Worst-case Quantum Hypothesis Testing with Separable Measurements

Le Phuc Thinh[1,2], Michele Dall'Arno[1,3,4], and Valerio Scarani[1,5]

[1]Centre for Quantum Technologies, National University of Singapore, Singapore

[2]Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstr. 2, 30167 Hannover, Germany

[3]Yukawa Institute for Theoretical Physics, Kyoto University, Kitashirakawa Oiwakecho, Sakyoku, Kyoto 606-8502, Japan

[4]Faculty of Education and Integrated Arts and Sciences, Waseda University, 1-6-1 Nishiwaseda, Shinjuku-ku, Tokyo 169-8050, Japan

[5]Department of Physics, National University of Singapore, Singapore

For any pair of quantum states (the hypotheses), the task of binary quantum hypotheses testing is to derive the tradeoff relation between the probability p_{01} of rejecting the null hypothesis and p_{10} of accepting the alternative hypothesis. The case when both hypotheses are explicitly given was solved in the pioneering work by Helstrom. Here, instead, for any given null hypothesis as a pure state, we consider the worst-case alternative hypothesis that maximizes p_{10} under a constraint on the distinguishability of such hypotheses. Additionally, we restrict the optimization to separable measurements, in order to describe tests that are performed locally. The case $p_{01} = 0$ has been recently studied under the name of "quantum state verification". We show that the problem can be cast as a semi-definite program (SDP). Then we study in detail the two-qubit case. A comprehensive study in parameter space is done by solving the SDP numerically. We also obtain analytical solutions in the case of commuting hypotheses, and in the case where the two hypotheses can be orthogonal (in the latter case, we prove that the restriction to separable measurements generically prevents perfect distinguishability). In regards to quantum state verification, our work shows the existence of more efficient strategies for noisy measurement scenarios.

YITP-20-101

1 Introduction

The task of quantum hypothesis testing [16], a subfield of quantum state estimation [1, 17, 21], is to optimally identify, according to some given payoff function, an unknown quantum state given as a black box. The strategy consists of performing a quantum measurement, whose optimality depends upon the payoff function and the prior information about the state, available in the form of a probability distribution over the state space. Several discrimination problems [2–4, 6–9, 12, 19, 22] are based on quantum hypothesis testing.

In the simplest non-trivial instance of the problem, the prior distribution has support over two states only, the *null* and the *alternative* hypotheses. Hence, binary quantum hypothesis testing corresponds to the derivation of the tradeoff relation between two error probabilities: I) the probability of rejecting the null hypothesis, and II) the probability of accepting the alternative hypothesis. The case when such hypotheses are given explicitly was solved analytically by Helstrom [16].

Here, instead, we consider the case in which only one state (the null hypothesis) is explicitly given. For the other state (the alternative hypothesis), we consider a constrained worst-case scenario. The worst-case alternative hypothesis is the one that maximizes the type-II error probability, under a given lower bound on the distinguishability of the two hypotheses. Additionally, we consider multipartite hypotheses, and we restrict the optimization to separable measurements only. This setup generalizes the so-called "quantum state verification" [18, 20, 23–27], by relaxing the assumption that the type-I error probability is null.

Our first contribution is a formulation of the aforementioned problem as a semi-definite program, that can be efficiently solved with readily available numerical tools. Then, we specify to the case in which the hypotheses are two-qubit states, and we derive an analytical form for the worst-case hypothesis. Finally, we analytically derive the tradeoff relation between type-I and type-II error probabilities in the case when the hypotheses commute. In regards to quantum state verification, our work shows the existence of more efficient strategies in certain parameter regimes for noisy measurement scenarios.

The structure of this paper is as follows. In Sec-

Le Phuc Thinh: thinh.le@itp.uni-hannover.de
Michele Dall'Arno: dallarno.michele@yukawa.kyoto-u.ac.jp
Valerio Scarani: physv@nus.edu.sg

tion 2 we recall the general problem of quantum hypothesis testing and we introduce the specific problem addressed here. In Section 3 we reformulate our problem as a semi-definite program, and we analytically derive the worst-case alternative hypothesis in the two-qubit case. In Section 4 we analytically derive the tradeoff relation between type-I and type-II error probabilities for commuting hypotheses. Section 5 summarizes our results.

2 Hypothesis testing of quantum states

The simplest scenario of hypothesis testing is binary *quantum state discrimination* between ρ_0 and ρ_1. In other words, one is asked to decide which is more likely between two hypotheses H_0 — the *null hypothesis* — representing the fact that the unknown state is ρ_0, and H_1 — the *alternative hypothesis* — corresponding to the unknown state being ρ_1. The decision process can be formalized by a POVM $\{\Omega, \mathbb{1}-\Omega\}$ where the element Ω accepts H_0 and $\mathbb{1}-\Omega$ accepts H_1. This naturally gives rise to two errors, type I or *false positive* $p_{01} = \mathrm{tr}(\rho_0(\mathbb{1}-\Omega))$ and type II or *false negative* $p_{10} = \mathrm{tr}(\rho_1\Omega)$. False positive probability captures the situation that the decision process accepts H_1 when hypothesis H_0 is true. False negative probability corresponds to the other situation where one accepts H_0 when H_1 is true. Therefore, in this language, the problem is to design an *optimal measurement* Ω that optimizes certain figure-of-merit. For example, Helstrom strategy minimizes the average probability of error $p_0 p_{01} + p_1 p_{10}$ where p_0 is the *a priori* probability of occurrence of hypothesis H_0 and ditto for p_1.

Several problems in quantum information such as quantum channel coding [13] and quantum illumination [19] can be seen as hypothesis testing problems by assigning appropriate sets to hypothesis and choosing appropriate figures-of-merit (see e.g. [14, 15]). Here we look at the task that has been called *quantum state verification* [20]. In this task, H_0 is the state $|\psi\rangle\langle\psi|$, and H_1 is the set of states σ such that $\langle\psi|\,\sigma\,|\psi\rangle \leq 1-\epsilon$. Previous works [18, 20, 23–27] considered strategies that have no false positive, i.e. $p_{01} = 0$, and set out to minimize the worst-case probability of false negative

$$p_{10}(\epsilon) := \min_{\substack{0\preceq\Omega\preceq\mathbb{1}\\ \langle\psi|\Omega|\psi\rangle=1\\ \Omega\in[\mathrm{set}]}} \max_{\substack{\sigma\succeq 0\\ \mathrm{tr}(\sigma)=1\\ \langle\psi|\sigma|\psi\rangle\leq 1-\epsilon}} \mathrm{tr}(\Omega\sigma)\,.$$

The set to which Ω belongs can be that of all effects, or a restricted one. When dealing with composite systems, a particularly relevant set is the set SEP of *separable* measurements because they are easier to implement than LOCC or richer local measurement classes and at the same time could provide a bound on the performance of other classes. In this work, we shall focus on this one and leave possible extensions to future work.

