Quantum states and quantum information

János A. Bergou
CUNY Hunter College

Theory

- Ulrike Herzog (Berlin)
- Mark Hillery (Hunter)
- Edgar Feldman (CUNY GC)
- Yuqing Sun
- Bing He

Experiment

- Aephraim Steinberg and Masoud Mohseni (Toronto)

HUNTER

Contemporary Physics, Islamabad,
March 29, 2007

Overview

1. A crash course on quantum information
2. Brief intro to unambiguous discrimination (UD) and minimum error (ME) discrimination between *known* states
3. Generalizations, experiment
4. Application I: the B'92 protocol
5. Discrimination of *unknown* states
6. Connection with UD of two *known mixed* states: systematic approach
7. Application II: a modified B'92 protocol
8. Summary and outlook

Quantum Information (pico intro)

Some basic ideas

QI/QC is

1. The representation

2. The processing

and

3. The readout (measurement)

of information by quantum mechanical means

1. Representation: by state of quantum system

Simplest system: Qubit

- carrier of quantum information unit
- quantum analogue of classical bit (cbit) which can be either

  0 or 1
- qubit is any 2-state quantum system
- states are labeled |0> and |1>
- { |0>, |1>} form orthonormal basis

Examples

- photon polarization
- electron spin (ESR)
- nuclear spin (NMR)
- two-level atoms

Difference between cbit and qubit

- Cbit: can be either 0 or 1 ONLY
- Qubit: can exist in superposition state

$$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$$

$|\psi\rangle$ legit qubit state with no classical analogue with

$$|\alpha|^2 + |\beta|^2 = 1$$

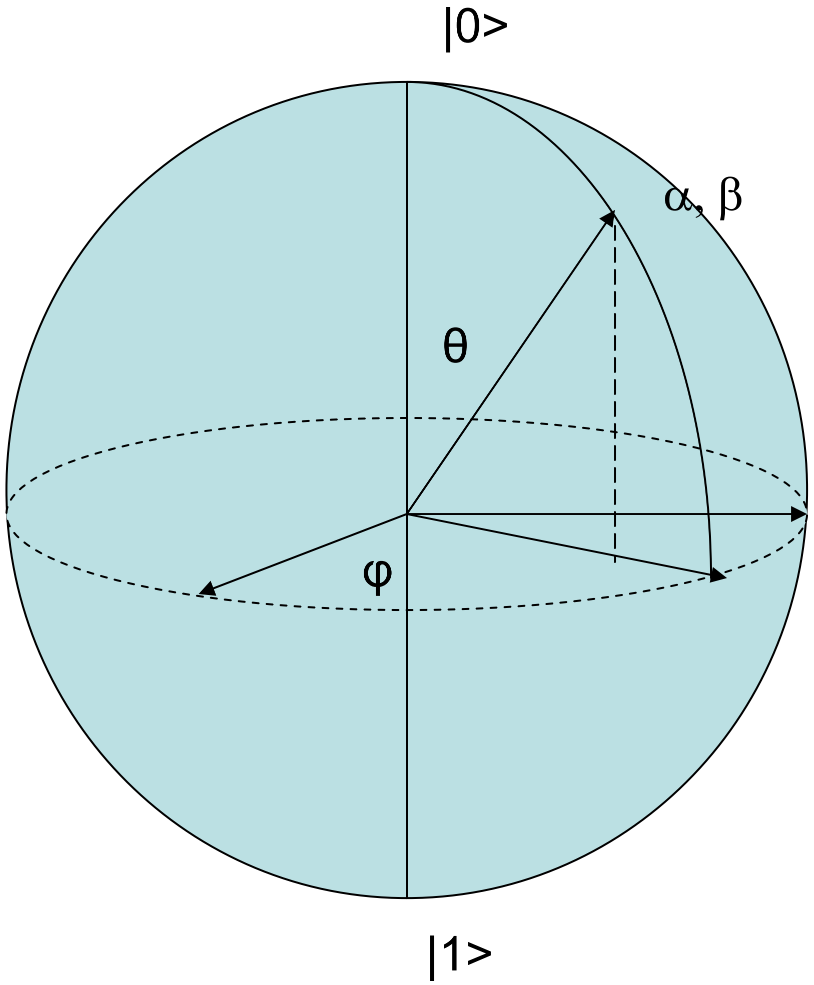
- Qbit Parametrization

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi} \sin(\theta/2)\,|1\rangle$$

- Can be represented as a point on unit sphere

BLOCH SPHERE

The Bloch sphere



General n-qubit states

|0>|0>…|0>|0> ❾ |00…00> ❾ |0>

|0>|0>…|0>|1> ❾ |00…01> ❾ |1>

|0>|0>…|1>|0> ❾ |00…10> ❾ |2>

.

.

|1>|1>…|1>|1> ❾ |11…11> ❾ |2^n-1>

- {|x>; x=0,…,2^n-1} where |x> is binary number such that $0 \leq x \leq 2^n-1$ form a basis
- $|\psi\rangle = \Sigma\, c_x\, |x\rangle$ general n-qubit state
- In general: |ψ> can not be factorized into products of single qubit states

❾ ENTANGLEMENT

Resources for QI/QC

- Nonclassical features of qubits

  ❿

  resources for quantum information and quantum computing

- Nonclassical features (resources)

  - Superposition ❾ parallel computing
  - Phase ❾ no classical analogue
  - ENTANGLEMENT ❾ nonclassical correlations

2. Processing of QI/QC

- In QM two kinds of transformations are possible:

  1. Unitary ❾ deterministic, reversible

  2. Measurements ❾ nondeterministic, nonunitary, nonreversible

- Obviously, we want **1.** for controllable processing ❾

  Quantum gates ❿ Unitary transformations (on one or more qubits)

- Consequence: quantum gates must be reversible, if we know output, we know input (NOT ALWAYS TRUE FOR CLASSICAL GATES)

3. The read-out

- Processed information ✹ final state of system
- Reading out the info ✹ determining final state
- Measurement ✹ determines actual state from among possible states

STATE DISCRIMINATION

Quantum information protocols

- We have all the ingredients
- Putting them together gives QI protocols
- This means putting

Resources ➉ entangled qubits

Quantum gates ➉ unitary transformations

Measurements ➉ nonunitary transformations

And classical communication (CC)

Together to accomplish a task gives a QI protocol

Examples of quantum protocols

- Teleportation
- Quantum cryptography
  - quantum key distribution (QKD)
  - authentication, fingerprinting
- Quantum secret sharing
- …
- Quantum computing
  - software: quantum algorithms
  - hardware: implementations

State discrimination: Important primitive in quantum information

- Carrier of information ↔ quantum system
- Information ↔ state of quantum system:
  → read-out after processing
- Problem: state is not an observable
  Solution: output from set of *known* states
- Orthogonal states: projective measurements
- Encoding into non-orthogonal states:
  state discrimination (e.g. QKD)

