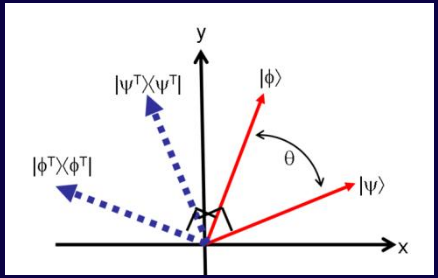
Quantum state discrimination with the "Pretty good Measurement"

Proudly presented by
Jonathan Lavoie

Theory of Quantum Communication

27 July 2010



Problem statement : discrimination of quantum states

$$|\mu_k\rangle = \Lambda^{-1/2}\,|s_k\rangle$$

The PGM as a decoding observable

$$P_E \leq 2/N \sum_i \left((1 - n_i) + \tfrac{1}{2} \sum_{j \neq i} \langle \psi_i | \psi_j \rangle^2 \right)$$

Derivation of an upper bound to the probability of error

Discrimination of quantum state

Fundamental to the theory of quantum communication

<u>The question is</u>:
How can we best discriminate between a known set of states $|\psi_i\rangle$, each having been prepared with a known probability p_i ?

A general measurement (POVM) is generally the best approach

However, the "optimality of a measurement" is relative to the problem

Unambiguous state discrimination

Allow our measurement to have inconclusive results

If not inconclusive, it is always correct!

Minimum-error discrimination

Exists a necessary and sufficient condition

Optimization of Mutual information

Has only a necessary condition

In general, one does not apply the other!

(i.g. Tetrahedron states of Assignment 2)

The pretty good measurement has desirable properties

It has a second name!: "The square-root measurement"

- **Its construction is simple ⇒ just need to know the ensemble of signal states**

- **Minimizes the probability of detection error for symmetric states of the form $|\psi_i\rangle = U|\psi_{i-1}\rangle = U^i|\psi_0\rangle$, i = 0, ..., N-1, and U^N = Identity**
(M. Ban *et al*, International Journal of Theoretical Physics, Vol. 36, No. 6, 1997)

- **It is "pretty good" to distinguish almost orthogonal states, and equally likely (Hausladen & Wootters, Journal of modern optics, 1994, Vol. 41, No. 12, 2385-2390)**

- **It is asymptotically optimal (hopefully what I can proof today...)**

- **Optimal for the Hidden Subgroup Problem (arxiv: quant-ph/0501044)**

PHYSICAL REVIEW A VOLUME 54, NUMBER 3 SEPTEMBER 1996

Classical information capacity of a quantum channel

Paul Hausladen,[1] Richard Jozsa,[2] Benjamin Schumacher,[3] Michael Westmoreland,[4] and William K. Wootters[5]

[1]*Department of Physics, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6396*
[2]*School of Mathematics and Statistics, University of Plymouth, Plymouth, Devon PL4 8AA, England*
[3]*Department of Physics and Astronomy, Kenyon College, Gambier, Ohio 43022*
[4]*Department of Mathematics, Denison University, Granville, Ohio 43023*
[5]*Department of Physics, Williams College, Williamstown, Massachusetts 01267*

(Received 26 June 1995; revised manuscript received 14 May 1996)

We consider the transmission of classical information over a quantum channel. The channel is defined by an ''alphabet'' of quantum states, e.g., certain photon polarizations, together with a specified set of probabilities with which these states must be sent. If the receiver is restricted to making separate measurements on the received ''letter'' states, then the Kholevo theorem implies that the amount of information transmitted per letter cannot be greater than the von Neumann entropy H of the letter ensemble. In fact the actual amount of transmitted information will usually be significantly less than H. We show, however, that if the sender uses a block coding scheme consisting of a choice of code words that respects the *a priori* probabilities of the letter states, and the receiver distinguishes whole words rather than individual letters, then the information transmitted per letter can be made arbitrarily close to H and never exceeds H. This provides a precise information-theoretic interpretation of von Neumann entropy in quantum mechanics. We apply this result to ''superdense'' coding, and we consider its extension to noisy channels. [S1050-2947(96)12209-5]

