Optimal input states for discrimination of quantum channels

Anna Jenčová

Mathematical Institute, Slovak Academy of Sciences
Bratislava, Slovakia
jencova@mat.savba.sk

1. Multiple hypothesis testing for quantum channels

Assume that a channel $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ is known to be one of $\Phi_1, \dots, \Phi_m$, with prior probabilities $\lambda_1, \dots, \lambda_m$. The task is to determine which one, with the greatest probability of success.
A most general scheme for this task is given by a triple $(\mathcal{H}_0, \rho, M)$, where $\rho \in \mathcal{S}(\mathcal{H} \otimes \mathcal{H}_0)$ is a (pure) input state and $M = \{M_1, \dots, M_n\}$ is a POVM on $B(\mathcal{K} \otimes \mathcal{H}_0)$. The value

$$\mathrm{Tr} M_i(\Phi_j \otimes id)(\rho)$$

is interpreted as the probability that Φ_i is chosen when the true channel is Φ_j. The average success probability is then

$$P(M, \rho) = \sum_i \lambda_i \mathrm{Tr}[M_i(\Phi_i \otimes id)(\rho)]. \quad (1)$$

The task is to maximize $P(M, \rho)$ over all input states ρ and POVMs M. It had been observed [6, 8] that entangled input states give greater success probability in some cases, however, there are situations when the maximally entangled input state is not optimal. It is therefore important to find out whether an optimal scheme with a given input state exists. A related problem was studied in [7].

2. Process POVMs and SDP formulation of the problem

Alternatively, channel measurements are described by process POVMs [9] (or testers [1], see also [3]), which is a collection $F = \{F_1, \dots, F_m\}$ of positive operators in $B(\mathcal{K} \otimes \mathcal{H})$, such that $\sum_i F_i = I \otimes \sigma$ for some state $\sigma \in \mathcal{S}(\mathcal{H})$. The average success probability is then

$$P(F) = \sum_i \lambda_i \mathrm{Tr}[C(\Phi_i)F_i], \quad (2)$$

where $C(\Phi)$ is the Choi operator of Φ, [2]. Using this form, our task becomes a problem of semidefinite programming:

$$\begin{aligned} &\max \mathrm{Tr}[CF] \\ &F \in B(\mathbb{C}^n \otimes K \otimes H) \\ &\mathrm{Tr}[F] = \dim(\mathcal{K}) \\ &\mathrm{Tr}[(I \otimes X_i)F] = 0, \quad i = 1, \dots, k \\ &F \geq 0 \end{aligned}$$

Here $C = \sum_i |i\rangle\langle i| \otimes C(\Phi_i)$ and $X_1, \dots, X_k$ is any basis of the (real) linear subspace

$$\mathcal{L} := \{X = X^* \in B(\mathcal{K} \otimes \mathcal{H}), \mathrm{Tr}_{\mathcal{K}} X = 0\}.$$

3. Optimality conditions

Using standard results of SDP, we obtain the following:
Theorem 1. *Let $\hat{F}$ be a process POVM. Then $\hat{F}$ is optimal if and only if there is some $\lambda_0 > 0$ and some channel Ψ, such that for $i = 1, \dots, m$,*

$$\lambda_i C(\Phi_i) \leq \lambda_0 C(\Psi)$$

and

$$(\lambda_0 C(\Psi) - \lambda_i C(\Phi_i))\hat{F}_i = 0.$$

Moreover, in this case, the optimal success probability is

$$\mathrm{Tr}[\hat{F}C] = \min_{\Phi} \min\{t > 0, \lambda_i C(\Phi_i) \leq tC(\Phi), \forall i\} = \lambda_0,$$

the minimum is taken over all channels $B(\mathcal{H}) \to B(\mathcal{K})$.
We can characterize optimal measurement schemes as follows:
Corollary 1. *Let $\rho \in \mathcal{S}(\mathcal{H} \otimes \mathcal{H})$ be such that $\sigma := \mathrm{Tr}_1 \rho$ is invertible. Then $(\mathcal{H}, \rho, M)$ is optimal if and only if*

$$Z := \sum_j \lambda_j M_j(\Phi_j \otimes id)(\rho) \geq \lambda_i(\Phi_i \otimes id)(\rho), \quad i = 1, \dots, m$$

and $\mathrm{Tr}_{\mathcal{K}} Z \propto \sigma$.
Similar results were obtained in [5], in a broader context and by different methods. Apart from the last condition on the partial trace of Z, these are optimality conditions for a POVM in MHT for the ensemble $\{\lambda_i, (\Phi_i \otimes id)(\rho)\}$, [4].

