,\mathbf{x}_m$ are llinearly independent. Observe that $G(\mathbf{x}_1,\ldots,\mathbf{x}_m)$ is a prinicple submatrix of $G(\mathbf{x}_1,\ldots,\mathbf{x}_m)$. Our previous results show that $G(\mathbf{x}_1,\ldots,\mathbf{x}_m)\succ 0$. In particular, the m rows of $G(\mathbf{x}_1,\ldots,\mathbf{x}_m)$ are linearly independent. Therefore the first m-row of $G(\mathbf{x}_1,\ldots,\mathbf{x}_n)$ are linearly independent. Hence $\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\ge m$. Recall that $\mathbf{x}_j=\sum_{i=1}^m a_{ji}\mathbf{x}_i$ for $j>m$. Now subtract from row j the sum of a_{ji} times row r_i for $j=m+1,\ldots,n$ to deduce that the new matrix has $n-m$ zero rows. So the rank of $G(\mathbf{x}_1,\ldots,\mathbf{x}_n)\le m$. Therefore $\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_m)=m$.

Suppose now that $\operatorname{rank} G(\mathbf{x}_1,\ldots,\mathbf{x}_n)=r, 1\le r<n$. If $G(\mathbf{x}_i)=\|\mathbf{x}_i\|^2=0$, i.e., the i-th diagonal entry is zero then $\mathbf{x}_i=$ and the row i and the column i are zero. Perform Algorithm 1.1 to deduce that $r=\dim\{\mathbf{x}_1,\ldots,\mathbf{x}_n\}$.

2. Suppose that $X\in\mathrm{S}_{n,+}$. Then $X=Q\Lambda Q^\top$, where $QQ^\top=Q^\top Q=I_n$ and $\Lambda=\operatorname{diag}(\lambda_1(X),\ldots,\lambda_n(X))$ where $\lambda_1(X)\ge\cdots\lambda_n(X)\ge 0$ for $i\in[n]$. Set $\Lambda^{\frac{1}{2}}=\operatorname{diag}(\sqrt{\lambda_1(X)},\ldots,\sqrt{\lambda_n(X)})$. Let $Y=\Lambda^{\frac{1}{2}}Q^\top$. Then $X=Y^\top Y$. Set $\mathbf{y}_i$ to be the i-th column of Y for $i\in[n]$. Then $X=G(\mathbf{y}_1,\ldots,\mathbf{y}_n)$. Assume that $\operatorname{rank} X=m$. So $\lambda_m(X)>0$ and $\lambda_{m+1}(X)=\cdots=\lambda_n(X)=0$. So the last $n-m$ rows of Y are zero. That is $\mathbf{y}_i^\top=(\mathbf{x}_i^\top,\mathbf{0})$, where $\mathbf{x}_i\in\mathbb{R}^m$ for $i\in[n]$. Thus $X=G(\mathbf{x}_1,\ldots,\mathbf{x}_n)$, where $\mathbf{x}_1,\ldots,\mathbf{x}_n\in\mathbb{R}^m$. As we claimed.

Let $O\in\mathbb{R}^{m\times m}$ be an ortthogonal matrix: $O^\top O=I_m$. Denote $\mathbf{z}_i=O\mathbf{x}_i$ for $i\in[n]$. Then $\mathbf{x}_i^\top\mathbf{x}_j=\mathbf{z}_i^\top\mathbf{z}_j$ for $i,j\in[n]$. Thus $G=G(\mathbf{x}_1,\ldots,\mathbf{x}_n)=G(\mathbf{z}_1,\ldots,\mathbf{z}_n)$, $\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{z}_1,\ldots,\mathbf{z}_n\in\mathbb{R}^m$ and $\operatorname{rank} G=m$.

