Consider the following classic problem in QI:

State distinguishability (All Hilbert spaces - finitedim.)

Given a single copy of a state $\rho_i \in \mathcal{L}(\mathcal{H})$, with probability $p_i$, $i=1, \ldots, n$, what measurement gives us the maximum probability of correctly identifying the given state?

Goal: Find a POVM $(E_i)_{i=1}^n$ such that $\sum_{i=1}^n p_i \text{Tr}(E_i \rho_i)$ is maximized.

Mathematically, we may state this as an optimization problem as follows:

$$\sup \sum_{i=1}^n p_i \text{Tr}(E_i \rho_i)$$

subject to: $\sum_{i=1}^n E_i = 1$

$E_i \succeq 0$, $i=1, \ldots, n$.

The variables here are the $E_i$, all PSD matrices that sum to 1 on $\mathcal{H}$ — linear constraints & linear obj. fn.

Notation: $A \succeq B$ if $A-B$ is PSD; $A \succ B$ if $A-B$ is positive definite.
This is an instance of a semi-definite program (SDP).

In general, an SDP looks like so:

$$\inf \quad \text{Tr}(C^TX)$$
subject to \( \Phi(X) \geq B \)

\( X > 0 \) \quad (P) primal

where \( X \) is the variable over which we optimize, and \( X \in L(H) \)
\((\dim(H) = N, \text{say})\), \( C \) is a given Hermitian matrix in \( L(H) \),
\( \Phi : L(H) \to L(K) \), \((\dim(K) = M, \text{say})\) maps Hermitian matrices to
Hermitian matrices and is linear, \( B \in L(K) \) in Hermitian.

(\text{finite})

\( \Phi \) is linear, \( \dim(H) = N \), \( \dim(K) = M \).

(\text{finite})

\( \Phi \) is linear, \( \dim(H) = N \), \( \dim(K) = M \).

\( \Phi(X) \) is a matrix valued function of \( X \) and maps \( H \otimes H \) to \( \mathbb{C}^{M \times M} \).

(\text{finite})

\( \Phi \) is linear, \( \dim(H) = N \), \( \dim(K) = M \).

Note:
(i) \( \text{Tr}(AB) = \langle A, B \rangle \) is the standard inner product on \( L(H) \).
(ii) This allows for complex SD matrices, and in a form
most suitable for our applications, but is equivalent to the
"standard form" in the literature (which deals with real SDP).

HW 1.

(iii) LPs are a special case of SDPs, where all matrices are diagonal.

Example: State distinguishability, we may bring it in the form above
\[ \sum_{i=1}^{N} E_i \geq 1 \] and \[ -\sum_{i=1}^{N} E_i \geq -1 \] \( \Rightarrow \sum_{i=1}^{N} E_i = 1 \).

\( X = \begin{bmatrix} E_1 & \cdots & E_n \\ \vdots & \ddots & \vdots \\ E_n & \cdots & E_1 \end{bmatrix} \)
may assume \( \odot \), as there do not
occur in the constraints or obj fn
value; variable over \( \oplus H \)

\( \Phi(X) = \begin{bmatrix} \sum_{i=1}^{N} E_i & \odot \\ \odot & -\sum_{i=1}^{N} E_i \end{bmatrix} \)

maps \( \oplus H \to \mathbb{H} \oplus \mathbb{H} \).

\( C = \begin{bmatrix} p_s & \odot \\ \odot & p_s \end{bmatrix} \) (negative so that sup \( \leq \inf \))
(as in any SDP)

In our example, the set of feasible solutions is convex, and the objective function is linear. Further, the feasible region is closed and bounded. Therefore, the optimum exists, and is achieved. This need not always be the case.

Example 11) \( \inf -x \)

such that \( x \geq 0 \)

is clearly unbounded. (Like LPs, SDPs may be infeasible, or when feasible, the opt may be unbounded)

\[ \begin{align*}
\inf & \quad x_1 \\
\text{subject to} & \quad \begin{bmatrix}
x_1 & 0 \\
0 & x_2
\end{bmatrix} \geq \begin{bmatrix}
0 & -1 \\
-1 & 0
\end{bmatrix} \\
& \quad \begin{bmatrix}
x_1 & 0 \\
0 & x_2
\end{bmatrix} \geq 0
\end{align*} \]

has optimum \( x_1 = 0 \), however, this is not achieved. (The constraints are \( x_1 \geq 0, x_2 \geq 0 \) & \( x_1 x_2 \geq 1 \).

Unlike LPs, when the opt is finite, it is not necessarily achieved.

What does the SDP tell us about state distinguishability?

We can establish certain algebraic properties of the optimum measurement by considering the dual SDP. For the general SDP \( \Phi \) above, the dual is given by

\[ \sup \langle B, y \rangle \]

subject to \( \Phi^*(y) \leq C \) \hspace{1cm} \text{(D) dual} \hspace{1cm} y > 0 \]

where the variable \( y \in L(K) \), \( \Phi^*: L(K) \rightarrow L(K) \) is the adjoint of the linear operator \( \Phi \), and \( B \) and \( C \) are as above.
Note: This is also an SDP equivalent to one of the form given by the primal. We can convert the sup to an inf by taking the negatives, same with the direction of the inequality. Need to verify that \( F^* \) maps Hermitian matrices to Hermitian matrices (HW).