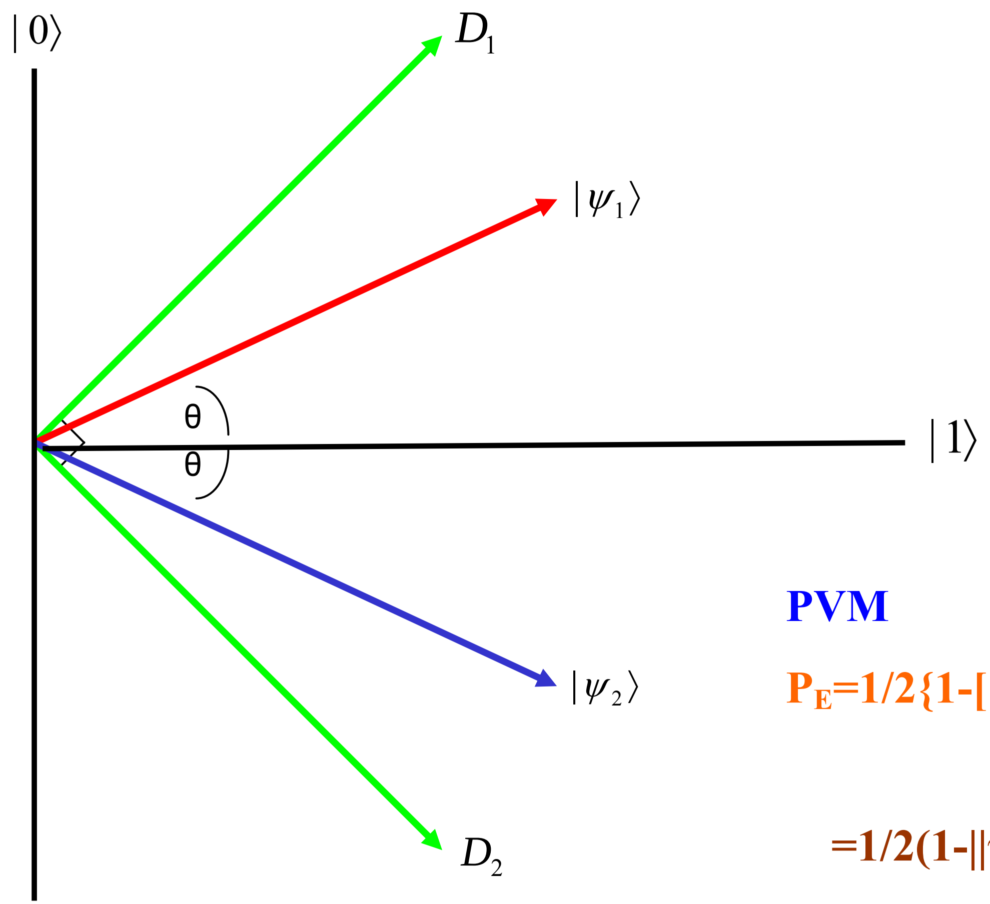
SD basics

- Set of known states $\{|\psi_1\rangle, |\psi_2\rangle, \ldots\}$
- Prior probabilities $\{\eta_1, \eta_2, \ldots\}$
- q_i=probability of failing to identify $|\psi_i\rangle$
- Find optimum measurement that minimizes average failure probability

$$Q = \eta_1 q_1 + \eta_2 q_2 \ldots$$

- Several strategies $\rightarrow$ very different optimal measurements (UD, ME, …)
- Optimal measurement often generalized measurement (POVM)