Assume that $G=G(\mathbf{x}_1,\ldots,\mathbf{x}_n)=G(\mathbf{z}_1,\ldots,\mathbf{z}_n)$, $\mathbf{x}_1,\ldots,\mathbf{x}_n,\mathbf{z}_1,\ldots,\mathbf{z}_n\in\mathbb{R}^m$ and $\operatorname{rank} G=m$. By renaming $\mathbf{x}_1,\ldots,\mathbf{x}_n$ and $\mathbf{z}_1,\ldots,\mathbf{z}_n$ accordingly, we can assume that $\mathbf{x}_1,\ldots,\mathbf{x}_m$ are linearly independent. So $G(\mathbf{x}_1,\ldots,\mathbf{x}_m)\succ 0$. Hence $G(\mathbf{z}_1,\ldots,\mathbf{z}_m)=G(\mathbf{x}_1,\ldots,\mathbf{x}_m)\succ 0$, so $\mathbf{z}_1,\ldots,\mathbf{z}_m$ are linearly idependent. Thus $X=[\mathbf{x}_1\cdots\mathbf{x}_m], Z=[\mathbf{z}_1\cdots\mathbf{z}_m]\in\mathbb{R}^{m\times m}$ are two invertible matrices. Therefore

$$G(\mathbf{x}_1,\ldots,\mathbf{x}_m)=X^\top X=G(\mathbf{z}_1,\ldots,\mathbf{z}_m)=Z^\top Z\Rightarrow\big((X^\top)^{-1}Z^\top\big)\big(ZX^{-1}\big)=I_n.$$

Hence the matrix $O=ZX^{-1}$ is an orthogonal matrix. Thus $O\mathbf{x}_i=\mathbf{z}_i$ for $i\in[m]$. Let $\mathbf{y}_j=O\mathbf{x}_j$ for $j=m+1,\ldots,n$. Observe next that

$$G(\mathbf{x}_1,\ldots,\mathbf{x}_n)=G(O\mathbf{x}_1,\ldots,O\mathbf{x}_n)=G(\mathbf{z}_1,\ldots,\mathbf{z}_m,\mathbf{y}_{m+1},\ldots,\mathbf{y}_n)=G(\mathbf{z}_1,\ldots,\mathbf{z}_n).$$

Hence $\langle\mathbf{y}_j,\mathbf{z}_i\rangle=\langle\mathbf{z}_j,\mathbf{z}_i\rangle$ for $i\in[m]$. That is $\langle\mathbf{y}_j-\mathbf{z}_j,\mathbf{z}_i\rangle=0$ for $i\in[m]$. As $\mathbf{z}_1,\ldots,\mathbf{z}_m$ are linearly independent in $\mathbb{R}^m$ they span $\mathbb{R}^m$. Therefore $\mathbf{y}_j=\mathbf{z}_j$ for $jm+1,\ldots,n$. That is $\mathbf{z}_j=O\mathbf{x}_j$ for $j=m+1,\ldots,n$. □

$X = [x_{ij}] \in \mathrm{S}_{n,+}$ is called a correlation matrix if $x_{ii} = 1$ for $i \in [n]$. So X is a correlation matrix if and only if $X = G(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ where $\|\mathbf{x}_1\| = \ldots = \|\mathbf{x}_n\| = 1$. Denote by $\mathcal{K}_n$ the convex set of correlation matrices:

$$\mathcal{K}_n = \{X \in \mathrm{S}_{n,+},\ \langle E_{ii}, X\rangle = 1, \quad i \in [n]\}. \tag{3.6}$$

Note that $\mathcal{K}_n$ is a compact set. Denote

$$\mathcal{X}_n = \{\mathbf{x}\mathbf{x}^\top,\ \mathbf{x} \in \{-1, 1\}^n\}. \tag{3.7}$$

Clearly, $\mathcal{X}_n \subset \mathcal{K}_n$. Observe next that

$$\nu_{\max}(B) = \max\{\langle B, X\rangle, X \in \mathcal{X}_n\} \quad \nu_{\min}(B) = \min\{\langle B, X\rangle, X \in \mathcal{X}_n\}. \tag{3.8}$$

