UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Local simultaneous state discrimination

Majenz, C.; Ozols, M.; Schaffner, C.; Tahmasbi, M.

DOI
10.48550/arXiv.2111.01209
10.1103/PhysRevA.109.052217

Publication date
2024

Document Version
Submitted manuscript

Published in
Physical Review A

License
CC BY

Link to publication

Citation for published version (APA):
Majenz, C., Ozols, M., Schaffner, C., & Tahmasbi, M. (2024). Local simultaneous state discrimination. *Physical Review A*, *109*(5), Article 052217. https://doi.org/10.48550/arXiv.2111.01209, https://doi.org/10.1103/PhysRevA.109.052217

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:08 11月 2026

arXiv:2111.01209v1 [quant-ph] 1 Nov 2021

Local simultaneous state discrimination

Christian Majenz*[1], Maris Ozols†[2], Christian Schaffner‡[3], and Mehrdad Tahmasbi§[4]

[1] *Department of Applied Mathematics and Computer Science, Technical University of Denmark*
[2] *Institute for Logic, Language, and Computation, Korteweg-de Vries Institute for Mathematics, and Institute for Theoretical Physics, University of Amsterdam and QuSoft*
[3] *Institute for Logic, Language, and Computation, University of Amsterdam and QuSoft*
[4] *Centrum Wiskunde & Informatica and QuSoft*

November 3, 2021

Abstract

Quantum state discrimination is one of the most fundamental problems studied in quantum information theory. Applications range from channel coding to metrology and cryptography. In this work, we introduce a new variant of this task: Local Simultaneous State Discrimination (LSSD). While previous distributed variants of the discrimination problem always allowed some communication between the parties to come up with a joint answer, the parties in LSSD cannot communicate and have to simultaneously answer correctly. This simultaneity implies, e.g., that for classical states, the problem does not trivialize to a non-distributed distinguishing task. While interesting in its own right, this problem also arises in quantum cryptography.

After introducing the problem, we give a number of characterization results. We give examples showing that i) the optimal strategy for local discrimination need not coincide with the optimal strategy for LSSD, even for classical states, ii) an additional entangled resource can increase the optimal success probability in LSSD, and iii) stronger-than-quantum non-signalling resources can allow for a higher success probability in some cases, compared to strategies using entanglement. Finally, we show that finding the optimal strategy in (classical) 3-party LSSD is NP-hard.

1 Introduction

Discriminating between a known set of quantum states is a well-studied and fundamental problem in quantum information theory, with a vast range of applications ranging from cryptography and quantum computing to quantum information and metrology [BK15]. A referee randomly picks a quantum state from a known set of states and sends it to Alice who tries to determine which state was sent to her. An interesting extension of the problem is *distributed* state discrimination where the states to be distinguished are bi-partite and Alice gets to examine register A and Bob register B. In the context of nonlocality, the most commonly considered scenario is *LOCC* where Alice and Bob are allowed to use *local operations and classical communication* in the discrimination process [CLM+14]. For example, any orthonormal set of product states can be prepared by local operations and discriminated by a global one, however discriminating them with only local operations is generally not possible, even when classical communication between parties is allowed [BDF+99, CLMO13]. In the LOCC setting, the discrimination task does not become more demanding by asking Alice and Bob to answer correctly *simultaneously* since the result can be communicated between the parties.

Surprisingly, the more restricted scenario where Alice and Bob can only use *local operations (LO)* without any classical communication has received only little attention in the published literature so far,

*chmaj@dtu.dk
†marozols@gmail.com
‡c.schaffner@uva.nl
§mehrdad@cwi.nl

see below for related work. In this scenario, asking both Alice and Bob to succeed simultaneously makes the task strictly more difficult compared with the case when at least one of the players should succeed. We call the resulting task *local simultaneous state discrimination (LSSD)*.

While LSSD is certainly interesting in its own right, one concrete motivation — in fact, our original motivation — comes from quantum cryptography. Here, one line of work has studied *unclonable cryptography* [Wie83, BB84, Got03, Aar09, BL20, ALL+21, CLLZ21, MST21]. An unclonable cryptographic scheme is a scheme where a certain asset (like a token, message or functionality) is encrypted in a way that makes it impossible to copy. Such features are clearly impossible to achieve with purely classical means, and constructions make crucial use of the so-called *quantum no-cloning principle* that states that quantum information, in general, cannot be copied. The general idea of using the no-cloning principle dates back to Wiesner [Wie83] who proposed a *quantum money* scheme where banknotes are quantum states, preventing copying. Later, quantum copy protection [Aar09, ALL+21, ALP21, CMP20] and unclonable encryption [BL20] were introduced, which provide more sophisticated assets in an unclonable way. Strengthening the standard encryption security notion of indistinguishability to *indistinguishable unclonability* [BL20] yields a security game that requires the adversary to perform LSSD.

Another motivation comes from the foundations of quantum mechanics. Quantum non-locality is a well-studied fundamental feature of quantum theory which has been key to charting the foundations of quantum physics. In particular, the characterization of non-local quantum correlations, both mathematically and operationally, constitutes a decades-old challenge, partially addressed by an impressive body of research (see, e.g., [BCP+14] and references therein). This work establishes LSSD as a new and natural member of the zoo of operational problems (like non-local games and zero-error communication settings) where the non-local nature of quantum correlations can provide an advantage over strategies restricted to purely classical means, and stronger-than-quantum non-local correlations (so-called non-signaling boxes) can provide an additional advantage.

1.1 Our contributions

In this work, we define and study the problem of *Local Simultaneous State Discrimination (LSSD)* which can be formalized by a tripartite cqq-state $\rho_{\mathsf{XAB}} = \sum_x P(x)|x\rangle\langle x|_{\mathsf{X}} \otimes \rho^x_{\mathsf{AB}}$, where the referee's register X is classical and ρ^x_{AB} are arbitrary two-partite quantum states. Alice and Bob act locally on their respective registers A and B to produce guesses x_A and x_B. They win the LSSD game if and only if both their guesses correctly identify the value x of the classical register X, i.e., $x = x_A = x_B$. As in non-local games, we can define optimal guessing probabilities by considering strategies for Alice and Bob that use different kinds of resources, namely: 1) shared randomness, 2) additional quantum entanglement, 3) non-signaling correlations. A priori, it is entirely unclear whether these extra resources allow Alice and Bob to increase their simultaneous guessing probability. The LSSD problem can also be naturally extended to more than two simultaneously distinguishing parties.

After setting the stage with these definitions, we provide a number of results for the LSSD problem where ρ_{XAB} is fully classical, i.e., Alice and Bob receive classical inputs a, b, correlated with the referee's x according to a joint distribution P_{XAB}. Our first result, Proposition 3.3, establishes that the three simultaneous guessing probabilities coincide if x, a, b are all bits. Additionally, if only a, b are bits, we prove a simple upper bound on the guessing probability with non-local correlations. In contrast, as our main contribution, we provide in Theorem 3.1 a simple distribution P_{XAB} for which the three simultaneous guessing probabilities defined above are strictly separated from each other. Hereby, we establish that as for non-local games, having entangled strategies is (in general) strictly more powerful than shared randomness (which in turn is easily seen to be useless, as for non-local games). Also, having stronger non-signaling strategies (using, e.g., a Popescu-Rorlich box [PR94]) can be strictly more powerful than entanglement in LSSD. Finally, in Section 4, we study the computational complexity of finding optimal simultaneous guessing strategies by investigating (again fully classical) problem instances naturally defined based on r-partite hypergraphs. By establishing a connection between simultaneous guessing and finding a maximum matching in 3-partite hypergraphs, we show that finding an optimal classical strategy for the three-party LSSD problem is NP-hard.

1.2 Related work

Earlier work by Buscemi [Bus12] studied a very general classof distributed tasks called "semi-quantum" non-local games where a referee picks from a fixed set a bi-partite quantum state and sends the registers as questions to two players Alice and Bob, and their answers are classical bitstrings. A subclass of such games, namely quantum *XOR games* have been studied in-depth by Regev and Vidick [RV15]. The restriction is that the players' answers are classical bits of which the referee only takes into account their XOR when computing the winning predicate. Our LSSD scenario is a similar subclass of semi-quantum games, where instead of the XOR condition, the players simultaneously have to guess the referee's choice. It is a very interesting open problem to investigate whether some of the results from quantum XOR games carry over to the LSSD setting. For instance, does there exist a family of games that can only be won optimally with an ever-increasing amount of entanglement?

Another notion of *extended non-local games* has been defined and investigated by Russo [Rus17]. In extended non-local games, the referee, Alice and Bob share a quantum state, but the referee's questions and player's answers remain classical. However, the winning predicate is computed by a measurement of the referee. This setting ties in well with monogamy-of-entanglement games [TFKW13], and it is shown in [Rus17] that some of the results [RV15] from quantum XOR games carry over to this setting. The main difference to our LSSD problem is that the initial quantum state is part of the players' strategy, and not prepared by the referee.

Another line of related work [MWW09, LW13, LPW18] studies the relation between various distinguishability norms with the goal of maximising the so-called data hiding ratio, i.e. how much worse restricted sets of measurements (such as local ones) perform in the task of state discrimination versus global measurements. In their setting, the "local operations" performed by the players can still be post-processed by the referee (akin to some form of communication), whereas in our LSSD setting, the players simultaneously have to guess the referee's input using only local measurements. This crucial difference is the reason why we observe interesting separations between the guessing probabilities already for the discrimination of fully classical states. When classical post-processing by a referee is allowed, the players can simply forward their classical inputs to the referee. Therefore, interesting effects in that setting only occur when distinguishing quantum inputs.

Very recent work in this line by Corrêa, Lami and Palazuelos [CLP21] is also concerned with optimal local discrimination. By a clever combination of previous results about data hiding and the noncommutative Grothendieck's theorem, the authors show that the ratio between the optimal global distinguishing measurement between two states and the optimal local measurement is at most $2\sqrt{2}d$ where d is the local dimension of Alice an Bob's system. Due to the classical post-processing by the referee, their results cannot easily be translated into our LSSD setting.

During the preparation of this manuscript, we have become aware of independent unpublished work by Chitambar and Mančinska [CM21] that also studies the LSSD problem for two bipartite quantum states that are in tensor product. This setting can be seen as a quantum version of our Example 1 below. It shows the same "two-regime behavior", where depending on a parameter, it is better to use the locally optimal discrimination strategy in one regime, whereas in the other regime, it is better for the players to correlate their errors.

1.3 Open problems

We believe that LSSD is a fascinating new problem in quantum information processing, as there are many associated open questions. Our results in this article are exclusively[1] concerned with the case where the referee uses classical states. How do the different success probabilities behave when distinguishing actual quantum states? Are there dimension constraints like in our Proposition 3.3 under which the classical and quantum values coincide?

As mentioned above, can the results about quantum XOR games from [RV15] be ported to LSSD? Does there exist a family of games that can only be won optimally with an ever-increasing amount of entanglement? Can we find efficiently computable lower or upper bounds on the various success probabilities?

While we establish the NP hardness of finding optimal classical distinguishing strategies for three parties, it is natural to ask whether the two-party LSSD problem is already hard.

[1] except Example 2, which we import from [MST21]

In terms of applications, we suggest to establish more links with uncloneable encryption and possibly with position-based cryptography.

1.4 Notation

We will denote by $\delta\big[\cdot\big]$ the indicator function that evaluates to one when its argument is true and to zero otherwise. We will use $\mathscr{X}, \mathscr{A}, \mathscr{B}$, respectively, to denote the finite sets from which the inputs to the referee, Alice, and Bob are drawn. Their joint input is described by a probability distribution P_{XAB} on $\mathscr{X} \times \mathscr{A} \times \mathscr{B}$, wher the system X belongs to the referee while A and B belong to Alice and Bob, respectively. The input and output sets will often be of the form $[d] := \{0, \ldots, d-1\}$, for some integer $d \geq 1$.