4. Optimal discrimination with a maximally entangled input state

Let $m = 2$. Using the known characterization of optimal POVMs in this case, we obtain a simple condition for existence of an optimal scheme with a maximally entangled input state:
Corollary 2. *Let $\Phi_1, \Phi_2 : B(\mathcal{H}) \to B(\mathcal{K})$ be channels, $\lambda \in (0, 1)$. An optimal scheme $(\mathcal{H}, \rho, M)$ with a maximally entangled input state ρ exists if and only if the Choi operators satisfy*

$$\mathrm{Tr}_{\mathcal{K}}|\lambda C(\Phi_1) - (1 - \lambda)C(\Phi_2)| = aI, \quad \text{(MEI)}$$

here $|X| = (X^*X)^{1/2}$. Moreover, in this case, the optimal success probability is $P_{opt} = \frac{a+1}{2}$.
We apply this last condition to check the existence of optimal procedures with maximally entangled input states for discrimination of some types of channels.

5. Examples

For two channels Φ_1, Φ_2 and $\lambda \in (0, 1)$, we put

$$\phi_\lambda = \lambda\Phi_1 - (1 - \lambda)\Phi_2.$$

For a unitary $U \in \mathcal{U}(\mathcal{H})$, let $\Phi_U : B(\mathcal{H}) \to B(\mathcal{H})$, $A \mapsto U^*AU$.

5.1 Covariant channels

Let G be a group and let $g \mapsto U_g \in \mathcal{U}(\mathcal{H})$, $g \mapsto V_g \in \mathcal{U}(\mathcal{K})$ be unitary representations. Let Φ_1 and Φ_2 satisfy

$$\Phi_i(U_g^* A U_g) = V_g^* \Phi_i(A) V_g, \quad g \in G, A \in B(\mathcal{H}), i = 1, 2.$$

Then

$$\bar{U}_g^* \mathrm{Tr}_{\mathcal{K}}|C(\phi_\lambda)|\bar{U}_g = \mathrm{Tr}_{\mathcal{K}}|C(\phi_\lambda \circ \Phi_{U_g})| = \mathrm{Tr}_{\mathcal{K}}|C(\phi_\lambda)|.$$

Assume that the representation $g \mapsto U_g$ is irreducible. Then (MEI) holds for Φ_1, Φ_2 and any $\lambda \in (0, 1)$.

5.2 Unitary channels

Let $U, V \in \mathcal{U}(\mathcal{H})$ and put $W := V^*U$. Then (MEI) holds for Φ_U, Φ_V and some $\lambda \in (0, 1)$ if and only if

$$\overline{\mathrm{Tr}[W]}W + \mathrm{Tr}[W]W^* \propto I.$$

Equivalently, either $\mathrm{Tr}W = 0$ or W has at most two distinct eigenvalues, both of the same multiplicity.

5.3 Qubit channels

Let $\Phi_1, \Phi_2 : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ be qubit channels. Then (MEI) holds if and only if

$$\mathrm{Tr}_{\mathcal{K}}|C(\phi_\lambda) + (\phi_\lambda(I) + (1 - 2\lambda)I) \otimes I| = \mathrm{Tr}_{\mathcal{K}}|C(\phi_\lambda)|.$$

In particular, if there is some $c > 0$ such that

$$\Phi_2(I) = c\Phi_1(I) + (1 - c)I,$$

then (MEI) holds with $\lambda = 1/(1 + c)$. If both channels are unital, it holds for any $\lambda \in (0, 1)$.
On the other hand, let $\Phi_1 = id$ and let $\Phi_2 = \Psi_{\alpha,\beta}$ be the channel

$$\Psi_{\alpha,\beta} : \sum_{i=0}^{3} w_i \sigma_i \mapsto w_0 I + \sum_{i=1}^{3} (\mathbf{t} + T\mathbf{w})_i \sigma_i$$

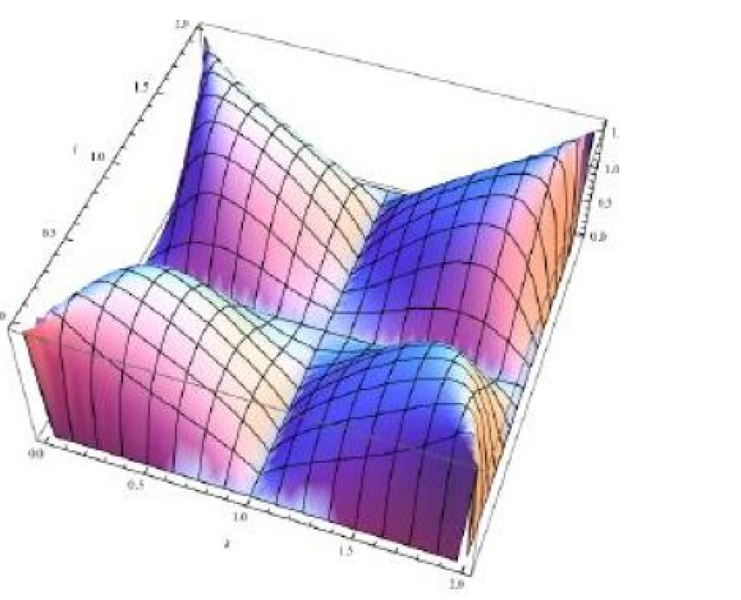
where $\sigma_0 = I, \sigma_1, \dots, \sigma_3$ are the Pauli matrices and