Basic strategies: Minimum error discrimination

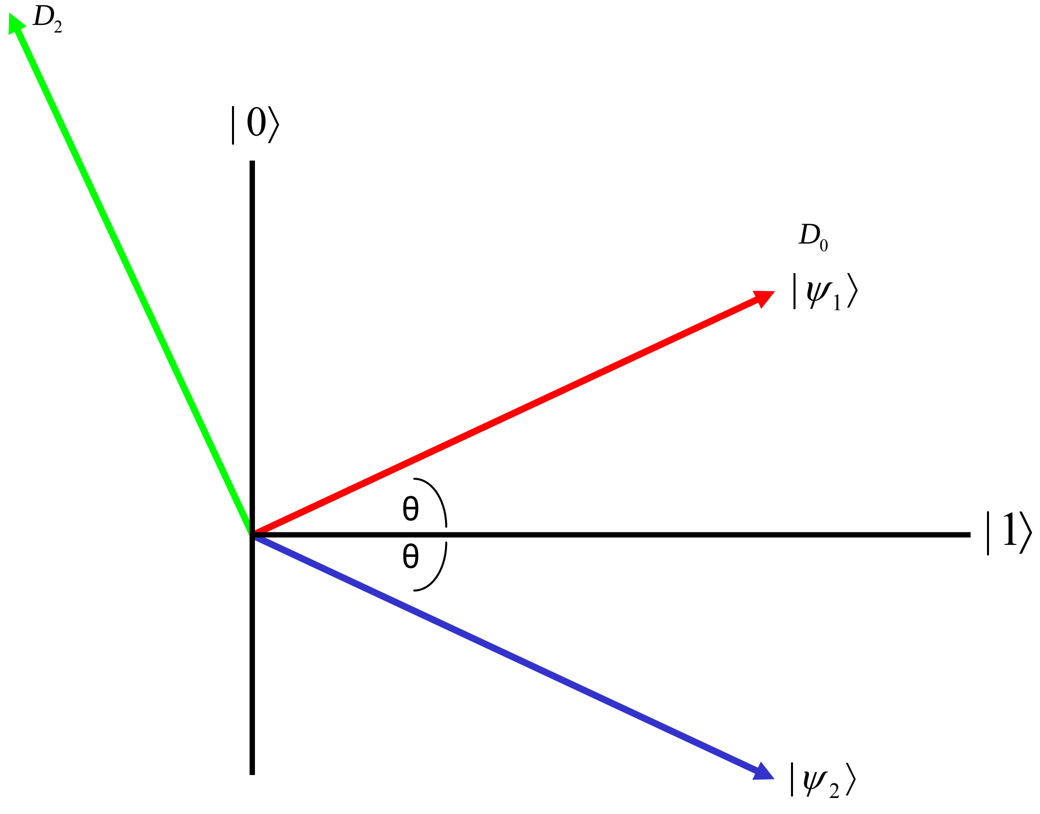


PVM

$P_E = 1/2\{1-[1-\eta_1(1-\eta_1)\cos^2\theta]^{1/2}\}$

$= 1/2(1-||\eta_1 \rho_1 - \eta_2 \rho_2||)$

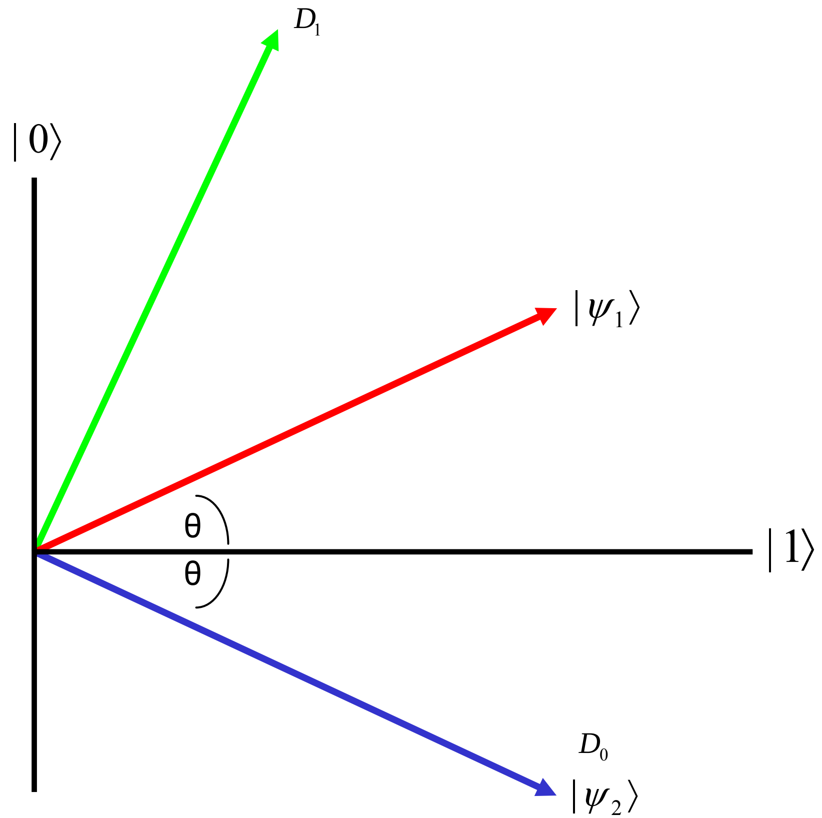
Unambiguous Discrimination 1



1^{st} von Neumann

$Q_1 = \eta_1 + (1 - \eta_1)\cos^2(2\theta)$
$= C^2 + (1 - C^2)\,\eta_1$

Unambiguous Discrimination 2



2nd von Neumann

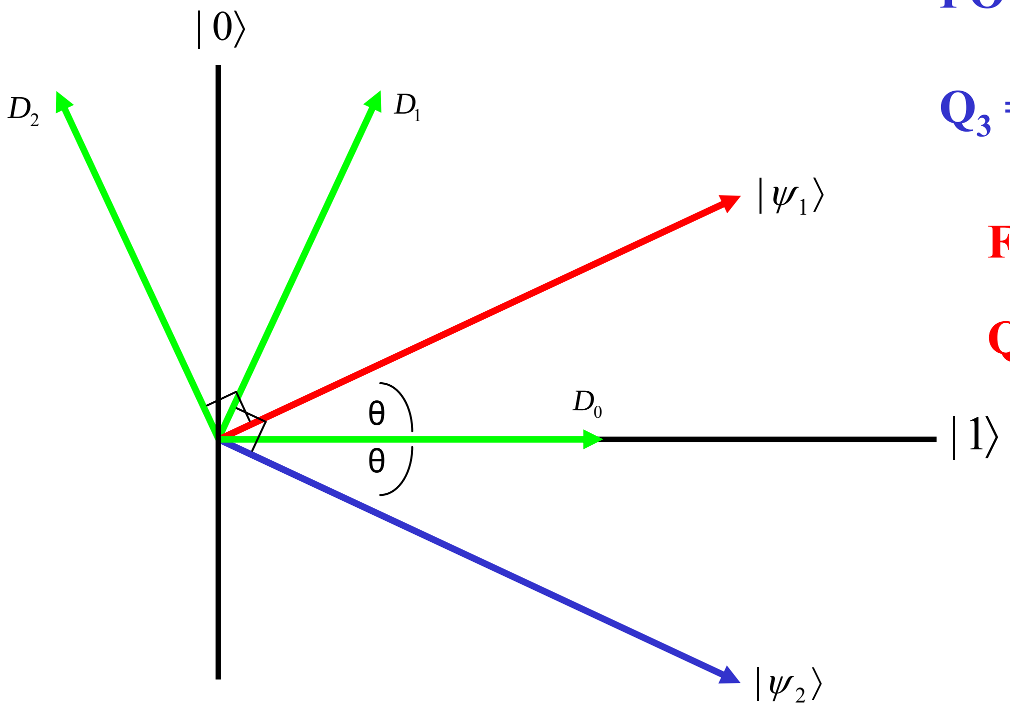
$$Q_2 = 1-\eta_1 + \eta_1 \cos^2(2\theta) = 1 - (1 - C^2)\,\eta_1$$

For $\eta_1 = 1-\eta_1 = ½$

$$Q_1 = Q_2 = ½ + ½\cos^2(2\theta)$$

B92's flip-flop detection
$Q > 50\%$

Unambiguous Discrimination 3



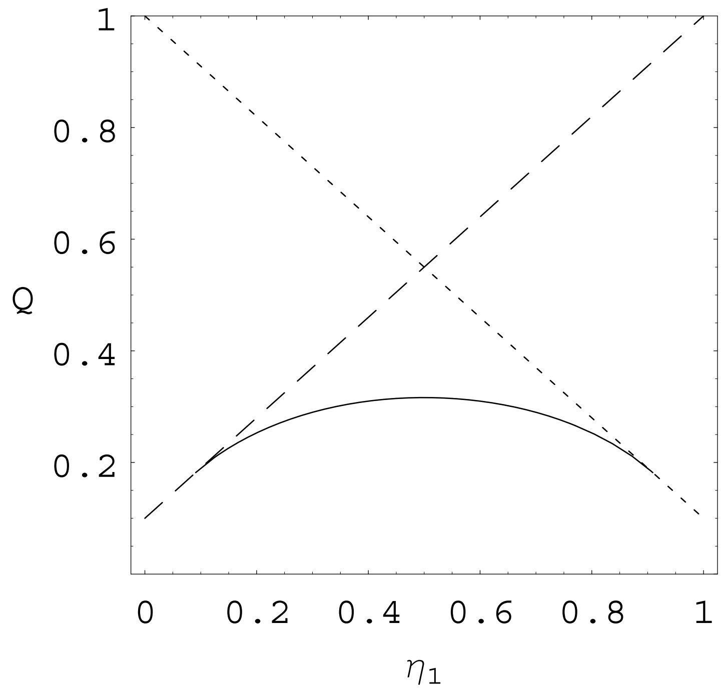
POVM

$Q_3 = 2\,[\eta_1\,(1 - \eta_1)\,\cos^2(2\theta)]^{1/2}$

For $\eta_1 = 1 - \eta_1 = ½$

$Q_3 = \cos(2\theta)$ can be <½

Comparison of UD failure probabilities



Generalizations, experiments

- Discrimination of N states: {1}, … , {N}

  PRA **64**, 022311 (2001) (N=3)
- Set discrimination: {1, …,m} {m+1,…,N}

  ME: PRA **65**, 050305(R) (2002); UD: PRA **66**, 032315 (2002) (N=3)
- Spec: Filtering, m=1: {1}, {2, … , N}