Here we relax the condition $p_{01} = 0$ to $p_{01} \leq \delta$, leading to the optimisation

$$p_{10}(\delta,\epsilon) := \min_{\substack{0\preceq\Omega\preceq\mathbb{1}\\ \langle\psi|\Omega|\psi\rangle\geq 1-\delta\\ \Omega\in\mathrm{SEP}}} \max_{\substack{\sigma\succeq 0\\ \mathrm{tr}(\sigma)=1\\ \langle\psi|\sigma|\psi\rangle\leq 1-\epsilon}} \mathrm{tr}(\Omega\sigma)\,. \qquad (1)$$

This generalisation is relevant, as it allows the study of the *tradeoff* between δ and $p_{10}(\delta,\epsilon)$. From the technical point of view, this study does not constitute a straightforward extension of previously employed mathematical tools for the following reason. The condition $\langle\psi|\,\Omega\,|\psi\rangle = 1$ forces Ω to commute with $|\psi\rangle\langle\psi|$, which provides a significant simplification in the number of parameters and structure of the problem. When that condition is relaxed to $\langle\psi|\,\Omega\,|\psi\rangle \geq 1-\delta$, commutativity can no longer be assumed *a priori* (and we shall show that, for some values of δ and the other parameters, the optimal strategy is indeed *not* the commuting one).

3 Reformulations of the optimisation

In this section, we first show that the optimisation (1) for separable measurements can be cast as a semidefinite program (SDP), which allows for reliable numerical solutions. Then, for the case of two-qubit states, we solve the optimisation of the inner problem, thus casting the optimisation in a form which will allow deriving some analytical results in Section 4.

3.1 Reformulation as a SDP

The problem we are considering is at first sight a min max problem involving two variables Ω, σ that appears bilinearly in the objective function. Though fixing each variable is separately a SDP and can be reliably solved to any precision, there is no guarantee on the optimality of remaining outer optimization if one deploys numerical methods. A closer analysis of the optimization problem shows that one can in fact use duality theory of semidefinite programming to reformulate the problem. We refer the reader to the classic book [5] for more information on duality in optimization.

Lemma 1. *The optimisation* (1) *can be reformulated as a semidefinite program*

$$\begin{aligned} p_{10}(\delta,\epsilon) = \min_{\Omega,y_1,y_2}\ & y_1 + (1-\epsilon)y_2 \\ s.\ t.\ & 0 \preceq \Omega \preceq \mathbb{1} \\ & \langle\psi|\,\Omega\,|\psi\rangle \geq 1-\delta \\ & \Omega \in \mathrm{SEP} \\ & y_1\mathbb{1} + y_2\,|\psi\rangle\langle\psi| \succeq \Omega \\ & y_1 \in \mathbb{R}, y_2 \geq 0 \end{aligned} \qquad (2)$$

Proof. The constraints on Ω (outer optimisation) remain the same, while we replace the inner optimisation

$$\max\{\operatorname{tr}(\Omega\sigma) : \sigma \succeq 0, \operatorname{tr}\sigma = 1, \langle\psi|\,\sigma\,|\psi\rangle \leq 1-\epsilon\}$$

by its dual, which is the semidefinite program

$$\min\{y_1 + (1-\epsilon)y_2 : y_1\mathbb{1} + y_2\,|\psi\rangle\!\langle\psi| \succeq \Omega^\dagger, y_2 \geq 0\}\,.$$

Moreover, strong duality holds because the primal is feasible, and thanks to $\Omega^\dagger = \Omega$ the dual is strictly feasible (choose $y_2 > 0$ such that $(y_1\mathbb{1} - \Omega + y_2\,|\psi\rangle\!\langle\psi| \succ 0)$. This means that the primal and dual optimum are the same, and also the primal optimum is attained. Hence, our minimax problem becomes (2). Note that separability is a SDP constraint albeit exponential in size [11] and not just a hierarchy of SDP constraints [10]. □

3.2 Two-qubit states

For two-qubit states $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$, we can proceed with additional analytic derivations. Without loss of generality, we consider the regime of parameters where $\theta \in [0, \pi/4]$, $\epsilon \in (0,1]$ and $\delta \in [0,1]$.

Lemma 2. *For two-qubit pure states* $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$*, the optimisation* (2) *reduces to an optimisation over real variables*

$$\begin{aligned}
p_{10}(\delta,\epsilon) = \min_{t,z,x,\omega,y_1,y_2}\; & y_1 + (1-\epsilon)y_2 \\
s.\ t.\ \; & 0 \preceq \begin{pmatrix} t+z & x \\ x & t-z \end{pmatrix} \preceq \mathbb{1} \\
& 0 \leq \omega \leq 1 \\
& t + z \geq 1 - \delta \\
& \omega \geq |x\cos 2\theta + z\sin 2\theta| \\
& \begin{pmatrix} y_1 + y_2 - (t+z) & -x \\ -x & y_1 - (t-z) \end{pmatrix} \succeq 0 \\
& y_1 - \omega \geq 0 \\
& y_1 \in \mathbb{R}, y_2 \geq 0
\end{aligned} \tag{3}$$

Proof. We first spend the symmetry present in the state. Define

$$\Omega_a := \frac{1}{2\pi}\int_0^{2\pi} (U_\phi \otimes U_{-\phi})\Omega(U_\phi \otimes U_{-\phi})^\dagger\,\mathrm{d}\phi \tag{4}$$

with $U_\phi = |0\rangle\!\langle 0| + e^{i\phi}\,|1\rangle\!\langle 1|$. For any feasible (Ω, y), the pair (Ω_a, y) remains feasible with the same value of the objective function. Moreover, the state is also invariant under swapping S of two qubits, so that $(\bar\Omega_a, y)$ with $\bar\Omega_a := (\Omega_a + S\Omega_a S^\dagger))/2$ is feasible as well. Lastly, $\bar\Omega_a$ can be taken to be real symmetric because the feasible region is preserved under taking entrywise complex conjugate, and the objective value is unchanged. We note that this same symmetrisation was carried out in [24] on the primal inner problem, thanks to the assumption that Ω commutes with $|\psi\rangle\,\langle\psi|$. It's by looking at the dual that we noticed that the symmetry is independent of the commutation assumption.