<u>The problem</u>: (Alice) Ensemble of *N* code words { $|s_i\rangle$ }, each used with equal frequency and *N* consist of *l* letters, s.t. $|s_i\rangle = |a_1\, a_2\, a_3 \ldots a_l\rangle$

Bob constructs a general measurement (POVM) to deduce the message with the *minimum probability of error*

Bob constructs a general measurement to distinguish the states (PGM)

Signal states

Measurement vectors given by:

$$|\mu_k\rangle = \Lambda^{-1/2} |s_k\rangle$$

with corresponding positive operator

$$|\mu_k\rangle\langle\mu_k|$$

and where

$$\Lambda = \sum_k |s_k\rangle\langle s_k|$$

Legitimate POVM since

$$\sum |\mu_k\rangle\langle\mu_k| = \Lambda^{-1/2} \sum |s_k\rangle\langle s_k| \Lambda^{-1/2} = \Lambda^{-1/2}\Lambda \Lambda^{-1/2} = 1$$

<u>Other properties of the measurement vectors</u>:

Construct the Gram matrix $S_{jk} = \langle s_j||s_k\rangle$ (Hermitian *N*x*N* matrix, with positive eigenvalues)

Then $|\mu_k\rangle$ vectors are related to the square-root of that matrix

$$(\sqrt{S})_{jk} = \langle\mu_j||s_k\rangle$$

Given the ensemble of input signals, we derive the average probability of error, using the PGM

Alice sends signal $|s_i\rangle$ with probability $1/N$

Probability that Bob has correct outcome is given by

$$P(\mu_i \mid s_i) = \mathrm{tr}\,(\,|\mu_i\rangle\langle\mu_i||s_i\rangle\langle s_i|\,) = |\langle\mu_i||s_i\rangle|^2$$

The *average* probability of error is therefore

$$P_E = 1 - 1/N \sum_i |\langle\mu_i||s_i\rangle|^2$$

➡ **find upper bound**

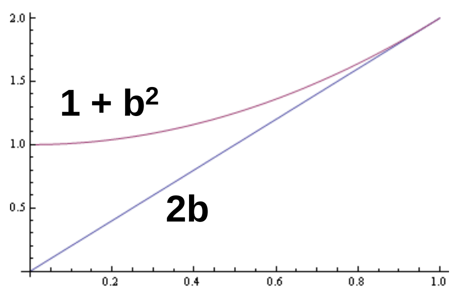
$$= 1/N \sum_i (1 - \langle\mu_i||s_i\rangle)\,(1 + \langle\mu_i||s_i\rangle)$$

$$\leq 2/N \sum (1 - \langle\mu_i||s_i\rangle)$$

My interpretation...

$(1\text{-}b)\,(1\text{+}b) = 1 - b^2 \leq 2 - 2b$

$\Rightarrow \quad 2b \leq 1 + b^2$



$$P_E \leq 2/N \sum (1 - (\sqrt{S})_{ii}\,)$$

In term of the Gram matrix

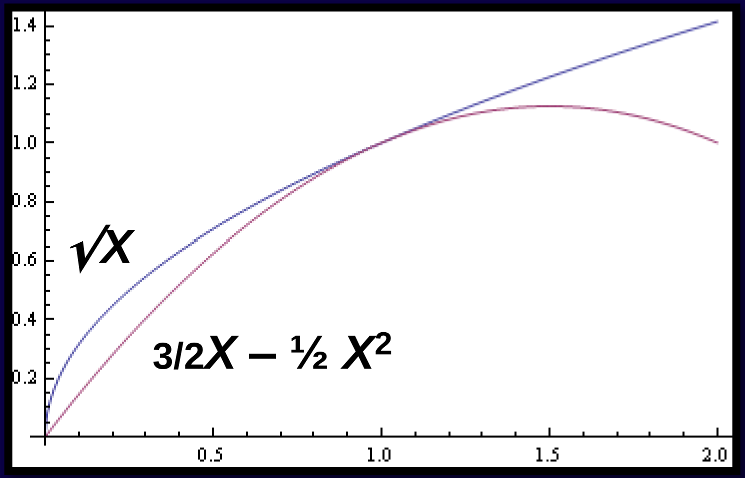
$$(\sqrt{S})_{jk} = \langle\mu_j||s_k\rangle$$

We can simplify a bit more ...

