Semidefinite Programming in Quantum Information Theory

Ramij Rahaman

Department of Mathematics
University of Allahabad
Allahabad 211002
UP, India

Table of contents

References

- John Watrous. Lecture CS 766/QIC 820 Theory of Quantum Information. University of Waterloo, Fall 2011.
- J. Watrous, lecture slide on Semidefinite Programming in the Theory of Quantum Information [Present talk is highly inspired by this Ref.].
- M Navascues, S Pironio and A Acin, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New Journal of Physics 10 (2008) 073013.
- Robert M. Freund, Introduction to Semidefinite Programming (SDP).
- J. F. Sturm, Optim. Methods Softw. 17, 6 (2002).
- J. F. Sturm, Optim. Methods Softw. 11, 625 (1999).
- J. W. Eaton, D. Bateman, and S. Hauberg, GNU Octave version 3.0.1 manual: a high-level interactive language for numerical computations (CreateSpace Independent Publishing Platform, 2009).
- L. Masanes, S. Pironio and Antonio Acin, Nature Communications 2, 238 (2011)

Basic notations:

Linear operators: A linear operator T is an operator such that

(i) the domain $\mathcal{D}(T)$ of T is a vector space and the range $\mathcal{R}(T)$ lies in a vector space over the same field.

(ii) for all $x, y \in \mathcal{D}(T)$ and scalars α, β,

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$$

For vector spaces $\mathcal{X}$ & $\mathcal{Y}$,

$$\begin{aligned} L(\mathcal{X}, \mathcal{Y}) &\equiv \{T \mid T \text{ is a linear mapping/operator from } \mathcal{X} \text{ to } \mathcal{Y}\} \\ L(\mathcal{X}) &= L(\mathcal{X}, \mathcal{X}) \end{aligned}$$

If $\mathcal{X} = \mathbb{C}^{\Lambda}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$, then $L(\mathcal{X}, \mathcal{Y})$ is the set of all matrices with rows indexed by Γ and columns indexed by Λ.

Basic notations:

Linear operators: A linear operator T is an operator such that

(i) the domain $\mathcal{D}(T)$ of T is a vector space and the range $\mathcal{R}(T)$ lies in a vector space over the same field.

(ii) for all $x, y \in \mathcal{D}(T)$ and scalars α, β,

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$$

For vector spaces $\mathcal{X}$ & $\mathcal{Y}$,

$$\begin{aligned} L(\mathcal{X}, \mathcal{Y}) &\equiv \{T \mid T \text{ is a linear mapping/operator from } \mathcal{X} \text{ to } \mathcal{Y}\} \\ L(\mathcal{X}) &= L(\mathcal{X}, \mathcal{X}) \end{aligned}$$

If $\mathcal{X} = \mathbb{C}^{\Lambda}$ and $\mathcal{Y} = \mathbb{C}^{\Gamma}$, then $L(\mathcal{X}, \mathcal{Y})$ is the set of all matrices with rows indexed by Γ and columns indexed by Λ.

Adjoint operator: Let $T \in L(\mathcal{X}, \mathcal{Y})$. Then the adjoint operator T^* of T is the operator $T^* : \mathcal{Y} \to \mathcal{X}$ such that for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$

$$\langle T(x), y \rangle = \langle x, T^*(y) \rangle$$

As a matrix, T^* is the conjugate transpose (or Hermitian transpose) of T, and is often denoted $T^\dagger$.

Inner product: For $A, B \in L(\mathcal{X}, \mathcal{Y})$, we define the inner product as

$$\langle A, B \rangle = \mathrm{Tr}\left(A^{\dagger} B\right)$$

Hermitian/self-adjoint operators: An operator $T \in L(\mathcal{X})$ is called Hermitian/self-adjoint if $T^{*} = T^{\dagger} = T$.

We will write Herm(X) to denote the set of all such operators of $L(\mathcal{X})$.

Positive semidefinite operators: Let $T \in$Herm$(\mathcal{X})$. Then T is said to be positive semidefinite, written

$$T \geq 0 \quad \text{if and only if} \quad \langle T(x), x \rangle \geq 0 \quad \text{for all } x \in \mathcal{X}$$

That is, eigenvalues of T are nonnegative.

We denote the set of all positive semidefinite operators from Herm$(\mathcal{X})$ by Psd$(\mathcal{X})$.

Remarks: Positive semidefinite operators having trace equal to one are called density operators.

$$D(\mathcal{X}) = \{\rho | \rho \in \mathrm{Psd}(\mathcal{X}) \ \& \ \mathrm{Tr}(\rho) = 1\}$$

Positive semidefinite operators: Let $T \in$Herm($\mathcal{X}$). Then T is said to be positive semidefinite, written

$$T \geq 0 \quad \text{if and only if} \quad \langle T(x), x\rangle \geq 0 \quad \text{for all } x \in \mathcal{X}$$

That is, eigenvalues of T are nonnegative.

We denote the set of all positive semidefinite operators from Herm($\mathcal{X}$) by Psd($\mathcal{X}$).

