arXiv:1310.7954v3 [quant-ph] 5 Mar 2014

Quantum hedging in two-round prover-verifier interactions

Srinivasan Arunachalam[2,3], Abel Molina, and Vincent Russo[1,3]
[1] *David R. Cheriton School of Computer Science, University of Waterloo*
[2] *Department of Combinatorics & Optimization, University of Waterloo*
[3] *Institute for Quantum Computing, University of Waterloo*

We are interested in the problem of quantum correlations that arise when considering hypothetical two-party interactions between Alice and Bob. In a recent work [1], the framework for these interactions was used in the context of a game where one of the players, Bob, could use correlations which exhibit strictly non-classical behavior to his advantage. This manifested in an ability of the player to make use of a form of *hedging*, where the risk of losing a first game was eliminated by offsetting that risk in a second game. In this paper we look at some follow-up questions to that result. We consider whether quantum hedging is possible in a variant of the interaction model motivated by experimental concerns. In particular, we ask whether the hedging behavior still occurs in the case when Bob is allowed to sometimes return no answer to a question, in which case the whole experiment starts again. Additionally, we present some results concerning the existence and amount of hedging in a game that generalizes several of the parameters of the main game studied in [1].

I. INTRODUCTION

This paper investigates the topic of quantum strategies in the context of a certain kind of two-player interaction. These interactions can be viewed as a competitive game played between players Alice and Bob, also referred to as the *verifier* and *prover* respectively. More exactly, the setting of the game we consider in this paper is as follows.

1. Alice prepares a question based on some predefined probabilistic function, and sends this question to Bob.

2. Bob applies some operation to the question, and generates an answer which he sends back to Alice.

3. Alice then evaluates this answer on some predefined metric based on the initial question and answer to determine whether a win or loss is obtained.

It is assumed that Bob has complete knowledge of the probability distribution used to determine Alice's question as well as the metric that she uses to determine if Bob has won or lost the game. Therefore, Bob may adopt a strategy prior to the start of the game based on his knowledge of the initial setup. One may consider *quantum strategies*, where quantum information (that might be entangled with the memories of the players) is transmitted. One might consider whether these strategies give rise to different behaviors than *classical strategies*, where only classical information (with only classical correlations with the memories of the players) is transmitted.

This game framework provides a setting then to study Bell-like inequality violations, with quantum strategies yielding probability outcomes forbidden for their classical counterparts. More famously considered by Bell [2], this type of violations has been observed in a number of game-like frameworks [3–8].

However, unlike in many of those frameworks, here we do not have two parties collaborating to achieve a non-classical outcome. Instead, we have a *prover-verifier* setting, in which Bob is trying to convince Alice in order to pass a test. Therefore, one can also view the games we study in the context of prover-verifier quantum interactive proof systems consisting of two rounds. In fact, the general setting that we have considered so far corresponds to the QIP(2) complexity class. This is a complexity class that has been studied several times and described as mysterious in the literature [9–12]. When analyzing the setting of our game, it will be convenient to use the quantum game formalism developed by Gutoski and Watrous [13, 14] to describe the behavior of Alice and Bob.

A specific combination of a game and a corresponding quantum strategy which exhibited a Bell-like inequality violation was presented in [1]. Their example involved running two parallel repetitions of a game where the optimal probability for Bob to win a single repetition is p. In all such games where only classical information is considered, Bob can win at least one of the two games with an optimal probability of $1-(1-p)^2$. In their example involving quantum information, it was shown that Bob is guaranteed to win one out of the two games. This result not only exhibited a Bell-like violation, but also illustrated that the technique of parallel repetition cannot be used to achieve strong error reduction for the QIP(2) class.

Two natural questions that arise from their analysis is whether or not these Bell-like violations persist when running n repetitions of the game, or when tweaking the quantum states used in the game. In other words, when is Bob still able to perfectly hedge one game out of n repetitions by using a quantum strategy? If so, what is the strategy that Bob uses to obtain this result? We answer this question by establishing (for a one-dimensional family of starting states and another one-dimensional family of measurements by Alice) when will Bob be able to win one game out of n parallel repetitions, along with an specific optimal quantum strategy for those cases.

We also consider the game when Bob has the choice to not respond to Alice in the second step of the protocol, with the protocol being repeated whenever this doesn't happen. This subtle change can be viewed as introducing communication errors into the model. This is motivated by experimental concerns, since in an actual experimental setup, quantum communication between parties is prone to various imperfections. A particularly relevant example is the case of photon loss whenever optical-based quantum information implementations are considered. A decision from Bob to not respond may be viewed as such an error in this framework. We analyze this framework and find that hedging is not possible for any choice of initial quantum state and evaluation procedure by Alice.