$$\mathbf{w} = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}, \mathbf{t} = \begin{pmatrix} 0 \\ 0 \\ \sin\alpha \sin\beta \end{pmatrix}, T = \begin{pmatrix} \cos\alpha & 0 & 0 \\ 0 & \cos\beta & 0 \\ 0 & 0 & \cos\alpha\cos\beta \end{pmatrix}$$

The graph below shows values of the function

$$d(\alpha, \beta) := \|I - \nu(\mathrm{Tr}_{\mathcal{K}}|C(\phi_{1/2})|)\|_1,$$

$\nu(A) = (2/\mathrm{Tr}[A])A$, the axes correspond to $\alpha = l\pi$, $\beta = k\pi$.



This suggests that (MEI) holds only if either $\alpha = \pi$ or $\beta = \pi$, that is if Φ_2 is unital (joint work with Tomasz Tylec).

5.4 Measurements

For a POVM $M = M_1, \dots, M_n$ on $B(\mathcal{H})$, we denote

$$\Phi_M : B(\mathcal{H}) \ni A \mapsto \sum_i \mathrm{Tr}[AM_i]|i\rangle\langle i| \in B(\mathbb{C}^n).$$

This is a qc-channel. If $\Phi_1 = \Phi_M$ and $\Phi_2 = \Phi_N$, (MEI) reads

$$\sum_i |\lambda M_i - (1 - \lambda)N_i| \propto I.$$

Let M and N be **von Neumann measurements**,

$$M_i = |\xi_i\rangle\langle\xi_i|, \quad N_i = |\eta_i\rangle\langle\eta_i|,$$

for two ONB's $|\xi_1\rangle, \dots, |\xi_n\rangle$ and $|\eta_1\rangle, \dots, |\eta_n\rangle$. Let $\lambda = 1/2$. Then (MEI) becomes

$$\sum_i c_i P_{\xi_i,\eta_i} = 2aI, \quad a = n^{-1}\sum_i c_i$$

where $c_i = \sqrt{1 - |\langle\xi_i, \eta_i\rangle|^2}$ and P_{ξ_i,η_i} is the projection onto $\mathrm{span}(\xi_i, \eta_i)$. This implies $c_i \neq 0$, for all i. An equivalent condition is that the matrix

$$(2aI - C)^{-1/2}(W - diag(W))C^{-1/2}$$

is unitary, where $W = (\langle\xi_i, \eta_j\rangle)$, $C = diag(c_1, \dots, c_n)$. Some results are listed below.

- For $n = 2$ (MEI) always holds (for any λ), since Φ_M and Φ_N are unital qubit channels.
- For $n = 3$, (MEI) holds if and only if there is a cyclic permutation σ of $\{1, 2, 3\}$, such that $\eta_i = \xi_{\sigma(i)}$.
- Let the bases be mutually unbiased (MUB), then

  $$W = \frac{1}{\sqrt{n}}H$$

  for a Hadamard matrix H. We may assume that $H_{ii} = 1$ for all i. Then (MEI) holds iff $H + H^* = 2I$.
- For MUB, $n = 4$, (MEI) holds iff $H = D^*H_0D$, where

  $$H_0 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$$

  and D is some diagonal unitary.

References

[1] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. 101 , 180501 (2008)

[2] M.D. Choi, Completely positive maps on complex matrices, Lin. Alg. Appl. 10 (1975), 285-290

[3] Gus Gutoski and John Watrous, Toward a general theory of quantum games. In *Proceedings STOC 2007*, 565–574, arXiv:quant-ph/0611234v2

[4] A. S. Holevo, Journal of Multivariate Analysis 3, 337 – 394 (1973)

[5] A. Jenčová, J Math. Phys. 55, 022201 (2014)

[6] A. Kitaev, Quantum computations: algorithms and error correction. Russian Mathematical Surveys, 52 (1997), 1191–1249

[7] K. Matsumoto, arXiv:1209.2392

[8] M. Piani and J. Watrous, Phys. Rev. Lett., 102(25):250501, (2009)

[9] M. Ziman, Phys. Rev. A 77, 062112 (2008)