This observation simplifies the number of variables in our optimisation. Specifically, let $|\psi^\perp\rangle = -\cos\theta\,|00\rangle + \sin\theta\,|11\rangle$, it suffices to optimize over real symmetric matrices

$$\bar\Omega_a = \begin{pmatrix} t+z & x & 0 & 0 \\ x & t-z & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega \end{pmatrix} \tag{5}$$

in the ordered basis $\{|\psi\rangle, |\psi^\perp\rangle, |01\rangle, |10\rangle\}$. Writing out the separability constraint, which for qubits is equivalent to positive partial transpose, we arrive at the final form given by the Lemma. □

Remarkably, what was the inner optimisation (now optimisation over y_1 and y_2) can be further solved analytically; besides, one can set $t = 1 - \delta - z$ and $\omega = |x\cos 2\theta + z\sin 2\theta|$ without loss of generality. The lengthy proof of these steps is presented in Appendix A. The farthest version of the optimisation that we can reach analytically reads:

Lemma 3. *For two-qubit pure states* $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$*, the optimisation* (2) *reduces to*

$$\begin{aligned}
p_{10}(\delta,\epsilon) = \min_{z,x}\; & f(|x\cos 2\theta + z\sin 2\theta|) \\
s.\ t.\ \; & 0 \preceq \begin{pmatrix} 1-\delta & x \\ x & 1-\delta-2z \end{pmatrix} \preceq \mathbb{1} \\
& 1 - \delta - 2z + \sqrt{\frac{1-\epsilon}{\epsilon}}|x| \leq |x\cos 2\theta + z\sin 2\theta|
\end{aligned} \tag{6}$$

where

$$f(y_1^*) := y_1^* + (1-\epsilon)\left[1 - \delta - y_1^* + \frac{x^2}{y_1^* - (1-\delta-2z)}\right].$$

4 Results

For our results, we keep focusing on the case of two qubits, although we recall that the SDP (2) is valid in general and one could therefore set out to solve it in any other case.

4.1 Commuting strategy

As we mentioned earlier, when $\delta = 0$, which is the case considered in [20, 24], the condition $\langle\psi|\,\Omega\,|\psi\rangle = 1$ immediately implies that Ω is diagonal in the same basis as $|\psi\rangle\,\langle\psi|$, that is $x = 0$ in our notation. When $\delta \neq 0$, there is no *a priori* guarantee that the optimal solution will be a commuting one; but we can obtain an upper bound $p_{10}^c(\delta,\epsilon)$ by *enforcing* $x = 0$. In this case, the optimisation (6) becomes trivial:

$$\begin{aligned}
p_{10}^c(\delta,\epsilon) = \min_z\; & z\epsilon\sin 2\theta + (1-\epsilon)(1-\delta) \\
\text{s. t. }\; & z \geq \frac{1-\delta}{2+\sin 2\theta}\,,
\end{aligned}$$

that is

$$p^c_{10}(\delta,\epsilon) = (1-\delta)\left[1 - \frac{\epsilon}{1+\sin\theta\cos\theta}\right]\,. \qquad (7)$$

This result could have been derived at an earlier stage than Lemma 3 (see Lemma 6 in the Appendix). In fact, it can also be derived without any reliance on the SDP formulation, by adapting the steps made in Ref. [24] to the case $\delta \neq 0$.

4.2 Analytical solution for $\epsilon = 1$

Next, we present the analytical solution of (6) for the special case $\epsilon = 1$. The optimisation now reads

$$\begin{aligned} p_{10}(\delta,1) = &\min_{z,x} |x\cos 2\theta + z\sin 2\theta| \\ &\text{s. t. } 1-\delta-z-\sqrt{x^2+z^2} \geq 0 \\ &\qquad 1-\delta-z+\sqrt{x^2+z^2} \leq 1 \\ &\qquad 1-\delta-2z \leq |x\cos 2\theta + z\sin 2\theta|\,. \end{aligned} \qquad (8)$$

where we have spelled out the two matrix constraints in (6). Even for this simple case, the study is heavy, though without intrinsic difficulties.

First we notice that for the maximally entangled state ($\cos 2\theta = 0$, $\sin 2\theta = 1$) the figure of merit is simply z, and the last constraint is $z \geq \frac{1-\delta}{3}$. The two quadratic constraints are both feasible for $z = \frac{1-\delta}{3}$, for a variety of values of x including $x = 0$. Thus, for $\theta = \frac{\pi}{4}$ we find $p_{10}(\delta,1) = p^c_{10}(\delta,1) = \frac{1-\delta}{3}$; both the commuting strategy and several non-commuting ones achieve this bound.

For $\cos 2\theta < 1$, the solution is unique and can be inferred by studying the feasible region and the figure of merit graphically in the (x,z) plane (Appendix B). The end result is:

$$p_{10}(\delta,1) = p^c_{10}(\delta,1) \,+\, x^*\,\frac{2\cos 2\theta}{2+\sin 2\theta} \qquad (9)$$

where $x^* = \max(x_0, x_1)$ is the optimal value of x determined by

$$\begin{aligned} x_0 &= (1-\delta)\left(\frac{\cos 2\theta - \sqrt{1+2\sin 2\theta}}{2+\sin 2\theta}\right)\,, \\ x_1 &= -\frac{\delta\cos 2\theta + \sqrt{\delta^2(1+2\sin 2\theta) + 2\delta(2+\sin 2\theta)}}{2+\sin 2\theta}\,. \end{aligned} \qquad (10)$$

Since both x_0 and x_1 are non-positive, $p_{10}(\delta,1) \leq p^c_{10}(\delta,1)$ as expected. Notice that (9) captures also the case $\theta = \frac{\pi}{4}$ (only, x^* is not unique in that case). Besides, $x_0 = 0$ holds only for $\cos 2\theta = 1$ i.e. for the product state; and $x_1 = 0$ holds only for $\delta = 0$. In summary, for $\epsilon = 1$, $0 < \delta < 1$, and $0 < \theta < \frac{\pi}{4}$, the optimal strategy is *not* the commuting one.