  PRL **90**, 257901 (2003)
- Linear optical implementation of a POVM

  JMO **47**, 487 (2000)
- Experiment for N = 3: Steinberg, Mohseni, JB

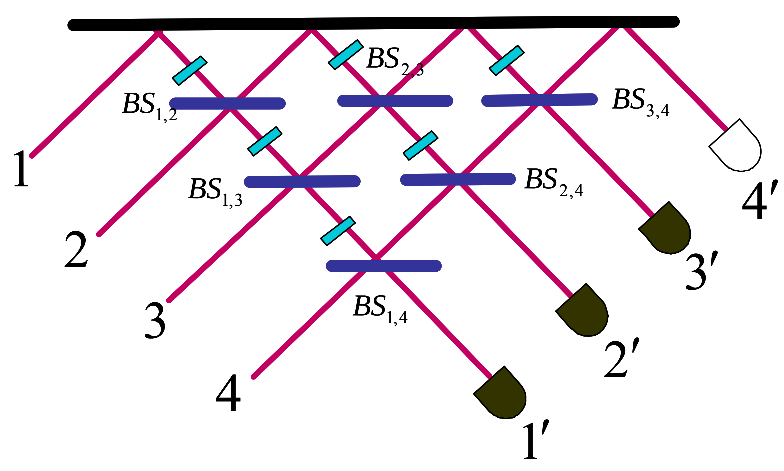
  PRL **93**, 200403 (2004)

Implementation of POVM

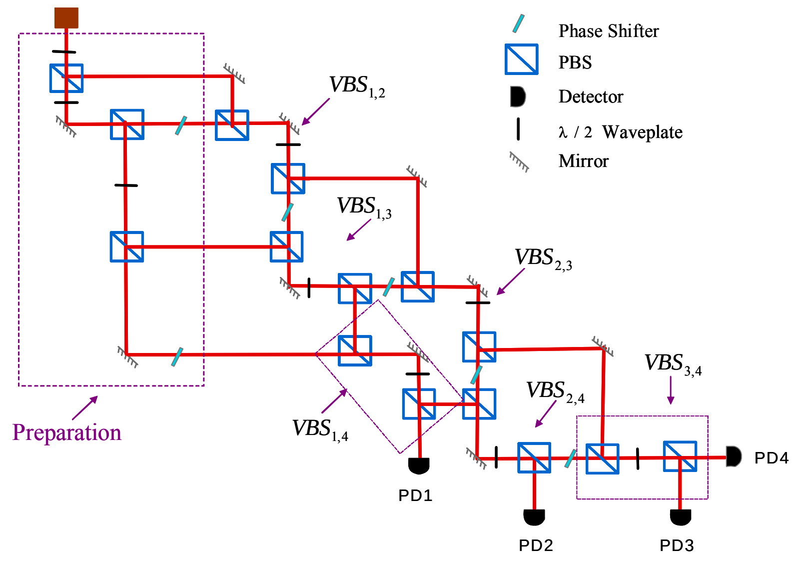
- Neumark's theorem:

- POVM = Unitary entanglement of system and ancilla
  - +
  - von Neumann measurement on larger system

Optical implementation based on Neumark's theorem



Theory



Experiment

Three non-orthogonal states

$$|\psi_1\rangle = \begin{pmatrix} \sqrt{2/3} \\ 0 \\ 1/\sqrt{3} \end{pmatrix}, \quad |\psi_2\rangle = \begin{pmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2/3} \end{pmatrix}, \quad |\psi_3\rangle = \begin{pmatrix} 0 \\ -1/\sqrt{3} \\ \sqrt{2/3} \end{pmatrix}$$

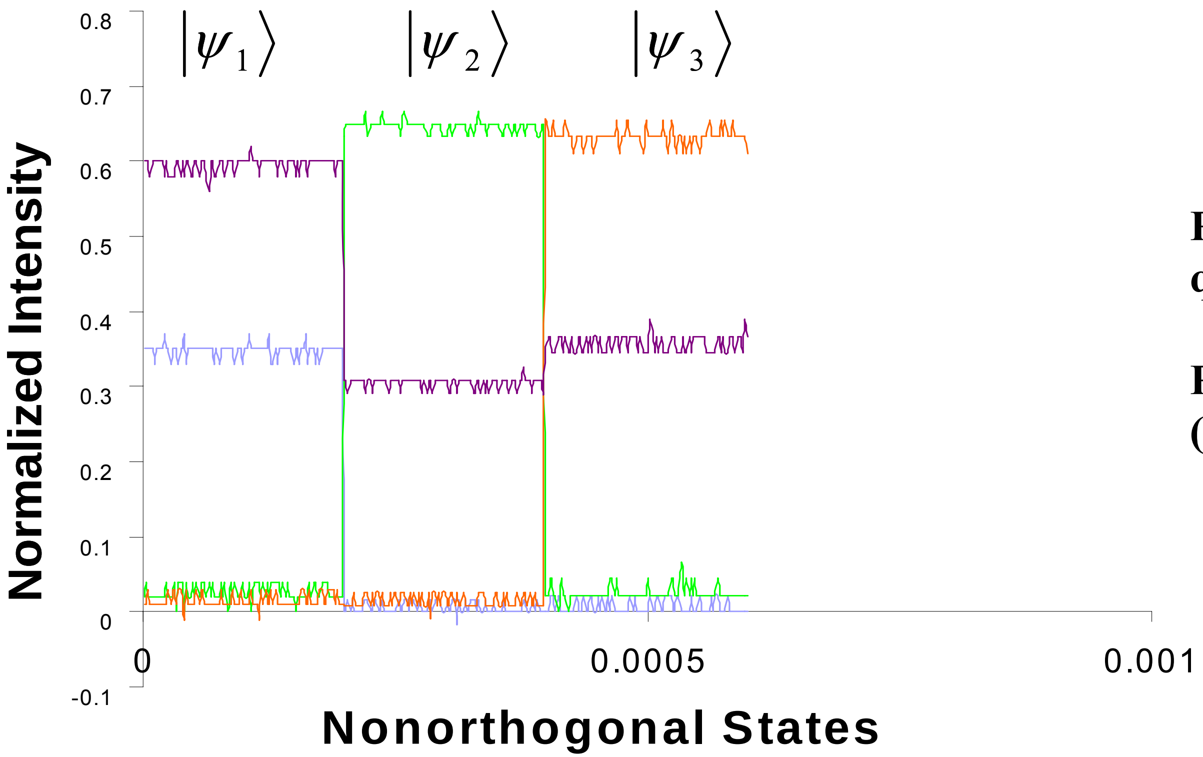
Projective measurements can distinguish these states with *certainty* less than 1/3 of the time.

