OPTIMAL DISCRIMINATION OF QUANTUM OPERATIONS

Massimiliano Federico Sacchi CNR-INFM and CNISM, Unità di Pavia University of Pavia, ITALY <u>www.qubit.it</u>





International School and Conference on Quantum Information 2008

4th - 12th March 2008, Bhubaneswar (India)

OUTLINE

0.

2.

review of optimal discrimination protocol for two quantum states

minimum-error discrimination of two

unitary transformations:

entanglement is <u>useless</u>!

minimum-error discrimination of two quantum operations:

entanglement can <u>improve</u> the discrimination !!

- 3. complete solution for two Pauli channels
- entanglement can improve the discrimination of EBC
 minimax discrimination

MINIMUM-ERROR DISCRIMINATION BETWEEN TWO QUANTUM STATES

 ρ_1 and ρ_2 with prior probability p_1 and $p_2 = 1 - p_1$

Look for the two-valued POVM $\{\Pi_1, \Pi_2\}$ with $\Pi_1 + \Pi_2 = I$

that minimizes the error probability

 $p_E = p_1 \operatorname{Tr}[\rho_1 \Pi_2] + p_2 \operatorname{Tr}[\rho_2 \Pi_1]$

Optimal POVM: Π_1 and Π_2 are the orthogonal projectors on the support of the positive and negative part of the operator (Helstrom, 1976) $p_1 \rho_1 - p_2 \rho_2$ $p_E = \frac{1}{2} \left(1 - \| p_1 \rho_1 - p_2 \rho_2 \|_1 \right) \quad \text{with} \quad \|A\|_1 = \text{Tr}\sqrt{A^{\dagger}A} = \max_U |\text{Tr}[UA]| = \sum_i s_i(A)$... for pure states $p_E = \frac{1}{2} \left[1 - \sqrt{1 - 4p_1 p_2} |\langle \psi_1 | \psi_2 \rangle|^2 \right]$

MINIMUM-ERROR DISCRIMINATION OF TWO UNITARY TRANSFORMATIONS



Choose ρ to minimize the error probability

 $p_E = \frac{1}{2} \left(1 - \| p_1 U_1 \rho U_1^{\dagger} - p_2 U_2 \rho U_2^{\dagger} \|_1 \right)$





using a maximally entangled state and a Bell measurement

WHAT ABOUT DISCRIMINATING BETWEEN TWO QUANTUM CHANNELS ?



Choose ρ to minimize the error probability

$$p'_E = \frac{1}{2} \left(1 - \max_{\rho \in \mathcal{H}} \| p_1 \mathcal{E}_1(\rho) - p_2 \mathcal{E}_2(\rho) \|_1 \right)$$

Can entanglement be useful ?



Example

$$p_{1} \qquad \mathcal{E}_{1}(\rho) = \rho \qquad \dim(\mathcal{H}) = 2$$

$$p_{2} \qquad \mathcal{E}_{2}(\rho) = \frac{1}{3}(\sigma_{x}\rho\sigma_{x} + \sigma_{y}\rho\sigma_{y} + \sigma_{z}\rho\sigma_{z}) = \frac{1}{3}(2I - \rho)$$

$$\mathcal{E}_{1}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \qquad |\psi\rangle \in \mathcal{H},$$

$$\mathcal{E}_{2}(|\psi\rangle\langle\psi|) = \frac{1}{3}(2I - |\psi\rangle\langle\psi|) \qquad |\psi\rangle \in \mathcal{H},$$

$$(\mathcal{E}_{1} \otimes \mathcal{I})(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \qquad |\psi\rangle \in \mathcal{H} \otimes \mathcal{H},$$

$$(\mathcal{E}_{2} \otimes \mathcal{I})(|\psi\rangle\langle\psi|) = \frac{1}{3}(2I \otimes \operatorname{Tr}_{1}[|\psi\rangle\langle\psi|] - |\psi\rangle\langle\psi|) \qquad |\psi\rangle \in \mathcal{H} \otimes \mathcal{H},$$

Without entanglement

$$p'_{E} = \frac{1}{2} \left(1 - \left| p_{1} - \frac{p_{2}}{3} \right| - \frac{2}{3} p_{2} \right) \quad \left\{ \begin{array}{ccc} \frac{1}{3} (1 - p_{1}) & \text{for} & p_{1} > \frac{1}{4} \\ \\ p_{1} & \text{for} & p_{1} \le \frac{1}{4} \end{array} \right.$$

Using a maximally entangled state $|\phi\rangle$



perfect discrimination

WHEN IS ENTANGLEMENT USEFUL ?