The rest of the paper proceeds as follows. We begin with Section I A, where we cover our notation and basic preliminaries. In Section II A, we first describe in greater detail the setting that generalizes the game in [1] which will be the focus in this section. We then examine the hedging behavior necessary for Bob to win one out of n repetitions of the game with certainty in this setting. Then in Section II B we consider a more general setting, but under the assumption that Bob may decide not to return an answer, and induce a repetition of the protocol. After examining some particular cases we finally prove that no hedging is possible in this setting. Finally, in Section III, we re-state our results and mention connections with other results and potential directions for future work.

A. Notation

Vector spaces associated with a quantum system are defined as complex Euclidean spaces. We denote these spaces by the capital script letters $\mathcal{X}, \mathcal{Y}$, and $\mathcal{Z}$. The complex vector space of linear operators of the form $A : \mathcal{X} \to \mathcal{Y}$ is denoted by $\mathrm{L}(\mathcal{X}, \mathcal{Y})$. We write $A \in \mathrm{L}(\mathcal{X})$ as a shorthand for $A : \mathcal{X} \to \mathcal{X}$. The adjoint X^* of an operator $X \in \mathrm{L}(X)$ is the operator such that for all $u, v \in \mathcal{X}$, $\langle u, Xv\rangle = \langle X^* u, v\rangle$. An operator $H \in \mathrm{L}(\mathcal{X})$ is *Hermitian* if $H = H^*$. We write $\mathrm{Herm}(\mathcal{X})$ to denote the set of all Hermitian operators. The inner product $\langle A, B\rangle = \mathrm{Tr}(AB)$ between two operators $A, B \in \mathrm{Herm}(\mathcal{X})$ is real and satisfies $\langle A, B\rangle = \langle B, A\rangle$. All the eigenvalues of a Hermitian operator A are real. If an operator $P \in \mathrm{L}(\mathcal{X})$, $P \in \mathrm{Herm}(\mathcal{X})$, and all eigenvalues of P are non-negative, then we call P *positive semidefinite*, and refer to all such operators as $P \in \mathrm{Pos}(\mathcal{X})$. If $A, B \in \mathrm{Herm}(\mathcal{X})$, we also use the notation $A \geq B$ and $B \leq A$ to indicate that $A - B \in \mathrm{Pos}(\mathcal{X})$ and $B - A \in \mathrm{Pos}(\mathcal{X})$, respectively. If some operator $P \in \mathrm{Pos}(\mathcal{X})$ and $\mathrm{Tr}(P) = 1$, then P is said to be a *density operator*, and is referred to as $P \in \mathrm{D}(\mathcal{X})$. We will often represent such operators in $\mathrm{D}(\mathcal{X})$ as lower case Greek letters ρ, σ, τ, etc. We adopt the convention of writing $\mathbb{1}_{\mathcal{X}}$ as opposed to $\mathbb{1}$ to indicate that the identity is acting on the space $\mathcal{X}$ when convenient to do so.

We also consider linear mappings of the form $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$. The space of all such mappings is denoted as $\mathrm{T}(\mathcal{X}, \mathcal{Y})$. For each $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$, a unique adjoint mapping $\Phi^* \in \mathrm{T}(\mathcal{Y}, \mathcal{X})$ is defined as

$$\langle Y, \Phi(X)\rangle = \langle \Phi^*(Y), X\rangle, \quad \forall X \in \mathrm{L}(\mathcal{X}), \forall Y \in \mathrm{L}(\mathcal{Y}).$$

Throughout this work, we define quantum states by the set of density operators $\rho \in \mathrm{D}(\mathcal{X})$ which reside in some complex Hilbert space $\mathcal{X}$. Associated with the space $\mathcal{X}$ one may consider a *register* denoted X in which the state ρ is contained. We consider measurements of a register, X, as being described by a set of positive semidefinite operators $\{P_a : a \in \Sigma\}$ indexed by a finite non-empty set of measurement outcomes which satisfies the constraint $\sum_{a\in\Sigma} P_a = \mathbb{1}_{\mathcal{X}}$. By performing a measurement on X in state ρ, the outcome $a \in \Sigma$ results with probability $\langle P_a, \rho\rangle$. Without loss of generality, we could also consider a set of n quantum states $\{\rho_1, \rho_2, \cdots, \rho_n\}$ stored across n registers $\{\mathsf{X}_1, \mathsf{X}_2, \cdots, \mathsf{X}_n\}$. We can describe the joint state of this system by a density operator $\sigma \in \mathrm{D}(\mathcal{X}_{1\cdots n})$ where $(\mathcal{X}_{1\cdots n})$ is shorthand for $(\mathcal{X}_1 \otimes \mathcal{X}_2 \otimes \cdots \otimes \mathcal{X}_n)$.

