COM-440, Introduction to Quantum Cryptography, Fall 2025

Notes on semidefinite programming

1 Semidefinite programs

In general a semidefinite program (SDP) is the optimization of a linear function under linear and semidefinite constraints. Let's see some examples.

1. For any symmetric matrix B, its largest eigenvalue can be expressed as

$$\begin{aligned} \min \quad & x_1 \\ \text{s.t.} \quad & x_1 \mathbb{I} - B \succeq 0 \end{aligned}$$

2. The following SDP

$$\begin{aligned} \inf \quad & x_1 \\ \text{s.t.} \quad & \begin{pmatrix} x_1 & 1 \\ 1 & x_2 \end{pmatrix} \succeq 0 \end{aligned}$$

is equivalent to $x_1, x_2 \geq 0$ and $x_1 x_2 \geq 1$. The optimum is 0, but this optimal value is not attained at any feasible point. This is an important difference with LPs. From now on we'll have to be careful and write "inf" or "sup" instead of "min" or "max" whenever we're writing an SDP for which we're not sure whether the optimum is attained.

3. This SDP

$$\begin{aligned} \inf \quad & x_n \\ \text{s.t.} \quad & x_0 \geq 2 \\ & \begin{pmatrix} 1 & x_0 \\ x_0 & x_1 \end{pmatrix} \succeq 0 \\ & \begin{pmatrix} 1 & x_1 \\ x_1 & x_2 \end{pmatrix} \succeq 0 \\ & \vdots \\ & \begin{pmatrix} 1 & x_{n-1} \\ x_{n-1} & x_n \end{pmatrix} \succeq 0 \end{aligned}$$

evaluates to 2^{2^n}. Here even writing down the optimum requires a number of bits (2^n) that is exponential in the instance size ($O(n)$ bits). This could not happen for LPs either.

1.1 Canonical form

In the following we will use the convenient notation $X \bullet Y = \mathrm{Tr}(XY^\dagger)$, which is valid whenever X, Y are two square matrices of the same size. Note that $\bullet$ is a valid inner product on the space of square matrices.

Just as linear programs, every SDP has a *canonical form* as follows:

$$\begin{aligned} (\mathcal{P}) \qquad \sup \quad & B \bullet X \\ \text{s.t.} \quad & A_i \bullet X = c_i \quad \forall i \in \{1, \ldots, m\} \\ & X \succeq 0, \end{aligned} \tag{1.1}$$

where $B \in \mathbb{C}^{n\times n}$ is Hermitian, $A_1,\ldots,A_m \in \mathbb{C}^{n\times n}$ are also Hermitian, and $c_i \in \mathbb{R}$.

Exercise 1.1. Write each of the three SDPs from the previous section in canonical form (i.e. specify what the matrices B, A_i, and the reals c_i should be).

The canonical form can be written in a slightly different, though equivalent, way by replacing the collection of constraints $A_i \bullet X \leq c_i$, for $i \in \{1,\ldots,m\}$, with a single constraint $\Phi(X) = C$ where Φ is a linear map that preserves Hermitianity and C is a matrix (not necessarily of the same dimension as X). To see that the two are equivalent, first note that the former can be converted to the latter by defining $\Phi(X) = \sum_i (A_i \bullet X)E_{i,i}$ with $E_{i,i}$ the diagonal matrix with a unique 1 in position (i,i) and 0 elsewhere. Conversely, the constraint $\Phi(X) = C$ can be replaced by the collection of constraints $H_i \bullet \Phi(X) = H_i \bullet C$ where H_i ranges over a Hermitian basis of square matrices of the correct size.

Summarizing, we have the following equivalent primal form:

$$\begin{aligned} (\mathcal{P}) \qquad \sup \quad & B \bullet X \\ \text{s.t.} \quad & \Phi(X) = C \\ & X \succeq 0, \end{aligned} \tag{1.2}$$

1.2 Dual of an SDP

Let's develop the duality theory for SDPs. What is the dual of $(\mathcal{P})$ given in (1.1)? Let's proceed in the same way as one derives the dual of an LP: form linear combinations of the constraints in order to prove upper bounds on the objective value. More precisely, for any $y_1,\ldots,y_m \in \mathbb{R}$, if

$$y_1A_1 + \ldots + y_mA_m \succeq B$$

then for any primal feasible X

$$B \bullet X \preceq (y_1A_1 + \ldots + y_mA_m) \bullet X = y^T c,$$

where the second inequality uses $A \leq Z \implies A \bullet X \leq Z \bullet X$ for any $X \geq 0$. We obtain the dual

$$\begin{aligned} (\mathcal{D}) \qquad \inf \quad & y^T c \\ \text{s.t.} \quad & y_1,\ldots,y_m \in \mathbb{R} \\ & y_1A_1 + \ldots + y_mA_m - B \succeq 0, \end{aligned}$$

and we just showed:

Theorem 1.2 (Weak Duality)**.** *If both the primal and the dual problems are feasible and bounded, then*

$$\mathrm{OPT}(\mathcal{P}) \leq \mathrm{OPT}(\mathcal{D}).$$

We can also write the dual of the form (1.2):

$$\begin{aligned} (\mathcal{D}) \qquad \inf \quad & C \bullet Y \\ \text{s.t.} \quad & Y \text{ Hermitian} \\ & \Phi^*(Y) \succeq B, \end{aligned}$$

where Φ^* is the dual map to Φ, i.e. such that $\Phi(X) \bullet Y = X \bullet \Phi^*(Y)$ for all X, Y.