When Alice and Bob's inputs are quantum, the overall input is a classical-quantum-quantum (cqq) state ρ_{XAB} where the classical register X belongs to the referee while the quantum registers A and B belong to Alice and Bob, respectively. We will denote the finite-dimensional complex Euclidean spaces underlying these registers by $\mathcal{X} = \mathbb{C}^{\mathscr{X}}$, $\mathcal{A} = \mathbb{C}^{\mathscr{A}}$, and $\mathcal{B} = \mathbb{C}^{\mathscr{B}}$.

A *quantum state* on $\mathbb{C}^d$ is a $d \times d$ positive semi-definite matrix of unit trace, i.e., $\rho \in \mathbb{C}^{d \times d}$ such that $\rho \succeq 0$ and $\operatorname{tr} \rho = 1$. We denote the set of all quantum states on $\mathbb{C}^d$ by $\mathrm{D}(\mathbb{C}^d)$. Operations on quantum states are described by *unitary* matrices, i.e., $U \in \mathbb{C}^{d \times d}$ such that $U^\dagger U = \mathbb{1}$ where $\mathbb{1}$ is the identity matrix. We denote the set of all unitaries on $\mathbb{C}^d$ by $\mathrm{U}(\mathbb{C}^d)$.

An n-outcome *measurement* or POVM on $\mathbb{C}^d$ is a collection of n positive semi-definite $d \times d$ matrices that sum to identity. We will denote a measurement by $M = \{M_1, \ldots, M_n\}$ where $M_i \succeq 0$ and $\sum_{i=1}^n M_i = \mathbb{1}$. We denote the set of all n-outcome measurements on $\mathbb{C}^d$ by $\mathrm{M}(\mathbb{C}^d)$ (since the outcome set is always clear from the context, we do not specify it). If $M_i^2 = M_i$ for all $i = 1, \ldots, n$, we call the measurement *projective*. We denote the set of all n-outcome projective measurements on $\mathbb{C}^d$ by $\mathrm{PM}(\mathbb{C}^d)$.

2 Local simultaneous state discrimination (LSSD) problem

A referee prepares a tripartite system XAB in a cqq state

$$\rho_{\mathsf{XAB}} = \sum_{x \in \mathscr{X}} P_{\mathsf{X}}(x) |x\rangle\langle x|_{\mathsf{X}} \otimes \rho^x_{\mathsf{AB}} \tag{1}$$

and passes the A and B subsystems to two distant parties, Alice and Bob, respectively, while keeping the system X. Alice and Bob know the state ρ_{XAB} and might share some resources (as will be precisely quantified later) prior to receiving their states, but no communication is allowed between them afterwards. Based on their received states and pre-shared resources, Alice and Bob output guesses x_A and x_B, respectively, to the referee. They win if both guesses are correct, i.e., $x = x_A = x_B$, and they aim at maximizing their probability of winning.

Most of our results are concerned with the case where ρ_{XAB} is completely classical, i.e., there exist orthonormal bases $\{|a\rangle : a \in \mathscr{A}\}$ and $\{|b\rangle : b \in \mathscr{B}\}$ for $\mathcal{A}$ and $\mathcal{B}$, respectively, that are independent of $x \in \mathscr{X}$, and probability distributions P^x_{AB} over $\mathscr{A} \times \mathscr{B}$ such that

$$\rho^x_{\mathsf{AB}} = \sum_{\substack{a \in \mathscr{A} \\ b \in \mathscr{B}}} P^x_{\mathsf{AB}}(a,b) |a\rangle\langle a|_{\mathsf{A}} \otimes |b\rangle\langle b|_{\mathsf{B}}. \tag{2}$$

Classical Strategies. In this case, there are no additional resources available to Alice and Bob beyond their received state.[2] The optimal probability of simultaneously guessing x correctly is

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_\rho := \sup_{\substack{M \in \mathrm{M}(\mathcal{A}) \\ N \in \mathrm{M}(\mathcal{B})}} \sum_{x \in \mathscr{X}} P_{\mathsf{X}}(x) \operatorname{tr}\big[\rho^x_{\mathsf{AB}}(M_x \otimes N_x)\big]. \tag{3}$$

[2] One can equivalently define classical strategies when only shared randomness is allowed between Alice and Bob. However, for the same reason as in non-local games, this purely classical resource does not help, as Alice and Bob could fix their randomness to a realization conditioned on which their probability of winning is maximized.

When ρ_{XAB} is classical and described by a probability distribution P_{XAB}, we can rewrite the optimal probability of winning as

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max_{\substack{Q_{\mathsf{X}_a|\mathsf{A}} \\ Q_{\mathsf{X}_b|\mathsf{B}}}} \sum_{\substack{x\in\mathscr{X} \\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) Q_{\mathsf{X}_a|\mathsf{A}}(x_a|a) Q_{\mathsf{X}_b|\mathsf{B}}(x_b|b) \tag{4}$$

$$\overset{(1)}{=} \max_{f,g} \sum_{\substack{x\in\mathscr{X} \\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\delta\big[f(a)=g(b)=x\big], \tag{5}$$

where the first maximum is taken over all conditional probability distributions $Q_{\mathsf{X}_a|\mathsf{A}}$ and $Q_{\mathsf{X}_b|\mathsf{B}}$, the second maximum is taken over all functions $f:\mathscr{A}\to\mathscr{X}$ and $g:\mathscr{B}\to\mathscr{X}$, and (1) follows since Alice and Bob can condition any local randomness on the realization that maximizes their probability of winning.

Quantum Strategies. In this case, Alice and Bob can share an entangled state prior to receiving their inputs. Let $\mathcal{A}' = \mathcal{B}' = \mathbb{C}^d$ be two complex Euclidean spaces of dimension d. Alice and Bob first jointly prepare a quantum state $\sigma_{\mathsf{A}'\mathsf{B}'}$ on $\mathcal{A}'\otimes\mathcal{B}'$, after which Alice and Bob keep systems A' and B', respectively. After receiving their inputs, Alice and Bob determine their output by measuring the registers AA' and BB' with local measurements M and N, respectively (this is the most general strategy because no communication is allowed).

When the local dimensions of the shared entangled state $\sigma_{\mathsf{A}'\mathsf{B}'}$ are limited to d for both parties, the optimal probability of winning is

$$\omega_{\mathrm{q}}^d(\mathsf{X}|\mathsf{A};\mathsf{B})_\rho := \sup_{\sigma_{\mathsf{A}'\mathsf{B}'}\in\mathrm{D}(\mathbb{C}^d\otimes\mathbb{C}^d)} \sup_{\substack{M\in\mathrm{M}(\mathcal{A}\otimes\mathbb{C}^d) \\ N\in\mathrm{M}(\mathcal{B}\otimes\mathbb{C}^d)}} \sum_{x\in\mathscr{X}} P_{\mathsf{X}}(x) \operatorname{tr}\big[(\rho_{\mathsf{AB}}^x\otimes\sigma_{\mathsf{A}'\mathsf{B}'})(M_x\otimes N_x)\big]. \tag{6}$$

When the dimensions of A' and B' are not limited, the optimal winning probability is

$$\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_\rho := \sup_{d\geq 1} \omega_{\mathrm{q}}^d(\mathsf{X}|\mathsf{A};\mathsf{B})_\rho. \tag{7}$$

When ρ_{XAB} is classical and described by a probability distribution P_{XAB}, we can simplify eq. (6) as follows:

$$\omega_{\mathrm{q}}^d(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{\sigma_{\mathsf{A}'\mathsf{B}'}\in\mathrm{D}(\mathbb{C}^d\otimes\mathbb{C}^d)} \sup_{\substack{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d) \\ N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)}} \sum_{\substack{x\in\mathscr{X} \\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) \operatorname{tr}\big[\sigma_{\mathsf{A}'\mathsf{B}'}\big(M_x(a)\otimes N_x(b)\big)\big] \tag{8}$$

$$= \sup_{\substack{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d) \\ N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)}} \left\| \sum_{\substack{x\in\mathscr{X} \\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a)\otimes N_x(b) \right\|, \tag{9}$$

where M and N are collections of measurements, i.e., for every input $a\in\mathscr{A}$ and $b\in\mathscr{B}$, we have that $M(a) = \{M_x(a) : x\in\mathscr{X}\}$ and $N(b) = \{N_x(b) : x\in\mathscr{X}\}$ are measurements on $\mathbb{C}^d$ with outcomes in $\mathscr{X}$. We show in Corollary B.2 that the optimization in $\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ can be restricted to projective measurements.

No-signaling Strategies. We define no-signaling strategies only when ρ_{XAB} is classical and described by a probability distribution P_{XAB}. Given classical inputs $a\in\mathscr{A}$ and $b\in\mathscr{B}$ for Alice and Bob, respectively, they output their estimates x_A and x_B of $x\in\mathscr{X}$ according to a conditional probability distribution $Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ on $\mathscr{X}\times\mathscr{X}\times\mathscr{A}\times\mathscr{B}$ satisfying

$$\forall x_B,a,a',b: \quad \sum_{x_A\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b) = \sum_{x_A\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a',b), \tag{10}$$

$$\forall x_A,a,b,b': \quad \sum_{x_B\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b) = \sum_{x_B\in\mathscr{X}} Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b'). \tag{11}$$

An optimal no-signaling strategy succeeds with probability

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P := \sup_{Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}} \sum_{\substack{x\in\mathscr{X} \\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x,x|a,b). \tag{12}$$

2.1 Examples

We discuss here two examples of LSSD games. The first example highlights particular features of LSSD such as the optimal local strategies are not necessarily optimal for simultaneous guessing, or the optimal guessing probability for product distributions is not the product of the optimal guessing probability of distributions in general. The second example is related to applications of LSSD to quantum cryptography.

Example 1. *Let X, Y, and Z be independent binary random variables such that $\Pr[X=1]=1/2$, $\Pr[Y=1]=\Pr[Z=1]=\alpha$ for some $0\leq\alpha\leq 1/2$. We also set $A:=X\oplus Y$ and $B:=X\oplus Z$ and denote the joint probability mass function of (X,A,B) by $P^{\alpha}_{\mathsf{XAB}}$. In other words, A and B are independent noisy versions of the uniform bit X. Consider the problem of simultaneously guessing X from A and B. When $1-\frac{1}{\sqrt{2}}<\alpha<\frac{1}{2}$, both parties always output 0 regardless of their inputs, which is a correct guess of X with probability $\frac{1}{2}$. When $0\leq\alpha\leq 1-\frac{1}{\sqrt{2}}$, Alice and Bob estimate X as A and B, respectively, which are simultaneously correct when $Y=Z=0$, an event that has probability $(1-\alpha)^2$. By a brute-force check, one finds that the aforementioned strategies are optimal without any extra resources and therefore*

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}=\begin{cases}\frac{1}{2} & 1-\frac{1}{\sqrt{2}}\leq\alpha\leq\frac{1}{2},\\ (1-\alpha)^2 & 0\leq\alpha\leq 1-\frac{1}{\sqrt{2}}.\end{cases} \tag{13}$$

Note that when $1-\frac{1}{\sqrt{2}}\leq\alpha\leq\frac{1}{2}$, optimal local estimators of X are not optimal for simultaneous guessing of X. We later show in Proposition 3.3 that when all X,A,B are binary, $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}=\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}=\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}$.