The square root function is bounded bellow by a parabola

$P_E \leq 2/N \sum(1 - (\sqrt{S})_{ii})$

Gram $S_{jk} = \langle s_j | s_k \rangle$



$\sqrt{X} \geq 3/2X - ½ X^2$

This inequality can be applied to the Gram matrix S !

$\sqrt{S} \geq 3/2S - ½ S^2$

WHY?

The matrix S is Hermitian with non-negative eigenvalues, therefore diagonalizable

$S = UDU^\dagger$

The inequality holds if $½ S^2 + \sqrt{S} - 3/2S \geq 0$

i.e. $½ UD^2U^\dagger + U\sqrt{D}U^\dagger - 3/2UDU^\dagger \geq 0$

$U [½ D^2 + \sqrt{D} - 3/2D] U^\dagger \geq 0$

$$\begin{pmatrix} ½ d_1^2 + \sqrt{d_1} - 3/2d_1 & 0 & \cdots \\ 0 & \ddots & \\ \vdots & & \end{pmatrix}$$

All eigenvalues positive!

Almost there ...

$P_E \leq 2/N \sum(1 - (\sqrt{S})_{ii})$

Gram $S_{jk} = \langle s_j | | s_k \rangle$

$\sqrt{S} \geq 3/2 S - ½ S^2$

$M \geq 0$

$\langle \psi | M | \psi \rangle \geq 0 \quad \forall \psi$

$M \geq N + P$

$M - N - P \geq 0$

$\langle \psi | M - N - P | \psi \rangle \geq 0 \quad \forall \psi$

$\langle \psi | M | \psi \rangle - \langle \psi | N | \psi \rangle - \langle \psi | P | \psi \rangle \geq 0$

$\langle \psi | M | \psi \rangle \geq \langle \psi | N | \psi \rangle + \langle \psi | P | \psi \rangle$

Therefore $\sqrt{S} \geq 3/2 S - ½ S^2$ means that, for a complex vector $|N\rangle$, with components z_k

$$\langle N | \sqrt{S} | N \rangle \geq 3/2 \langle N | S | N \rangle - ½ \langle N | S^2 | N \rangle$$

Which is the same as

$$\sum_{k,l} z_k^* (\sqrt{S})_{kl} z_l \geq 3/2 \sum_{k,l} z_k^* S_{kl} z_l - ½ \sum_{k,l,j} z_k^* S_{kj} S_{jl} z_l$$

Very general, but for given i, we can choose $z_i = 1$ and $z_k = 0$ for $k \neq i$.

This yields

$$(\sqrt{S})_{ii} \geq 3/2 S_{ii} - ½ \sum_j S_{ij} S_{ji}$$

and using $S_{ii} = n_i$

$$= 3/2 n_i - ½ n_i^2 - ½ \sum_{j \neq i} S_{ij} S_{ji}$$

Finally ... The upper bound on decoding errors

Given that

$$P_E \le 2/N \sum (1 - (\sqrt{S})_{ii})$$

and

$$(\sqrt{S})_{ii} \ge 3/2\, n_i - \tfrac{1}{2} n_i^2 - \tfrac{1}{2} \sum_{j \ne i} S_{ij} S_{ji}$$

then

$$P_E \le 2/N \sum_i (1 - 3/2\, n_i + \tfrac{1}{2} n_i^2 + \tfrac{1}{2} \sum_{j \ne i} S_{ij} S_{ji})$$

$$= 2/N \sum_i ((1 - n_i)(1 - n_i/2) + \tfrac{1}{2} \sum_{j \ne i} S_{ij} S_{ji})$$

$$P_E \le 2/N \sum_i ((1 - n_i) + \tfrac{1}{2} \sum_{j \ne i} S_{ij} S_{ji})$$

$$\boxed{P_E \le 2/N \sum_i ((1 - n_i) + \tfrac{1}{2} \sum_{j \ne i} |\langle s_i | s_j \rangle|^2)}$$

with $S_{ii} = n_i$
$|s_i\rangle$ = signal states