While weak duality always holds under the same conditions as for LPs, strong duality can fail dramatically!

Example 1.3. Consider the optimization problem

$$\begin{array}{ll} \inf & -y_1 \\ \text{s.t.} & \begin{pmatrix} 0 & y_1 & 0 \\ y_1 & y_2 & 0 \\ 0 & 0 & 1-y_1 \end{pmatrix} \succeq 0 \qquad\qquad y_1, y_2 \geq 0. \end{array} \tag{1.3}$$

A block matrix is PSD if and only if each block is PSD. The determinant of a PSD matrix should be no less than 0, thus $0 \times y_2 - y_1^2 \geq 0$, and the optimum of the above SDP is 0. You can check that its dual is given by

$$\begin{array}{ll} \sup & -X_{33} \\ \text{s.t.} & X_{12} + X_{21} - X_{33} \leq -1 \\ & X_{22} \leq 0 \\ & X \succeq 0. \end{array}$$

Since $X_{22} \leq 0$, for X to be PSD it must be 0. The PSD condition then implies $X_{12} = X_{21} = 0$, so $-X_{33} \leq -1$ and the optimum is -1.

In spite of this strong duality does hold as long as both the primal and dual SDPs are *strictly feasible*:

Theorem 1.4 (Strong Duality)**.** *Suppose both the primal $\mathcal{P}$ and the dual $\mathcal{D}$ are strictly feasible and bounded, then*

$$\mathrm{OPT}(\mathcal{P}) = \mathrm{OPT}(\mathcal{D}).$$

1.3 Solving SDPs

Example 3 in the introduction demonstrates that an SDP cannot always be solved exactly in polynomial time, even if it is both feasible and bounded. Two additional conditions will allow us to give polynomial-time algorithms. First, we will only solve SDPs approximately. This takes care of the second example: we will only require the solver to return a feasible point that achieves an objective value at least $\mathrm{opt} - \varepsilon$, for any $\varepsilon > 0$ (the running time will depend on ε). Second, the SDP solver will require as input an a priori bound on the size of the solution. This gets rid of the third example. Finally, we will also need to require that the SDP is *strictly feasible*, meaning that there is a feasible point X that is strictly positive.

Under these three conditions it is possible to show that SDPs can be solved efficiently. Here is one of the best results known:

Theorem 1.5. *For any $\varepsilon > 0$ and any SDP such that the feasible region K is such that $\exists r, R > 0$, $\vec{O}$ with*

$$B(\vec{O}, r) \subset K \subset B(\vec{O}, R),$$

a feasible X such that $B \bullet X \geq \mathrm{OPT}(SDP) - \varepsilon$ can be computed in time $\mathrm{poly}(\log \frac{R}{r} + |SDP| + \log \frac{1}{\varepsilon})$, where $|SDP|$ denotes the number of bits required to completely specify the SDP instance.

2 The Joi-Jamiolkowski representation

Consider a linear map $\Phi : \mathbb{C}^{d \times d} \to \mathbb{C}^{d' \times d'}$. Further fix a standard basis $\{|1\rangle, \ldots, |d\rangle\}$ and $\{|1\rangle, \ldots, |d'\rangle\}$ of $\mathbb{C}^d$ and $\mathbb{C}^{d'}$ respectively. With respect to this basis, the *Choi-Jamiołkowski representation* of Φ is defined as

$$J(\Phi) = \sum_{1 \leq i,j \leq d} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j| \in \mathbb{C}^{d \times d} \otimes \mathbb{C}^{d' \times d'}.$$

The operator $J(\Phi)$ uniquely determines Φ, and the following is a useful lemma relating the two representations.

Lemma 2.1. *Φ is a valid quantum channel if and only if $J(\Phi)$ is positive semidefinite and $\mathrm{Tr}_2(J(\Phi)) = I$. (Here, by Tr_2 we mean tracing out the second system, the one of dimension d'.)*

Finally we state the well-known and easy to verify relation

$$\langle \phi | \Phi(|\psi\rangle\langle\psi|) | \phi \rangle = \langle \phi \otimes \overline{\psi} | J(\Phi) | \phi \otimes \overline{\psi} \rangle$$

for any choice of vectors $|\psi\rangle \in \mathbb{C}^d$ and $|\phi\rangle \in \mathbb{C}^{d'}$, with complex conjugation taken with respect to the standard basis.