We define a *quantum channel* as a linear mapping $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ which is completely positive and trace preserving. A channel transforms some state ρ stored in register X into the state $\Phi(\rho)$ of another register Y. The set of all channels is denoted by $\mathrm{C}(\mathcal{X}, \mathcal{Y})$, and is a compact and convex set. Note that the channel corresponding to an unitary operator U is the one that maps a quantum state σ to $U\sigma U^*$.

For spaces $\mathcal{X}$ and $\mathcal{Y}$, one may define the Choi representation of an operator $\Phi \in \mathrm{T}(\mathcal{X}, \mathcal{Y})$ as

$$J(\Phi) = \sum_{i,j} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|,$$

where $J : \mathrm{T}(\mathcal{X}, \mathcal{Y}) \to \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$. The Choi representation has a number of interesting qualities, but there are three specific properties which will be useful to us. The first is that the mapping Φ is completely positive if and only if $J(\Phi) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$. The second is that the mapping Φ is trace preserving if and only if $\mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{1}_{\mathcal{X}}$. The third is that $\Phi(Z) = \mathrm{Tr}_{\mathcal{X}}\left[J(\Phi)\left(\mathbb{1}_{\mathcal{Y}} \otimes Z^{\mathrm{T}}\right)\right]$. We refer the reader to [15] for further details on the notation.

II. ANALYSIS OF THE HEDGING MODEL

A. General hedging model

A formal description of the game setting we consider in this section is the following setup:

1. Alice prepares her question as a pair of qubits in registers (X, Z) in an entangled state

$$u = \alpha|00\rangle + \sqrt{1-\alpha^2}\,|11\rangle \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Z}), \qquad (1)$$

where $\alpha \in (0, 1]$, and she sends X to Bob. We denote $uu^* = \rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Z})$ as the density matrix corresponding to this initial state.

2. Bob applies a quantum channel, Φ, to X, which yields the content of Y. We have now two qubits in the pair of registers (Y,Z), with $\sigma \in \mathrm{D}(\mathcal{Y}\otimes\mathcal{Z})$ as the corresponding state.

3. Alice performs a projective measurement $\{P_0, P_1\}$ on (Y,Z) corresponding to outcomes $\{0,1\}$ where $P_1 = vv^*$ for

$$v = \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle \in \mathrm{L}(\mathcal{Y}\otimes\mathcal{Z}), \qquad (2)$$

and $P_0 = \mathbb{1} - P_1$. The value '0' corresponds to the losing outcome and the value '1' corresponds to the winning outcome for Bob.

This is a generalization of the game analyzed in [1], where $\alpha = 1/\sqrt{2}$ and $\theta = \pi/8$.

One can imagine running n repetitions of this protocol in parallel as is illustrated in Figure 1. In this setting, Bob applies his quantum channel, $\Phi \in \mathrm{C}(\mathcal{X}_{1\cdots n}, \mathcal{Y}_{1\cdots n})$, to the combined state that Alice prepares, which yields Bob's response $\Phi(\rho^{\otimes n}) = \sigma \in \mathrm{D}(\mathcal{Y}_{1\cdots n}\otimes\mathcal{Z}_{1\cdots n})$. Alice then performs a series of n projective measurements on σ with respect to the operators $\{P_a\}$ for $a \in \{0,1\}$, which give n outcomes of either '0' or '1'. Since Bob's actions are not required to respect the independence of the measurements, this may cause a correlation to arise in the n measurement outcomes.

In the situation that concerns us here, Bob's goal, once n repetitions in parallel are considered, is to obtain the '1' outcome in at least 1 repetition. In particular, we are interested in when it is useful for Bob to cause correlations that arise between the n measurements by not playing independently in the n repetitions. Note that if Bob's goal was to obtain outcome '1' in all repetitions, it is proved in [13] that it is optimal for Bob to play independently in each of the repetitions.