Isomorphism between operators on \mathcal{H} and bipartite vectors on $\mathcal{H} \otimes \mathcal{H}$ $|A | \blacktriangleleft | A \rangle \equiv \sum \langle n | A | m \rangle | n \rangle \otimes | m \rangle = A \otimes I | I \rangle = I \otimes A^{\tau} | I \rangle$ $\operatorname{Tr}[A^{\dagger}B] = \langle\!\langle A|B \rangle\!\rangle$ n,m $|A\rangle\!\rangle = |UDV\rangle\!\rangle = U \otimes V^{\tau} |D\rangle\!\rangle = U \otimes V^{\tau} \sum^{\cdot} d_n |n\rangle \otimes |n\rangle \qquad \text{rank}(A) = \text{Schmidt number of } |A\rangle\!\rangle$ maximally entangled state $=\frac{1}{\sqrt{d}}|U\rangle$, with U unitary and $d = \dim(\mathcal{H})$ $\Delta = [p_1(\mathcal{E}_1 \otimes I) - p_2(\mathcal{E}_2 \otimes I)]|I\rangle\rangle\langle\langle I|$ $p_1 \quad \mathcal{E}_1$, $p_2 \quad \mathcal{E}_2$ $\max_{|\xi\rangle\rangle} \|[p_1(\mathcal{E}_1 \otimes \mathcal{I}) - p_2(\mathcal{E}_2 \otimes \mathcal{I})]|\xi\rangle\rangle \langle\langle\!\langle \xi | \|_1 = \max_{\mathrm{Tr}[\xi^{\dagger}\xi]=1} \|I \otimes \xi^{\tau} \Delta I \otimes \xi^{*}\|_1$ minimum-error probability

$$p_E = \frac{1}{2} \left(1 - \max_{\operatorname{Tr}[\xi^{\dagger}\xi]=1} \|I \otimes \xi^{\tau} \Delta I \otimes \xi^{*}\|_{1} \right) = \frac{1}{2} \left(1 - \max_{P \ge 0, \operatorname{Tr}[P^2]=1} \|I \otimes P \Delta I \otimes P\|_{1} \right)$$

No need of entanglement IFF the maximum can be achieved by a <u>rank-one P</u> (MFS, 2005)

DISCRIMINATING TWO QUANTUM CHANNELS : a relevant case

 Δ diagonal on a "Bell basis"

$$\Delta = \sum_{n} r_n |U_n\rangle \langle \langle U_n | \qquad \text{Tr}[U_m^{\dagger} U_n] = d\delta_{n,m}$$

$$\max_{\operatorname{Tr}[\xi^{\dagger}\xi]=1} \|I \otimes \xi^{\tau} \Delta I \otimes \xi^{*}\|_{1} \leq \sum_{n} |r_{n}| \max_{\operatorname{Tr}[\xi^{\dagger}\xi]=1} \|U_{n} \otimes I|\xi\rangle\rangle \langle\!\langle \xi|U_{n}^{\dagger} \otimes I\|_{1} = \sum_{n} |r_{n}|$$

Any maximally entangled state saturates the bound

example: <u>two generalized</u> <u>Pauli channels</u>

$$\begin{aligned} \mathcal{E}_{i}(\rho) &= \sum_{n} q_{n}^{(i)} U_{n} \rho U_{n}^{\dagger} , \qquad \sum_{n} q_{n}^{(i)} = 1 \\ r_{n} &= p_{1} q_{n}^{(1)} - p_{2} q_{n}^{(2)} \end{aligned}$$