The following max and min problems are called the SDP relaxations of the above max and min problems:

$$\gamma_{\max}(B) = \{\langle B, X\rangle, X \in \mathcal{K}_n\}, \quad \gamma_{\min}(B) = \min\{\langle B, X\rangle, X \in \mathcal{K}_n\}. \tag{3.9}$$

Clearly

$$\nu_{\max}(B) \le \gamma_{\max}(B), \quad \gamma_{\min}(B) \le \nu_{\min}(B). \tag{3.10}$$

Theorem 3.3 *Let $B \in \mathrm{S}_n$. The the dual SDP problem to the maximum problem characterizing $\gamma_{\max}(B)$ is the following minimum problem*

$$\min\{\sum_{i=1}^n z_i,\ \sum_{i=1}^n z_i E_{ii} \succeq B\}. \tag{3.11}$$

Both problems has positive definite feasible solutions. Hence the strong duality holds. Furthermore, the dual problem (3.11) *is equal to the minimum problem* (3.4).

Proof. Let

$$\mathcal{H}_n = \{X \in \mathrm{S}_n, \quad \langle E_{ii}, X\rangle = 1, i \in [n]\}. \tag{3.12}$$

Then $\mathcal{K}_n = \mathcal{H}_n \cap \mathrm{S}_{n,+}$. Thus

$$\gamma_{\max}(B) = \{\max\langle B, X\rangle,\ X \succeq 0, \langle E_{ii}, X\rangle = 1,\ \text{for } i \in [n]\}. \tag{3.13}$$

Note that $0 \prec I_n \in \mathcal{K}_n$. Hence (3.11) is the dual problem of (3.13). The inequality $\sum_{i=1}^n z_i E_{ii} \succeq B$ can be stated as an equation:

$$-Y + \sum_{i=1}^n z_i E_{ii} = B, \quad Y \succeq 0. \tag{3.14}$$

By choosinf $z_i \gg 0$ for $i \in [n]$ we deduce that there is a feasible solution in the above system with $Y \succ 0$. Hence the dual also a positive definite solution. In particular the strong duality holds.

It is left to show that the minimum in (3.11) is the minimum in (3.4). Clearly $\sum_{i=1}^n z_i E_{ii} = D(\mathbf{z})$, where $\mathbf{z} = (z_1, \ldots, z_n)^\top$. Set $u_i = -z_i + \frac{1}{n}\sum_{i=1}^n z_i$. Let $\mathbf{u} = (u_1, \ldots, u_n)^\top$. Note that $\mathbf{1}_n^\top \mathbf{u} = 0$. Then the condition $D(\mathbf{z}) \succeq B$ is equivalent to $\frac{\sum_{i=1}^n z_i}{n} I_n \succeq (B + D(\mathbf{u}))$. The last condition is equivalent to $\sum_{i=1}^n z_i \ge n\lambda_1(B + D(\mathbf{u}))$. Since we are minimizing $\sum_{i=1}^n z_i$ for fixed $\mathbf{u}$ satisfying $\mathbf{1}_n^\top \mathbf{u} = 0$ we choose $\sum_{i=1}^n z_i = n\lambda_1(B + D(\mathbf{u}))$. This arguments yields that the minimum in (3.11) is the minimum in (3.4). $\square$

In a similar way we deduce:

Corollary 3.4 *The dual SDP problem to $\gamma_{\min}(B)$ is*

$$\omega_{\max}(B) = \max\{n\lambda_{\min}(B + D(\mathbf{u})), \mathbf{u} = (u_1, \ldots, u_n)^\top \in \mathbb{R}^n, \mathbf{1}_n^\top \mathbf{u} = 0\}. \tag{3.15}$$