Since we have set $\epsilon = 1$, which means that σ can be orthogonal to $|\psi\rangle$, it is natural to check also when $p_{10}(\delta,1) = 0$, which would be obviously the case if we

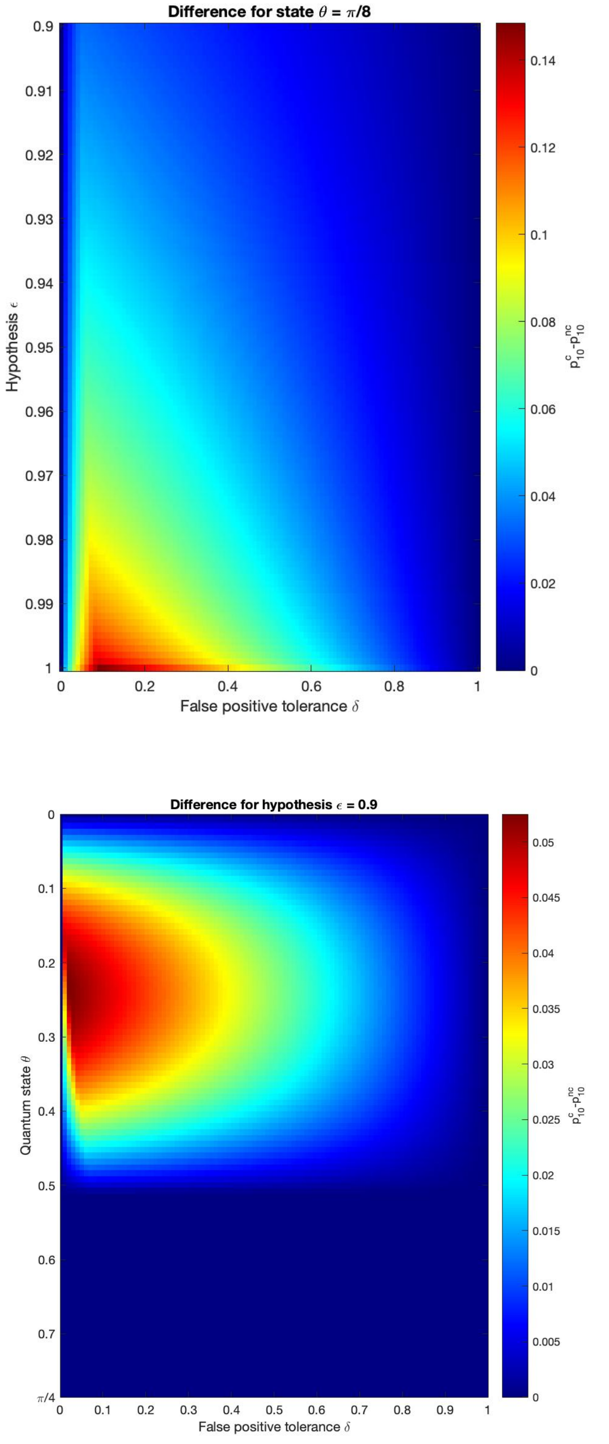

Figure 1: Difference $p^c_{10}(\delta,\epsilon) - p_{10}(\delta,\epsilon)$ between worst-case type II error probability for commuting and non-commuting strategies. Upper panel: in the plane (δ,ϵ) for fixed state $\theta = \pi/8$. For values of $\epsilon \in [0, 0.9]$ the difference is negligible and has been omitted from the plot. Lower panel: in the plane (δ,θ) for fixed $\epsilon = 0.9$.

had not added the constraint that Ω must be separable. By inspection, we see that this is the case only for $\theta = 0$, i.e. when the state itself is product (in which case it is trivial: one can find an orthogonal product state and check the orthogonality locally).

4.3 Numerical solutions of the SDP

We have seen that, even in the case $\epsilon = 1$ when the figure of merit is at its simplest, the analytical solution requires some work and yields a not-so-transparent result. In view of this, for arbitrary values of ϵ we leave aside any attempt of solving the optimisation (6) analytically, and resort rather to numerical solutions of the SDP (2).

The results are presented in Fig. 1. We see that, in a large portion of parameter space, a commuting strategy is very close to being optimal (if not exactly so). A significant difference is seen only for $\epsilon \gtrsim 0.8$, that is, when the state σ is allowed to be almost orthogonal to $|\psi\rangle$.

5 Conclusions

We have worked in the quantum hypothesis testing scenario that has been called "quantum state verification", in which the the null hypothesis is a pure state $|\psi\rangle$, while the alternative hypothesis may be any state σ that is "distinguishable enough" from $|\psi\rangle$ (quantified by $\langle\psi|\sigma|\psi\rangle \leq 1-\epsilon$). Like previous works, we focused on entangled states shared by two distant players, and studied hypothesis testing under separable operations. We studied the tradeoff between the probability of false negative and that of false positive (the latter had been set to zero in previous studies, which amounts at assuming that the optimal POVM for the discrimination is implemented perfectly). The bilinear nature of the resulting optimization is overcome by reformulating the problem as a SDP. Then we presented the detailed solution for the case of two qubits, including analytical results for some extreme cases. We showed that, in general, the solution is a non-trivial modification of previous constructions: in particular, the optimal POVM may not commute with the closest state σ.

Acknowledgements

We thank Masahito Hayashi for discussions about our modifications of the hypotheses, and more generally the connection between quantum verification and hypothesis testing. This work is supported by the National Research Foundation and the Ministry of Education, Singapore, under the Research Centres of Excellence programme. L.P.T acknowledges support from the Alexander von Humboldt Foundation. M. D. acknowledges support from MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant No. JPMXS0118067285, JSPS KAKENHI Grant Number JP20K03774, and the International Research Unit of Quantum Information, Kyoto University.

References

[1] Holevo A. *Probabilistic and Statistical Aspects of Quantum Theory*. North-Holland, Amsterdam, 1st edition, 1982. DOI: 10.1007/978-88-7642-378-9. URL https://doi.org/10.1007/978-88-7642-378-9.

[2] A. Acín. Statistical distinguishability between unitary operations. *Phys. Rev. Lett.*, 87:177901, Oct 2001. DOI: 10.1103/PhysRevLett.87.177901. URL https://link.aps.org/doi/10.1103/PhysRevLett.87.177901.

[3] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, jan 2015. DOI: 10.1088/1751-8113/48/8/083001. URL https://doi.org/10.1088%2F1751-8113%2F48%2F8%2F083001.

[4] Alessandro Bisio, Michele Dall'Arno, and Giacomo Mauro D'Ariano. Tradeoff between energy and error in the discrimination of quantum-optical devices. *Phys. Rev. A*, 84:012310, 2011. DOI: 10.1103/PhysRevA.84.012310.