As shown in [1], and previously in a more general setting in [13], it is possible to define operators $\{Q_a\}$ such that the probability of obtaining outcomes $(a_1,\ldots,a_n)$ in the games corresponding to $\{\mathcal{Z}_1,\ldots,\mathcal{Z}_n\}$ is given by:

$$p(a) = \langle Q_{a_1}\otimes\ldots\otimes Q_{a_n}, J(\Phi)\rangle, \qquad (3)$$

where Q_a is an operator that depends on the initial state ρ held by Alice, and the measurement P_a performed by Alice at the end of the protocol. More precisely, let $\Psi_\rho \in \mathrm{L}(\mathcal{Z},\mathcal{X})$ be the mapping such that $J(\Psi_\rho) = \overline{\rho}$. Then Q_a is given by $(\mathbb{1}_{\mathrm{L}(\mathcal{Y})}\otimes\Psi_\rho)P_a$.

It follows from this and the facts in I A involving quantum channels and the Choi representation, that this setting can be described in terms of a semidefinite program (SDP) where the optimum value corresponds to Bob's probability of winning. In particular, we can define an SDP that corresponds to playing n repetitions of the game, where the optimum value corresponds to the minimum probability that Bob will lose all of the n games.

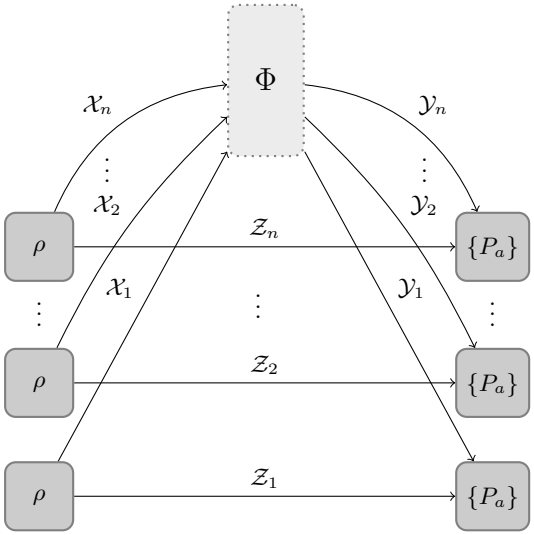

FIG. 1. A competitive game between Alice and Bob of the kind we consider where n repetitions of the game are carried out independently. Alice independently prepares her questions $\rho^{\otimes n} \in \mathrm{D}(\mathcal{X}_{1\cdots n}\otimes\mathcal{Z}_{1\cdots n})$ in each of the n games played. She sends half of the state to Bob, where he applies a quantum channel to the set of Alice's questions $\Phi(\rho^{\otimes n}) = \sigma$ which yields Bob's response labelled by the $\sigma \in \mathrm{D}(\mathcal{Y}_{1\cdots n}\otimes\mathcal{Z}_{1\cdots n})$ state. Bob sends σ back to Alice where she measures with respect to projective measurement operators $\{P_a\}$, yielding n outcomes of either '0' or '1' which correspond to either losses or wins for Bob respectively.

$$\begin{array}{rl} & \underline{\text{Primal problem}} \\ \text{minimize:} & \langle Q_0^{\otimes n}, X\rangle \\ \text{subject to:} & \mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}(X) = \mathbb{1}_{\mathcal{X}_{1\cdots n}}, \\ & X \in \mathrm{Pos}(\mathcal{Y}_{1\cdots n}\otimes\mathcal{X}_{1\cdots n}). \end{array} \qquad (4)$$

$$\begin{array}{rl} & \underline{\text{Dual problem}} \\ \text{maximize:} & \mathrm{Tr}(Y) \\ \text{subject to:} & \mathbb{1}_{\mathcal{Y}_{1\cdots n}}\otimes Y \le Q_0^{\otimes n}, \\ & Y \in \mathrm{Herm}(\mathcal{X}_{1\cdots n}). \end{array} \qquad (5)$$

It can be also noted that strong duality holds for the above SDP, by choosing the primal and dual feasible solutions (X,Y) for the application of Slater's theorem as a scalar multiple of the identity.

Our contribution in this section is to firstly determine for fixed n and α the range of the *angle*, θ, which characterizes the projective measurements for which perfect hedging occurs (i.e. Bob can win 1 out of n parallel repetitions). We also determine a *strategy*, Φ, that Bob can apply to obtain the perfect hedging situation. Secondly we look into the regions where perfect hedging is not possible and present a strategy which seems to give Bob an optimal probability to win 1 out of n games in those regions.