Example: State distinguishability

The dual program is given by a variable \( Y \) over \( L(H \otimes H) \):

\[
F^* : L(H \otimes H) \rightarrow L(\bigoplus^n H)
\]

By definition, \( \langle F^*(Y), X \rangle = \langle Y, F(X) \rangle \)

\[
= \text{Tr} \left[ \begin{bmatrix} Y_{12}^- \end{bmatrix}^T \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \right]
\]

\[
= \text{Tr} \begin{bmatrix} Y_{12}^- \end{bmatrix}^T \begin{bmatrix} \sum_{i=1}^n x_i & 0 \\ 0 & -\sum_{i=1}^n x_i \end{bmatrix}
\]

\[
= \text{Tr} \begin{bmatrix} Y_{12}^- \sum_{i=1}^n x_i \end{bmatrix} - \text{Tr} \begin{bmatrix} Y_{21}^- \sum_{i=1}^n x_i \end{bmatrix}
\]

\[
= \text{Tr} \left( (Y_{12}^- - Y_{21}^-) \sum_{i=1}^n x_i \right)
\]

\[
= \text{Tr} \begin{bmatrix} Y_{12}^- - Y_{21}^- \end{bmatrix} \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}
\]

So \( F^* \begin{bmatrix} Y_{12}^- \end{bmatrix} = \begin{bmatrix} Y_{12}^- - Y_{21}^- \end{bmatrix} \)
So the dual is (equivalent to):

\[
\sup_{Y} \text{Tr}(Y_i - Y_{2})
\]
subject to \( Y_i - Y_{2} \leq -\beta_i \), \( \forall \ i = 1, \ldots, n \)
- \( Y_i \geq 0, \ Y_{2} \geq 0 \)

(Can be simplified further...)

What does the dual tell us about the original problem? Under certain conditions, the optima are equal. Moreover, the optimum feasible solutions are related to each other by complementary slackness. This helps us characterize optimal measurement in some cases.

**Theorem**

1. **Weak duality**: If \( X \) & \( Y \) are feasible for \( P \) & \( D \) respectively, then \( \langle C, X \rangle \geq \langle B, Y \rangle \). (Primal & Dual optima are finite & primal opt \( \geq \) dual opt.)

   \( \text{(sketch)} \)

2. **Strong duality**: If, further, the dual has a strictly feasible solution \( Y \) (i.e. \( Y > 0 \) s.t. \( \Phi^*(Y) < C \)), then the primal opt is achieved, and equals the dual opt.

   (Since the dual of the dual is the primal, a symmetric condition in terms of a primal strictly feasible solution may be stated.)

**Note**: The strictly feasible solution is called a Slater point.

Let's see weak duality, proof of (2) in refs.

**Complementary slackness**:

(ii) If \( X, Y \) are primal and dual opt. solutions, then

\[
Y(\Phi(X) - C) = 0 = (\Phi(X) - C)^{\ast}Y
\]

\[
X(\beta - \Phi^*(Y)) = 0 = (\beta - \Phi^*(Y))^{\ast}X
\]

iff primal opt = dual opt.
Proof:

\[ (a) \text{ If } A, B \geq 0, \quad T_n(AB) = 0 \iff AB = 0 = BA. \]

(a) \quad (b) \quad (c) \quad (d)

\[ (A, B) = (B, A), \quad \text{if } A, B \text{ are Hermitian.} \]

\[ \langle c, x \rangle = \langle \Phi^*(y), x \rangle, \quad \text{since} \quad x > 0 \quad \text{and} \quad \Phi^*(y) \leq c, \]

\[ = \langle y, \Phi(x) \rangle, \quad \text{by defn of } \Phi^* \]

\[ \geq \langle \Phi(x), y \rangle, \quad \text{(by } (ii) \text{ above)} \]

\[ > \langle b, y \rangle \quad \text{since} \quad y > 0 \quad \text{and} \quad \Phi(x) \geq b. \]

\( (ii) \) follows from the proof of \((i) \) & \((a) \) above. \( \text{\( \square \)} \)

Example: State distinguishability. Primal is feasible: take \( E_i = \frac{1}{i}, \quad E_i = 0, \quad \forall i > 1. \)

Dual is feasible: take \( y_2 = 1, \quad y_i = 0. \)

Dual has a Slater point: take \( \{ y_2 = +21, \) so strong duality holds.