For a given $B \in \mathrm{S}_n \cap \mathbb{Q}^{n\times n}$ and $0 < \varepsilon \in \mathbb{Q}$ one can find a ε aprroximation of $\gamma_{\max}(B)$ in a polynomial time in the data $\langle B\rangle + \langle\varepsilon\rangle$ by an interior method. Indeed, consider the hyperplane (3.12) It can be identified with $\mathbb{R}^{\frac{n(n-1}{2}}$. So $\mathcal{K}_n$ is a convex set in H_n, with an interior point I_n. The open ball

$$B(I_n, 1) = \{X \in \mathcal{H}_n, \langle X - I_n, X - I_n\rangle < 1\} \tag{3.16}$$

is contained in the interior of $\mathcal{K}_n$. Hence the interior method for finding $\gamma(A)$ is applicable. So we can have an approximate solution $X_0 \in \mathcal{K}_n$: $\langle B, X_0\rangle \le \gamma_{\max}(B)$, such that (theoretically) $\langle B, X_0\rangle \ge \gamma_{\max}(B) - \varepsilon$.

Next, the dual problem (3.11) has also a feasible solution $Y = aI_n$ for some $z_i = b, i \in [n]$. Hence we also apply the interior method to find upper bound $\gamma_{\max}(B)$. Combining together we obtain the practical bound for $\gamma_{\max}(B)$:

$$\langle B, X_0\rangle \le \gamma_{\max}(B) \le \mathbf{1}_n^\top \mathbf{z}_0. \tag{3.17}$$

In particular, if $\mathbf{1}_n^\top \mathbf{z}_0 - \langle B, X_0\rangle$ are not satisfactory small, we can iterate the interiror methods for X_0 and $\mathbf{z}_0$ to improve (3.17).

A theoretical problem is to supply an estimate how far $\gamma_{\max}(B)$ is from $\nu_{\max}(B)$, (and similarly how far $\gamma_{\min}(B)$ is from $\nu_{\min}(B)$)?

The major result in this area is a result contained in Rietz [6] and usually attributed to Nesterov [7]:

Theorem 3.5 *Let $B \in \mathrm{S}_{n,+}$. Then*

$$\nu_{\max}(B) \ge \frac{2}{\pi}\gamma_{\max}(B). \tag{3.18}$$

We will point out a proof of this inequality in §3.3. We also explain Rietz's result in the context of the Grothendieck inequality.

3.2 Boolean least square

Given $A \in \mathbb{R}^{m\times n}, \mathbf{b} \in \mathbb{R}^m$ find

$$\alpha(A) = \min\{\|A\mathbf{x} - \mathbf{b}\|^2,\ \mathbf{x} = (x_1, \ldots, x_n)^\top \text{ subject } \mathbf{x} \in \{-1, 1\}\}. \tag{3.19}$$

See Stephen Boyd 's Zaborsky Disitnguished Lecture Series, September 18, 2016: https://ese.wustl.edu/eseatwashu/Documents/Seminars/BoydLecture1.pdf

SDP approximation: Observe first

$$\|A\mathbf{x} - \mathbf{b}\|^2 = \mathbf{x}^\top A^\top A\mathbf{x} - 2\mathbf{b}^\top A\mathbf{x} + \mathbf{b}^\top\mathbf{b}.$$

Set

$$A_1 = \begin{bmatrix} A^\top A & \mathbf{b}^\top \\ \mathbf{b} & \mathbf{b}^\top\mathbf{b} \end{bmatrix}.$$

Note that $A_1 \succeq 0$. Then

$$\alpha(A) = \min\{\mathbf{y}^\top A\mathbf{y}, \mathbf{y} \in \{-1, 1\}^{n+1}\} = \nu_{\min}(A_1).$$

Indeed, by considering $\pm\mathbf{y}$ it is enough to assume that $\mathbf{y}^\top = (\mathbf{x}^\top, -1)$. Then we get $\mathbf{y}^\top A_1 \mathbf{y} = \|A\mathbf{x} - \mathbf{b}\|^2$. Hence a lower bound for $\alpha(A)$ is the $\gamma_{\min}(A_1)$:

$$\alpha(A) \ge \gamma_{\min}(A_1).$$

Since $A_1 \succeq 0$ and $X \in \mathcal{K}_{n+1}$ is positive semidefinite then by Lemma 1.2 $\langle A_1, X\rangle \ge 0$. Hence $\gamma_{\min}(A_1) \ge 0$. The strong duality theorem combined with Corollary 3.4 yields that $\gamma_{\min}(A_1) = \omega_{\max}(A_1)$. Note that Theorem 3.5 is not applicable here. Of course it would be nice if there was an explicit constant not depending on n such that $\alpha(A) \le C\gamma_{\min}(A_1)$ at least for some interesting cases of A!