As a next observation, we set $\alpha:=1-\frac{1}{\sqrt{2}}$ and let (X',A',B') be an independent copy of (X,A,B). We consider the simultaneous guessing of (X,X') from (A,A') and (B,B'), and define a strategy as follows: both Alice and Bob output $(1,1)$ if their input bits are $(1,1)$ and output $(0,0)$ otherwise. The probability of simultaneously guessing correctly is

$$\frac{1}{4}(1-\alpha^2)^2+\frac{1}{4}(1-\alpha)^4\approx 0.271447. \tag{14}$$

Hence, $\omega_{\mathrm{c}}(\mathsf{XX'}|\mathsf{AA'};\mathsf{BB'})_{P^{\alpha}\times P^{\alpha}}>\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}\omega_{\mathrm{c}}(\mathsf{X'}|\mathsf{A'};\mathsf{B'})_{P^{\alpha}}$ while (X,A,B) and (X',A',B') are independent. Because $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}=\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}=\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}$, we also have

$$\omega_{\mathrm{q}}(\mathsf{XX'}|\mathsf{AA'};\mathsf{BB'})_{P^{\alpha}\times P^{\alpha}}>\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}\omega_{\mathrm{q}}(\mathsf{X'}|\mathsf{A'};\mathsf{B'})_{P^{\alpha}}, \tag{15}$$

$$\omega_{\mathrm{ns}}(\mathsf{XX'}|\mathsf{AA'};\mathsf{BB'})_{P^{\alpha}\times P^{\alpha}}>\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{P^{\alpha}}\omega_{\mathrm{ns}}(\mathsf{X'}|\mathsf{A'};\mathsf{B'})_{P^{\alpha}}. \tag{16}$$

Example 2. *Let $\mathcal{A}=\mathcal{B}=\mathbb{C}^3$ with an orthonormal basis $\{|0\rangle,|1\rangle,|\perp\rangle\}$ and let $|\phi^x\rangle_{\mathsf{AB}}:=\frac{1}{\sqrt{2}}(|x\rangle\otimes|\perp\rangle+|\perp\rangle\otimes|x\rangle)$ for $x\in[2]$. We also set $\rho_{\mathsf{XAB}}:=\frac{1}{2}\sum_{x\in[2]}|x\rangle\langle x|_{\mathsf{X}}\otimes|\phi^x\rangle\langle\phi^x|_{\mathsf{AB}}$. The authors of [MST21] showed that $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_{\rho}\geq\frac{9}{16}$ and used this fact to prove impossibility of uncloneable encryption, as defined in [MST21], using pure states as ciphertext.*

3 Strict quantum and no-signaling separations for LSSD

Our main result is the following theorem that gives a simple example of an LSSD problem for which the guessing probabilities for players with different types of shared resources are all distinct. Namely, $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})<\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})<\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})$.

Theorem 3.1. *Let $\mathscr{X}=\{0,1,2\}$ and $\mathscr{A}=\mathscr{B}=\{0,1\}$, and let P_{XAB} be the uniform distribution over $\{(0,1,0),(0,1,1),(1,0,0),(1,1,0),(2,0,1)\}$. Then*

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P=2/5=0.4, \tag{17}$$

$$\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P=\omega_{\mathrm{q}}^2(\mathsf{X}|\mathsf{A};\mathsf{B})_P=\frac{16+\sqrt{13}}{45}\approx 0.435679, \tag{18}$$

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P=1/2=0.5. \tag{19}$$

Our proof relies on the following characterization of the classical and no-signaling guessing probabilities $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ and $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ when $|\mathscr{A}|=|\mathscr{B}|=2$ (see Appendix A for proof).

Lemma 3.2. *Let P_{XAB} be a probability distribution over $\mathscr{X}\times\mathscr{A}\times\mathscr{B}$ with $\mathscr{A}=\mathscr{B}=\{0,1\}$ and $\mathscr{X}=[d]$, $d\geq 2$. The classical and no-signaling winning probabilities for P_{XAB} are given by*

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max_{\substack{s,t\in\mathscr{X}\\ s\neq t}} \max\Big\{P_{\mathsf{X}}(s), P_{\mathsf{XAB}}(s,0,0)+P_{\mathsf{XAB}}(t,1,1), P_{\mathsf{XAB}}(s,0,1)+P_{\mathsf{XAB}}(t,1,0)\Big\}, \tag{20}$$

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max\Big\{\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P, \max_{k\in\{2,\ldots,d\}} \max_{f,g} \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}\big(f(x,a),g(x,b)|a,b\big)\Big\}, \tag{21}$$

where the final maximization in eq. (21) is over all functions $f:\mathscr{X}\times\mathscr{A}\to\mathscr{X}$ and $g:\mathscr{X}\times\mathscr{B}\to\mathscr{X}$ such that $f(\cdot,a), g(\cdot,b):\mathscr{X}\to\mathscr{X}$ are permutations for every $a\in\mathscr{A}$ and $b\in\mathscr{B}$, and the conditional probability distribution $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ on $\mathscr{X}\times\mathscr{X}\times\mathscr{A}\times\mathscr{B}$ is given by

$$Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b) := \begin{cases} \frac{1}{k} & \text{if } x_A,x_B\in[k] \text{ and } (x_A-x_B) \bmod k = ab,\\ 0 & \text{otherwise.}\end{cases} \tag{22}$$

Proof (of Theorem 3.1). The given distribution P_{XAB} has $P_{\mathsf{X}}(0)=P_{\mathsf{X}}(1)=2/5$, $P_{\mathsf{X}}(2)=1/5$, and $P_{\mathsf{XAB}}(x,a,b)\leq 1/5$ for all x,a,b. Equation (17) then follows by applying Lemma 3.2. An explicit strategy achieving success probability $2/5$ is when both parties ignore their inputs and always output 0.

x	0	1	2
$f(x,0)$	2	**1**	**0**
$f(x,1)$	**0**	**1**	2
$g(x,0)$	**0**	**1**	2
$g(x,1)$	**1**	2	**0**

x	a	b	ab	$f(x,a)$	$g(x,b)$
0	1	0	0	0	0
0	1	1	1	0	1
1	0	0	0	1	1
1	1	0	0	1	1
2	0	1	0	0	0

Table 1: (Left) An optimal choice of functions f and g for no-signaling strategies, see eq. (21). (Right) We verify that for any (x,a,b) with $P_{\mathsf{XAB}}(x)>0$, $f(x,a),g(x,b)\in\{0,1\}$ (in bold) and $f(x,a)\oplus g(x,b)=ab$, hence this choice is compatible with eq. (22) when $k=2$.

Next, let us prove eq. (19). Since $|\mathscr{X}|=3$, we only need to consider $k=2$ and $k=3$ in eq. (21) of Lemma 3.2. Note from eq. (22) that $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b)\leq\frac{1}{k}$ for any x_A,x_B,a,b, so the corresponding term in eq. (21) is at most

$$\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}\big(f(x,a),g(x,b)|a,b\big) \leq \frac{1}{k}\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) = \frac{1}{k}. \tag{23}$$

If $k=2$ and we choose $f,g:[3]\times[2]\to[3]$ according to Table 1 then, for all (x,a,b) with $P_{\mathsf{XAB}}(x,a,b)>0$, we have $f(x,a),g(x,b)\in\{0,1\}$ and $f(x,a)\oplus g(x,b)=ab$, so the inequality in eq. (23) becomes tight. According to eq. (21), this lower bounds the success probability by $1/2$. Since $k=3$ can lower bound it by at most $1/3$, we do not need to consider this case. Thus, according to Lemma 3.2, $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max\{2/5,1/2\}=1/2$ which proves eq. (19).

It remains to prove eq. (18). Let us denote the claimed optimal quantum value in eq. (18) by

$$t_* := \frac{16+\sqrt{13}}{45}. \tag{24}$$

We will first settle the case when the local dimension of the shared entangled state is $d=2$, i.e., each party has a single qubit, and then reduce the general case of $d\geq 2$ to this one.

Towards establishing eq. (18), let us first prove that $\omega^2_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P\geq t_*$. Alice and Bob can achieve the value t_* by using the following strategy. Their shared two-qubit state is

$$|\sigma\rangle_{\mathsf{A'B'}} := s_+|00\rangle_{\mathsf{A'B'}} + s_-|11\rangle_{\mathsf{A'B'}}, \qquad s_\pm := \sqrt{\frac{1}{2}\pm\frac{1}{78}\sqrt{715-182\sqrt{13}}}. \tag{25}$$

To describe their measurements, we denote the qubit state at angle θ and the corresponding projector by

$$|\psi(\theta)\rangle := \cos\theta\,|0\rangle + \sin\theta\,|1\rangle = \begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}, \qquad \Pi(\theta) := |\psi(\theta)\rangle\langle\psi(\theta)| = \begin{pmatrix}\cos^2\theta & \cos\theta\sin\theta\\ \sin\theta\cos\theta & \sin^2\theta\end{pmatrix}. \tag{26}$$

Depending on their local inputs $a, b \in \{0,1\}$, Alice and Bob apply the projective measurements $M(a) := \{M_0(a), M_1(a), M_2(a)\}$ and $N(b) := \{N_0(b), N_1(b), N_2(b)\}$ given in Table 2.

x	0	1	2
$M_x(0)$	0	$\Pi(\alpha_0)$	$\mathbb{1} - \Pi(\alpha_0)$
$M_x(1)$	$\Pi(\alpha_1)$	$\mathbb{1} - \Pi(\alpha_1)$	0
$N_x(0)$	$\Pi(\beta_0)$	$\mathbb{1} - \Pi(\beta_0)$	0
$N_x(1)$	$\Pi(\beta_1)$	0	$\mathbb{1} - \Pi(\beta_1)$

Table 2: Measurements for Alice and Bob's quantum strategies. The projector $\Pi(\theta)$ is defined in eq. (26) and their angles are given in eq. (27).

For each measurement, one of their operators is 0 while the other two are of the form $\Pi(\theta)$ and $\mathbb{1} - \Pi(\theta)$, for some angles $\theta \in [-\pi/2, \pi/2]$. The angles used in Table 2 are chosen as follows:

$$(\alpha_0, \alpha_1, \beta_0, \beta_1) := (-\theta_1, \theta_2, \tfrac{\pi}{2} - \theta_2, \theta_1), \quad \theta_1 := \tfrac{1}{4}\arccos\Big(\tfrac{121+52\sqrt{13}}{477}\Big), \quad \theta_2 := \tfrac{1}{4}\arccos\Big(\tfrac{-431+4\sqrt{13}}{477}\Big). \tag{27}$$

The angles θ_1 and θ_2 satisfy $\cos(4\theta_1) = 12 + 13\cos(4\theta_2)$ and have the following explicit cosines:

$$\cos\theta_1 = \sqrt{\frac{1}{318}\Big(159 + \sqrt{689\big(23+2\sqrt{13}\big)}\Big)}, \qquad \cos\theta_2 = \sqrt{\frac{1}{318}\Big(159 + \sqrt{53\big(23+2\sqrt{13}\big)}\Big)}. \tag{28}$$

Using a computer algebra system, one can verify that

$$\langle\sigma|_{\mathsf{A'B'}}\Bigg(\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a)\otimes N_x(b)\Bigg)|\sigma\rangle_{\mathsf{A'B'}} = \frac{16+\sqrt{13}}{45} = t_*. \tag{29}$$

In fact, $|\sigma\rangle_{\mathsf{A'B'}}$ is the principal eigenvector of the above operator.[3]