Remarks: Positive semidefinite operators having trace equal to one are called density operators.

$$D(\mathcal{X}) = \{\rho | \rho \in \mathrm{Psd}(\mathcal{X}) \ \& \ \mathrm{Tr}(\rho) = 1\}$$

Linear mappings on operators: Let us define

$$\mathrm{T}(\mathcal{X},\mathcal{Y}) \equiv \{\Phi |\ \Phi : L(\mathcal{X}) \to L(\mathcal{Y}),\ \text{a linear map}\}$$

For every $\Phi \in \mathrm{T}(\mathcal{X},\mathcal{Y})$, we define the adjoint mapping $\Phi^* \in \mathrm{T}(\mathcal{Y},\mathcal{X})$ to be the unique mapping that satisfies

$$\langle Y, \Phi(X)\rangle = \langle \Phi^*(Y), X\rangle \ \text{ for all } X \in L(\mathcal{X}) \ \&\ Y \in L(\mathcal{Y}).$$

A mapping $\Phi \in \mathrm{T}(\mathcal{X},\mathcal{Y})$ is Hermiticity-preserving if $\Phi(X) \in \text{Herm}(\mathcal{Y})$ for all $X \in \text{Herm}(\mathcal{X})$.

Semidefinite Program (SDP)

A semidefinite program (SDP) is a pair of optimization problems (Primal & Dual), specified by a triple (Φ, A, B), where

1. $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is a Hermiticity-preserving mapping,
2. $A \in \mathrm{Herm}(\mathcal{X})$, and
3. $B \in \mathrm{Herm}(\mathcal{Y})$.

Then the concerning pair of optimization problems are:

Primal problem		Dual problem	
Maximize:	$\langle A, X \rangle$	Minimize:	$\langle B, Y \rangle$
Subject to:	$\Phi(X) = B$	Subject to:	$\Phi^*(Y) \geq A$
	$X \in \mathrm{Psd}(\mathcal{X})$		$Y \in \mathrm{Herm}(\mathcal{Y})$

Semidefinite Program (SDP)

A semidefinite program (SDP) is a pair of optimization problems (Primal & Dual), specified by a triple (Φ, A, B), where

1. $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ is a Hermiticity-preserving mapping,
2. $A \in \mathrm{Herm}(\mathcal{X})$, and
3. $B \in \mathrm{Herm}(\mathcal{Y})$.

Then the concerning pair of optimization problems are:

Primal problem

Maximize: $\langle A, X \rangle$
Subject to: $\Phi(X) = B$
$X \in \mathrm{Psd}(\mathcal{X})$

Dual problem

Minimize: $\langle B, Y \rangle$
Subject to: $\Phi^*(Y) \geq A$
$Y \in \mathrm{Herm}(\mathcal{Y})$

Let α be the optimal value of the primal problem

$$\begin{array}{rl} \text{Maximize:} & \langle A, X\rangle \\ \text{Subject to:} & \Phi(X) = B \\ & X \in \mathrm{Psd}(\mathcal{X}) \end{array}$$

$$\alpha = \sup_{X\in\mathscr{A}}\langle A, X\rangle; \quad \mathscr{A} = \{X \in \mathrm{Psd}(\mathcal{X})|\ \Phi(X) = B\}$$

and β be the optimal value of the dual problem

$$\begin{array}{rl} \text{Minimize:} & \langle B, Y\rangle \\ \text{Subject to:} & \Phi^*(Y) \geq A \\ & Y \in \mathrm{Herm}(\mathcal{Y}) \end{array}$$

$$\beta = \inf_{Y\in\mathscr{B}}\langle B, Y\rangle; \quad \mathscr{B} = \{Y \in \mathrm{Herm}(\mathcal{Y})|\ \Phi^*(Y) \geq A\}$$

Remarks: Sup/inf cannot be replaced by a maximum/minimum in general, in some cases the optimal values will not be achieved.

Let α be the optimal value of the primal problem

$$\begin{array}{rl} \text{Maximize:} & \langle A, X\rangle \\ \text{Subject to:} & \Phi(X) = B \\ & X \in \mathrm{Psd}(\mathcal{X}) \end{array}$$

$$\alpha = \sup_{X\in\mathscr{A}}\langle A, X\rangle; \quad \mathscr{A} = \{X \in \mathrm{Psd}(\mathcal{X}) | \ \Phi(X) = B\}$$

and β be the optimal value of the dual problem

$$\begin{array}{rl} \text{Minimize:} & \langle B, Y\rangle \\ \text{Subject to:} & \Phi^*(Y) \geq A \\ & Y \in \mathrm{Herm}(\mathcal{Y}) \end{array}$$

$$\beta = \inf_{Y\in\mathscr{B}}\langle B, Y\rangle; \quad \mathscr{B} = \{Y \in \mathrm{Herm}(\mathcal{Y}) | \ \Phi^*(Y) \geq A\}$$

Remarks: Sup/inf cannot be replaced by a maximum/minimum in general, in some cases the optimal values will not be achieved.

Example 1: Let us consider,

$$\mathcal{X} = \mathbb{C}^n \quad \& \mathcal{Y} = \mathbb{C},$$

and for any $A \in \mathrm{Herm}(\mathbb{C}^n)$ we take $\Phi \equiv \mathrm{Tr}$ and $B = 1$.