(No more than one member of an orthonormal basis is orthogonal to *two* of the above states, so only one pair may be ruled out.)

But a unitary transformation in a 4-dimensional Hilbert space produces:

$$|\psi_1\rangle_{out} = \begin{pmatrix} 1/\sqrt{3} \\ 0 \\ 0 \\ \sqrt{2/3} \end{pmatrix}, \quad |\psi_2\rangle_{out} = \begin{pmatrix} 0 \\ \sqrt{2/3} \\ 0 \\ 1/\sqrt{3} \end{pmatrix}, \quad |\psi_3\rangle_{out} = \begin{pmatrix} 0 \\ 0 \\ \sqrt{2/3} \\ 1/\sqrt{3} \end{pmatrix}$$

Three State Discrimination



POVM: P=5/9
q_1=2/3 q_2=q_3=1/3

PVM: P=2/9
(q_1=1/3 q_2=q_3=1)

Application I: QKD via two non-orthogonal states (B'92)

- Alice prepares a qubit in one of two non-orthogonal states
  $|\psi_1\rangle = |0\rangle$ ✸ "0" ; $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ ✸ "1"
  and sends it to Bob

- Bob applies optimum USD to determine what state the qubit he received was in. His success rate will be

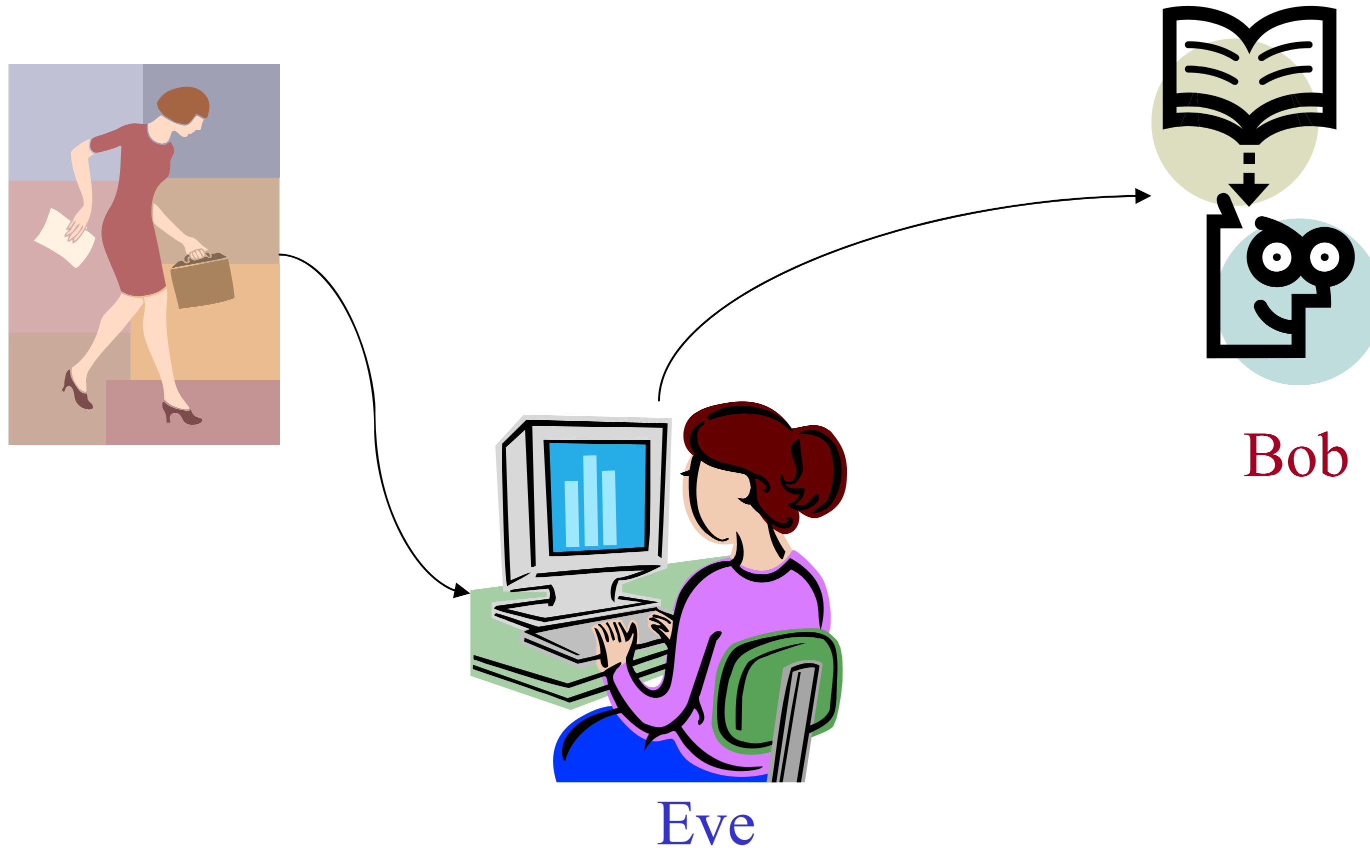
$$1 - \langle \psi_1 | \psi_2 \rangle = 1 - 1/\sqrt{2} = 0.29$$

- Bob tells Alice over a public classical channel whether succeeded or failed but not the result. They keep the bit if Bob succeeded

- A and B repeat the above steps a large number of times and keep the bits when Bob succeeds, establishing a shared key

Eavesdropping

- Alice



Eavesdropping

- An eavesdropper, Eve, in the middle can apply USD and succeeds 29% of the time. In the remaining 71% she has to guess what state to send Bob. She guesses randomly, so half the time she guesses right, half the time wrong. She will introduce an error rate

$$\frac{1}{2} \times 71\% = 35.5\%$$

- A and B modify their strategy. After establishing a shared sequence they publicly compare a part of it. If they find an error rate of 35.5% they know there is Eve and simply discard the string and start all over