Next, let us prove that the above strategy is optimal if the shared entangled state has local dimension $d = 2$ and Alice and Bob use only projective measurements (we will later reduce the case of general measurements in any finite dimension d to this). For now, our goal is to show that

$$\sup_{\substack{\Pi:\mathscr{A}\to\mathrm{PM}(\mathbb{C}^2)\\ \Sigma:\mathscr{B}\to\mathrm{PM}(\mathbb{C}^2)}} \Bigg\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\Pi_x(a)\otimes\Sigma_x(b)\Bigg\| \le t_*. \tag{30}$$

First, by Proposition B.3 we can assume that

$$\Pi_0(0) = \Pi_2(1) = \Sigma_2(0) = \Sigma_1(1) = 0 \tag{31}$$

since Alice should not guess 0 if $a = 0$ and 2 if $a = 1$, and Bob should not guess 2 if $b = 0$ and 1 if $b = 1$. The remaining operators form two 2-outcome projective measurements for each party:

$$\Pi(0) = \{\Pi_1(0), \Pi_2(0)\}, \quad \Pi(1) = \{\Pi_0(1), \Pi_1(1)\}, \quad \Sigma(0) = \{\Sigma_0(0), \Sigma_1(0)\}, \quad \Sigma(1) = \{\Sigma_0(1), \Sigma_2(1)\}. \tag{32}$$

To simplify notation, let us set $(A_0, A_1, B_0, B_1) := \big(\Pi_0(0), \Pi_0(1), \Sigma_0(0), \Sigma_0(1)\big)$ so that

$$\Pi(0) = \{A_0, A_0^\perp\}, \qquad \Pi(1) = \{A_1, A_1^\perp\}, \qquad \Sigma(0) = \{B_0, B_0^\perp\}, \qquad \Sigma(1) = \{B_1, B_1^\perp\} \tag{33}$$

[3] Indeed, one can check that its eigenvalues are $\frac{16+\sqrt{13}}{45}$, $\frac{25+\sqrt{13}}{90}$, $\frac{7+\sqrt{13}}{45}$, $\frac{19-5\sqrt{13}}{90}$.

where $A_i^\perp := \mathbb{1} - A_i$ and $B_i^\perp := \mathbb{1} - B_i$. Our matrix of interest is then

$$\Omega := \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\Pi_x(a)\otimes\Sigma_x(b) \tag{34}$$

$$= \frac{1}{5}\big(\Pi_0(1)\otimes\Sigma_0(0) + \Pi_0(1)\otimes\Sigma_0(1) + \Pi_1(0)\otimes\Sigma_1(0) + \Pi_1(1)\otimes\Sigma_1(0) + \Pi_2(0)\otimes\Sigma_2(1)\big) \tag{35}$$

$$= \frac{1}{5}\big(A_1\otimes B_0 + A_1\otimes B_1 + A_0\otimes B_0^\perp + A_1^\perp\otimes B_0^\perp + A_0^\perp\otimes B_1^\perp\big). \tag{36}$$

We see from eq. (33) that if any of the remaining Alice's measurement operators is 0 then all her operators commute. By Lemma B.4 their winning probability cannot exceed the classical value $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = 2/5$. Hence, all remaining Alice's measurement operators are rank-1, and similarly for Bob.

By applying a local unitary change of basis on Alice and Bob's systems, we can assume without loss of generality that, for some angles $\alpha,\beta\in[0,2\pi]$,

$$A_0 = \begin{pmatrix}1&0\\0&0\end{pmatrix}, \qquad A_1 = \Pi\Big(\frac{\alpha}{2}\Big), \qquad B_0 = \begin{pmatrix}1&0\\0&0\end{pmatrix}, \qquad B_1 = \Pi\Big(\frac{\pi-\beta}{2}\Big), \tag{37}$$

where $\Pi(\theta)$ is the projector defined in eq. (26). With this choice, Ω from eq. (36) can be written as

$$\Omega = \begin{pmatrix} -(a+1)(b-3) & (a+1)\sqrt{1-b^2} & -\sqrt{1-a^2}(b-3) & \sqrt{1-a^2}\sqrt{1-b^2}\\ (a+1)\sqrt{1-b^2} & ab-a+b+7 & \sqrt{1-a^2}\sqrt{1-b^2} & \sqrt{1-a^2}(b-1)\\ -\sqrt{1-a^2}(b-3) & \sqrt{1-a^2}\sqrt{1-b^2} & ab-3a+b+5 & -(a+1)\sqrt{1-b^2}\\ \sqrt{1-a^2}\sqrt{1-b^2} & \sqrt{1-a^2}(b-1) & -(a+1)\sqrt{1-b^2} & -ab-b+a+5 \end{pmatrix} \tag{38}$$

where $a := \cos\alpha$ and $b := \cos\beta$. Our goal is to show that $\|\Omega\| \le t_*$ over all $a,b\in[-1,1]$. Using a computer algebra system we find that the characteristic polynomial of Ω in variable t is

$$f(t,a,b) = t^4 - t^3 + \frac{32+(1+a)(1+b)}{100}t^2 - \frac{16+3(1+a)(1+b)}{500}t + \frac{(1+a)(1+b)\big(4-(1-a)(1-b)\big)}{5000}. \tag{39}$$

Since the largest eigenvalue of Ω is equal to the largest root of f, our goal is to show that f has no roots $t > t_*$. In Lemma C.1 in Appendix C we find an exact sum of squares decomposition for f which shows that $f(t,a,b) > 0$ for any $t > t_*$ and $a,b\in[-1,1]$. This implies that f has no roots larger than t_*.

It remains to show that $\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \le t_*$. We will do this by reducing a general strategy to the above $d=2$ problem. Let us fix any dimension $d\ge 2$ and consider arbitrary local quantum strategies for Alice and Bob. They are based on a shared state $|\sigma\rangle_{\mathsf{A'B'}}\in\mathbb{C}^d\otimes\mathbb{C}^d$ and collections of measurements $M : \mathscr{A}\to \mathrm{M}(\mathbb{C}^d)$ and $N : \mathscr{B}\to\mathrm{M}(\mathbb{C}^d)$. By invoking Proposition B.3 and then Corollary B.2 we can reduce M and N to two two-outcome projective measurements that look the same as in eq. (33), except that A_i and B_i are projectors in some finite-dimensional space $\mathbb{C}^{d'}$ where $d'\le d\max\{|\mathscr{A}|,|\mathscr{B}|\}$.

For now, let us focus just on Alice's measurements. They are fully parameterized by two projectors, A_0 and A_1. By Jordan's Lemma [Jor75] (also known as *CS decomposition* [BR08]), there is a unitary change of basis on Alice's system that simultaneously block-diagonalizes A_0 and A_1:

$$A_0 = \begin{pmatrix} \bigoplus_{j=1}^k \begin{pmatrix}1&0\\0&0\end{pmatrix} & & & & \\ & \mathbb{1} & & & \\ & & \mathbb{1} & & \\ & & & 0 & \\ & & & & 0 \end{pmatrix}, \qquad A_1 = \begin{pmatrix} \bigoplus_{j=1}^k \Pi(\theta_j) & & & & \\ & \mathbb{1} & & & \\ & & 0 & & \\ & & & \mathbb{1} & \\ & & & & 0 \end{pmatrix}. \tag{40}$$

Here the first k blocks are of size 2×2 and contain rank-1 projectors onto 1-dimensional subspaces at angle θ_j between them, see eq. (26). The remaining blocks are 1×1 and contain values $(1,1)$, $(1,0)$, $(0,1)$, and $(0,0)$ (the number of times each pair occurs is determined by the sizes of the identity and all-zeroes matrices). Note that $A_0^\perp$ and $A_1^\perp$ have similar block decompositions in the same basis.

We are interested in the largest eigenvalue of Ω defined in eq. (36). Since all Alice's projectors are block-diagonal, Ω is also block-diagonal (each Alice's block gets tensored by Bob's operator). Since the

largest eigenvalue of Ω must occur in one of these blocks, Alice might as well restrict her strategy to this single block. Since each of her blocks has size at most two, her strategy does not require more than two dimensions. By a similar argument, Bob's system can also be reduced to two dimensions. Since we already analyzed strategies based on orthogonal measurements on a shared state with local dimension two, the same upper bound t_* also applies to the general case. □

In the following proposition, we show that the example presented in Theorem 3.1 is the "smallest" example illustrating a separation between the $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ and $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ in a sense that when $\mathscr{A}$ and $\mathscr{B}$ have cardinality two, three is the minimum cardinality of $\mathscr{X}$ such that there exists such a separation. We also upper-bound the gap between $\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ and $\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ when $\mathscr{A}$ and $\mathscr{B}$ have cardinality two and $\mathscr{X}$ is arbitrary.

Proposition 3.3. *Let P_{XAB} be such that $|\mathscr{A}| = |\mathscr{B}| = 2$. If $|\mathscr{X}| = 2$ then*

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. \tag{41}$$

If $|\mathscr{X}| > 2$ then

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \leq \min\Big\{2\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P, \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P + \frac{1}{8}\Big\}. \tag{42}$$

Proof. To show eq. (41), WLOG we assume that $\mathscr{A} = \mathscr{B} = \mathscr{X} = [2]$. By Lemma 3.2, it suffices to show that

$$\omega_{\mathrm{c}}(X|A;B)_P \geq \max_{f,g} \frac{1}{2}\mathrm{Pr}_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [2] \text{ and } f(A,X) - g(B,X) \bmod 2 = AB], \tag{43}$$

where the maximum is taken over all functions $f, g : [2] \times [2] \to [2]$. Note first that

$$\max_{f,g} \frac{1}{2}\mathrm{Pr}_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [2] \text{ and } f(A,X) - g(B,X) \bmod 2 = AB] \leq \frac{1}{2}. \tag{44}$$

Because $\mathscr{X}$ is of size two, we also have

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \geq \max_{x\in\mathscr{X}} P_{\mathsf{X}}(x) \geq \frac{1}{2}. \tag{45}$$

Therefore we have eq. (43) as desired.

When $\mathscr{X} = [d]$ for $d > 2$, we fix two functions $f, g : [2] \times [d] \to [d]$ such that for all $a, b \in [2]$, $f(a,\cdot) : [d] \to [d]$ and $g(b,\cdot) : [d] \to [d]$ are bijections. Let $f', g' : [2] \times [d] \to [d]$ be such that for all a, b, x, x', we have

$$f(a,x) = x' \iff f'(a,x') = x, \tag{46}$$
$$g(b,x) = x' \iff g'(b,x') = x. \tag{47}$$

Then,

$$\begin{aligned}
&\mathrm{Pr}_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [k] \text{ and } f(A,X) - g(B,X) \bmod k = AB], && (48)\\
&\leq \sum_{i=0,1} \mathrm{Pr}_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [k] \text{ and } f(A,X) - g(B,X) \bmod k = i] && (49)\\
&\leq \sum_{i=0,1}\sum_{j\in[k]} \mathrm{Pr}_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X) = j, g(B,X) = (j+i) \bmod k] && (50)\\
&\leq \sum_{i=0,1}\sum_{j\in[k]} \mathrm{Pr}_{(X,A,B)\sim P_{\mathsf{XAB}}}[f'(A,j) = X, g'(B,(j+i) \bmod k) = X] && (51)\\
&\leq 2k\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. && (52)
\end{aligned}$$

Since f, g are arbitrary, we conclude by Lemma 3.2 that $\omega_{\mathrm{ns}}(X|A;B)_P \leq 2\omega_{\mathrm{c}}(X|A;B)_P$.