DISCRIMINATION FOR PAULI CHANNELS

$$p_{1} \quad \mathcal{E}^{(1)}(\rho) = \sum_{i=0}^{3} q_{i}^{(1)} \sigma_{i} \rho \sigma_{i} , \qquad p_{2} \quad \mathcal{E}^{(2)}(\rho) = \sum_{i=0}^{3} q_{i}^{(2)} \sigma_{i} \rho \sigma_{i}$$
$$\Delta = \sum_{i=0}^{3} r_{i} |\sigma_{i}\rangle\rangle \langle\langle \sigma_{i} | \qquad r_{i} = p_{1} q_{i}^{(1)} - p_{2} q_{i}^{(2)}$$

Any maximally entangled state is optimal

$$p_E = \frac{1}{2} \left(1 - \sum_{i=0}^3 |r_i| \right)$$

When does entanglement strictly improve the discrimination ?

$$p'_{E} = \frac{1}{2} \left(1 - \max_{P'} \|I \otimes P' \Delta I \otimes P'\|_{1} \right) ;$$

$$P' = \left(\begin{array}{c} x \\ \sqrt{x(1-x)}e^{-i\phi} & 1-x \end{array} \right) , \quad \operatorname{rank}(P') = 1$$

$$0 \le x \le 1 , \quad 0 \le \phi \le 2\pi .$$

$$p'_{E} = \frac{1}{2} \left(1 - M \right) , \quad M = \max \left\{ |r_{0} + r_{3}| + |r_{1} + r_{2}|, |r_{0} + r_{1}| + |r_{2} + r_{3}|, |r_{0} + r_{2}| + |r_{1} + r_{3}| \right\}$$

input an eigenstate of $\dot{\sigma}_z$ $\dot{\sigma}_x$ $\dot{\sigma}_y$ No need of entanglement IFF $M = \sum_{i=0}^3 |r_i|$ IFF $\det(\Delta) \ge 0$

ENTANGLEMENT CAN IMPROVE THE DISCRIMINATION OF ENTANGLEMENT-BREAKING CHANNELS

EBC IFF for any bipartite Γ $(\mathcal{E} \otimes I)\Gamma$ is separable

IFF $\mathcal{E}(\rho) = \sum_{k} \langle \phi_{k} | \rho | \phi_{k} \rangle | \psi_{k} \rangle \langle \psi_{k} |$ with $\sum_{k} | \phi_{k} \rangle \langle \phi_{k} | = I$

EBC can be simulated by a measure-and-prepare channel

Two depolarizing channels

$$\mathcal{E}_{i}^{D}(\rho) = q_{i} \rho + \frac{1 - q_{i}}{3} \sum_{\alpha=1}^{3} \sigma_{\alpha} \rho \sigma_{\alpha} , \qquad q_{1} \neq q_{2} , \qquad p_{1} = p \text{ and } p_{2} = 1 - p$$

Entanglement improves the discrimination IFF $\Pi_{\alpha=0}^{3} r_{\alpha} < 0$

$$\begin{aligned} r_0 &= p \, q_1 - (1-p) \, q_2 \ , \\ r_1 &= r_2 = r_3 = p \, \frac{1-q_1}{3} - (1-p) \, \frac{1-q_2}{3} \ . \\ \frac{1-q_2}{2-q_1-q_2} & q_2 \ . \end{aligned}$$

For $q_1, q_2 \leq 1/2$ both channels are EBC

p prior probability of a depolarizing channel with $q \le 1/2$ (1-p) prior probability of a completely depolarizing channel Both channels are EBC



In the blue region a maximally entangled state <u>strictly</u> improves the distinguishability

MINIMAX DISCRIMINATION BETWEEN TWO QUANTUM STATES

Two quantum states ρ_1 and ρ_2

No a priori probabilities

Look for the two-valued POVM $\{\Pi_1, \Pi_2\}$ that minimizes

the largest of the probabilities of misidentification

 $R_{M}(\rho_{1},\rho_{2}) = \min_{\{\Pi_{1},\Pi_{2}\}} \max(\mathrm{Tr}[\rho_{1}\Pi_{2}],\mathrm{Tr}[\rho_{2}\Pi_{1}])$