Then the primal problem associated with this SDP as follows:

$$\begin{array}{rl} \text{Maximize:} & \langle A, X \rangle \\ \text{Subject to:} & \Phi(X) = \mathrm{Tr}(X) = 1 \\ & X \in \mathrm{Psd}(\mathbb{C}^n) \end{array} \quad \Rightarrow \quad \begin{array}{rl} \text{Maximize:} & \langle A, \rho \rangle \\ \text{Subject to:} & \rho \in D(\mathbb{C}^n). \end{array}$$

Example 1: Let us consider,

$$\mathcal{X} = \mathbb{C}^n \quad \& \mathcal{Y} = \mathbb{C},$$

and for any $A \in \text{Herm}(\mathbb{C}^n)$ we take $\Phi \equiv$Tr and $B = 1$.

Then the primal problem associated with this SDP as follows:

$$\begin{array}{rl} \text{Maximize:} & \langle A, X \rangle \\ \text{Subject to:} & \Phi(X) = \text{Tr}(X) = 1 \\ & X \in \text{Psd}(\mathbb{C}^n) \end{array} \quad \Rightarrow \quad \begin{array}{rl} \text{Maximize:} & \langle A, \rho \rangle \\ \text{Subject to:} & \rho \in D(\mathbb{C}^n). \end{array}$$

$$A = \sum_{k=1}^{n} \lambda_k | x_k \rangle \langle x_k |.$$

Here, $\lambda_1 \geq \cdots \geq \lambda_n$ are eigenvalues of A and $\{| x_1 \rangle, \ldots, | x_n \rangle\}$ is an orthonormal basis of $\mathbb{C}^n$ consisting of corresponding eigenvectors.

Example 1: Let us consider,

$$\mathcal{X} = \mathbb{C}^n \quad \& \mathcal{Y} = \mathbb{C},$$

and for any $A \in \mathrm{Herm}(\mathbb{C}^n)$ we take $\Phi \equiv \mathrm{Tr}$ and $B = 1$.

Then the primal problem associated with this SDP as follows:

$$\begin{array}{rl} \text{Maximize:} & \langle A, X \rangle \\ \text{Subject to:} & \Phi(X) = \mathrm{Tr}(X) = 1 \\ & X \in \mathrm{Psd}(\mathbb{C}^n) \end{array} \quad \Rightarrow \quad \begin{array}{rl} \text{Maximize:} & \langle A, \rho \rangle \\ \text{Subject to:} & \rho \in D(\mathbb{C}^n). \end{array}$$

$$A = \sum_{k=1}^{n} \lambda_k | x_k \rangle \langle x_k |.$$

Here, $\lambda_1 \geq \cdots \geq \lambda_n$ are eigenvalues of A and $\{| x_1 \rangle, \ldots, | x_n \rangle\}$ is an orthonormal basis of $\mathbb{C}^n$ consisting of corresponding eigenvectors.

$$A = \sum_{k=1}^{n} \lambda_k | x_k \rangle \langle x_k |.$$

For any $\rho \in D(\mathbb{C}^n)$, we have

$$\langle A, \rho \rangle = \sum_{k=1}^{n} \lambda_k \langle | x_k \rangle \langle x_k |, \rho \rangle,$$

The optimal value is $\alpha = \lambda_1$ (the largest eigenvalue of A).

Now the associate dual problem for our example
[$\mathcal{X} = \mathbb{C}^n, \mathcal{Y} = \mathbb{C}, \Phi \equiv$Tr, and $B = 1$] is

$$\begin{aligned} \text{Minimize:} \quad & \langle B, Y \rangle \\ \text{Subject to:} \quad & \Phi^*(Y) \geq A \\ & Y \in \text{Herm}(\mathbb{C}) \end{aligned} \quad \Rightarrow \quad \begin{aligned} \text{Minimize:} \quad & y \\ \text{Subject to:} \quad & y\mathbb{I} \geq A \\ & y \in \mathbb{R} \end{aligned}$$

If $\Phi \in \mathrm{T}(\mathbb{C}^n, \mathbb{C})$ defined as $\Phi(X) = Tr(X)$ then $\Phi^* \in \mathrm{T}(\mathbb{C}, \mathbb{C}^n)$ will be

$$\Phi^*(y) = \lambda \mathbb{I},$$

as $\langle y, Tr(X) \rangle = \langle y\mathbb{I}, X \rangle$.

Then $\beta = \lambda_1$ [Check this].

Usually $\alpha = \beta$ happens i.e., optimal value of the primal = optimal of the dual problem.

Now the associate dual problem for our example
[$\mathcal{X} = \mathbb{C}^n, \mathcal{Y} = \mathbb{C}, \Phi \equiv$Tr, and $B = 1$] is

$$\begin{array}{rl} \text{Minimize:} & \langle B, Y \rangle \\ \text{Subject to:} & \Phi^*(Y) \geq A \\ & Y \in \text{Herm}(\mathbb{C}) \end{array} \quad \Rightarrow \quad \begin{array}{rl} \text{Minimize:} & y \\ \text{Subject to:} & y\mathbb{I} \geq A \\ & y \in \mathbb{R} \end{array}$$

If $\Phi \in \mathrm{T}(\mathbb{C}^n, \mathbb{C})$ defined as $\Phi(X) = Tr(X)$ then $\Phi^* \in \mathrm{T}(\mathbb{C}, \mathbb{C}^n)$ will be

$$\Phi^*(y) = \lambda \mathbb{I},$$

as $\langle y, Tr(X) \rangle = \langle y\mathbb{I}, X \rangle$.