Next with re-labeling a and b we can always assume that $\Pr[AB=1] \le 1/4$. Then

$$\Pr_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [k] \text{ and } f(A,X) - g(B,X) \bmod k = AB] \tag{53}$$

$$= \sum_{i=0,1} \Pr_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [k] \text{ and } f(A,X) - g(B,X) \bmod k = i \text{ and } AB = i]\Pr[AB=i] \tag{54}$$

$$\le \Pr_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [k] \text{ and } f(A,X) - g(B,X) \bmod k = 0] + 1/4. \tag{55}$$

With the same argument as before,

$$\Pr_{(X,A,B)\sim P_{\mathsf{XAB}}}[f(A,X), g(B,X) \in [k] \text{ and } f(A,X) - g(B,X) \bmod k = 0] \le k\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. \tag{56}$$

Applying Lemma 3.2 again,

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P \le \sup_{k\ge 2} \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P + \frac{1}{4k} \le \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P + \frac{1}{8}, \tag{57}$$

as desired. □

4 Multipartite LSSD is NP-hard

In this section we consider the multipartite LSSD problem. We show in Corollary 4.3 that finding an optimal strategy is NP-hard already for three parties with classical inputs. All games considered in this section are based on probability distributions that corresponds to a uniform distribution over edges of a hypergraph.

4.1 Hypergraphs and (partial) matchings

A *hypergraph* G is a pair $(\mathscr{V}, \mathscr{E})$ where $\mathscr{V}$ is a set of vertices and $\mathscr{E}$ is a set of hyperedges, which are non-empty subsets of $\mathscr{V}$. A *matching* of a hypergraph $G = (\mathscr{V}, \mathscr{E})$ is a subset $\mathscr{M} \subset \mathscr{E}$ of mutually disjoint hyperedges. We denote by $\nu(G)$ the maximum cardinality of a matching of G. A *fractional matching* of a hypergraph $G = (\mathscr{V}, \mathscr{E})$ is a function $g : \mathscr{E} \to [0,1]$ such that $\sum_{e\in\mathscr{E}: v\in e} g(e) \le 1$ for all $v \in \mathscr{V}$. We denote by $\nu_f(G)$ the maximum of $\sum_{e\in\mathscr{E}} g(e)$ for all fractional matchings g. For any matching $\mathscr{M}$, $g : e \mapsto \delta\big[e \in \mathscr{M}\big]$ is a fractional matching and therefore we always have $\nu(G) \le \nu_f(G)$.

We call a hypergraph $G = (\mathscr{V}, \mathscr{E})$ *r-partite* if $\mathscr{V}$ can be partitioned into r parts such that each hyperedge contains precisely one vertex from each part. If we denote the r parts by $\mathscr{A}_1, \dots, \mathscr{A}_r$, we can characterize a hyperedge e by $(a_1, \dots, a_r) \in \mathscr{A}_1 \times \cdots \times \mathscr{A}_r$ where a_i is the unique vertex in $e \cap \mathscr{A}_i$. We can thus represent an r-partite hypergraph by $(\mathscr{A}_1, \dots, \mathscr{A}_r, \widetilde{\mathscr{E}})$ where $\widetilde{\mathscr{E}} \subset \mathscr{A}_1 \times \cdots \times \mathscr{A}_r$.

4.2 Hypergraph games

For each hpyergraph, we can introduce a probability distribution and a corresponding LSSD game. Note that we need to extend all definitions from Section 2 from two guessing parties to multi-party guessing, which can be done in a natural way.

Definition 4.1. *Let $G = (\mathscr{A}_1, \dots, \mathscr{A}_r, \mathscr{E})$ be an r-partite hypergraph. We define a probability distribution over $\mathscr{E} \times \mathscr{A}_1 \times \cdots \times \mathscr{A}_r$ as*

$$P^G_{\mathsf{EA}_1\cdots\mathsf{A}_r}(e, a_1, \dots, a_r) := \frac{1}{|\mathscr{E}|}\delta\big[e = (a_1, \dots, a_r)\big]. \tag{58}$$

In other words, the random variable E is a uniformly chosen hyperedge of G and A_i is the vertex of E in $\mathscr{A}_i$.

Our main result of this section relates the optimal guessing probability of the game associated to a hypergraph to its maximum matching.

Theorem 4.2. *For any r-partite hypergraph $G = (\mathscr{A}_1, \ldots, \mathscr{A}_r, \mathscr{E})$,*

$$\omega_{\mathrm{c}}\left(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r\right)_{P^G} = \frac{\nu(G)}{|\mathscr{E}|}, \tag{59}$$

$$\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r)_{P^G} \leq \frac{\nu_f(G)}{|\mathscr{E}|}. \tag{60}$$

Proof. Consider a matching $\mathscr{M}$ of G. For a fixed $1 \leq i \leq r$ we define $h_i : \mathscr{A}_i \to \mathscr{E}$ as follows. Given $a \in \mathscr{A}_i$, there is at most one $e = (a_1, \ldots, a_r) \in \mathscr{M}$ such that $a_i = a$. We set $f_i(a) = e$ if there is such hyperedge e and set $f_i(a)$ to an arbitrary hyperedge otherwise. The probability of winning for this strategy is

$$\sum_{e,a_1,\ldots,a_r} P^G_{\mathsf{E}\mathsf{A}_1\cdots\mathsf{A}_r}(e,a_1,\ldots,a_r)\delta\big[h_1(a_1) = \cdots = h_r(a_r) = e\big] \tag{61}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e,a_1,\ldots,a_r} \delta\big[e = (a_1,\ldots,a_r))\big]\delta\big[h_1(a_1) = \cdots = h_r(a_r) = e\big] \tag{62}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}} \delta\big[h_1(a_1) = \cdots = h_r(a_r) = e\big] \tag{63}$$

$$\leq \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\ldots,a_r)\in\mathscr{M}} \delta\big[h_1(a_1) = \cdots = h_r(a_r) = e\big] \tag{64}$$

$$= \frac{|\mathscr{M}|}{|\mathscr{E}|}, \tag{65}$$

which implies that $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r)_{P^G} \geq \frac{\nu(G)}{|\mathscr{E}|}$.

To show the other direction, consider an arbitrary classical strategy described by functions $h_1, \ldots, h_r$. Define the subset

$$\mathscr{M} := \{e = (a_1,\ldots,a_r) \in \mathscr{E} : h_1(a_1) = \cdots = h_r(a_r) = e\}. \tag{66}$$

To show that $\mathscr{M}$ is a matching, let $e = (a_1, \ldots, a_r)$ and $e' = (a'_1, \ldots, a'_r)$ be two distinct hyperedges in $\mathscr{M}$. Also suppose that $a_i = a'_i$ for some i. From the definition of $\mathscr{M}$, we have $e = h_i(a_i) = h_i(a'_i) = e'$ which contradicts the distinctness of e and e'. Therefore, e and e' differ in all vertices and $\mathscr{M}$ is a matching. Next, note that

$$\sum_{e,a_1,\ldots,a_r} P^G_{\mathsf{E}\mathsf{A}_1\cdots\mathsf{A}_r}(e,a_1,\ldots,a_r)\delta\big[h_1(a_1) = \cdots = h_r(a_r) = e\big] \tag{67}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e,a_1,\ldots,a_r} \delta\big[e = (a_1,\ldots,a_r)\big]\delta\big[h_1(a_1) = \cdots = h_r(a_r) = e\big] \tag{68}$$

$$= \frac{1}{|\mathscr{E}|}\sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}} \delta\big[h_1(a_1) = \cdots = h_r(a_r) = e\big] \tag{69}$$

$$= \frac{|\mathscr{M}|}{|\mathscr{E}|}. \tag{70}$$

Therefore, $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r)_{P^G} \leq \frac{\nu(G)}{|\mathscr{E}|}$.

We now prove eq. (60). Let $Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}$ be a no-signaling strategy. For $e = (a_1, \ldots, a_r) \in \mathscr{E}$, we define

$$g(e) := Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\ldots,e|a_1,\ldots,a_r). \tag{71}$$

We have $g(e) \in [0,1]$ and for any $a \in \mathscr{A}_i$

$$\sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}:a_i=a} g(e) = \sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}:a_i=a} Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\ldots,e|a_1,\ldots,a_r) \tag{72}$$

$$\leq \sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}:a_i=a} \sum_{e_1,\ldots,e_{i-1},e_{i+1},\ldots,e_r} Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e_1,\ldots,e_{i-1},e,e_{i+1},\ldots,e|a_1,\ldots,a_r) \tag{73}$$

$$= \sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}:a_i=a} Q_{\mathsf{E}_i|\mathsf{A}_1,\ldots,\mathsf{A}_r}(e|a_1,\ldots,a_r) \tag{74}$$

$$\overset{(a)}{=} \sum_{e=(a_1,\ldots,a_r)\in\mathscr{E}:a_i=a} Q_{\mathsf{E}_i|\mathsf{A}_i}(e|a) \tag{75}$$

$$\overset{(b)}{\leq} 1, \tag{76}$$

where (a) follows since $Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}$ is non-signaling and (b) follows since $Q_{\mathsf{E}_i|\mathsf{A}_i}$ is a conditional probability distribution. Therefore, g is a fractional matching. We can upper-bound the probability of winning for the non-signaling strategy $Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}$ as

$$\sum_{e,a_1,\ldots,a_r} P^G_{\mathsf{E}\mathsf{A}_1\cdots\mathsf{A}_r}(e,a_1,\ldots,a_r) Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\ldots,e|a_1,\ldots,a_r) \tag{77}$$

$$= \frac{1}{|\mathscr{E}|} \sum_{e=(a_1,\ldots,a_r)} Q_{\mathsf{E}_1\cdots\mathsf{E}_r|\mathsf{A}_1\cdots\mathsf{A}_r}(e,\ldots,e|a_1,\ldots,a_r) \tag{78}$$

$$= \frac{1}{|\mathscr{E}|} \sum_{e=(a_1,\ldots,a_r)} g(e) \tag{79}$$

$$\leq \frac{\nu_f(G)}{|\mathscr{E}|}, \tag{80}$$

which completes the proof of eq. (60). □

Corollary 4.3. *For a 3-partite hypergraph G, finding $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G}$ is an NP-hard problem.*

Proof. According to Theorem 4.2, finding $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G}$ is equivalent to finding the size of the maximum matching in G, which is NP-hard [Kar72]. □

Corollary 4.4. *Given the assumption* P $\neq$ NP*, there exists a 3-partite hypergraph G such that*

$$\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G} < \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G}. \tag{81}$$

Proof. For the sake of contradiction, suppose that for all 3-partite hypergraphs G,

$$\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G} = \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G}. \tag{82}$$

Since $\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G}$ can be formulated as a linear program of size polynomial in $|\mathscr{A}_1||\mathscr{A}_2||\mathscr{A}_3|$, we can find $\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G}$ in polynomial time. Therefore, by our assumption in eq. (82), we can also find $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2;\mathsf{A}_3)_{P^G}$ in polynomial time, which is in contradiction with Corollary 4.3 and the assumption P $\neq$ NP. □

Corollary 4.5. *For any r-partite hypergraph $G = (\mathscr{A}_1,\ldots,\mathscr{A}_r,\mathscr{E})$,*

$$\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r)_{P^G} \leq (r-1)\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\ldots;\mathsf{A}_r)_{P^G}. \tag{83}$$

Proof. For any r-partite hypergraph G, we have $\nu_f(G) \leq (r-1)\nu(G)$ [Für81]. Combining this with Theorem 4.2 completes the proof. □

Corollary 4.6. *For a bipartite graph G,*

$$\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G} = \omega_{\mathrm{q}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G} = \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G}. \tag{84}$$

Proof. Applying Corollary 4.5 when $r = 2$, we have $\omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G} \leq \omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G}$. On the other hand, $\omega_{\mathrm{c}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G} \leq \omega_{\mathrm{q}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G} \leq \omega_{\mathrm{ns}}(\mathsf{E}|\mathsf{A}_1;\mathsf{A}_2)_{P^G}$ by definition. Therefore, eq. (84) holds. □

Acknowledgements

We would like to thank Laura Mančinska and Eric Chitambar for useful discussions and for sharing a draft of [CM21] with us. CM was supported by an NWO Veni grant (Project No. VI.Veni.192.159). MO was supported by an NWO Vidi grant (Project No. VI.Vidi.192.109). CS and MT were supported by an NWO Vidi grant (Project No. 639.022.519).