3.3 Max-cut

Let $G = (V, E)$ be a simple graph. Assume that $|V| = n$ and $|E| = m$. Let $V = \{v_1, \ldots, v_n\}$ We associate with G the symmetric $0-1$ matrix $A(G) = [a_{ij}] \in \mathrm{S}_n$ as follows: $a_{ij} = 1$ if and only if the edge $v_i v_j \in E$. All other entries are zero. (In particular $a_{ii} = 0$ for $i \in [n]$.) $A(G)$ is called the adjacency matrix of the G. Suppose that each edge $e \in E$ in the graph has weight $w(e)$. Let $\mathbf{w} : E \to \mathbb{R}$. Then we have a weighted graph $G_{\mathbf{w}} = (V, E, \mathbf{w})$. Denote by $w(E) = \sum_{e\in E} w(e)$. The the corresponding weighted matrix is a weighted adjacency matrix $A(G, \mathbf{w}) = [a_{ij}] \in \mathrm{S}_n$. So $a_{ij} = 0$ if $v_i v_j \notin E$ and $a_{ij} = a_{ji} = w(e)$ if $e = v_i v_j$. A cut in G is a of nonempty strict subset of vertices $W \subset V$. Denote $\delta(W) \subset E$ the set of all edges whose one end is in W and the other one in $V \setminus W$. The set $\delta(W)$ is called a cut, (an edge-cut), Then the weight of is given as

$$\mathbf{w}(\delta(W)) = \sum_{e\in\delta(W)} w(e) = \sum_{v_i\in W, v_j\in V\setminus W} a_{ij}. \tag{3.20}$$

Denote by $\mathbf{x}_W = (x_1, \ldots, x_n)^\top \in \{-1, 1\}^n$ a modified characteristic vector of the set W. Namely $x_i = 1$ if $v_i \in W$ and $x_j = -1$ if $j \in V \setminus W$. Denote by $\mathbf{1}_V = \mathbf{1}_n = (1, \ldots 1)^\top$, the characteristic vector of V. A straightforward calculation shows

$$\mathbf{w}(\delta(W)) = \frac{1}{2}(\mathbf{1}_n^\top A(G, \mathbf{w})\mathbf{1}_n - \mathbf{1}_W^\top A(G, \mathbf{w})\mathbf{1}_W). \tag{3.21}$$

Recall that if $\mathbf{w} \ge \mathbf{0}$ then the min-cut problem $\min\{\mathbf{w}(\delta(W),\ W, \emptyset \ne W \subset V\}$ can be solved in polynomial time using flows or contraction algorithms [1]. The max-cut problem is

$$\mu(G, \mathbf{w}) = \max\{\mathbf{w}(\delta(W),\ W, \emptyset \ne W \subset V\}. \tag{3.22}$$

If $\mathbf{w} = \mathbf{1}_E$, i.e., all edges in G are given the weight 1, then $\mu(G) = \mu(G, \mathbf{1}_E)$, and $\mu(G)$ is called the max-cut of G. The problem of deciding if $\mu(G) \le k$ for an integer $k(\le \frac{n(n-1)}{2})$ is NP-complete [3].