[5] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004. DOI: 10.1017/CBO9780511804441.

[6] J. Calsamiglia, J. I. de Vicente, R. Muñoz Tapia, and E. Bagan. Local discrimination of mixed states. *Phys. Rev. Lett.*, 105:080504, Aug 2010. DOI: 10.1103/PhysRevLett.105.080504. URL https://link.aps.org/doi/10.1103/PhysRevLett.105.080504.

[7] Andrew M. Childs, John Preskill, and Joseph Renes. Quantum information and precision measurement. *Journal of Modern Optics*, 47(2-3):155–176, 2000. DOI: 10.1080/09500340008244034. URL https://www.tandfonline.com/doi/abs/10.1080/09500340008244034.

[8] Sarah Croke, Erika Andersson, Stephen M. Barnett, Claire R. Gilson, and John Jeffers. Maximum confidence quantum measurements. *Phys. Rev. Lett.*, 96:070401, Feb 2006. DOI: 10.1103/PhysRevLett.96.070401. URL https://link.aps.org/doi/10.1103/PhysRevLett.96.070401.

[9] Michele Dall'Arno, Alessandro Bisio, Giacomo Mauro D'Ariano, Martina Mikova, Miroslav Jezek, and Miloslav Dusek. Experimental implementation of unambiguous quantum reading. *Phys. Rev. A*, 85:012308, 2012. DOI: 10.1103/PhysRevA.85.012308.

[10] A. C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett.*, 88:187904, Apr 2002. DOI: 10.1103/PhysRevLett.88.187904. URL `https://link.aps.org/doi/10.1103/PhysRevLett.88.187904`.

[11] Aram W. Harrow, Anand Natarajan, and Xiaodi Wu. An improved semidefinite programming hierarchy for testing entanglement. *Communications in Mathematical Physics*, 352(3):881–904, Jun 2017. ISSN 1432-0916. DOI: 10.1007/s00220-017-2859-0. URL `https://doi.org/10.1007/s00220-017-2859-0`.

[12] A. Hayashi, T. Hashimoto, and M. Horibe. State discrimination with error margin and its locality. *Phys. Rev. A*, 78:012333, Jul 2008. DOI: 10.1103/PhysRevA.78.012333. URL `https://link.aps.org/doi/10.1103/PhysRevA.78.012333`.

[13] M. Hayashi and H. Nagaoka. General formulas for capacity of classical-quantum channels. *IEEE Transactions on Information Theory*, 49(7):1753–1768, July 2003. DOI: 10.1109/TIT.2003.813556.

[14] Masahito Hayashi. Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing. *New Journal of Physics*, 11(4):043028, apr 2009. DOI: 10.1088/1367-2630/11/4/043028. URL `https://doi.org/10.1088%2F1367-2630%2F11%2F4%2F043028`.

[15] Masahito Hayashi, Keiji Matsumoto, and Yoshiyuki Tsuda. A study of LOCC-detection of a maximally entangled state using hypothesis testing. *Journal of Physics A: Mathematical and General*, 39(46):14427–14446, nov 2006. DOI: 10.1088/0305-4470/39/46/013. URL `https://doi.org/10.1088%2F0305-4470%2F39%2F46%2F013`.

[16] Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1 (2):231–252, 1969. DOI: 10.1007/BF01007479.

[17] Z. Hradil. Quantum-state estimation. *Phys. Rev. A*, 55:R1561–R1564, Mar 1997. DOI: 10.1103/PhysRevA.55.R1561. URL `https://link.aps.org/doi/10.1103/PhysRevA.55.R1561`.

[18] Ye-Chao Liu, Xiao-Dong Yu, Jiangwei Shang, Huangjun Zhu, and Xiangdong Zhang. Efficient verification of dicke states. *Phys. Rev. Applied*, 12:044020, Oct 2019. DOI: 10.1103/PhysRevApplied.12.044020. URL `https://link.aps.org/doi/10.1103/PhysRevApplied.12.044020`.

[19] Seth Lloyd. Enhanced sensitivity of photodetection via quantum illumination. *Science*, 321(5895):1463–1465, 2008. ISSN 0036-8075. DOI: 10.1126/science.1160627. URL `https://science.sciencemag.org/content/321/5895/1463`.

[20] Sam Pallister, Noah Linden, and Ashley Montanaro. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.*, 120:170502, Apr 2018. DOI: 10.1103/PhysRevLett.120.170502. URL `https://link.aps.org/doi/10.1103/PhysRevLett.120.170502`.

[21] Matteo Paris and Jaroslav Rehacek. *Quantum State Estimation.* Springer Publishing Company, Incorporated, 1st edition, 2010. ISBN 3642061036, 9783642061035. DOI: 10.1007/b98673.

[22] Stefano Pirandola. Quantum reading of a classical digital memory. *Phys. Rev. Lett.*, 106:090504, Mar 2011. DOI: 10.1103/PhysRevLett.106.090504. URL `https://link.aps.org/doi/10.1103/PhysRevLett.106.090504`.

[23] Yuki Takeuchi and Tomoyuki Morimae. Verification of many-qubit states. *Phys. Rev. X*, 8:021060, Jun 2018. DOI: 10.1103/PhysRevX.8.021060. URL `https://link.aps.org/doi/10.1103/PhysRevX.8.021060`.

[24] Kun Wang and Masahito Hayashi. Optimal verification of two-qubit pure states. *Phys. Rev. A*, 100:032315, Sep 2019. DOI: 10.1103/PhysRevA.100.032315. URL `https://link.aps.org/doi/10.1103/PhysRevA.100.032315`.

[25] Xiao-Dong Yu, Jiangwei Shang, and Otfried Gühne. Optimal verification of general bipartite pure states. *npj Quantum Information*, 5(1):112, 2019. ISSN 2056-6387. DOI: 10.1038/s41534-019-0226-z. URL `https://doi.org/10.1038/s41534-019-0226-z`.

[26] Huangjun Zhu and Masahito Hayashi. Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A*, 99:052346, May 2019. DOI: 10.1103/PhysRevA.99.052346. URL `https://link.aps.org/doi/10.1103/PhysRevA.99.052346`.

[27] Huangjun Zhu and Masahito Hayashi. Efficient verification of hypergraph states. *Phys. Rev. Applied*, 12:054047, Nov 2019. DOI: 10.1103/PhysRevApplied.12.054047. URL `https://link.aps.org/doi/10.1103/PhysRevApplied.12.054047`.