"minimum risk"

equiv. to maximize the smallest of the probabilities of correct detection $\max_{\{\Pi_1,\Pi_2\}} \min(\operatorname{Tr}[\rho_1\Pi_1], \operatorname{Tr}[\rho_2\Pi_2])$

Relation bewteen MINIMAX and MINIMUM-ERROR strategies

(D'Ariano, MFS, Kahn, 2005)

"Bayes risk"
$$R_B(p) = \frac{1}{2} \left(1 - \|p\rho_1 - (1-p)\rho_2\|_1 \right)$$

Thm I: There is a measurement $\{\Pi_1, \Pi_2\}$ that is optimal in the Bayes scheme for some a priori probability $(p_*, 1-p_*)$ such that $\operatorname{Tr}[\rho_1 \Pi_1] = \operatorname{Tr}[\rho_2 \Pi_2]$. This measurement is optimal in the minimax scheme as well, and one has $R_M(\rho_1, \rho_2) = R_B(p_*) = \operatorname{Tr}[\rho_1 \Pi_2]$.

Thm 2: The minimum risk is given by $R_M(\rho_1, \rho_2) = \max_p R_B(p)$, and the a priori probability achieving the maximum is $p = p_*$ of Thm I

Optimal minimax measurement given by a non-orthogonal POVM

Consider
$$\rho_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \rho_2 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}.$$

 $\mathcal{R}_B(p)$ is maximal for $p = \frac{1}{3}$
Imposing $\operatorname{Tr}[\rho_1 \Pi_1] = \operatorname{Tr}[\rho_2 \Pi_2] = \frac{1}{3}$

The optimal minimax POVM is unique and non-orthogonal

$$P_1 = \begin{bmatrix} \frac{2}{3} & 0\\ 0 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} \frac{1}{3} & 0\\ 0 & 1 \end{bmatrix}.$$

Conclusions & open problems

- The problems of discriminating between two unitary transformations and between two quantum operations have quite different solutions
- Entanglement can improve the discrimination
- Even if both QO's are <u>entanglement-breaking</u>
- Multiple copies of QO: serial, parallel, mixed schemes
- Suitable distance measure is still lacking
- Unambigous discrimination
- LOCC discrimination
- Minimax discrimination

ERASABLE AND UNERASABLE CORRELATIONS

Massimiliano Federico Sacchi CNR-INFM and CNISM, Unità di Pavia University of Pavia, ITALY <u>www.qubit.it</u>





Joint work with G.M. D'Ariano, R. Demkowicz-Dobrzanski, and P. Perinotti

International School and Conference on Quantum Information 2008

4th - 12th March 2008, Bhubaneswar (India)

Intro

- No-go theorems better understanding of Q.M.
- What about correlations ?
- Quantum/classical
- Beneficial/detrimental for specific tasks
- Correlation of optimal clones are the <u>worst</u> for state estimation (Demkowicz-Dobrzanzki, PRA 2005)
- Features of correlations between clones ?
- Cloning without correlations ?
- Can we erase correlations ? Qudits vs Continuous Variables
- Quantum version of the classical cocktail-party problem ?

Cocktail-party problem



Noise deconvolution

Demixing by Independent Component Analysis: the p.d. of the sum of independent random variables is "more Gaussian" than the p.d. of the independent random variables themselves

Quantum cocktail-party problem



courtesy by Tomasz Szkodziński



V, U_A, U_B unknown



quite hard...

Faithful decorrelation

N-partite quantum state $\rho \in S$

 $\mathcal{D}(\rho) = \rho_1 \otimes \ldots \otimes \rho_N$

 ρ_i is the *i*th party reduced density matrix of ρ

IMPOSSIBLE (nonlinear) if S = all density matrices Terno, PRA 1999

IMPOSSIBLE if S contains ρ', ρ'' and a convex combination of them, and the reduced states of ρ', ρ'' are different at least for two parties DDPS, PRL 2007

What about approximate decorrelation ?