Assume that $\mathbf{w} \ge \mathbf{0}$. Then $2w(E) = \mathbf{1}_n^\top A(G, \mathbf{w})\mathbf{1}_n \ge \mathbf{1}_W^\top A(G, \mathbf{w})\mathbf{1}_W$. Hence (3.21) yields

$$\mu(G, \mathbf{w}) = w(E) + \frac{1}{2}\nu(-A(G, \mathbf{w})), \quad \mathbf{w} \ge 0,\ w(E) = \frac{1}{2}\mathbf{1}_n A(G, \mathbf{w})\mathbf{1}_n. \tag{3.23}$$

For $\mathbf{w} \ge 0$ denote by $L(G, \mathbf{w}) \in \mathrm{S}_{n,+}$ the weighted Laplacian matrix corresponding $G_{\mathbf{w}}$:

$$L(G, \mathbf{w}) = D(A(G, \mathbf{w})\mathbf{1}_n) - A(G, \mathbf{w}). \tag{3.24}$$

So the off-diagonal entries of $L(G,\mathbf{w})$ are the off-diagonal of $-A(G,\mathbf{w})$, the diagonal entry are nonnegative and each row sum is 0: $L(G,\mathbf{w})\mathbf{1}_n=\mathbf{0}$. It is well known that $L(G,\mathbf{w})\succeq 0$ [2, §6.6]. As

$$\mathbf{x}^\top D(A(G,\mathbf{w})\mathbf{1}_n)\mathbf{x}=2w(E),\ \text{for each } \mathbf{x}\in\{-1,1\}^n,$$

it follows that

$$\mu(G,\mathbf{w})=\frac{1}{2}\nu_{\max}(L(G,\mathbf{w}))\text{ for }\mathbf{w}\geq 0. \tag{3.25}$$

Hence the SDP relaxation of $\mu(G,\mathbf{w})$ is $\frac{1}{2}\gamma_{\max}(L(G,\mathbf{w}))$. Combine the above result to deduce that with Theorem 3.5 to deduce the inequality

$$\frac{1}{\pi}\gamma_{\max}(L(G,\mathbf{w}))\leq\mu(G,\mathbf{w})\leq\frac{1}{2}\gamma_{\max}(L(G,\mathbf{w})).$$

We now point out briefly a "proof" of (3.18) using the identity of Goemens-Williamson[4]. For $x\in[-1,1]$ denote by $\arcsin x$ the principal value of the Arcsine of x. Hence $\arcsin x\in[-\frac{\pi}{2},\frac{\pi}{2}]$. Recall that teh convergent series of $\arcsin x$:

$$\arcsin x=x+\frac{1}{2}\frac{x^3}{3}+\frac{1\times 3}{2\times 4}\frac{x^5}{4}+\cdots,\quad |x|<1. \tag{3.26}$$

Note that the coefficients of even powers are zero and the coefficient of odd powers are positive. For $X=]x_{ij}]\in \mathrm{S}_n$ and a positive integer k denote by $X^{\circ k}=[x_{ij}^k]$, the $k-th$ Schur power of X. It is well known that if $X\in\mathrm{S}_{n,+}$ then $X^{\circ k}\in\mathrm{S}_{n,+}$ [2, Chapter 5]. (Note that $\otimes^k X\succeq 0$. Then $X^{\circ k}$ is a principal submatrix of $\otimes^k X$.)

Let

$$\mathrm{S}_n([-1,1])=\{Y=[y_{ij}]\in\mathrm{S}_n,\quad |y_{ij}|\leq 1,\ \text{for } i,j\in[n]\}. \tag{3.27}$$

Observe next that if $X=[x_{ij}]\in\mathcal{K}_n$ then $|x_{ij}|\leq 1$. (This follows from the fact that all 2×2 minors of X are nonnegative.) Hence $\mathcal{K}_n\subset\mathrm{S}_n([-1,1])$.

For $Y=[y_{ij}]\in\mathrm{S}_n([-1,1])$ define $\arcsin Y=[\arcsin y_{ij}]$. Observe that the following map maps $\mathrm{S}_n([-1,1])$ to itself:

$$\phi:\mathrm{S}_n([-1,1])\to\mathrm{S}_n([-1,1],\quad \phi(Y)=\frac{2}{\pi}\arcsin Y. \tag{3.28}$$

Denote the set of fixed points of ϕ by $\mathrm{Fix}(\phi)$. As $\frac{2}{\pi}arcsinx$ has exactly 3 fixed points on $[-1,1]$ it follows that $Y\in$Fix(ϕ) if and only if all the entries of Y are in $\{-1,0,1\}$. (The graph of $y=\arcsin x$ is strictly convex on $[0,1]$ and strictly concave on $[-1,0]$.)

