Wiki: proposal by Thursday

Ph 452 Lecture 23

Quantum State Discrimination: Which state do I have?
Prior probability distribution: ρ_i w/prob η_i, $i=1,\ldots,N$

can only estimate state

- **Quantum State Estimation**: any state possible ($N=\infty$)

- **Quantum Set Discrimination / Quantum Hypothesis Testing**: Which subset is ρ_i in?

e.g., ρ in $\{\rho_1\}$ or $\{\rho_2,\rho_3,\rho_4\}$ or $\{\rho_5,\rho_6\}$?
[Usu. imagine only one copy of ρ available]

- **Quantum Filtering**: $\{\rho_1\}$ or $\{\rho_2,\ldots,\rho_N\}$?

→ Same as $\{|\psi_1\rangle\}$ or $\{\rho_2\}$ (Bergou, Herzog, Hillery 2005)

redundant with, I know,

- **Quantum State Discrimination**: $\{\rho_1\}$ or ... or $\{\rho_N\}$?

"Better to guess than to keep quiet"

- **Minimum Error Discrimination** (MED)
  - → Always guess *some* state $\rho_1,\ldots,\rho_n$
  - → Goal is to minimize average *error* probability

"Better to keep quiet than be wrong."

- **Unambiguous State Discrimination** (USD)
  - Drama! wait to write.
  - → Always guess correctly (or is inconclusive)
  - → Goal is to minimize average *inconclusive* probability.

N.B. MED, USD are good topics for Wiki articles!

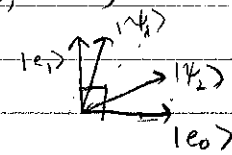
Ph 452 Lecture 23

Current Status: When is optimal measurement known?

MED:

SDP

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



May give Helstrom meas. as HW

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

$$\boxed{P_{err}^{min} = \frac{1}{2} - D(\eta_1\rho_1, \eta_2\rho_2)}$$ [Helstrom limit]

$N>2$ unsolved except special cases

- P_{err}^{min} even unknown for $N>2$, but bounds are known.

USD:

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

plagarism? →

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

Q: D, I need 2 or 2!. A: Yes.

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

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

- P_{inc}^{min} unknown, but bounds known for $N\geq 2$

$N=2$, one pure state, one mixed state solved (Bergou, Herzog, Hillery 200[illegible]) ["Quantum Filtering"]

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

What I was trying to show in last lecture →

$$\boxed{\begin{array}{l}N=2 \text{ pure states, } \eta_i = 1/2 \text{ solved analytically} \\ \text{(Ivanovic; Dieks; Peres 1987)}\end{array}}$$

Ph 452 Lecture 23

USD, $N=2$ pure states: $|\psi_1\rangle, |\psi_2\rangle$, $\eta_i = 1/2$ $\quad \langle\psi_1|\psi_2\rangle \neq 0$

NC §2.2.6

$$P^{max}_{conclusive} = \max_{\substack{POVMs \\ \{E_i\}_{i=1}^{N+1}}} 1 - \sum \eta_i \, tr(E_? \rho_i) \quad ; \quad P^{min}_I = \min_{\substack{POVMs \\ \{E_i\}}} \sum \eta_i \, tr(E_? \rho_i)$$

Strategy 1: $\quad E_1 = |\psi_1^\perp\rangle\langle\psi_1^\perp| \rightarrow$ guess $|\psi_2\rangle$

$$E_? = |\psi_1\rangle\langle\psi_1| \rightarrow \text{inconclusive}$$

$$P_c^{(1)} = 1 - \tfrac{1}{2} tr(|\psi_1\rangle\langle\psi_1|\psi_1\rangle\langle\psi_1|) - \tfrac{1}{2} tr(|\psi_1\rangle\langle\psi_1|\psi_2\rangle\langle\psi_2|)$$

$$= 1 - \tfrac{1}{2}|\underbrace{\langle\psi_1|\psi_1\rangle}_{1}|^2 - \tfrac{1}{2}|\langle\psi_1|\psi_2\rangle|^2$$

$$\boxed{P_c^{(1)} = \tfrac{1}{2} - \tfrac{1}{2}|\langle\psi_1|\psi_2\rangle|^2} \quad \begin{cases} |\psi_1\rangle = |\psi_2\rangle : & P_c = 0 \\ |\psi_1\rangle \perp |\psi_2\rangle : & P_c = 1/2 \end{cases}$$

b/c we say $|\psi_1^\perp\rangle$ is inconclusive, even though it is.

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

$$E_? = I - E_1 - E_2$$

$$P_c^{(2)} = 1 - \tfrac{1}{2} tr(E_? |\psi_1\rangle\langle\psi_1|) - \tfrac{1}{2} tr(E_? |\psi_2\rangle\langle\psi_2|)$$

$$= 1 - \tfrac{1}{2}\langle\psi_1|E_?|\psi_1\rangle - \tfrac{1}{2}\langle\psi_2|E_?|\psi_2\rangle$$

$$= \cancel{1} - \cancel{\tfrac{1}{2}} + \tfrac{1}{2}\underbrace{\langle\psi_1|E_1|\psi_1\rangle}_{0} + \tfrac{1}{2}\underbrace{\langle\psi_1|E_2|\psi_1\rangle}_{1-|\langle\psi_1|\psi_2\rangle|}$$

$$- \cancel{\tfrac{1}{2}} + \tfrac{1}{2}\underbrace{\langle\psi_2|E_1|\psi_2\rangle}_{1-|\langle\psi_1|\psi_2\rangle|} + \tfrac{1}{2}\underbrace{\langle\psi_2|E_2|\psi_2\rangle}_{0}$$

$$\boxed{P_c^{(2)} = 1 - |\langle\psi_1|\psi_2\rangle| \leq P_c^{(1)}} \quad !! \quad \begin{cases} |\psi_1\rangle = |\psi_2\rangle : & P_c = 0 \\ |\psi_1\rangle \perp |\psi_2\rangle : & P_c = 1 \end{cases}$$

"Not a proof that this measurement is optimal. Only a demonstration that POVMs could offer improvements."