Then $\beta = \lambda_1$ [Check this].

Usually $\alpha = \beta$ happens i.e., optimal value of the primal = optimal of the dual problem.

Example 2: Take $\mathcal{X} = \mathbb{C}^2 = \mathcal{Y}$ and define $A, B \in$Herm$(\mathbb{C}^2)$ and the Hermiticity-preserving linear map $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ as

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ \ \& \ \ \Phi(X) = \begin{pmatrix} 0 & X_{12} \\ X_{21} & 0 \end{pmatrix},$$

for all $X \in L(\mathcal{X})$. Now the primal problem is

$$\begin{array}{rl} \text{Maximize:} & \langle A, X \rangle \\ \text{Subject to:} & \Phi(X) = B \\ & X \in \mathrm{Psd}(\mathbb{C}^2) \end{array} \quad \Rightarrow \quad \begin{array}{rl} \text{Maximize:} & -X_{11} \\ \text{Subject to:} & X_{12} = 1 = X_{21}. \end{array}$$

It holds that $\alpha = 0$, but there does not exist an optimal primal solution to this SDP.

Example 2: Take $\mathcal{X} = \mathbb{C}^2 = \mathcal{Y}$ and define $A, B \in \mathrm{Herm}(\mathbb{C}^2)$ and the Hermiticity-preserving linear map $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ as

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \& \quad \Phi(X) = \begin{pmatrix} 0 & X_{12} \\ X_{21} & 0 \end{pmatrix},$$

for all $X \in L(\mathcal{X})$. Now the primal problem is

$$\begin{array}{rl} \text{Maximize:} & \langle A, X \rangle \\ \text{Subject to:} & \Phi(X) = B \\ & X \in \mathrm{Psd}(\mathbb{C}^2) \end{array} \quad \Rightarrow \quad \begin{array}{rl} \text{Maximize:} & -X_{11} \\ \text{Subject to:} & X_{12} = 1 = X_{21}. \end{array}$$

It holds that $\alpha = 0$, but there does not exist an optimal primal solution to this SDP.

The condition $\Phi(X) = B$ implies that X takes form

$$X = \begin{pmatrix} X_{11} & 1 \\ 1 & X_{22} \end{pmatrix}$$

Since $X \geq 0$, so we must have $X_{11} \geq 0$ and $\det(X) = X_{11}X_{22} - 1 \geq 0$.

Therefore, $X_{11} > 0$. Hence $\langle A, X \rangle = -X_{11} < 0$.

On the other hand take $X = \begin{pmatrix} \frac{1}{n} & 1 \\ 1 & n^2 \end{pmatrix}$.

Then $\langle A, X_n \rangle = -\frac{1}{n}$ and $\alpha \geq -\frac{1}{n}$.

The condition $\Phi(X) = B$ implies that X takes form

$$X = \begin{pmatrix} X_{11} & 1 \\ 1 & X_{22} \end{pmatrix}$$

Since $X \geq 0$, so we must have $X_{11} \geq 0$ and $\det(X) = X_{11}X_{22} - 1 \geq 0$.

Therefore, $X_{11} > 0$. Hence $\langle A, X \rangle = -X_{11} < 0$.

On the other hand take $X = \begin{pmatrix} \frac{1}{n} & 1 \\ 1 & n^2 \end{pmatrix}$.

Then $\langle A, X_n \rangle = -\frac{1}{n}$ and $\alpha \geq -\frac{1}{n}$.

Weak Duality

For a SDP specified by (Φ, A, B), the optimal primal value α and the optimal dual value β defined as

$$\begin{aligned}\alpha &= \sup\{\langle A, X\rangle : X \in \mathrm{Psd}(\mathcal{X}), \Phi(X) = B\},\\ \beta &= \inf\{\langle B, Y\rangle : Y \in \mathrm{Herm}(\mathcal{Y}), \Phi^*(Y) \geq A\}\end{aligned}$$

Proposition: (Weak duality) For every SDP specified by (Φ, A, B) it holds that $\alpha \leq \beta$.

Proof. *Suppose X is primal feasible and Y is dual feasible then*

$$\langle A, X\rangle \leq \langle \Phi^*(Y), X\rangle = \langle Y, \Phi(X)\rangle = \langle Y, B\rangle = \langle B, Y\rangle$$
$$\Rightarrow \quad \alpha \leq \beta$$

Weak Duality

For a SDP specified by (Φ, A, B), the optimal primal value α and the optimal dual value β defined as

$$\begin{aligned}\alpha &= \sup\{\langle A, X\rangle : X \in \mathrm{Psd}(\mathcal{X}), \Phi(X) = B\},\\ \beta &= \inf\{\langle B, Y\rangle : Y \in \mathrm{Herm}(\mathcal{Y}), \Phi^*(Y) \geq A\}\end{aligned}$$

Proposition: (Weak duality) For every SDP specified by (Φ, A, B) it holds that $\alpha \leq \beta$.

Proof. Suppose X is primal feasible and Y is dual feasible then

$$\langle A, X\rangle \leq \langle \Phi^*(Y), X\rangle = \langle Y, \Phi(X)\rangle = \langle Y, B\rangle = \langle B, Y\rangle$$
$$\Rightarrow \quad \alpha \leq \beta$$

Strong Duality

The condition $\alpha = \beta$ is known as strong duality.