References

[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *24th Annual IEEE Conference on Computational Complexity*, pages 229–242. IEEE, 2009. arXiv:1110.5353, doi:10.1109/CCC.2009.42.

[ALL+21] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. New approaches for quantum copy-protection. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – Crypto 2021*, pages 526–555, Cham, 2021. Springer. arXiv:2004.09674, doi:10.1007/978-3-030-84242-0_19.

[ALP21] Prabhanjan Ananth and Rolando L. La Placa. Secure software leasing. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – Eurocrypt 2021*, pages 501–530, Cham, 2021. Springer. arXiv:2005.05289, doi:10.1007/978-3-030-77886-6_17.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984. URL: https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf, arXiv:2003.06557.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86(2):419–478, Apr 2014. arXiv:1303.2849, doi:10.1103/RevModPhys.86.419.

[BDF+99] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A*, 59(2):1070–1091, Feb 1999. arXiv:quant-ph/9804053, doi:10.1103/PhysRevA.59.1070.

[BK15] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, Feb 2015. arXiv:1707.02571, doi:10.1088/1751-8113/48/8/083001.

[BL20] Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:22, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. arXiv:1903.00130, doi:10.4230/LIPIcs.TQC.2020.4.

[BLM+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71(2):022101, Feb 2005. arXiv:quant-ph/0404097, doi:10.1103/PhysRevA.71.022101.

[BPT12] Grigoriy Blekherman, Pablo A. Parrilo, and Rekha R. Thomas. *Semidefinite Optimization and Convex Algebraic Geometry*. Society for Industrial and Applied Mathematics, Philadelphia, PA, 2012. doi:10.1137/1.9781611972290.

[BR08] Julio Benítez and Vladimir Rakočević. Applications of CS decomposition in linear combinations of two orthogonal projectors. *Applied Mathematics and Computation*, 203(2):761–769, 2008. doi:10.1016/j.amc.2008.05.053.

[Bus12] Francesco Buscemi. All entangled quantum states are nonlocal. *Physical Review Letters*, 108(20):200401, May 2012. arXiv:1106.6095, doi:10.1103/PhysRevLett.108.200401.

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – Crypto 2021*, pages 556–584, Cham, 2021. Springer. arXiv:2107.05692, doi:10.1007/978-3-030-84242-0_20.

[CLM+14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, 2014. arXiv:1210.4583, doi:10.1007/s00220-014-1953-9.

[CLMO13] Andrew M. Childs, Debbie Leung, Laura Mančinska, and Maris Ozols. A framework for bounding nonlocality of state discrimination. *Communications in Mathematical Physics*, 323(3):1121–1153, 2013. arXiv:1206.5822, doi:10.1007/s00220-013-1784-0.

[CLP21] Willian H. G. Corrêa, Ludovico Lami, and Carlos Palazuelos. Maximal gap between local and global distinguishability of bipartite quantum states. 2021. arXiv:2110.04387.

[CM21] Eric Chitambar and Laura Mančinska. Friend or foe in quantum state discrimination. Personal communication, 2021.

[CMP20] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. 2020. URL: https://ia.cr/2020/1194, arXiv:2009.13865.

[Faw18] Hamza Fawzi. Topics in convex optimisation, 2018. Lecture notes at University of Cambridge. URL: http://www.damtp.cam.ac.uk/user/hf323/M18-OPT/index.html.

[Für81] Zoltán Füredi. Maximum degree and fractional matchings in uniform hypergraphs. *Combinatorica*, 1(2):155–162, Jun 1981. doi:10.1007/BF02579271.

[Got03] Daniel Gottesman. Uncloneable encryption. *Quantum Information & Computation*, 3(6):581–602, Nov 2003. arXiv:quant-ph/0210062, doi:10.26421/QIC3.6-2.

[Jor75] Camille Jordan. Essai sur la géométrie à n dimensions. *Bulletin de la Société Mathématique de France*, 3:103–174, 1875. doi:10.24033/bsmf.90.

[Kar72] Richard M. Karp. Reducibility among combinatorial problems. In Raymond E. Miller, James W. Thatcher, and Jean D. Bohlinger, editors, *Proceedings of a symposium on the Complexity of Computer Computations*, pages 85–103, Boston, MA, 1972. Springer. doi:10.1007/978-1-4684-2001-2_9.

[LPW18] Ludovico Lami, Carlos Palazuelos, and Andreas Winter. Ultimate data hiding in quantum mechanics and beyond. *Communications in Mathematical Physics*, 361(2):661–708, Jun 2018. arXiv:/1703.03392, doi:10.1007/s00220-018-3154-4.

[LW13] Cécilia Lancien and Andreas Winter. Distinguishing multi-partite states by local measurements. *Communications in Mathematical Physics*, 323(2):555–573, Oct 2013. arXiv:1206.2884, doi:10.1007/s00220-013-1779-x.

[MST21] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding. 2021. URL: https://ia.cr/2021/408, arXiv:2103.14510.

[MWW09] William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291(3):813–843, Nov 2009. arXiv:0810.2327, doi:10.1007/s00220-009-0890-5.

[PR94] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, Mar 1994. doi:10.1007/BF02058098.

[Rus17] Vincent Russo. *Extended nonlocal games*. PhD thesis, University of Waterloo, Mar 2017. URL: https://hdl.handle.net/10012/11620, arXiv:1704.07375.

[RV15] Oded Regev and Thomas Vidick. Quantum XOR games. *ACM Trans. Comput. Theory*, 7(4):15, Aug 2015. arXiv:1207.4939, doi:10.1145/2799560.

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, Oct 2013. arXiv:1210.4359, doi:10.1088/1367-2630/15/10/103002.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, Jan 1983. doi:10.1145/1008908.1008920.

A Proof of Lemma 3.2

Lemma A.1. *Let P_{XAB} be a probability distribution over $\mathscr{X}\times\mathscr{A}\times\mathscr{B}$ with $\mathscr{A}=\mathscr{B}=\{0,1\}$ and $\mathscr{X}=[d]$, $d\geq 2$. The classical and no-signaling winning probabilities for P_{XAB} are given by*

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max_{\substack{s,t\in\mathscr{X}\\ s\neq t}} \max\Big\{P_{\mathsf{X}}(s), P_{\mathsf{XAB}}(s,0,0)+P_{\mathsf{XAB}}(t,1,1), P_{\mathsf{XAB}}(s,0,1)+P_{\mathsf{XAB}}(t,1,0)\Big\}, \tag{20}$$

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \max\Big\{\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P, \max_{k\in\{2,\ldots,d\}}\max_{f,g}\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}\big(f(x,a),g(x,b)|a,b\big)\Big\}, \tag{21}$$

where the final maximization in eq. (21) is over all functions $f:\mathscr{X}\times\mathscr{A}\to\mathscr{X}$ and $g:\mathscr{X}\times\mathscr{B}\to\mathscr{X}$ such that $f(\cdot,a), g(\cdot,b):\mathscr{X}\to\mathscr{X}$ are permutations for every $a\in\mathscr{A}$ and $b\in\mathscr{B}$, and the conditional probability distribution $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ on $\mathscr{X}\times\mathscr{X}\times\mathscr{A}\times\mathscr{B}$ is given by

$$Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x_A,x_B|a,b) := \begin{cases} \frac{1}{k} & \text{if } x_A,x_B\in[k] \text{ and } (x_A-x_B) \bmod k = ab,\\ 0 & \text{otherwise.}\end{cases} \tag{22}$$

Proof. In the classical case, it is enough to consider only deterministic strategies. They can be described by functions $f:\mathscr{A}\to\mathscr{X}$ and $g:\mathscr{B}\to\mathscr{X}$ that locally map Alice and Bob's inputs to outputs. Their success probability is given by

$$\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\delta\big[f(a)=x\big]\delta\big[g(b)=x\big] \tag{85}$$

$$= \sum_{a,b} P_{\mathsf{XAB}}(f(a),a,b)\delta\big[f(a)=g(b)\big]. \tag{86}$$

There are two possibilities: Alice can either ignore her input and always produce a fixed output, or she can take her input into account.

In the first case, $f(0)=f(1)=:s$ and their success probability is

$$\sum_{a,b} P_{\mathsf{XAB}}(s,a,b)\delta\big[s=g(b)\big]. \tag{87}$$

It is maximized when Bob also ignores his input and outputs the same fixed value s as Alice, i.e., $g(0)=g(1)=s$. This results in success probability

$$\sum_{a,b} P_{\mathsf{XAB}}(s,a,b) = P_{\mathsf{X}}(s) \tag{88}$$

where $s \in \{0,1\}$. This accounts for the first term in eq. (20).

If Alice does *not* ignore her input then $f(0) \neq f(1)$. We can assume that neither does Bob, i.e., $g(0) \neq g(1)$. Indeed, if Bob were to ignore his input, Alice could improve her strategy by outputting the same value as Bob and we would again arrive at eq. (88). To maximize the success probability in eq. (86), the strategies f and g should be coordinated so that $\{f(0), f(1)\} = \{g(0), g(1)\}$ as sets. In other words, either $f(0) = g(0)$ and $f(1) = g(1)$, or $f(0) = g(1)$ and $f(1) = g(0)$. These two cases result in success probabilities

$$P_{\mathsf{XAB}}(f(0), 0, 0) + P_{\mathsf{XAB}}(f(1), 1, 1), \qquad P_{\mathsf{XAB}}(f(0), 0, 1) + P_{\mathsf{XAB}}(f(1), 1, 0). \tag{89}$$

Letting $\{s, t\} := \{f(0), f(1)\} \subseteq \mathscr{X}$ we recover the last two terms in eq. (20).

We now prove eq. (21). Recall from eq. (12) that

$$\omega_{\mathrm{ns}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P := \sup_{Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}} \sum_{\substack{x \in \mathscr{X} \\ a \in \mathscr{A}, b \in \mathscr{B}}} P_{\mathsf{XAB}}(x, a, b) Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}(x, x|a, b). \tag{90}$$

where $Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ is a conditional probability distribution satisfying the no-signaling conditions in eqs. (10) and (11). Since the objective function and all constraints are linear, an optimal $Q_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ is an extreme point of the set of all non-signaling conditional probability distributions. A *local* extreme point can achieve success probability at most $\omega_c(\mathsf{X}|\mathsf{A};\mathsf{B})_P$, corresponding to the first term in eq. (21).

According to [BLM+05, Theorem 1], any *non-local* extreme point of the two-party non-signaling polytope where each party has two inputs and d outputs, is given by $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ in eq. (22), for some $k \in \{2, \ldots, d\}$, up to reversible local relabeling. Intuitively, eq. (22) says that we choose $x_B \in [k]$ uniformly at random and set

$$x_A = \begin{cases} x_B + 1 \pmod k & \text{if } (a,b) = (1,1), \\ x_B & \text{otherwise.} \end{cases} \tag{91}$$

A reversible local relabeling means that each party can locally permute their input as well as output values, and the output permutation may depend on the local input value. The extreme distributions in eq. (22) have the property that any local permutation of input values can be achieved by instead locally permuting outputs conditioned on inputs. For example, the input permutation $a \mapsto 1 - a$ for Alice can be achieved by first negating both variables (i.e., $x_A \mapsto -x_A$ and $x_B \mapsto -x_B$) and then Bob increasing his output by one (i.e., $x_B \mapsto x_B + 1$) whenever $b = 1$. Indeed, this will cause $x_A = x_B + 1$ whenever $(a, b) = (0, 1)$ and $x_A = x_B$ otherwise, see eq. (91).

