Ph 453  Lecture 2-3

Quantum State Discrimination: Which state do I have?
Prior probability distribution: $p_i \propto \text{prob}_i$, $i = 1, \ldots, N$

Quantum State Estimation: any state possible (N = ∞)

Quantum Set Discrimination: Which subset is $p_i$ in?

Quantum Hypothesis Testing

1. $p_i \in \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ or $\mathcal{P}_4, \mathcal{P}_5, \mathcal{P}_6, \mathcal{P}_7, \mathcal{P}_8, \mathcal{P}_9$?
   [Usual: imagine only one copy of p available]

   Quantum Filtering: $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$?

   $\Rightarrow$ Same as $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ (Borgs, Herzog, Hillery does)

   Quantum State Discrimination: $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots, \mathcal{P}_9$?

"Better to guess than to keep quiet."

Minimum Error Discrimination (MED)

$\Rightarrow$ Always guess some state $p_1, \ldots, p_N$.
$\Rightarrow$ Goal is to minimize average error probability.

"Better to keep quiet than to guess."

Unambiguous State Discrimination (USD)
$\Rightarrow$ Always guess correctly (or is inclusive).
$\Rightarrow$ Goal is to minimize average inclusive probability.

N.B. MED, USD are good topics for Wiki articles!
Current Status: When is optimal measurement known?

**M E D:**

SDP

Nec. & sufficient conditions for $N$ mixed states. (Holevo, 1972)

$N=2$ solved analytically (Helstrom, 1976)

$\rho_{\text{in}} = \frac{1}{2} - D(m_1, m_2)$ [Helstrom limit]

$N > 2$ unsolved except special cases

$\rho_{\text{in}}$ even unknown for $N > 2$, but bounds are known.

**U S D:**

Nec. & suff. conditions for $N$ pure states. (Chefles, 1998)

$N$ pure states solved? (Jafarizadeh et al., Aug 2007)

N mixed states unsolved (even $N=2$!)

Nec. & suff. results for $N=2$ mixed states (Furuok, Jezek 2003)

$p_{\text{in}}$ known, but bounds known for $N > 2$

$N=2$, one pure state, one mixed state solved (Bergou, Heron, Hilley and "Quantum Filling"

What I was trying to show in last lecture

$N=2$ pure states solved analytically (Järger, Shimony 1995)

$N=2$ pure states, $m_2 = \frac{1}{2}$ solved analytically

(Ivanovic, Dicks, Peres 1987)
USD, N=2 pure states: $|\psi_1\rangle, |\psi_2\rangle$, $m_i = \frac{1}{2}$, $\langle \psi_1 | \psi_2 \rangle \neq 0$

\[
P_{\text{cond.}} = \max_{\rho \in \mathcal{C}_{N=2}} 1 - \text{Tr} \left( E_{\rho} \rho \right) ; \quad p_{\text{min}} = \min_{\rho \in \mathcal{C}_{N=2}} \text{Tr} \left( E_{\rho} \rho \right)
\]

Strategy 1: $E_1 = |\psi_1\rangle \langle \psi_1| \rightarrow \text{guess } |\psi_1\rangle$

$E_2 = |\psi_2\rangle \langle \psi_2| \rightarrow \text{in general}$

\[
p_{(1)} = 1 - \frac{1}{2} \text{Tr} \left( E_1 |\psi_1\rangle \langle \psi_1| \right) - \frac{1}{2} \text{Tr} \left( E_2 |\psi_2\rangle \langle \psi_2| \right)
\]

\[
p_{(1)} = 1 - \frac{1}{2} |\langle \psi_1 | \psi_1 \rangle|^2 - \frac{1}{2} |\langle \psi_2 | \psi_2 \rangle|^2
\]

Strategy 2: $E_1 = \frac{1 - |\langle \psi_1 | \psi_1 \rangle|}{1 + |\langle \psi_1 | \psi_1 \rangle|}, \quad E_2 = \frac{1 - |\langle \psi_2 | \psi_2 \rangle|}{1 + |\langle \psi_2 | \psi_2 \rangle|}$

$E_3 = I - E_1 - E_2$

\[
p_{(2)} = 1 - \frac{1}{2} \text{Tr} \left( E_3 |\psi_1\rangle \langle \psi_1| \right) - \frac{1}{2} \text{Tr} \left( E_3 |\psi_2\rangle \langle \psi_2| \right)
\]

\[
p_{(2)} = 1 - \frac{1}{2} \left( |\langle \psi_1 | E_3 \psi_2 \rangle|^2 - \frac{1}{2} |\langle \psi_1 | E_3 \psi_1 \rangle|^2 - \frac{1}{2} |\langle \psi_2 | E_3 \psi_2 \rangle|^2 \right)
\]

\[
p_{(2)} = 1 - \frac{1}{2} \left( |\langle \psi_1 | E_3 \psi_2 \rangle|^2 - \frac{1}{2} |\langle \psi_1 | E_3 \psi_1 \rangle|^2 - \frac{1}{2} |\langle \psi_2 | E_3 \psi_2 \rangle|^2 \right)
\]

\[
p_{(2)} \leq p_{(1)} \quad \forall \langle \psi_1 | E_2 \psi_2 \rangle
\]