A Solution of the inner optimisation

In this Appendix, we show how to go from Lemma 2 to Lemma 3, while proving a few other intermediate results.

We begin by simplifying the inequality constraints on $t+z$ and ω.

Lemma 4. *Without loss of generality, the optimisa-*

tion (3) *in Lemma* 2 *becomes*

$$\begin{aligned} p_{10}(\delta,\epsilon) = \min_{t,z,x,y_1,y_2} \; & y_1 + (1-\epsilon) y_2 \\ \textit{s. t.} \; & 0 \preceq \begin{pmatrix} t+z & x \\ x & t-z \end{pmatrix} \preceq \mathbb{1} \\ & t+z = 1-\delta \\ & \begin{pmatrix} y_1+y_2-(t+z) & -x \\ -x & y_1-(t-z) \end{pmatrix} \succeq 0 \\ & y_1 \geq \omega := |x\cos 2\theta + z \sin 2\theta| \\ & y_1 \in \mathbb{R}, y_2 \geq 0 \end{aligned} \tag{11}$$

Proof. With the notation introduced in the proof of Lemma 2, for any feasible $(\bar{\Omega}_a, y_1, y_2)$ with $\langle\psi|\,\bar{\Omega}_a\,|\psi\rangle > 1-\delta \geq 0$ for $\delta \in [0,1]$ there is another feasible $(\bar{\Omega}'_a, y_1, y_2)$, where

$$\bar{\Omega}'_a = \frac{(1-\delta)}{\langle\psi|\,\bar{\Omega}_a\,|\psi\rangle}\bar{\Omega}_a$$

ensures $\langle\psi|\,\bar{\Omega}'_a\,|\psi\rangle = 1-\delta$, achieving the same objective value, we can without loss of generality assume that $t+z = 1-\delta$.

It is clear that by reducing ω, we increase the size of the feasible region of the inner optimisation over variables y_1, y_2. Therefore since $|x\cos 2\theta + z\sin 2\theta| \leq 1$ follows from other constraints, we have that $0 \leq |x\cos 2\theta + z\sin 2\theta| \leq \omega \leq 1$, which means it suffices to take ω equal the lower bound. □

We now solve the inner optimisation, that is the optimisation over y_1 and y_2. It is natural to split our consideration into commuting strategy $x=0$ and non-commuting strategy $x \neq 0$, as the commuting case is a simpler linear programming problem.

Lemma 5. *For the commuting strategy $x = 0$, the solution of the inner optimisation is*

$$y_1^* + (1-\epsilon)\max\{0, t+z-y_1^*\} \tag{12}$$

where $y_1^* := \max\{t-z, |z\sin 2\theta|\}$.

Proof. By Sylvester's criterion for psd, the inner minimization becomes

$$\begin{aligned} \min_{y_1,y_2} \; & y_1 + (1-\epsilon) y_2 \\ \text{s. t.} \; & y_1 + y_2 - (t+z) \geq 0 \\ & y_1 - (t-z) \geq 0 \\ & (y_1+y_2-(t+z))(y_1-(t-z)) \geq x^2 \\ & y_1 \geq |x\cos 2\theta + z\sin 2\theta|, y_2 \geq 0 \end{aligned}$$

When $x = 0$ the quadratic constraint trivially follows from the inequality constraints so we can drop it and the optimisation is linear. The constraints are

$$\begin{aligned} y_1 &\geq \max\{t-z, |x\cos 2\theta + z\sin 2\theta|\} \\ y_2 &\geq \max\{0, (t+z) - y_1\} \end{aligned}$$

so that the minimum is reached at the lower bounds. □

Lemma 6. *For the commuting strategy $x = 0$, the optimal error probability is given by*

$$p_{10}(\delta,\epsilon) = (1-\delta)\left[1 - \frac{\epsilon}{1+\sin\theta\cos\theta}\right] \tag{13}$$

Proof. Since $x = 0$, we are left with the program

$$\begin{aligned} \min_z \; & y_1^* + (1-\epsilon)\max\{0, t+z-y_1^*\} \\ \text{s. t.} \; & 0 \leq t-z \leq 1 \\ & t+z = 1-\delta \\ & y_1^* := \max\{t-z, |z\sin 2\theta|\} \end{aligned}$$

The objective function can be rewritten as

$$\max\{y_1^*, (1-\epsilon)(1-\delta) + \epsilon y_1^*\}$$

from which we consider two cases. If $y_1^* \geq 1-\delta$ then

$$\begin{aligned} \min_z \; & y_1^* \\ \text{s. t.} \; & 0 \leq 1-\delta-2z \leq 1 \\ & y_1^* := \max\{1-\delta-2z, |z\sin 2\theta|\} \geq 1-\delta \end{aligned}$$

Here $y_1^* \geq 0$ always, so the minimum is at least $1-\delta$. If $y_1^* \leq 1-\delta$ then

$$\begin{aligned} \min_z \; & (1-\epsilon)(1-\delta) + \epsilon y_1^* \\ \text{s. t.} \; & 0 \leq 1-\delta-2z \leq 1 \\ & y_1^* := \max\{1-\delta-2z, |z\sin 2\theta|\} \leq 1-\delta \end{aligned}$$

It is straightforward to see that the minimum is achieved when

$$0 \leq 1-\delta-2z = |z\sin 2\theta| \leq 1-\delta$$

corresponding to an optimal solution $z^* = \frac{1-\delta}{2+\sin 2\theta}$ with optimum value

$$(1-\delta)\left[1 - \frac{\epsilon}{1+\sin\theta\cos\theta}\right].$$

Since the global minimum is the smaller value of these two cases, the proof of the Lemma is complete. □

We remark that the structure of the optimal verification operator among all commuting strategies is rather simple. Explicitly we have that

$$\Omega^* = \begin{pmatrix} 1-\delta & 0 & 0 & 0 \\ 0 & \omega^* & 0 & 0 \\ 0 & 0 & \omega^* & 0 \\ 0 & 0 & 0 & \omega^* \end{pmatrix}, \quad \omega^* = \frac{(1-\delta)\sin 2\theta}{2+\sin 2\theta}. \tag{14}$$

This can be seen as a generalization of the optimal commuting strategy that Wang and Hayashi found for $\delta = 0$ case [24] to the $\delta \in [0,1]$ case.

We now consider the noncommuting case, which is no longer a linear optimisation problem.