Remarks: Unlike weak duality, strong duality does not hold for every SDP, as the following example shows.

Example 3: Take $\mathcal{X} = \mathbb{C}^3, \mathcal{Y} = \mathbb{C}^2$ and define

$$A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

and $$\Phi(X) = \begin{pmatrix} X_{11} + X_{23} + X_{32} & 0 \\ 0 & X_{22} \end{pmatrix} \quad \forall\, X \in L(\mathcal{X})$$

Check that $\alpha = -1$ and $\beta = 0$.

Strong Duality

The condition $\alpha = \beta$ is known as strong duality.

Remarks: Unlike weak duality, strong duality does not hold for every SDP, as the following example shows.

Example 3: Take $\mathcal{X} = \mathbb{C}^3, \mathcal{Y} = \mathbb{C}^2$ and define

$$A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

and $$\Phi(X) = \begin{pmatrix} X_{11} + X_{23} + X_{32} & 0 \\ 0 & X_{22} \end{pmatrix} \quad \forall\, X \in L(\mathcal{X})$$

Check that $\alpha = -1$ and $\beta = 0$.

Slater's Theorem

For any SDP (Φ, A, B) followings are hold

1. Let $\mathscr{A}$ be the set of primal feasible solutions. If $\mathscr{A} = \emptyset$ and there exists a Hermitian operator Y for which $\Phi^*(Y) > A$, then $\alpha = \beta$ and there exists a primal feasible operator $X \in \mathscr{A}$ for which $\langle A, X \rangle = \alpha$.

2. Let $\mathscr{B}$ be the set of dual feasible solutions. If $\mathscr{B} = \emptyset$ and there exists a positive semidefinite operator X for which $\Phi(X) = B$ and $X > 0$, then $\alpha = \beta$ and there exists a dual feasible operator $Y \in \mathscr{B}$ for which $\langle B, Y \rangle = \beta$.

Slater's Theorem

For any SDP (Φ, A, B) followings are hold

1. Let $\mathscr{A}$ be the set of primal feasible solutions. If $\mathscr{A} = \emptyset$ and there exists a Hermitian operator Y for which $\Phi^*(Y) > A$, then $\alpha = \beta$ and there exists a primal feasible operator $X \in \mathscr{A}$ for which $\langle A, X \rangle = \alpha$.

2. Let $\mathscr{B}$ be the set of dual feasible solutions. If $\mathscr{B} = \emptyset$ and there exists a positive semidefinite operator X for which $\Phi(X) = B$ and $X > 0$, then $\alpha = \beta$ and there exists a dual feasible operator $Y \in \mathscr{B}$ for which $\langle B, Y \rangle = \beta$.

Alternate form of SDP

What is the dual problem of the following primal problem?

Primal problem

$$\begin{aligned} \text{Maximize:} \quad & \langle A, X \rangle \\ \text{Subject to:} \quad & \Phi(X) \leq B \\ & X \in \mathrm{Psd}(\mathcal{X}) \end{aligned}$$

Let for some $Z \in \mathrm{Psd}(\mathcal{Y})$, the constraint $\Phi(X) \leq B$ can be reduced to $\Phi(X) + Z = B$.

Let us define $\Psi \in \mathrm{T}(\mathcal{X} \otimes \mathcal{Y}, \mathcal{Y})$ by

$$\Psi \begin{pmatrix} X & V \\ W & Z \end{pmatrix} = \Phi(X) + Z$$

for all $X \in L(\mathcal{X}),\ Y \in L(Y),\ V \in L(\mathcal{Y}, \mathcal{X})\ W \in L(\mathcal{X}, \mathcal{Y})$.

Also define C as $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$.

Let for some $Z \in \mathrm{Psd}(\mathcal{Y})$, the constraint $\Phi(X) \leq B$ can be reduced to $\Phi(X) + Z = B$.

Let us define $\Psi \in \mathrm{T}(\mathcal{X} \otimes \mathcal{Y}, \mathcal{Y})$ by

$$\Psi \begin{pmatrix} X & V \\ W & Z \end{pmatrix} = \Phi(X) + Z$$

for all $X \in L(\mathcal{X}),\ Y \in L(Y),\ V \in L(\mathcal{Y}, \mathcal{X})\ W \in L(\mathcal{X}, \mathcal{Y})$.

Also define C as $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$.

The primal and dual problems associated with the SDP (Ψ, C, B) are:

Primal problem

$$\text{Max.} \quad \left\langle \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} X & V \\ W & Z \end{pmatrix}, X \right\rangle$$

$$\text{Sub. to:} \quad \Psi \begin{pmatrix} X & V \\ W & Z \end{pmatrix} = B$$

$$\begin{pmatrix} X & V \\ W & Z \end{pmatrix} \in \mathrm{Psd}(\mathcal{X} \oplus \mathcal{Y})$$

Dual problem

$$\text{Min.} \quad \langle B, Y \rangle$$

$$\text{Sub. to:} \quad \Psi^*(Y) \geq \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$$

$$Y \in \mathrm{Herm}(\mathcal{Y})$$

where, $\Psi^*(Y) = \begin{pmatrix} \Phi^*(Y) & 0 \\ 0 & Y \end{pmatrix}$

$\therefore$ The primal & dual problems associated with SDP (Φ, A, B) are:

Primal problem

$$\begin{array}{rl} \text{Maximize:} & \langle A, X\rangle \\ \text{Subject to:} & \Phi(X) \leq B \\ & X \in \mathrm{Psd}(\mathcal{X}) \end{array}$$

Dual problem

$$\begin{array}{rl} \text{Minimize:} & \langle B, Y\rangle \\ \text{Subject to:} & \Phi^*(Y) \geq A \\ & Y \in \mathrm{Psd}(\mathcal{Y}) \end{array}$$

SDP with equality & inequality constraints

Let $\Phi_k : L(\mathcal{X}) \to L(\mathcal{Y}_k)$ (for $k = 1, 2$) be Hermiticity-preserving maps,
let $A \in$Herm$(\mathcal{X})$ and $B_k \in$Herm$(\mathcal{Y}_k)$ (k=1,2), be Hermitian operators.

Primal problem

$$\begin{aligned} \text{Maximize:} \quad & \langle A, X \rangle \\ \text{Subject to:} \quad & \Phi(X) = B_1 \\ & \Phi(X) \leq B_2 \\ & X \in \mathrm{Psd}(\mathcal{X}) \end{aligned}$$

Dual problem

$$\begin{aligned} \text{Minimize:} \quad & \langle B_1, Y_1 \rangle + \langle B_2, Y_2 \rangle \\ \text{Subject to:} \quad & \Phi_1^*(Y_1) + \Phi_2^*(Y_2) \geq A \\ & Y_1 \in \mathrm{Herm}(\mathcal{Y}_1) \\ & Y_2 \in \mathrm{Psd}(\mathcal{Y}_2) \end{aligned}$$

Standard form of SDP

Primal problem		Dual problem	
Maximize:	$\langle A, X \rangle$	Minimize:	$\sum_{j=1}^{m} \gamma_j y_j$
Subject to:	$\langle B_k, X \rangle = \gamma_k$	Subject to:	$\sum_{j=1}^{m} y_j B_j \geq A$
	$k = 1, \cdots, 2$		$y_j \in \mathbb{R}$
	$X \in \text{Psd}(\mathcal{X})$		$j = 1, \cdots, m$

Here, $B_k \in$Herm$(\mathcal{X})$.

SDP in Quantum Information

Optimal measurements: Suppose that we have an ensemble of states

$$\mathcal{E} = \{(p_j, \rho_j)\}_{j=1}^{m}$$

where p_j is a probability for the density operator $\rho_j \in D(\mathcal{Y})$, $j = 1, 2, .., m$.

Task: Identify the correct value of k (i.e., ρ_k) for a given(randomly) single copy of a quantum state from ρ_k $k \in \{1, 2, .., m\}$.

In other words, we wish to choose a measurement $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ so as to maximize the quantity

$$\sum_{k=1}^{m} p_k \langle M_k, \rho_k \rangle$$

So our optimization problem is:

$$\text{Maximize:} \quad \sum_{k=1}^{m} p_k \langle \rho_k, M_k \rangle$$

$$\text{Subject to:} \quad \sum_{i=1}^{m} M_i = \mathbb{I}$$

$$\forall\ i = 1, 2, \ldots, m; \quad M_i \in \mathrm{Psd}(\mathcal{Y})$$

This is, the primal problem corresponding to (Φ, A, B) where

$$\Phi \begin{pmatrix} M_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & M_m \end{pmatrix} = \sum_{k=1}^{m} M_k, \qquad A = \begin{pmatrix} p_1\rho_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & p_m\rho_m \end{pmatrix}$$

and $B = \mathbb{I}$, where we have taken $\mathcal{X} = \mathcal{Y} \oplus \cdots \oplus \mathcal{Y}$ (m-times).

Now observe that:

$$\Phi \begin{pmatrix} M_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & M_m \end{pmatrix} = \sum_{k=1}^{m} M_k, \quad \Rightarrow \quad \Phi^*(Y) = \begin{pmatrix} Y & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & Y \end{pmatrix}$$

Hence the dual problem is given by

Minimize: $\mathrm{Tr}(Y)$

subject to: $\begin{pmatrix} Y & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & Y \end{pmatrix} \geq \begin{pmatrix} p_1\rho_1 & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ \cdot & \cdots & p_m\rho_m \end{pmatrix}$

$Y \in \mathrm{Herm}(\mathcal{Y})$

$\therefore$ The SDP of the concerning problem is

Primal problem

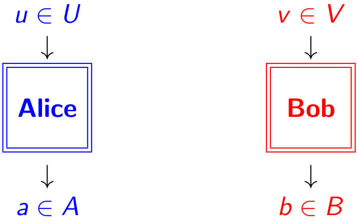
$$\begin{aligned} \text{Maximize:} \quad & \sum_{k=1}^{m} p_k \langle \rho_k, M_k \rangle \\ \text{subject to:} \quad & \sum_{k=1}^{m} M_k = \mathbb{I} \\ & M_k \in \mathrm{Psd}(\mathcal{Y}) \quad \forall \end{aligned}$$

Dual problem

$$\begin{aligned} \text{Minimize:} \quad & \mathrm{Tr}(Y) \\ \text{subject to:} \quad & Y \geq p_k \rho_k \\ & Y \in \mathrm{Herm}(\mathcal{Y}) \end{aligned}$$

Nonlocal Game

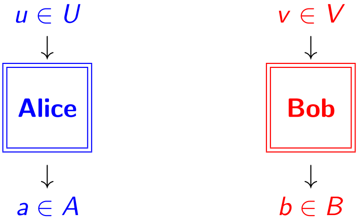
Two cooperative players (Alice and Bob) playing a game against the Referee.