- Better: Eve can apply minimum error strategy. Her error rate is then

$$[1-1/\sqrt{2}]/2 = 14.6\%$$

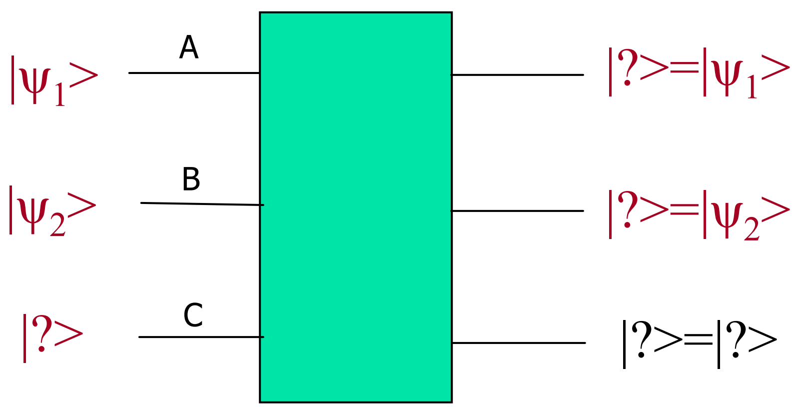
- Still, comparing part of their shared string, A and B can detect Eve

- ❾ for Bob USD is optimum strategy, for Eve ME is optimum strategy

A programmable discriminator for *unknown* quantum states [PRL **94**, 160501 (2005)]

Ad hoc approach:

unknown states are given as program



A and B program registers

C data register

How the discriminator works

- Inputs (with η_1 η_2 prior probabilities)

$$|\Psi_1\rangle = |\psi_1\rangle_A |\psi_2\rangle_B |\psi_1\rangle_C$$

or

$$|\Psi_2\rangle = |\psi_1\rangle_A |\psi_2\rangle_B |\psi_2\rangle_C$$

- All we have is symmetry properties → POVMs:

$$\Pi_1 = c_1\, I_A \otimes A_{BC} \quad \Pi_2 = c_2\, I_B \otimes A_{AC} \quad \Pi_1 + \Pi_2 + \Pi_0 = I_{ABC}$$

$$\langle\Psi_1|\, \Pi_1\, |\Psi_1\rangle = p_1 \;;\; \langle\Psi_1|\, \Pi_0\, |\Psi_1\rangle = q_1 \;;\; \langle\Psi_1|\, \Pi_2\, |\Psi_1\rangle = 0 \;;$$

$$p_1 + q_1 = 1$$

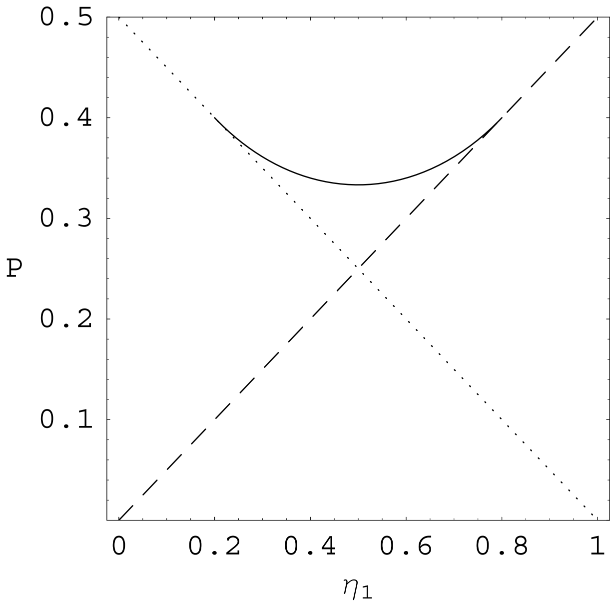
Success probabilities and measurement operators

- $P_1 = \frac{1}{2}\eta_1$
- $P_2 = \frac{1}{2} - \frac{1}{2}\eta_1$
- $c_1 = \frac{2}{3}(2 - (\eta_2/\eta_1)^{1/2})$
- $c_2 = \frac{2}{3}(2 - (\eta_1/\eta_2)^{1/2})$
- P_{POVM}

  $= \frac{2}{3}(1 - [\eta_1(1 - \eta_1)]^{1/2})$

  all P's in units of

  $(1 - |\langle\Psi_1|\Psi_2\rangle|^2)$



Averaging the results

$$P_{POVM} = \tfrac{2}{3}\,(1 - [\eta_1 (1- \eta_1)]^{1/2})$$
$$\otimes\,(1 - |\langle\Psi_1|\Psi_2\rangle|^2)$$

$$P_{AVE} = \tfrac{2}{3} \otimes \tfrac{1}{2} \otimes \tfrac{1}{2} = 1/6$$

$$P_{PVM} = \tfrac{1}{4} \quad \eta_{min} = \tfrac{1}{8}$$

A quantum circuit for the programmable SD

[JB, M. Orszag, JOSA B **24**, 384 (2007)]

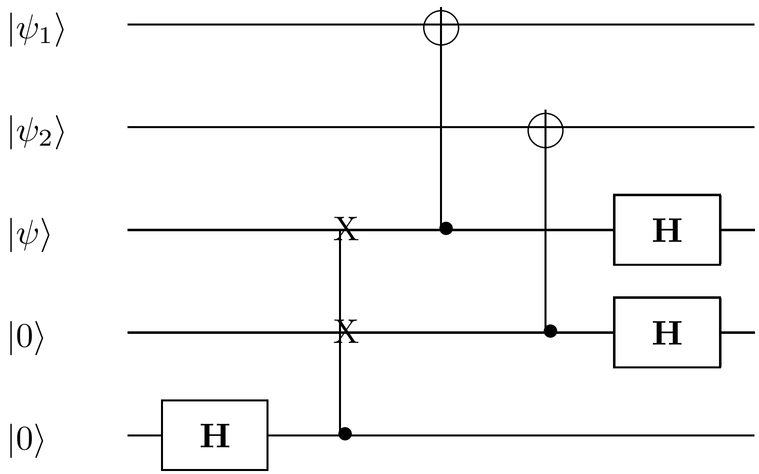


Figure 1: A simplified quantum circuit for the full implementation of the programmable state discriminator. If, at the output, the reading in the program qubit 1, data qubit 3 and control bit 5 is $|010\rangle_{135}$, the data state is $|\psi_2\rangle$. If, at the output, the reading in the program qubit 2, data qubit 4 and control bit 5 is $|011\rangle_{245}$, the data state is $|\psi_1\rangle$. The average probability of either alternative is 1/8.

Programmable discrimination as discrimination of mixed states

- Inputs for programmable discriminators:

  $|\Psi_1> = |\psi_1>_A|\psi_1>_B|\psi_2>_C$ ✹ $\rho_1 = \{|\Psi_1><\Psi_1|\}_{av}$ ✹ $\frac{1}{3} S_{AB} \otimes \frac{1}{2} I_C$

  $|\Psi_2> = |\psi_1>_A|\psi_2>_B|\psi_2>_C$ ✹ $\rho_2 = \{|\Psi_2><\Psi_2|\}_{av}$ ✹ $\frac{1}{2} I_A \otimes \frac{1}{3} S_{BC}$

- ρ_1 and ρ_2 with η_1 and η_2 priors
- S_{ij}: projector to symmetric subspace of i,j; I_i: identity for qubit I
- **Unknown pure states ↔ known mixed states**

Does it help?