Lemma 7. *For the noncommuting strategy $x \neq 0$, the solution of the inner optimisation is*

$$y_1^* + (1-\epsilon)\left[(t+z) - y_1^* + \frac{x^2}{y_1^* - (t-z)}\right] \tag{15}$$

with the value

$$y_1^* = \begin{cases} \omega \text{ if } \hat{y}_1 \leq \omega \\ \hat{y}_1 \text{ if } \omega < \hat{y}_1 < t + \sqrt{x^2+z^2} \\ t + \sqrt{x^2+z^2} \text{ if } \hat{y}_1 > t + \sqrt{x^2+z^2} \end{cases} \tag{16}$$

for $\omega = |x\cos 2\theta + z \sin 2\theta|$ *and* $\hat{y}_1 = (t-z) + \sqrt{\frac{1-\epsilon}{\epsilon}}|x|$.

Proof. When $x \neq 0$ (noncommuting strategy), the feasible region excludes the points (y_1, y_2) where

$$y_1 - (t-z) = 0, \text{ or } y_1 + y_2 - (t+z) = 0$$

and so the optimisation becomes

$$\begin{aligned} &\min_{y_1,y_2} y_1 + (1-\epsilon)y_2 \\ &\text{s. t. } y_1 > t-z, y_1 \geq \omega \\ &\qquad y_2 \geq \max\left\{0, (t+z) - y_1 + \frac{x^2}{y_1-(t-z)}\right\} \end{aligned}$$

Here the optimisation splits into two branches. Firstly, consider the branch

$$(t+z) - y_1 + \frac{x^2}{y_1 - (t-z)} \leq 0$$

equivalently under the condition $y_1 > t-z$

$$((t-z) - y_1)((t+z) - y_1) - x^2 \geq 0$$

and explicitly in terms of the roots

$$\begin{aligned} y_1 &\leq \lambda_{\min} := t - \sqrt{x^2+z^2} \text{ or },\\ y_1 &\geq \lambda_{\max} := t + \sqrt{x^2+z^2} \end{aligned}$$

But then $t - \sqrt{x^2+z^2} < t - z < t + \sqrt{x^2+z^2}$ implies that the feasible region is $y_1 \geq \max\{\omega, \lambda_{\max}\}$ leading to the optimum value $y_1^* = \max\{\omega, \lambda_{\max}\}$ which is always at least $\lambda_{\max}$. Secondly, the remaining branch

$$(t+z) - y_1 + \frac{x^2}{y_1-(t-z)} \geq 0\,,$$

which is equivalent to

$$t - \sqrt{x^2+z^2} =: \lambda_{\min} \leq y_1 \leq \lambda_{\max} := t + \sqrt{x^2+z^2}$$

could be infeasible depending on ω. However, whenever feasible, i.e. $\omega \leq \lambda_{\max}$, the minimum is upper bounded by the value of the objective function

$$y_1 + (1-\epsilon)\left[(t+z) - y_1 + \frac{x^2}{y_1-(t-z)}\right]$$

at the feasible point $y_1 = \lambda_{\max}$, i.e. for which the objective value is $\lambda_{\max} + (1-\epsilon) * 0$. Therefore, without loss of generality we consider this latter branch whenever feasible.

The inner optimisation becomes

$$\begin{aligned} &\min_{y_1} y_1 + (1-\epsilon)\left[(t+z) - y_1 + \frac{x^2}{y_1-(t-z)}\right] \\ &\text{s. t. } y_1 > t-z, \omega \leq y_1 \leq \lambda_{\max}, \omega \leq \lambda_{\max} \end{aligned}$$

from which is is clear that the minimum is reached at the stationary point $\hat{y}_1$ which is the largest solution of

$$\epsilon(\hat{y}_1 - (t-z))^2 = (1-\epsilon)x^2$$

whenever this point is feasible, or at the endpoints ω if $y_1^* < \omega$ and $\lambda_{\max}$ if $y_1^* > \lambda_{\max}$. (Note that $x \neq 0$ ensures $\hat{y}_1 > t-z$ if exists so that the smallest solution is always infeasible.) □

Finally, we present the proof of Lemma 3:

Proof. With y_1^* given before, we have to solve

$$\begin{aligned} p_{10}(\delta,\epsilon) = &\min_{t,z,x} f(y_1^*) \\ &\text{s. t. } 0 \preceq \begin{pmatrix} t+z & x \\ x & t-z \end{pmatrix} \preceq \mathbb{1} \\ &\qquad t+z = 1-\delta \end{aligned} \tag{17}$$

This becomes an optimisation over two real variables z, x after eliminating t. To see the branch reduction, we consider feasible (z,x) that satisfies

$$0 \preceq \begin{pmatrix} 1-\delta & x \\ x & 1-\delta-2z \end{pmatrix} \preceq \mathbb{1} \tag{18}$$

and show that objective value (abuse of notation and redefine the function f eliminating variable t)

$$f(y_1^*) := y_1^* + (1-\epsilon)\left[1 - \delta - y_1^* + \frac{x^2}{y_1^* - (1-\delta-2z)}\right]$$

is smaller in the region **I** defined by

$$1 - \delta - 2z + \sqrt{\frac{1-\epsilon}{\epsilon}}|x| \leq |x\cos 2\theta + z\sin 2\theta|\,.$$

In the region **III** defined by the inequality

$$1 - \delta - 2z + \sqrt{\frac{1-\epsilon}{\epsilon}}|x| \geq 1 - \delta - z + \sqrt{x^2+z^2}$$

the objective function takes the value

$$\begin{aligned} &f(1-\delta-z+\sqrt{x^2+z^2}) \\ &= (1-\delta) + \epsilon(-z+\sqrt{x^2+z^2}) + \frac{(1-\epsilon)x^2}{z+\sqrt{x^2+z^2}} \\ &= (1-\delta) + \epsilon(-z+\sqrt{x^2+z^2}) - (1-\epsilon)(z-\sqrt{x^2+z^2}) \\ &= 1-\delta-z+\sqrt{x^2+z^2} \end{aligned}$$

which is a function of two independent variables z, x, and is increasing in terms of $|x|$ for a fixed value of z.