Since we only need to take into account local output permutations that may depend on local inputs, any non-local extreme point of the non-signaling polytope is of the form

$$\widetilde{Q}^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}\big(x_A, x_B|a, b\big) = Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}\big(f(x_A, a), g(x_B, b)|a, b\big), \tag{92}$$

where $Q^k_{\mathsf{X}_A\mathsf{X}_B|\mathsf{AB}}$ is given by eq. (22) and $f : \mathscr{X} \times \mathscr{A} \to \mathscr{X}$ and $g : \mathscr{X} \times \mathscr{B} \to \mathscr{X}$ are functions such that $f(\cdot, a), g(\cdot, b) : \mathscr{X} \to \mathscr{X}$ are permutations for every $a \in \mathscr{A}$ and $b \in \mathscr{B}$. This establishes eq. (21). □

B Constraints on optimal measurements

The following proposition shows that any measurement can be replaced by a projective measurement on a larger space.

Proposition B.1. *For any an n-outcome measurement $M = \{M_1, \ldots, M_n\}$ on $\mathbb{C}^d$, there is a projective measurement $\{\Pi_1, \ldots, \Pi_n\}$ on $\mathbb{C}^d \otimes \mathbb{C}^n$ and an isometry $U : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^n$ such that, for all $i = 1, \ldots, n$,*

$$M_i = U^\dagger \Pi_i U. \tag{93}$$

Proof. Let $U := \sum_{i=1}^{n} \sqrt{M_i} \otimes |i\rangle$ and $\Pi_i := \mathbb{1} \otimes |i\rangle\langle i|$. Clearly, each Π_i is a projector and $\sum_{i=1}^{n} \Pi_i = \mathbb{1}$. Equation (93) holds since

$$U^\dagger \Pi_i U = \left(\sum_{j=1}^{n} \sqrt{M_j} \otimes \langle j|\right) \Pi_i \left(\sum_{k=1}^{n} \sqrt{M_k} \otimes |k\rangle\right) \tag{94}$$

$$= \sum_{j,k=1}^{n} \sqrt{M_j} \mathbb{1} \sqrt{M_k} \otimes \langle j|i\rangle\langle i|k\rangle \tag{95}$$

$$= M_i. \tag{96}$$

Finally, U is an isometry since $U^\dagger U = U^\dagger \big(\sum_{i=1}^{n} \Pi_i\big) U = \sum_{i=1}^{n} U^\dagger \Pi_i U = \sum_{i=1}^{n} M_i = \mathbb{1}$. □

Using the above result, we can show that it suffices to consider only projective measurements when determining the optimal winning probability for quantum strategies assisted by an entangled state of an arbitrarily large dimension. Our argument is similar to [TFKW13, Lemma 9].

Corollary B.2. *If P_{XAB} is a probability distribution over $\mathscr{X} \times \mathscr{A} \times \mathscr{B}$ then*

$$\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{d \geq 1} \omega_{\mathrm{q}}^{d}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{d \geq 1} \sup_{\substack{\Pi : \mathscr{A} \to \mathrm{PM}(\mathbb{C}^d) \\ \Sigma : \mathscr{B} \to \mathrm{PM}(\mathbb{C}^d)}} \left\| \sum_{\substack{x \in \mathscr{X} \\ a \in \mathscr{A}, b \in \mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) \Pi_x(a) \otimes \Sigma_x(b) \right\|, \tag{97}$$

where the last supremum is over collections of projective measurements.

Proof. The first equality in eq. (97) is by definition, see eq. (7). For the second equality, recall from eq. (9) that

$$\omega_{\mathrm{q}}^{d}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{\substack{M : \mathscr{A} \to \mathrm{M}(\mathbb{C}^d) \\ N : \mathscr{B} \to \mathrm{M}(\mathbb{C}^d)}} \left\| \sum_{\substack{x \in \mathscr{X} \\ a \in \mathscr{A}, b \in \mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a) \otimes N_x(b) \right\|. \tag{98}$$

We need to show that, at the cost of increasing the dimension d, the optimization here can be restricted to just projective measurements. For convenience, let

$$\Omega_{\mathsf{A'B'}} := \sum_{\substack{x \in \mathscr{X} \\ a \in \mathscr{A}, b \in \mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a) \otimes N_x(b). \tag{99}$$

where M_x^a and N_x^b act on registers $\mathsf{A'}$ and $\mathsf{B'}$ of dimension d.

Let us fix a dimension $d \geq 1$ and set $\mathcal{A} = \mathbb{C}^{\mathscr{A}}$ and $\mathcal{B} = \mathbb{C}^{\mathscr{B}}$ as usual. Using Proposition B.1, we can find collections of isometries $U_a : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathcal{A}$ and $V_b : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathcal{B}$ and projective measurements $\Pi(a) \in \mathrm{PM}(\mathbb{C}^d \otimes \mathcal{A})$ and $\Sigma(b) \in \mathrm{PM}(\mathbb{C}^d \otimes \mathcal{B})$ such that

$$M_x(a) = U_a^\dagger \Pi_x^a U_a, \qquad\qquad N_x(b) = V_b^\dagger \Sigma_x^b V_b, \tag{100}$$

for all $a \in \mathscr{A}$, $b \in \mathscr{B}$, and $x \in \mathscr{X}$. Then

$$\Omega_{\mathsf{A'B'}} = \sum_{\substack{x \in \mathscr{X} \\ a \in \mathscr{A}, b \in \mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) \big(U_a \otimes V_b\big)^\dagger \big(\Pi_x(a) \otimes \Sigma_x(b)\big) \big(U_a \otimes V_b\big). \tag{101}$$

Let $|\sigma\rangle_{\mathsf{A'B'}} \in \mathbb{C}^d \otimes \mathbb{C}^d$ denote its principal eigenvector.

Let us fix some arbitrary states $|\alpha\rangle \in \mathcal{A}$ and $|\beta\rangle \in \mathcal{B}$, and arbitrarily extend the isometries U_a and V_b to unitaries $\widetilde{U}_a \in \mathrm{U}(\mathbb{C}^d \otimes \mathcal{A})$ and $\widetilde{V}_b \in \mathrm{U}(\mathbb{C}^d \otimes \mathcal{B})$ so that

$$U_a = \widetilde{U}_a \big(\mathbb{1}_{\mathsf{A'}} \otimes |\alpha\rangle_{\mathsf{A}}\big), \qquad\qquad V_b = \widetilde{V}_b \big(\mathbb{1}_{\mathsf{B'}} \otimes |\beta\rangle_{\mathsf{B}}\big). \tag{102}$$

Furthermore, we promote $|\sigma\rangle_{\mathsf{A'B'}} \in \mathbb{C}^d \otimes \mathbb{C}^d$ to $|\widetilde{\sigma}\rangle_{\mathsf{A'A,B'B}} \in (\mathbb{C}^d \otimes \mathcal{A}) \otimes (\mathbb{C}^d \otimes \mathcal{B})$ by defining

$$|\widetilde{\sigma}\rangle_{\mathsf{A'A,B'B}} := |\sigma\rangle_{\mathsf{A'B'}} \otimes |\alpha\rangle_{\mathsf{A}} \otimes |\beta\rangle_{\mathsf{B}}, \tag{103}$$

where the registers on the right-hand side should be rearranged accordingly. Then

$$\big(U_A \otimes V_b\big)|\sigma\rangle_{\mathsf{A'B'}} = \big(\widetilde{U}_a \otimes \widetilde{V}_b\big)|\widetilde{\sigma}\rangle_{\mathsf{A'A,B'B}} \tag{104}$$

because of eq. (102). Substituting this in eq. (101),

$$\langle\sigma|\Omega|\sigma\rangle = \langle\widetilde{\sigma}|\left(\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\big(\widetilde{\Pi}_x(a)\otimes\widetilde{\Sigma}_x(b)\big)\right)|\widetilde{\sigma}\rangle \tag{105}$$

where $\widetilde{\Pi}_x(a) := \widetilde{U}_a^\dagger \Pi_x(a)\widetilde{U}_a$ and $\widetilde{\Sigma}_x(b) := \widetilde{V}_b^\dagger \Sigma_x(b)\widetilde{V}_b$ are projectors on $\mathbb{C}^d \otimes \mathcal{A}$ and $\mathbb{C}^d \otimes \mathcal{B}$.

Hence, we have promoted the original d-dimensional strategy to one in dimension $d\max\{|\mathscr{A}|,|\mathscr{B}|\}$ that uses only projective measurements and achieves the same success probability. Since $\omega_{\mathrm{q}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P$ in eq. (97) is defined as a supremum over all $d \geq 1$, this increase of dimension does not matter. Hence, we can obtain the optimal quantum value by optimizing only over projectors. □

Intuitively, Alice and Bob should never guess values of x that cannot occur based on their local inputs. The following result shows that optimal measurements for Alice and Bob's quantum strategies can always be assumed to have this property.

Proposition B.3. *Let P_{XAB} be a probability distribution on $\mathscr{X}\times\mathscr{A}\times\mathscr{B}$ and $d \geq 1$ an integer. The supremum in*

$$\omega_{\mathrm{q}}^d(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \sup_{\substack{M:\mathscr{A}\to\mathrm{M}(\mathbb{C}^d)\\ N:\mathscr{B}\to\mathrm{M}(\mathbb{C}^d)}} \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b) M_x(a)\otimes N_x(b)\right\| \tag{106}$$

is achieved by collections of measurements $M(a) = \{M_x(a) : x\in\mathscr{X}\}$ and $N(b) = \{N_x(b) : x\in\mathscr{X}\}$ on $\mathbb{C}^d$ with

$$M_x(a) = 0 \quad \text{if } P_{\mathsf{XA}}(x,a) = 0 \text{ and } P_{\mathsf{A}}(a) > 0, \tag{107}$$

$$N_x(b) = 0 \quad \text{if } P_{\mathsf{XB}}(x,b) = 0 \text{ and } P_{\mathsf{B}}(b) > 0. \tag{108}$$

In particular, if the supremum can be achieved by projective measurements then it can also be achieved by projective measurements that satisfy eqs. (107) and (108).