1. Referee randomly selects questions: $u \in U$ for Alice, $v \in V$ for Bob.
2. Alice responds with a $a \in A$, Bob responds with $b \in B$.

Nonlocal Game

Two cooperative players (Alice and Bob) playing a game against the Referee.

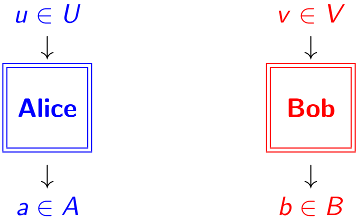


1. Referee randomly selects questions: $u \in U$ for Alice, $v \in V$ for Bob.
2. Alice responds with a $a \in A$, Bob responds with $b \in B$.
3. Referee evaluates some fixed predicate on (u, v, a, b) to determine the result: **Alice and Bob win** or Alice and Bob lose.

Communication between Alice and Bob is not allowed after the game start.

Nonlocal Game

Two cooperative players (Alice and Bob) playing a game against the Referee.



1. Referee randomly selects questions: $u \in U$ for Alice, $v \in V$ for Bob.
2. Alice responds with a $a \in A$, Bob responds with $b \in B$.
3. Referee evaluates some fixed predicate on (u, v, a, b) to determine the result: **Alice and Bob win** or Alice and Bob lose.

Communication between Alice and Bob is not allowed after the game start.

Particular Case: CHSH game is a nonlocal game in which $A = B = \{0, 1\}$ and

1. The referee chooses $u, v \in \{0, 1\}$ uniformly at random.
2. Alice and Bob respond with $a, b \in \{0, 1\}$.
3. They win iff $a \oplus b = u \wedge v$ [for general XOR game, $a \oplus b = f(u, v)$].

Particular Case: CHSH game is a nonlocal game in which $A = B = \{0, 1\}$ and

1. The referee chooses $u, v \in \{0, 1\}$ uniformly at random.
2. Alice and Bob respond with $a, b \in \{0, 1\}$.
3. They win iff $a \oplus b = u \wedge v$ [for general XOR game, $a \oplus b = f(u, v)$].

We know that classically (i.e., without entanglement) Alice and Bob can win with probability at most 3/4.

But, using entanglement they can win with probability $\cos^2(\pi/8) \approx 0.85$.

Particular Case: CHSH game is a nonlocal game in which $A = B = \{0, 1\}$ and

1. The referee chooses $u, v \in \{0, 1\}$ uniformly at random.
2. Alice and Bob respond with $a, b \in \{0, 1\}$.
3. They win iff $a \oplus b = u \wedge v$ [for general XOR game, $a \oplus b = f(u, v)$].

We know that classically (i.e., without entanglement) Alice and Bob can win with probability at most 3/4.

But, using entanglement they can win with probability $\cos^2(\pi/8) \approx 0.85$.

Strategy for Alice and Bob in an XOR game:

1. A shared entangled state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$.
2. A choice of binary-valued (projective) measurements:

$$\{\Pi_0^u, \Pi_1^u\}_{u \in U} \text{ for Alice,} \qquad \{\Pi_0^v, \Pi_1^v\}_{v \in V} \text{ for Bob.}$$

Strategy for Alice and Bob in an XOR game:

1. A shared entangled state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$.
2. A choice of binary-valued (projective) measurements:

$$\{\Pi_0^u, \Pi_1^u\}_{u \in U} \text{ for Alice,} \qquad \{\Pi_0^v, \Pi_1^v\}_{v \in V} \text{ for Bob.}$$

The probability they output (a, b) on questions (u, v) is therefore

$$\langle\psi|\Pi_a^u \otimes \Pi_b^v|\psi\rangle$$

The probability that such a strategy wins an XOR game defined by the function $f : U \times V \to \{0, 1\}$ is

$$\frac{1}{2} + \frac{1}{2}\sum_{u,v} \pi(u, v)(-1)^{f(u,v)}\langle|(\Pi_0^u - \Pi_1^v) \otimes (\Pi_0^u - \Pi_1^v)\rangle$$

[Probability of winning minus losing.]

Strategy for Alice and Bob in an XOR game:

1. A shared entangled state $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$.
2. A choice of binary-valued (projective) measurements:

$$\{\Pi_0^u, \Pi_1^u\}_{u \in U} \text{ for Alice,} \qquad \{\Pi_0^v, \Pi_1^v\}_{v \in V} \text{ for Bob.}$$

The probability they output (a, b) on questions (u, v) is therefore

$$\langle\psi|\Pi_a^u \otimes \Pi_b^v|\psi\rangle$$

The probability that such a strategy wins an XOR game defined by the function $f : U \times V \to \{0, 1\}$ is

$$\frac{1}{2} + \frac{1}{2}\sum_{u,v} \pi(u, v)(-1)^{f(u,v)}\langle|(\Pi_0^u - \Pi_1^v) \otimes (\Pi_0^u - \Pi_1^v)\rangle$$

[Probability of winning minus losing.]