Ph 452 Lecture 23

QI Quick Review

- Unambiguous State Discrimination
- Trace distance

After thinking about it some, I like this notation better b/c absolute value could be confusing!

$$D = \tfrac{1}{2}\| \rho - \sigma \|_{tr}, \quad \|A\|_{tr} = tr\sqrt{A^\dagger A}$$

- Fidelity: $F = \| \rho^{1/2} \sigma^{1/2} \|_{tr} = tr \sqrt{\rho^{1/2} \sigma \rho^{1/2}}$

Erratum

$$\boxed{1 - F \leq D \leq \sqrt{1-F}}$$

- QEC criteria:

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

and $\underbrace{\mathcal{E} = \{E_a\}}_{\text{errors}} \subseteq \underbrace{\mathcal{N} = \{N_a \mid \sum N_a^\dagger N_a = I\}}_{\text{noise channel}}$

Not "=" b/c $\sum E_k^\dagger E_k \leq I$ generally (not trace preserving)

$$(\exists_{q.op}\ \mathcal{R})(\forall \rho_{code} \text{ on } \mathcal{C})(\mathcal{R} \circ \mathcal{E}(\rho_{code}) \propto \rho_{code})$$

iff $\exists\ C = C^\dagger$ s.t.

$$\boxed{\langle \bar{i} | E_a^\dagger E_b | \bar{j} \rangle = C_{ab}\, \delta_{ij}}$$

Notation: $\mathcal{C}$ is an $[\![n,k]\!]$ code for $\mathcal{E}$.

Ph 452 Lecture 23

Important special case:

$\{E_k\} = \{$ Pauli tensor products with Pauli weight $\leq t\}$

e.g.
$pw(-iXY11ZZ) = 4$
$pw(XX1) = 2$
$pw(-ZZ1 + X1X) = $ undef.
$pw(1111) = 0$

$n=3,\ t=1:\quad \{E_k\} = \{X11, Y11, Z11,$
$1X1, 1Y1, 1Z1,$
$11X, 11Y, 11Z, 111\}$

Def: An $[\![n,k]\!]$ code for $\mathcal{E} = \{E_k \mid pw(E_k) \leq t\}$ is called an $[\![n,k,2t+1]\!]$ code.

n = length of the code
$d = 2t+1$ = distance of code $=$: min pw(Pauli op taking one codeword to a different one)
e.g. Shor code: $d=3$
$Z_1 Z_4 Z_7$

$\frac{k}{n}$ = (information) rate of the code

$\frac{t}{n}$ = (error) rate of the code

Good code: $\limsup_{n\to\infty} \frac{k}{n} > 0,\quad \lim_{n\to\infty} \frac{t}{n} > 0$

Meaning of QEC criteria:

① E_a on $|\bar{i}\rangle$ distinguishable from E_b on $|\bar{j}\rangle$:

$$\langle \bar{i} | E_a^\dagger E_b | \bar{j} \rangle = 0 \quad \text{if } i \neq j$$

② Errors don't distinguish codewords:

$$\langle \bar{i} | E_a^\dagger E_b | \bar{i} \rangle = \langle \bar{j} | E_a^\dagger E_b | \bar{j} \rangle.$$

Ph 452 Lecture 22

QEC Features:

If each error E_a maps codespace S_0 to an orthogonal space S_a, then $C_{ab} = \delta_{ab}$ and code is non-degenerate

E.g. Bit-flip code: $\mathcal{E} = \{X_1, X_2, X_3\}$

Note: "I" doesn't have to be an error if it is known that some error occurred.

$\mathcal{C}_0 = \text{span}(|000\rangle, |111\rangle)$
$\mathcal{C}_1 = \text{span}(|001\rangle, |110\rangle)$
$\mathcal{C}_2 = \text{span}(|010\rangle, |101\rangle)$
$\mathcal{C}_3 = \text{span}(|100\rangle, |011\rangle)$

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

E.g. Shor code $|\bar{0}\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|000\rangle + |111\rangle)^{\otimes 3}$
$|\bar{1}\rangle = \left(\frac{1}{\sqrt{2}}\right)^3 (|000\rangle - |111\rangle)^{\otimes 3}$

Will show later that E_i, E_j correctible $\Rightarrow$ any linear combo of E_i, E_j correctible. So $Z_1 - Z_2 \in \mathcal{E}$

$$\langle \bar{0} | (Z_1 - Z_2)^\dagger (Z_1 - Z_2) | \bar{0} \rangle = 0 \neq 1$$

Got This Far

Quantum Hamming Bound:

Let $[[n, k, 2t+1]]$ be a nondegenerate code.

$\binom{n}{j}$ places where j errors can occur
Each place has 3 Pauli errors: X, Y, Z

$\rightarrow \sum_{j=0}^{t} \binom{n}{j} 3^j$ total errors

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