In [1], they consider a case where Bob wins 1 out of 2 games with certainty for $\theta = \pi/8$ and $\alpha = 1/\sqrt{2}$ and give a corresponding strategy that results in perfect hedging.

Our primary result here generalizes this to any θ where 1 out of n hedging occurs for arbitrary n and α.

Theorem 1. *The angles which completely characterize Alice's rank-1 projective measurements $\{P_0, P_1\}$ for which perfect hedging is achieved by Bob to win 1 out of the n games contain the range $\theta \in [\theta_1, \theta_2]$ for*

$$\begin{aligned}\theta_1 &= \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(2^{1/n}-1\right)\right),\\ \theta_2 &= \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(\frac{1}{2^{1/n}-1}\right)\right),\end{aligned} \tag{6}$$

where the trigonometric domain is restricted to $\theta \in [0, \pi/2]$.

The example from [1] illustrated perfect hedging when $\theta_1 = \pi/8$, $n = 2$, and $k = 1$. We obtain this angle as well from Theorem 1, but also that perfect hedging can be attained for this setting up to $\theta_2 = 3\pi/8$. It can be noted that, as the number of games n increases, the probability that Bob wins also increases. Within this region, irrespective of the initial entangled state prepared, the value of this game is the same since Bob has a strategy to win 1 out of n repetitions. The proof of Theorem 1 follows immediately from Lemma 3 and Lemma 4.

Corollary 2. *Perfect hedging occurs for the largest range, θ, when Alice initially prepares a maximally entangled state.*

Proof. The proof for the corollary follows from directly maximizing $\theta_2 - \theta_1$ over all α

$$\begin{aligned}\max_{\alpha} \quad &\left[\tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(\frac{1}{2^{1/n}-1}\right)\right) - \right.\\ &\left.\tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(2^{1/n}-1\right)\right)\right]\end{aligned} \tag{7}$$

by taking the derivate with respect to α, and observing that the maximum occurs for all n at $\alpha = 1/\sqrt{2}$, or, equivalently, when the state is maximally entangled. □

We elaborate over an optimal choice for Bob of the channel Φ that he applies to the part of the state he receives from Alice in the following lemmas:

Lemma 3. *For angles θ_1 and θ_2 as defined in Theorem 1, Bob's strategies for winning 1 out of n games can be defined as Φ_1 and Φ_2 corresponding to unitary operations:*

$$\begin{aligned}\Phi_1 &: \sum_{\vec{r}} (-1)^{\wedge\vec{r}+\bigoplus\vec{r}} |\vec{r}\rangle\langle\vec{r}|,\\ \Phi_2 &: \sum_{\vec{r}} (-1)^{\vee\vec{r}+\bigoplus\vec{r}} |\vec{r}\rangle\langle\vec{r}|,\end{aligned} \tag{8}$$

where $\vec{r} \in \{0,1\}^n$, and $\wedge\vec{r}, \vee\vec{r}$, and $\bigoplus\vec{r}$ refer to the logical AND, OR, and XOR of the bits of $\vec{r}$ respectively.

This shows the existence of strategies $\{\Phi_1, \Phi_2\}$ for Bob at $\{\theta_1, \theta_2\}$ that achieve a value of 0 for the SDP, and the next lemma proves that for all points within these two bounds there exists a strategy as well. Note that these strategies Φ_1 and Φ_2 do not depend on α. Also, note that in the case when $n = 2$, Bob's strategy Φ_1 on the two qubits that he receives corresponds to the unitary:

$$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & -1\end{pmatrix}, \tag{9}$$

which is similar to the strategy defined in [1] up to a global phase. The proof of this lemma has been deferred to Appendix A 1.

Lemma 4. *In the scenario where the projective measurements are parametrized by $\theta \in [\theta_1, \theta_2]$ for θ_1 and θ_2 defined as in Theorem 1, Bob can apply the strategy corresponding to the following unitary operator to achieve perfect hedging for 1 out of n games.*

$$(-1)^n|\vec{0}\rangle\langle\vec{0}| - |\vec{1}\rangle\langle\vec{1}| + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\ |\vec{r}|=i}} (-1)^{n+i} k_{\vec{r}}\,|\vec{r}\rangle\langle\vec{r}|, \tag{10}$$

where $|\vec{r}|$ computes the sum of the bits of $\vec{r}$

$$|\vec{r}| = \sum_{i=0}^{n-1} \vec{r}_i, \tag{11}$$

and for a fixed choice of $|\vec{r}| = i$, $k_{\vec{r}}$ defines the following piecewise function