Tsirelson's correspondence

The winning probability

$$\frac{1}{2}+\frac{1}{2}\sum_{u,v}\pi(u,v)(-1)^{f(u,v)}\langle|(\Pi_0^u-\Pi_1^v)\otimes(\Pi_0^u-\Pi_1^v)\rangle$$

It is not difficult to prove that there must necessarily exist collections of real unit vectors $\{|e_u\rangle\}_{u\in U}$ and $\{|f_v\rangle\}_{v\in V}$ such that

$$\langle e_u|f_v\rangle=\langle\psi|(\Pi_0^u-\Pi_1^u)\otimes(\Pi_0^v-\Pi_1^v)|\psi\rangle$$

Tsirelson's correspondence establishes that this is also a sufficient condition.

Tsirelson's correspondence

That is, given any two collections of real unit vectors $\{kete_u\}_{u\in U}$ and $\{|f_v\rangle\}_{v\in V}$ there must exist

1. a shared entangled state $|\psi\rangle \in \mathcal{A} \times \mathcal{B}$, and
2. a choice of binary-valued measurements: $\{\Pi_0^u, \Pi_1^v\}_{u\in U}$ for Alice, $\{\Pi_0^v, \Pi_1^v\}_{v\in V}$ for Bob, such that

$$\langle e_u|f_v\rangle = \langle\psi|(\Pi_0^u - \Pi_1^u)\otimes(\Pi_0^v - \Pi_1^v)|\psi\rangle$$

The proof is based on the Weyl-Brauer matrices:

$$\sigma_z \otimes \cdots \otimes \sigma_z \otimes \sigma_x \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$$
$$\sigma_z \otimes \cdots \otimes \sigma_z \otimes \sigma_x \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$$

Tsirelson's correspondence

That is, given any two collections of real unit vectors $\{kete_u\}_{u \in U}$ and $\{| f_v\rangle\}_{v \in V}$ there must exist

1. a shared entangled state $|\psi\rangle \in \mathcal{A} \times \mathcal{B}$, and
2. a choice of binary-valued measurements: $\{\Pi_0^u, \Pi_1^v\}_{u \in U}$ for Alice, $\{\Pi_0^v, \Pi_1^v\}_{v \in V}$ for Bob, such that

$$\langle e_u | f_v \rangle = \langle \psi | (\Pi_0^u - \Pi_1^u) \otimes (\Pi_0^v - \Pi_1^v) | \psi \rangle$$

The proof is based on the Weyl-Brauer matrices:

$$\sigma_z \otimes \cdots \otimes \sigma_z \otimes \sigma_x \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$$
$$\sigma_z \otimes \cdots \otimes \sigma_z \otimes \sigma_x \otimes \mathbb{I} \otimes \cdots \otimes \mathbb{I}$$

Now the expression of the winning probability reduces to

$$\sum_{u,v} \pi(u,v)(-1)^{f(u,v)}\langle e_u|f_v\rangle,$$

over all collections of real unit vectors $\{|\,e_u\rangle\}_{u\in U}$ and $\{|\,f_v\rangle\}_{v\in V}$.

Now define a matrix C (indexed by $U \times V$) as

$$C(u,v) = \pi(u,v)(-1)^{f(u,v)}$$

and an operator $A \in \mathrm{Herm}(\mathbb{C}^U \oplus \mathbb{C}^V)$ as

$$A = \frac{1}{2}\begin{pmatrix} 0 & C \\ C & 0 \end{pmatrix}$$

Now, for a given collection of real unit vectors, consider the matrix X, indexed by the disjoint union $U \bigcup V$, as follows:

$$X = \left(\begin{array}{c|c} \langle e_{u_0}, e_{u_1} \rangle & \langle e_{u_0}, f_{v_1} \rangle \\ \hline \langle f_{v_0}, e_{u_1} \rangle & \langle f_{v_0}, f_{u_1} \rangle \end{array} \right)$$

In words, this is the Gram matrix of the collection of vectors $\{e_u\}_{u \in U} \bigcup \{f_v\}_{v \in V}$.

It is necessarily positive semidefinite, has real entries, and diagonal entries equal to 1.

Conversely, any matrix with these properties must be obtained from a collection of real unit vectors $\{e_v\}_{v \in U} \bigcup \{f_v\}_{v \in V}$ in this way.

SDP associated to the give XOR game:

	Primal problem		Dual problem
Maximize:	$\langle A, X \rangle$	Minimize:	$\mathrm{Tr}(Y)$
subject to:	$\Delta(X) = \mathbb{I}$	subject to:	$\Delta \geq A$
	$X \in \mathrm{Psd}(\mathbb{C}^U \oplus \mathbb{C}^V)$		$Y \in \mathrm{Herm}(\mathbb{C}^U \oplus \mathbb{C}^V$

where $A = \frac{1}{2} \begin{pmatrix} 0 & C \\ C^* & 0 \end{pmatrix}$ and the mapping Δ is the completely dephasing channel, which zeroes out all off-diagonal entries and leaves diagonal entries unchanged.