"Not a proof that this measurement is optimal. "
101: Quick Review

- Unambiguous State Discrimination
  - Trace distance
    \[ D = \frac{1}{2} \| p - \sigma \|_1, \quad \| A \|_1 = \text{tr} \sqrt{A^2} \]

- Fidelity:
  \[ F = \| p^\phi \sigma^\phi \|_1 = \| \text{tr} \sqrt{p^\phi \sigma^\phi} \|_1 \]

  \[ 1 - F \leq D \leq \sqrt{1 - F^2} \]

  **Erroratum**

- QEC criteria:

  Given a "codeword" \( C \) spanned by \( k \) n-qubit states \( | \bar{i} \rangle \), \( i = 0, \ldots, k-1 \) and

  \[ E = \sum E_a \bar{s} \leq e = \sum N_a | \sum N_a \bar{s} = I \]

  and not three preserving

  \[ \sum E_a \bar{s} \]

  \[ \sum E_a \bar{s} \]

  Notation: \( C \) is an \( [n, k, \ell] \) code (for \( E \))
Important special case:

\[ \mathcal{E} \mathcal{E}_x^3 = \mathcal{E} \text{ Pauli tensor products with weight } \leq 6 \]

e.g., \( \text{pw}(-11122) = 4 \)
\( \text{pw}(1111) = 0 \)
\( \text{pw}(1111) = 0 \)
\( \text{pw}(1111) = 0 \)
\( \text{pw}(1111) = 0 \)

Def: An \( n, k, \mathcal{E} \) code for \( \mathcal{E} = \mathcal{E}_x \), 1 \( \text{pw} (\mathcal{E}_k) \leq 6 \) is called an \( \mathcal{E}_x, k, 2t+1 \) code.

\[ n = \text{length of the code} \]
\[ d = 2t+1 = \text{distance of the code} = \min \text{pw}(\text{Pauli op taking one column to differ}) \]

\[ \frac{1}{n} = \text{rate of the code} \]

\[ \frac{1}{n} = \text{rate of the code} \]

\[ \text{Good code: } \lim_{n \to \infty} \frac{k}{n} > 0, \lim_{n \to \infty} \frac{d}{n} > 0 \]

Meaning of GEC criteria:

1. \( E_a \) on \( \uparrow \uparrow \) distinguishable from \( E_b \) on \( \downarrow \downarrow \):

\[ \langle \uparrow \downarrow | E_a^+ E_b^- \uparrow \downarrow \rangle = 0 \text{ if } i \neq j \]

2. Errors don't distinguish codewords:

\[ \langle \uparrow \downarrow | E_a^+ E_b^- | \uparrow \downarrow \rangle = \langle \downarrow \uparrow | E_a^+ E_b^- | \downarrow \uparrow \rangle \]
QEC Features:

If each error \( E_a \) maps codespace \( S_o \) to an orthogonal space \( S_o' \), then \( C_{ab} = S_{ab} \) and code is non-degenerate

\[ E = \{ E_{x_1}, E_{x_2}, E_{y_3} \} \]

**Note:** I don't know how to flip an error. Fix some error occurred.

\[ C_o = \text{span}(1000, 1111) \]
\[ C_1 = \text{span}(1001, 1110) \]
\[ C_2 = \text{span}(1010, 1101) \]
\[ C_3 = \text{span}(1100, 1011) \]

Otherwise, \( C_{ab} \) does not have maximum rank (it is singular), and code is degenerate.

\[ \text{E.g. } \text{Shor code } \begin{pmatrix} 10 \end{pmatrix} = \left( \frac{1}{\sqrt{2}} \right)^3 \begin{pmatrix} 1000 & 1111 \end{pmatrix} \begin{pmatrix} 0 \end{pmatrix}^3 \]
\[ \begin{pmatrix} 1 \end{pmatrix} = \left( \frac{1}{\sqrt{2}} \right)^3 \begin{pmatrix} 1000 & 1111 \end{pmatrix} \begin{pmatrix} 0 \end{pmatrix}^3 \]

Will show later that \( E_1, E_2 \) resolvable \( \Rightarrow \) any linear combo of \( E_1, E_2 \) resolvable. So \( 2 + 2 \leq n \)

Got this far:

\[ \langle \overline{0} | (Z_1 - Z_2) + (Z_1 - Z_2) | 10 \rangle = 0 \neq 1 \]

Quantum Hamming Bound:

Let \( [n, k, 2^{t+1}] \) be a non-degenerate code,

\( \binom{n}{j} \) places where \( j \) errors can occur

Each place has 3 Pauli errors: \( X, Y, Z \)

\[ \sum_{j=0}^{t} \binom{n}{j} 3^j t_{\leq j+1} \text{ errors} \]

Each error space holds \( k \) qubits: \( \dim = 2^k \)