Likewise, in the region **II** defined by the inequality

$$\begin{aligned}|x\cos 2\theta + z\sin 2\theta| &\le 1-\delta-2z+\sqrt{\frac{1-\epsilon}{\epsilon}}|x| \\ &\le 1-\delta-z+\sqrt{x^2+z^2}\end{aligned}$$

the objective function take the value

$$\begin{aligned}&f\left(1-\delta-2z+\sqrt{\frac{1-\epsilon}{\epsilon}}|x|\right) \\ &= (1-\epsilon)(1-\delta)+\epsilon\left(1-\delta-2z+\sqrt{\frac{1-\epsilon}{\epsilon}}|x|\right)+\epsilon \\ &= (1-\delta)+\epsilon-2\epsilon z+\sqrt{\epsilon(1-\epsilon)}|x|\,,\end{aligned}$$

which is also increasing in $|x|$. Moreover, at the boundary between two regions, the objective functions agree.

The argument now goes as follows: for each feasible z, we look at the set of feasible x that is defined by (18). For any feasible x_1, x_2 in region **III** (if exist), since the objective function is increasing, the point with smaller $|x_j|$ achieves a lower objective value. Hence for minimization, it suffices to consider feasible x in the boundary of region **III**. Since this boundary is also contained in region **II**, we have shown that without loss of generality it suffices to consider the feasible x that belong to regions **I** and **II**. Now the argument can be repeated: points x_3, x_4 in region **II** with smaller $|x_j|$ achieve small objective value. This reduces the feasible region to region **I** only. □

B The optimal solution for $\epsilon = 1$

In this Appendix, we proceed to solve (8).

The feasible region is the intersection of three regions in the (x, z) plane:

- The constraint $1-\delta-z-\sqrt{x^2+z^2} \ge 0$ defines the region

$$\mathbf{P_0} : z \le -\frac{x^2}{2(1-\delta)}+\frac{1-\delta}{2}\,, \qquad (19)$$

upper-bounded by a parabola whose maximum at $(x,z) = (0, \frac{1-\delta}{2})$.

- The constraint $1-\delta-z+\sqrt{x^2+z^2} \le 1$ defines the region

$$\mathbf{P_1} : z \ge \frac{x^2}{2\delta}-\frac{\delta}{2}\,, \qquad (20)$$

lower-bounded by parabola whose minimum is at $(x,z) = (0, -\frac{\delta}{2})$

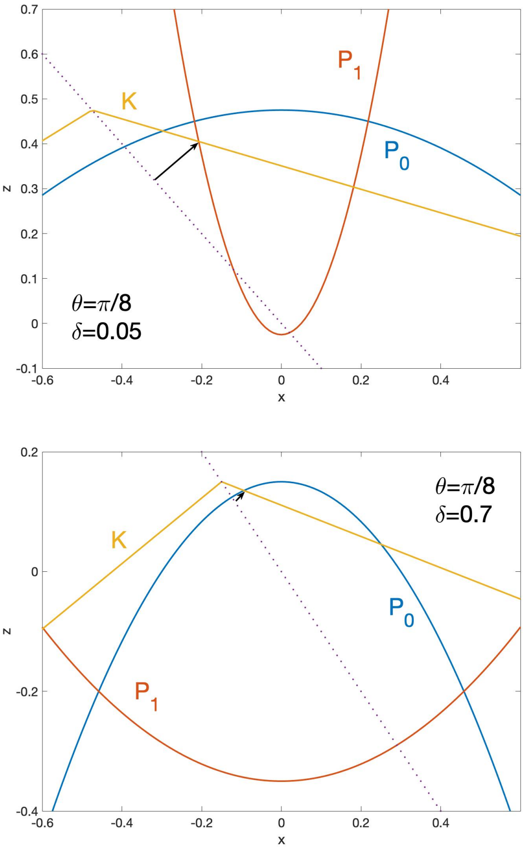

Figure 2: Graphic determination of the solution of the optimisation (8). These two examples are plotted for $\theta = \frac{\pi}{8}$ and two values of δ. The solid lines are the boundaries of the regions defined in Eqs (19), (20) and (21). The dotted line is $z = -\cot 2\theta x$: the solution of the optimisation is the point of the feasible region that is closest to this line, in either direction. For small δ, the solution is at the intersection $x_1 < 0$ of $\mathbf{P_1}$ and $\mathbf{K}$; for large δ, at the intersection $x_0 < 0$ of $\mathbf{P_0}$ and $\mathbf{K}$.

- The constraint $1-\delta-2z \le |x\cos 2\theta + z\sin 2\theta|$ defines the region

$$\mathbf{K} : \begin{cases} z \ge \frac{1-\delta+x\cos 2\theta}{2-\sin 2\theta} & \text{for} \quad x \le x_k \\ z \ge \frac{1-\delta-x\cos 2\theta}{2+\sin 2\theta} & \text{for} \quad x \ge x_k \end{cases} \qquad (21)$$

lower-bounded by a broken line with kink at $x_k = -\frac{1-\delta}{2}\tan(2\theta)$ the intersection with $x\cos 2\theta + z\sin 2\theta = 0$.

The figure of merit to be minimised is $|x\cos 2\theta + z\sin 2\theta|$: this means that $p_{10}(\delta,\epsilon)$ is given by the smallest distance between the line $z = -\cot 2\theta x$ and a point of the feasible region. A graphical inspection (see Figs 2 and 3) shows that this minimal distance is always achieved by the point that is the intersection of either $\mathbf{P_0}$ or $\mathbf{P_1}$ with the line $z \ge \frac{1-\delta-x\cos 2\theta}{2+\sin 2\theta}$. These are the points whose x coordinates have been called x_0 and x_1, given in Eq. (10) in the main text. A more fully analytical proof of this result would not bring further clarity (and for good measure, the correctness of the result has been double-checked numerically with the solution of the corresponding SDP).

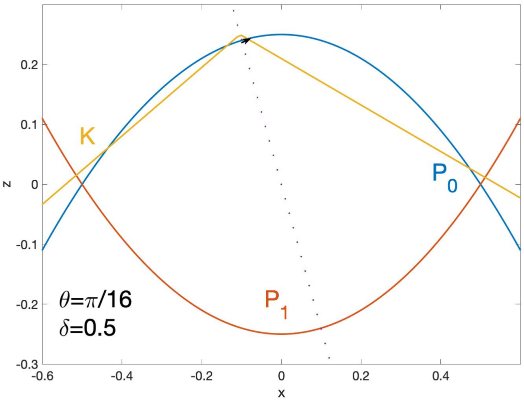

Figure 3: When θ is reduced, the slope of the left segment of K increases and also cuts P_0, whence the feasible region consists of two disjoint sets. Nonetheless, the closest point to the line $z = -\cot 2\theta x$ remains the one on the right segment of K.