Proof. The set of all measurements on a finite-dimensional complex Euclidean space and with a finite output set $\mathscr{X}$ is compact. Since the objective function is continuous, the maximum is achieved by some collections of measurements $M(a)$ and $N(b)$. We can potentially improve Alice's measurement M^a by absorbing those measurement operators $M_{x'}(a)$ that correspond to pairs (x',a) that never occur into other operators. More specifically, for each $a\in\mathscr{A}$ with $P_{\mathsf{A}}(a) > 0$ there exists some $x_a \in \mathscr{X}$ with $P_{\mathsf{XA}}(x_a,a) > 0$, so we can absorb all $M_{x'}(a)$ with $P_{\mathsf{XA}}(x',a) = 0$ into $M_{x_a}(a)$:

$$\widetilde{M}_x^a := \begin{cases} 0 & \text{if } P_{\mathsf{XA}}(x,a) = 0 \text{ and } P_{\mathsf{A}}(a) > 0,\\ M_x(a) + \sum_{x':P_{\mathsf{XA}}(x',a)=0} M_{x'}(a) & \text{if } P_{\mathsf{A}}(a) > 0 \text{ and } x = x_a,\\ M_x(a) & \text{otherwise.}\end{cases} \tag{109}$$

We can perform a similar procedure for Bob's measurements $N(b)$ to obtain $\widetilde{N}(b)$. It is clear that all $\widetilde{M}(a)$ and $\widetilde{N}(b)$ are still measurements, and that they satisfy eqs. (107) and (108). In particular, if $M(a)$ are projective measurements then so are $\widetilde{M}(a)$. Moreover,

$$P_{\mathsf{XAB}}(x,a,b)\widetilde{M}_x(a)\otimes\widetilde{N}_x(b) \succeq P_{\mathsf{XAB}}(x,a,b)M_x(a)\otimes N_x(b), \tag{110}$$

for all x,a,b. Indeed, if $P_{\mathsf{XAB}}(x,a,b) = 0$ then this holds trivially, and if $P_{\mathsf{XAB}}(x,a,b) > 0$ then $\widetilde{M}_x(a) \succeq M_x(a)$ and $\widetilde{N}_x(b) \succeq N_x(b)$, so $\widetilde{M}_x(a)\otimes\widetilde{N}_x(b) \succeq M_x(a)\otimes N_x(b)$. Since eq. (110) still holds when summig over all x,a,b,

$$\left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\widetilde{M}_x(a)\otimes\widetilde{N}_x(b)\right\| \geq \left\| \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)M_x(a)\otimes N_x(b)\right\|, \tag{111}$$

as desired. □

Lemma B.4. *Let P_{XAB} be a joint probability distribution. We fix a quantum strategy consisting of a quantum bi-partite state $\sigma_{\mathsf{A'B'}}$ with $\mathcal{A}' = \mathcal{B}' = \mathbb{C}^d$ and collections of measurement $M : \mathscr{A} \to \mathrm{M}(\mathbb{C}^d)$ and $N : \mathscr{B} \to \mathrm{M}(\mathbb{C}^d)$ with output on $\mathscr{X}$. Let M be such that $[M(a)_x, M(a')_{x'}] = 0$ for all $a, a' \in \mathscr{A}$ and for all $x, x' \in \mathscr{X}$. Then,*

$$\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\operatorname{tr}\Big[\sigma_{\mathsf{A'B'}}\big(M_x(a)\otimes N_x(b)\big)\Big] \le \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P. \tag{112}$$

Proof. Because Alice's measurement operators commute, she can jointly perform all measurements for all inputs $a \in \mathscr{A}$ *before* receiving her input to obtain a collection of random variables $\{X_a : a \in \mathscr{A}\}$ and use X_a as her output when her input is a. Let $\widetilde{\mathsf{X}}$ denote the register containing all $\{X_a : a \in \mathscr{A}\}$. Equivalently, Alice and Bob can share $\sigma_{\widetilde{\mathsf{X}}\mathsf{B'}}$ in the first place, which is a cq state and therefore separable. Let $\sigma_{\widetilde{\mathsf{X}}\mathsf{B'}} = \sum_i p_i \sigma^{(i)}_{\widetilde{\mathsf{X}}} \otimes \sigma^{(i)}_{\mathsf{B'}}$ where $\{p_i\}$ is a probability distribution. For any collection of measurements $\widetilde{M} : \mathscr{A} \to \mathrm{M}(\widetilde{\mathcal{X}})$,

$$\sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\operatorname{tr}\Big[\sigma_{\widetilde{\mathsf{X}}\mathsf{B'}}\big(\widetilde{M}_x(a)\otimes N_x(b)\big)\Big] \tag{113}$$

$$= \sum_i p_i \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\operatorname{tr}\Big[\Big(\sigma^{(i)}_{\widetilde{\mathsf{X}}}\otimes\sigma^{(i)}_{\mathsf{B'}}\Big)\big(\widetilde{M}_x(a)\otimes N_x(b)\big)\Big] \tag{114}$$

$$= \sum_i p_i \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\operatorname{tr}\Big[\sigma^{(i)}_{\widetilde{\mathsf{X}}}\widetilde{M}_x(a)\Big]\operatorname{tr}\Big[\sigma^{(i)}_{\mathsf{B'}}N_x(b)\Big]. \tag{115}$$

Therefore, for each i, Alice and Bob can use classical strategies $Q_{\mathsf{X}_A|\mathsf{A}}(x_a|a) := \operatorname{tr}\big[\sigma^{(i)}_{\widetilde{\mathsf{X}}}\widetilde{M}_x(a)\big]$ and $Q_{\mathsf{X}_B|\mathsf{B}}(x_b|b) := \operatorname{tr}\big[\sigma^{(i)}_{\mathsf{B'}}N_x(b)\big]$, respectively. Hence,

$$\sum_i p_i \sum_{\substack{x\in\mathscr{X}\\ a\in\mathscr{A},b\in\mathscr{B}}} P_{\mathsf{XAB}}(x,a,b)\operatorname{tr}\Big[\sigma^{(i)}_{\widetilde{\mathsf{X}}}\widetilde{M}_x(a)\Big]\operatorname{tr}\Big[\sigma^{(i)}_{\mathsf{B'}}N_x(b)\Big] \le \sum_i p_i\omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P = \omega_{\mathrm{c}}(\mathsf{X}|\mathsf{A};\mathsf{B})_P, \tag{116}$$

as desired. □

C SOS representation

Lemma C.1. *For any $t > t_* = \frac{16+\sqrt{13}}{45}$ and $a, b \in [-1, 1]$, the polynomial*

$$f(t,a,b) = t^4 - t^3 + \frac{32+(1+a)(1+b)}{100}t^2 - \frac{16+3(1+a)(1+b)}{500}t + \frac{(1+a)(1+b)\big(4-(1-a)(1-b)\big)}{5000} \tag{117}$$

is strictly positive.

Proof. Let us first establish that $f(t, a, b) \ge 0$ for all $t \ge t_*$ and $a, b \in [-1, 1]$. This would be evident if we managed to find a representation of f of the form

$$f(t,a,b) = v(t,a,b)^{\mathsf{T}}\Big(Q_1 + (t-t_*)Q_2 + (1-a^2)Q_3 + (1-b^2)Q_4\Big)v(t,a,b), \tag{118}$$

where Q_i are fixed positive semi-definite matrices and $v(t, a, b)$ is a vector whose entries depend on t, a, b (e.g., are monomials in them). Generally such "sums of squares" representations can be found using semi-definite programming (see Lectures 10–14 of Hamza Fawzi [Faw18] or Section 3.4.4 of [BPT12]). In our case this is a semi-definite feasibility problem where the matrices Q_i are subject to $Q_i \succeq 0$ and a set of linear constraints obtained by comparing the coefficients of the polynomials in eqs. (117) and (118).

We found the following exact solution of this problem:

$$v(a,b,t) = \begin{pmatrix} 1 \\ a \\ b \\ ab \\ t \\ t^2 \end{pmatrix}, \quad Q_1 = \begin{pmatrix} \alpha & \beta & \beta & \gamma & \delta & \varepsilon \\ \beta & \zeta & \eta & \theta & -\frac{3}{1000} & \frac{1}{200} \\ \beta & \eta & \zeta & \theta & -\frac{3}{1000} & \frac{1}{200} \\ \gamma & \theta & \theta & \iota & -\frac{3}{1000} & \frac{1}{200} \\ \delta & -\frac{3}{1000} & -\frac{3}{1000} & -\frac{3}{1000} & \kappa & -\frac{1}{2} \\ \varepsilon & \frac{1}{200} & \frac{1}{200} & \frac{1}{200} & -\frac{1}{2} & 1 \end{pmatrix}, \tag{119}$$

$$Q_2 = \begin{pmatrix} \lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad Q_3 = \begin{pmatrix} \mu & 0 & \theta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \theta & 0 & \nu & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad Q_4 = \begin{pmatrix} \mu & \theta & 0 & 0 & 0 & 0 \\ \theta & \nu & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{120}$$

where the values of the missing matrix entries are as follows:

$$\alpha = \frac{973343 + 240821\sqrt{13}}{371790000}, \quad \beta = \frac{33139 - 617\sqrt{13}}{82620000}, \quad \gamma = \frac{20 - \sqrt{13}}{45000}, \quad \delta = -\frac{1721 + 62\sqrt{13}}{81000}, \tag{121}$$

$$\varepsilon = \frac{25 - 2\sqrt{13}}{600}, \quad \zeta = \frac{21592 - 2903\sqrt{13}}{185895000}, \quad \eta = \frac{-2 + \sqrt{13}}{45000}, \quad \theta = \frac{-91 + 617\sqrt{13}}{82620000}, \tag{122}$$

$$\iota = \frac{-47 + 127\sqrt{13}}{4590000}, \quad \kappa = \frac{37 + \sqrt{13}}{150}, \quad \lambda = \frac{91 + 31\sqrt{13}}{20250}, \quad \mu = \frac{8203 - 1325\sqrt{13}}{743580000}, \tag{123}$$

$$\nu = \frac{871 + 127\sqrt{13}}{9180000}. \tag{124}$$

The correctness of this decomposition can be verified by plugging these values into eq. (118) and comparing the resulting polynomial with eq. (117).

To verify that Q_i are positive semi-definite, we can simply compute their eigenvalues. The non-zero eigenvalues of Q_1 are

$$\begin{gathered} 1.255390507\ldots \\ 0.020376547\ldots \\ 0.000059985\ldots \\ 0.000024167\ldots \\ 0.000015112\ldots \end{gathered} \tag{125}$$

The remaining matrices Q_2, Q_3, Q_4 have rank one and their only non-zero eigenvalues are

$$\frac{91 + 31\sqrt{13}}{20250}, \qquad \frac{39377 + 4481\sqrt{13}}{371790000}, \qquad \frac{39377 + 4481\sqrt{13}}{371790000}. \tag{126}$$

To prove that $f(a,b,t) > 0$ when $t > t_*$, expand eq. (118) to obtain

$$f(t,a,b) = v^\mathsf{T} Q_1 v + (t - t_*) v^\mathsf{T} Q_2 v + (1 - a^2) v^\mathsf{T} Q_3 v + (1 - b^2) v^\mathsf{T} Q_4 v. \tag{127}$$

Note that all terms are non-negative when $t \geq t_*$ and $a, b \in [-1, 1]$. Since $\lambda > 0$, the second term

$$(t - t_*) v^\mathsf{T} Q_2 v = (t - t_*)\lambda \tag{128}$$

is strictly positive when $t > t_*$. □

The above solution was found using *Mathematica*. First, we used the `SemidefiniteOptimization` function to find an initial solution. Then, for all sufficiently small matrix entries, we included additional linear constraints that force them to be exactly zero. This resulted in a preliminary solution with sufficiently many zeroes. Our hope was to convert this to an exact algebraic solution using the `RootApproximant` function. However, this would work only if the solution is isolated (i.e., cannot

be perturbed to other nearby solutions) and of sufficiently high accuracy. Unfortunately, the built-in `SemidefiniteOptimization` function cannot obtain high-accuracy solutions.

To overcome this, we had to rely on the generic `NMinimize` and `FindMinimum` routines that support `WorkingPrecision` option. However, since they do not support semi-definite constraints, we had to use the preliminary solution to choose a sufficiently simple ansatz matrix A_i and set $Q_i = A_i^\mathsf{T} A_i$. This automatically guarantees that all Q_i are positive semi-definite. By further tweaking the ansatz we managed to obtain an isolated solution.

To get an exact algebraic solution, we supplied this isolated numerical solution as an initial point to the `FindMinimum` routine and, by increasing the `WorkingPrecision` option, dialed up the accuracy to several hundreds of digits. Finally, applying `RootApproximant` to Q_i, followed by `ToRadicals`, produced the above exact algebraic solution.