- Can two mixed states be discriminated unambiguously?
- Yes. But how?

A little technicality

- Support: subspace spanned by nonzero eigenvectors
- Kernel: subspace orthogonal to support
- Measurement in kernel of one identifies the other unambiguously

Lower bound on the failure probability

- Geometric mean > arithmetic mean

$$Q = \eta_1 q_1 + \eta_2 q_2 \geq 2[\eta_1\eta_2 Tr(\rho_1\Pi_0)Tr(\rho_2\Pi_0)\ ]^{1/2}$$

- Using CS inequality

$$Tr(A^\dagger A)Tr(B^\dagger B) \geq |Tr(A^\dagger B)|^2$$

- in Q gives

$$Q \geq 2[\eta_1\eta_2]^{1/2}\ Tr|\rho_1{}^{1/2}\Pi_0\rho_2{}^{1/2}|$$
$$= 2[\eta_1\eta_2]^{1/2}\ Tr|\rho_1{}^{1/2}(1-\Pi_1-\Pi_2)\ \rho_2{}^{1/2}|$$
$$= 2[\eta_1\eta_2]^{1/2}\ Tr|\rho_1{}^{1/2}\rho_2{}^{1/2}|$$

Lower bound

- $Q_{POVM} \geq 2[\eta_1\eta_2]^{1/2}F(\rho_1, \rho_2)$ (*)

  $F(\rho_1, \rho_2)=\mathrm{Tr}|\rho_1^{1/2}\, \rho_2^{1/2}|$ fidelity

- (*) established as lower bound
  Rudolph et al., PRA **68**, 010301(R) (2003)

- (*) saturated for rank 1 vs. rank N and in most rank 2 vs. rank N cases

- Conjecture: (*) range of validity decreases rapidly with increasing rank
  PRA **71**(RC), 050301 (2005)

An inequality for ME and UD

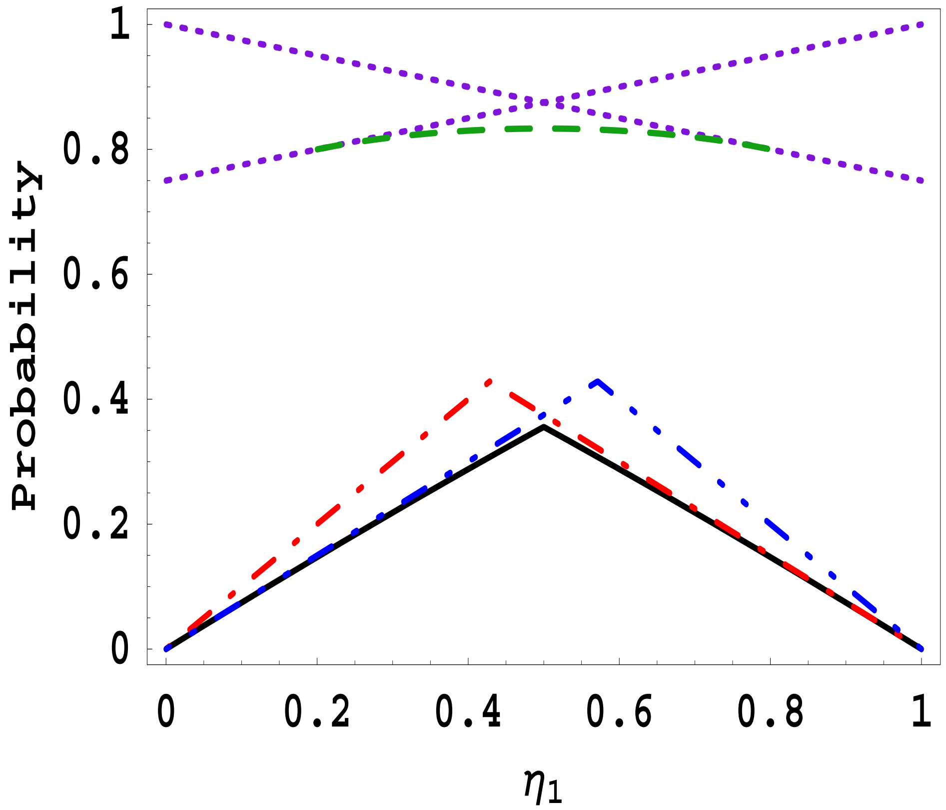
[PRA **70**, 022302 (2004)]

- $P_E = ½(1 - \| \eta_1\rho_1 - \eta_2\rho_2 \|)$ for ME
- $Q_{POVM} \geq 2[\eta_1\eta_2]^{1/2} F(\rho_1, \rho_2)$ for UD

$$P_E \leq ½\, Q_{POVM}$$

Comparison of UD and ME programmable discriminators

Q_f and P_E vs. η_1



Application II: QKD via unknown states

- A modified B'92 protocol: communicating via patterns
- Pattern 1: third qubit matches first

$$|\Psi_1> = |\psi_1>_A|\psi_2>_B|\psi_1>_C$$ ❾ "0"

- Pattern 2: third qubit matches second

$$|\Psi_1> = |\psi_1>_A|\psi_2>_B|\psi_1>_C$$ ❾ "1"

- Advantage:

  no need for shared reference frame

  robust against unitary errors

  Eve's options are severely limited

Comparison of B'92 to QKD via patterns

	B'92	QKD via Patterns
P_{Bob} (UD)	0.29 (0.25)	1/6 (1/8)
P_{Eve} (UD)	0.29 (0.25)	1/6 (1/8)
P_{error} by Eve UD	0.35 (0.38)	0.42 (0.44)
P_{Eve} (ME)	0.85	0.65
P_{error} by Eve ME	0.15	0.35

Summary

- Effect of POVM demonstrated (filtering and full UD)
- UD of mixed states
- Unknown pure states ✹ known mixed states
- Programmable quantum state discriminators (UD and ME)
- Applications:
  - probabilistic algorithms
  - QKD via patterns
  - Operator discrimination (entanglement does not always help)
  - entanglement concentration, purification, distillation, ...
- Review

  LNP **649**: Quantum States Estimation, 417-465 (Springer, 2004)

Quantum computing

- Quantum algorithm
  - preparation of input state (initialization)
  - processing: perform unitaries (gates)
  - to yield desired output(s)
  - measure to obtain final answer
- Execution of quantum algorithm by actual implementation (Quantum Computer)
- Problem: only a handful of quantum algorithms

Application: A probabilistic quantum algorithm for the discrimination between sets of Boolean functions

[PRL **90**, 257901 (2003); PRA **72**, 012302 (2005)]

- f(x) Boolean if f(x) =0 or 1 for {x|0,1,…,2^{n-1}}

- Balanced: 0 on half of {x}, 1 on other half
  Biased: otherwise (0 on m_0, 1 on $m_1=N-m_0$ with $N=2^{n-1}$ and $m_1 < m_0$)