Complementary slackness conditions: If \((E_i)\) and \((y_1, y_2)\) are optimal feasible solutions, then:

\[ \begin{aligned}
& y_j (\sum_{i} E_i - 1) = 0 = (\sum_{i} E_i - 1) y_j, \\
& \quad j = 1, 2.
\end{aligned} \]

(Trivial, as \( \sum E_i = 1 \) for any feasible \( \Phi \))

and \[ E_i (p_i y_i - y_0) = 0 = (p_i y_i - y_0) E_i, \quad \forall i = 1, 2, \ldots, n. \]

\[ \text{equality} \quad \text{(2nd follows from Hermiticity well)} \]

\[ \text{Complementary slackness} \quad \text{(strict duality)} \]

\[ \sum_{i=1}^{n} E_i (y_i - y_0) = 0 \quad (y_i - y_0) E_i \]

\[ \text{(strict duality)} \quad \text{(strict duality)} \]

\[ \Rightarrow \quad E_i y_0 = \sum_{i=1}^{n} E_i \text{Is} \quad (E_2 y_0 = \sum_{i=1}^{n} E_2 \text{Is} \quad \text{etc}) \quad y_i E_i = p_i \text{Is} \quad E_i \]

\[ \Rightarrow \quad y_0 = \sum_{i=1}^{n} p_i \text{Is} \quad \ldots = \sum_{i=1}^{n} p_i \text{Is} \quad E_i, \quad \text{--- } (**) \]

Since \( \text{**} \) implies dual obj = primal obj, \( y_0 \) is opt & feasible.

So, \((E_i)\) are optimal iff \( y_0 = \sum_{i=1}^{n} p_i \text{Is} \quad \text{in feasible } \& \text{ feasible } \)

(i.e., \( y_0 \geq p_i \text{Is} \quad \forall i = 1, \ldots, n \))
Proposition. Let $A, B \geq 0$. Then $A B \geq 0$ iff $(AB)^\dagger = BA = AB$ $(AB$ in Hermitian$)$.

$(\Rightarrow)$ $A B \geq 0 \Rightarrow (A B)^\dagger = A B$

$(\Leftarrow)$ $A B = BA$, they are simultaneously diagonalizable.

If $A B = BA$, they are simultaneously diagonalizable.

$A = \sum_i \lambda_i a_i a^\dagger_i$, $B = \sum_i \mu_i a_i a^\dagger_i$

$A B = \sum_i \lambda_i \mu_i a_i a^\dagger_i$

(Don't need the above for the Helmer, Yuen, Kennedy, Lax conditions)

Helmer, Yuen, Kennedy, Lax conditions

Theorem. $(E_i)$ is an optimal POVM for measuring $(p_i, \psi_i)$ iff

(i) $\sum_{i=1}^n p_i E_i = \sum_{i=1}^n p_i E_i \psi_i \psi_i^\dagger$, and

(ii) $\forall j = 1, 2, \ldots, n$, $\sum_{i=1}^n p_i E_i \psi_i \psi_i^\dagger \geq p_j \psi_j \psi_j^\dagger$.

The complementary slackness & above conditions have been used to show that

(a) The Fourier basis is the optimal one for distinguishing hidden subgroup states (by '03) for abelian groups

(b) The "pretty good measurement" is optimal for Dihedral groups (Childs, van Dam '03)

(c) Have been studied further - Sarah might talk about this in her module.
Example 8

State Distinguishability

\[ n = 2 \]

\[ E_1 = \text{projection onto the one eigen-space of } p_{1} - p_{2} \]

\[ E_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \leq 0 \]

Consider

\[ p_{1}E_1 + p_{2}E_2 \]

\[ = p_{1}E_1 - p_{2}E_2 + p_{2}E_2 + p_{2}E_2 \]

\[ = (p_{1} - p_{2})E_1 + p_{2}E_2 + (E_1 + E_2) \]

\[ = E_1(p_{1} - p_{2}) + p_{2}E_2 \]

\[ = p_{1}E_1 + p_{2}E_2 \]

by similar steps in reverse.

Moreover,

\[ p_{1}E_1 + p_{2}E_2 \geq p_{1} \]

\[ \Rightarrow p_{1}(E_1 - 1) + p_{2}E_2 \geq 0 \]

\[ \Rightarrow -p_{1}E_1 + p_{2}E_2 \geq 0 \]

\[ \Rightarrow -(p_{1} - p_{2})E_2 \geq 0 \]

True!

So this is the optimal measurement.

---

Example

Strong Duality doesn't always hold.

Primal

\[ \text{inf} \begin{pmatrix} x_{1} - x_{2} \end{pmatrix} \]

subject to

\[ \begin{pmatrix} 0 & 0 & x_{1} & 0 \\ 0 & 0 & x_{2} & 0 \end{pmatrix} \]

\[ \begin{pmatrix} x_{1} - x_{2} \end{pmatrix} \geq 0 \]

Feasible region: \( x_{1} = x_{3}, x_{2} \geq 0 \).

Opt = 0

Dual

\[ \sup \begin{pmatrix} -y_{33} \end{pmatrix} \]

subject to

\[ \begin{pmatrix} y_{11} - y_{12} - y_{13} & y_{21} \end{pmatrix} \begin{pmatrix} x_{1} \end{pmatrix} \leq \begin{pmatrix} 0 \\ 0 \end{pmatrix} \]

\[ \begin{pmatrix} -y_{22} - y_{23} & y_{33} \end{pmatrix} \leq \begin{pmatrix} 0 \\ 0 \end{pmatrix} \]

\[ y_{22} \leq 0, \quad y_{23} \leq 0 \]

Opt = -1