Decorrelation for covariant set of states

§ N-partite "seed" quantum state ρ

§ Encode information via a UIR of a group G

$$\rho_{g} := U_{g_{1}} \otimes \ldots \otimes U_{g_{N}} \rho U_{g_{1}}^{\dagger} \otimes \ldots \otimes U_{g_{N}}^{\dagger}$$

§ Look for a decorrelating map that maximizes the averaged single-site fidelity

$$\overline{F}[\rho,\mathscr{D}] = \frac{1}{N} \sum_{i=1}^{N} \int_{G^N} d\boldsymbol{g} \ F(U_{g_i} \operatorname{Tr}_{\overline{i}}[\rho] U_{g_i}^{\dagger}, \operatorname{Tr}_{\overline{i}}[\mathscr{D}(U_{\boldsymbol{g}} \rho U_{\boldsymbol{g}}^{\dagger})]),$$

§ w.l.o.g. look for covariant map

$$\mathbf{P}\left(\mathscr{D}_{\boldsymbol{g}}\rho U_{\boldsymbol{g}}^{\dagger}\right) = U_{\boldsymbol{g}}\mathscr{D}\left(\rho\right)U_{\boldsymbol{g}}^{\dagger} \quad \forall \rho.$$

that decorrelates the seed state $\mathscr{D}(\rho) = \tilde{\rho}_1 \otimes \ldots \tilde{\rho}_N$

Thanks to covariance, correlations in <u>all states</u> of the orbit will be erased

I. Two qubits with different signals

§ Permutation invariant seed state => ρ_{AB} block diagonal form w.r.t. singlet-triplet subspaces

 $\rho_{AB}(\alpha,\beta) = U(\alpha) \otimes U(\beta) \rho_{AB} U(\alpha)^{\dagger} \otimes U(\beta)^{\dagger}$

§ Local states:

$$\rho_A(\alpha) = \operatorname{Tr}_B[\rho_{AB}(\alpha, \beta)] = \frac{1}{2}[1 + \eta n_A(\alpha) \cdot \boldsymbol{\sigma}],$$

$$\rho_B(\beta) = \operatorname{Tr}_A[\rho_{AB}(\alpha, \beta)] = \frac{1}{2}[1 + \eta n_B(\beta) \cdot \boldsymbol{\sigma}],$$

§ Group and permutational covariant maps:

tput states:

$$\mathcal{D}(\rho_{AB}) = a\rho_{AB} + b\mathcal{D}_1(\rho_{AB}) + c\mathcal{D}_2(\rho_{AB}),$$

where
$$\mathcal{D}_{1}(\rho_{AB}) = \frac{1}{3}(\rho_{A} \otimes \mathbb{1} + \mathbb{1} \otimes \rho_{B} - \rho_{AB}),$$

 $\mathcal{D}_{2}(\rho_{AB}) = \frac{1}{9}(4\mathbb{1} \otimes \mathbb{1} - 2\rho_{A} \otimes \mathbb{1} - 2\mathbb{1} \otimes \rho_{B} + \rho_{AB}),$
 $a + b + c = 1$
 $\tilde{\rho}_{A}(\alpha) = \frac{1}{2}[\mathbb{1} + \tilde{\eta}\boldsymbol{n}_{A}(\alpha) \cdot \boldsymbol{\sigma}],$
 $\tilde{\rho}_{B}(\beta) = \frac{1}{2}[\mathbb{1} + \tilde{\eta}\boldsymbol{n}_{B}(\beta) \cdot \boldsymbol{\sigma}],$

§ Imposing $\mathcal{D}(\rho_{AB}) = \tilde{\rho}^{\otimes 2} = [\frac{1}{2}(1 + \tilde{\eta}\sigma_z)]^{\otimes 2}$

nontrivial decorrelation ($\tilde{\eta} > 0$) is possible only when the seed state has the form

$$\rho_{AB} = \frac{1}{4} [\mathbb{1} \otimes \mathbb{1} + \eta(\sigma_z \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_z) - \lambda \sigma_z \otimes \sigma_z].$$

- § All states are separable
- § Maximal achievable $\tilde{\eta}$ vs η and λ



II. Two qubits with identical signals

§ The decorrelation condition $\mathcal{D}(\rho_{AB}) = \tilde{\rho}^{\otimes 2}$ is nontrivially satisfied for ρ_{AB} diagonal in the singlet-triplet basis