Assume that $Y=[y_{ij}]$ is in the interior of $\mathrm{S}_n([-1,1])$, i.e., $|y_{ij}|<1$ for $i,j\in[n]$. In view of (3.26) it follows that

$$\arcsin Y=Y+\frac{1}{2}\frac{Y^{\circ 3}}{3}+\frac{1\times 3}{2\times 4}\frac{Y^{\circ 5}}{4}+\cdots.$$

Suppose furthermore that $Y\succeq 0$. The above identity yields that $\arcsin Y\succeq Y$. The continuity argument yield that

$$\arcsin X\succeq X\text{ for }X\in\mathcal{K}_n. \tag{3.29}$$

Lemma 1.2 yields:

$$\langle A, \arcsin X\rangle \geq \langle A, X\rangle \text{ if } A \in \mathrm{S}_{n,+} \text{ and } X \in \mathcal{K}_n. \tag{3.30}$$

The last step in the proof of (3.18) is the identity of Goemans-Williamson [4]:

$$\nu_{\max}(A) = \frac{2}{\pi} \max\{\langle A, \arcsin X\rangle,\ X \in \mathcal{K}_n\},\ \text{for } A \in \mathrm{S}_n. \tag{3.31}$$

This result is equivalent to the following statement:

Lemma 3.6 *The closed set $\phi(\mathcal{K}_n)$ is contained in the convex hull spanned $\mathcal{X}_n = \{\mathbf{x}\mathbf{x}^\top, \mathbf{x} \in \{-1,1\}^n\}$.*

Proof. Recall that $\mathcal{X}_n \subset$Fix(ϕ). Hence $\phi(\mathcal{K}_n) \supset \mathcal{X}_n$. Suppose to the contrary that conv $\mathcal{X}_n$ does not $\phi(\mathcal{K}_n)$. Hence conv $\phi(\mathcal{K}_n)$ contains an extreme point $X \in \phi(\mathcal{K}_n)$ which is not in $\mathcal{X}_n$. Then there must be a linear functional on $\mathcal{H}_n$ which supports conv $\phi(\mathcal{K}_n)$ at X. This linear functional is $\langle A, \cdot\rangle$ for some $A \in \mathrm{S}_n$. (We can assume that A has zero diagonal.) That is $\nu(A) < \langle A, X\rangle$ which contradicts (3.31).

3.4 The Grothendieck inequality

References

[1] W.J. Cook, W.H. Cunningham, W.R. Pulleyblank, and A.Schrijver, *Combinatorial Optimization*, Wiley, 1998.

[2] S. Friedland, *Matrices: Algebra, Analysis and Applications*, World Scientific, 596 pp., 2015, Singapore, http://www2.math.uic.edu/∼friedlan/bookm.pdf

[3] M.R. Garey, and S. D. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W.H. Freeman, 1979.

[4] M.X. Goemans and D.P. Williamson, Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming, *J. ACM* 42 (1995), 1115–1145.

[5] C. Helmberg, Semidefinite Progrmming for Combinatorial Optimization, https://www-user.tu-chemnitz.de/ helmberg/semidef.html

[6] R.E. Rietz, A proof of the Grothendieck inequality, *Israel Journal of Mathematics*, 19 (1974), 271–276.

[7] Y. Nesterov, Semidefinite relaxation and nonconvex quadratic optimization, *Optimization Methods and Software* 9 (1998), 141–160.

[8] P.A. Parrilo, Binary optimization, 2006, https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-972-algebraic-techniques-and-semidefinite-optimization-spring-2006/lecture-notes/lecture_03.pdf

[9] R.T. Rockafellar, *Convex analysis*, Princeton University Press, 1997.