- For classical discrimination: $N/2+m_1+1$ realizations are necessary (generalization of Deutsch-Jozsa algorithm)

Application

- f-CNOT (or Deutsch) mapping:

  $|x>|y> \rightarrow |x>|y+f(x)>$

  takes $|x>(|0>-|1>) \rightarrow (-1)^{f(x)}|x>(|0>-|1>)$

- $\Sigma_{\{x=0 \text{ to } N\}}|x> \rightarrow \Sigma_{\{x=0 \text{ to } N\}}(-1)^{f(x)}|x> \rightarrow \{|v_f>\}$

- $\{|v_f>\}$ for balanced f(x) is not orthogonal to $\{|v_f>\}$ for biased f(x)

- Filtering discriminates in single step

A little aside: UD of two mixed states

- Two mixed states of arbitrary rank:

ρ_1 and ρ_2 with η_1 and η_2 priors

- POVM for UD:

$$\Pi_1 + \Pi_2 + \Pi_0 = I$$

- UD condition:

$$\Pi_1 \rho_2 = \Pi_2 \rho_1 = 0$$

UD of two mixed states

- Probability of successfully detecting the individual states

$$p_1 = Tr(\Pi_1 \rho_1) \quad p_2 = Tr(\Pi_2 \rho_2)$$

- Probability of failing to detect the individual states (NOT error!)

$$q_1 = Tr(\Pi_0 \rho_1) \quad q_2 = Tr(\Pi_0 \rho_2)$$

- Want to minimize average failure probability

$$Q = \eta_1 q_1 + \eta_2 q_2$$

Equalities not just bounds: subspace discrimination

- If two mixed states are of the spectral form

  $\rho_1 = \Sigma_i r_i|r_i\rangle\langle r_i|$ and $\rho_2 = \Sigma_i s_i|s_i\rangle\langle s_i|$ with $\langle r_i|s_j\rangle=\delta_{ij} \cos \theta_i$

- spectral representation coincides with Jordan basis

- Spec.: subspace discrimination $r_i=1/d_1$ $s_i=1/d_2$ [PRA **73**, 032107 (2006)]
- In Jordan basis: discrimination of 2N Rank 1 subspaces ❾ N separate pure state discriminations
- Optimal failure probability:

  $$Q = \Sigma_i Q_i$$

  where Q_i is the failure probability for subspace i

Pick up where we left off: discrimination of unknown states [PRA **73**, 062334 (2006)]

- Inputs for programmable discriminators in Jordan form

$|\Psi_1\rangle = |\psi_1\rangle_A|\psi_1\rangle_B|\psi_2\rangle_C$ ✹ $\rho_1 = \frac{1}{3} S_{AB} \otimes \frac{1}{2} I_C = 1/6\, [S_{ABC} + |g_1\rangle\langle g_1| + |g_2\rangle\langle g_2|]$

$|\Psi_2\rangle = |\psi_1\rangle_A|\psi_2\rangle_B|\psi_2\rangle_C$ ✹ $\rho_2 = \frac{1}{2} I_A \otimes \frac{1}{3} S_{BC} = 1/6\, [S_{ABC} + |h_1\rangle\langle h_1| + |h_2\rangle\langle h_2|]$

- Two mixed states of rank 6 each:

ρ_1 and ρ_2 with η_1 and η_2 priors

- S_{ABC}: projector to fully symmetric subspace of 3 qubits A,B,C (4 dim)

- $\langle g_i|g_j\rangle = \langle h_i|h_j\rangle = \delta_{ij}$ $\qquad \langle g_i|h_j\rangle = -\frac{1}{2}\delta_{ij}$

Bonus: Minimum error discrimination

- Helstrom bound

$$P_E = \tfrac{1}{2}\,(1 - \| \eta_2 \rho_2 - \eta_1 \rho_1 \|)$$

- For programmable discriminators

$$P_E = \eta_{\min}\left(1 - \frac{1}{2}\frac{\eta_{\max}}{\eta_{\max} - \eta_{\min} + \sqrt{1 - \eta_{\max}\eta_{\min}}}\right)$$

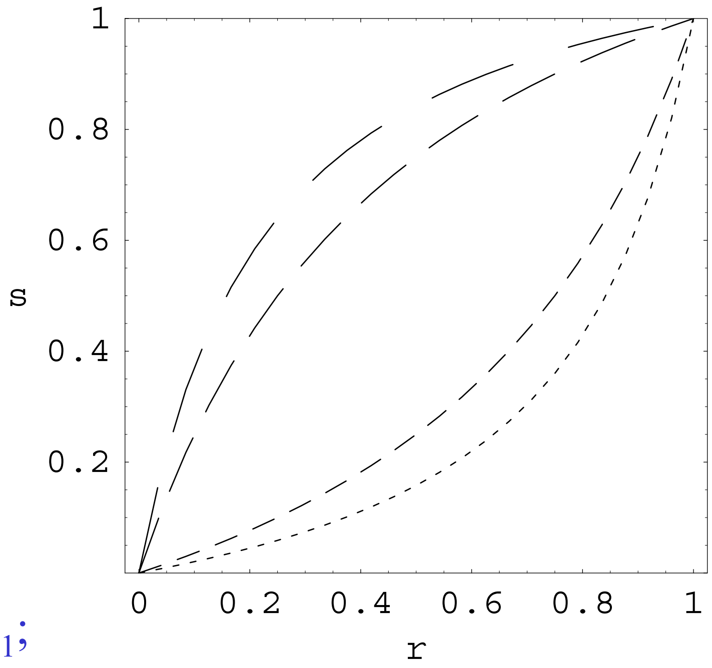
Boundaries in the parameter space

Dotted line: $s_1(r)$
Short dashed line: $s_2(r)$
Medium dashed line: $s_3(r)$
Long dashed line: $s_4(r)$

Below $s_1(r)$ and above $s_4(r)$
fidelity bound can not be reached;

Between $s_1(r)$ and $s_2(r)$,
and between $s_3(r)$ and $s_4(r)$
fidelity bound can be reached for some η_1;

Between $s_2(r)$ and $s_3(r)$ fidelity bound
can always be reached.



A simple example where (*) cannot always be saturated

- $\rho_1 = \Sigma_{\{i=1,2\}} r_i|r_i\rangle\langle r_i|$
  $r_1=r \quad r_2=1-r$
- $\rho_2 = \Sigma_{\{i=1,2\}} s_i|s_i\rangle\langle s_i|$
  $s_1=s \quad s_2=1-s$
- $\langle r_i|s_j\rangle=\delta_{ij}/2^{1/2}$
- $0 \le r, s \le 1$
- in shaded area of r,s plane fidelity bound can be reached for some values of η_1 and η_2, but not outside