 $\rho_{AB} = p |\Psi^-\rangle \langle \Psi^-| + (1-p) \rho_{sym}$ with

 $\rho_{\text{sym}} = \frac{1}{4} [\mathbbm{1} \otimes \mathbbm{1} + \eta(\sigma_z \otimes \mathbbm{1} + \mathbbm{1} \otimes \sigma_z) + (1 + \lambda)/2(\sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y) - \lambda \sigma_z \otimes \sigma_z].$

§ Correlation cannot be erased for p = 1 maximally entangled

$$\eta = 0$$
 diagonal on Bell basis ~

output clones of a universal cloning machine!!!





N to M universal cloning of qudits without correlations is impossible

- § w.l.o.g. M=N+I and pure states
 (use partial trace and depolarizing channels)
- § Universal covariance implies $\Lambda[(|\phi\rangle\langle\phi|)^{\otimes N}] = \left(\eta|\phi\rangle\langle\phi| + \frac{1-\eta}{2}\mathbb{1}\right)^{\otimes N+1}$
- § Consider $|\phi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$,
- => r.h.s. poly($e^{\pm i\phi}$) with degree N+1 and I.h.s poly($e^{\pm i\phi}$) with degree at most N (for linearity)

§ Should hold for any
$$\phi$$
 => necessarily $\eta = 0$

§The proof just uses linearity => impossible even for asymmetric and probabilistic cloning

more generally...

cloning with <u>factorized clones</u> is <u>impossible</u> for any set of pure states which contains a finite arch of states of the form

 $|\phi\rangle := \sqrt{p}|0\rangle + \sqrt{1-p}e^{i\phi}|1\rangle$

What about discrete set of states ?

Conjecture: <u>linearly dependent</u> set of states cannot be cloned without correlations

Linear independent states can be probabilistically perfectly cloned via unambiguous state discrimination

III. Gaussian states

§ It is always possible to decorrelate any state in the set

 $D(\alpha) \otimes D(\beta) \rho_{AB} D(\alpha)^{\dagger} \otimes D(\beta)^{\dagger}$

where ρ_{AB} is a two-mode Gaussian state

$$\rho_{AB} = \frac{1}{\pi^2} \int d^4 \boldsymbol{q} \, e^{-\frac{1}{2} \boldsymbol{q}^T \boldsymbol{M} \boldsymbol{q}} D(\boldsymbol{q})$$

§ Just use a covariant Gaussian decorrelating channel

$$\mathscr{D}(\rho) = \frac{\sqrt{\det \boldsymbol{G}}}{(2\pi)^2} \int d^4 \boldsymbol{x} \, e^{-\frac{1}{2}\boldsymbol{x}^T \boldsymbol{G} \boldsymbol{x}} D(\boldsymbol{x}) \rho D^{\dagger}(\boldsymbol{x})$$

with suitable positive matrix G.

§ $\mathscr{D}(\rho_{AB})$ will be still Gaussian, with new block-diagonal covariance matrix \widetilde{M} , i.e. decorrelated

§ The channel is covariant => decorrelation for any α , β

Cloning without correlations for GS

- 1. Use N-splitter to concentrate the signal in one mode
- 2. Amplify the signal by a PIA with power gain M/N
- Distribute the amplified mode by a M-splitter with (M-1)

thermal states with suitable photon number



Conclusions & open problems

- Only few states can be decorrelated if the covariance group is "large"
- <u>Any</u> joint Gaussian state can be decorrelated
- Covariant cloning without correlations: <u>NO for qudits</u>, <u>YES for CV</u>
- ? Experimental set-up for covariant decorrelation for qudits
- ? Optimal decorrelators for CV
- ? Restriction to bilocal or LOCC operations
- ? No-cloning without correlations for <u>discrete set</u> of states



G.M. D'Ariano, R. Demkowicz-Dobrzanski, P. Perinotti, and M.F. Sacchi, PRL 2007

G.M. D'Ariano, R. Demkowicz-Dobrzanski, P. Perinotti, and M.F. Sacchi, PRA 2008

Thank you !