$$k_{\vec{r}} = \begin{cases}\overline{\beta} & \text{for } \left\lfloor \binom{n}{i}/2 \right\rfloor \text{ of the possible choices of } \vec{r},\\ \beta & \text{for } \left\lfloor \binom{n}{i}/2 \right\rfloor \text{ of the possible choices of } \vec{r},\\ -1 & \text{for the remaining choice of } \vec{r} \text{ when } \binom{n}{i}\\ & \quad \text{is odd and } \tan(\theta) \geq \sqrt{\frac{1}{\alpha^2}-1},\\ 1 & \text{for the remaining choice of } \vec{r} \text{ when } \binom{n}{i}\\ & \quad \text{is odd and } \tan(\theta) < \sqrt{\frac{1}{\alpha^2}-1},\end{cases}$$

where $\beta = s + i\sqrt{1-s^2}$ refers to a point on the complex unit circle, and s is a parameter dependent on θ, α and n.

Since Bob has complete knowledge of the game, for any $\theta \in [\theta_1, \theta_2]$, Bob can apply the strategy corresponding to the angle θ selected. Note that it's clear that the optimal strategies Bob can apply are not unique, since our definition doesn't uniquely specify which coefficients $k_{\vec{r}}$ correspond to which values of $\vec{r}$. The proof of this lemma has been deferred to Appendix A 2.

We have thus far considered the case when perfect hedging is possible. The following result, observed when

running experiments in MATLAB, and for which we present a proof approach in Appendix A 2, deals with characterizing the scenario when perfect hedging is not possible, and provides a corresponding strategy for Bob to play optimally.

Result 5. *For regions corresponding to* $\theta \in [0, \theta_1) \cup (\theta_2, \pi/2]$ *hedging does not occur, and the strategies* Φ_1 *and* Φ_2 *mentioned in Lemma 3 are respective optimal strategies for Bob.*

It is interesting to note that the strategy Bob adopts is independent of the parameter θ, implying that the strategy is optimal regardless of the projective measurements chosen by Alice when perfect hedging is not possible. The optimal probability with which Bob can win for a given α appears in Appendix A, and is minimized for $\theta = \{0, \pi/2\}$. These cases simply correspond to a standard basis measurement done by Alice, and Bob has a probability of $(1-\alpha^2)^n$ and α^{2n} for winning, respectively. It can also be observed then from our results that a unitary (and in fact, a diagonal in the computational basis) strategy is sufficient for Bob to win with optimal probability in the entire interval of Alice's projective measurements parametrized by $\theta \in [0, \pi/2]$.

We point the reader to [16] for MATLAB code which solves the SDPs for the situation we analyze, using the CVX convex optimization package [17].

B. Hedging model with protocol errors

We consider in this section a variation of the prover-verifier setting where Bob has the choice to not respond to Alice in the second step of the protocol. Bob might want to do this whenever using his complete knowledge of the game he can predict an answer will result in a loss. If an answer is not obtained, the game is repeated again, and this goes on until an answer is returned from Bob. To see how this variation produces nontrivial changes on the result of an interaction, consider the following interaction where Bob is always forced to return an answer:

1. Alice prepares the maximally entangled state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and sends the second qubit to Bob.
2. Bob responds by sending a qubit to Alice.
3. Alice ignores Bob's answer, and measures the qubit she kept with respect to the projective measurement $\{P_0, P_1\}$, where $P_0 = |1\rangle\langle 1|$ and $P_1 = |0\rangle\langle 0|$.

It is clear that the maximum probability with which Bob can pass this test is 50%. This follows from the fact that the actions of Bob cannot alter the reduced state that Alice holds, and the outcome of the interaction depends only on this state. However, the situation changes drastically when Bob is allowed to return no answer in the second step. In that case, consider the situation when Bob chooses to perform a measurement using the computational basis on the qubit he receives. If he obtains the outcome corresponding to P_1, he will return an answer, and otherwise he won't. The entanglement between the qubit that Alice keeps and the one that Bob receives guarantees then that the outcome of the interaction will always be the successful one.

We will assume in our analysis that Bob always has a nonzero chance of winning a single repetition. Indeed, if this were not the case, the question of whether or not hedging occurs would be uninteresting. This is because the probability of winning k out of n repetitions for Bob would always be zero. Otherwise, Bob could play a single game and simulate $n-1$ additional repetitions in such a way that there would be a non vanishing chance of winning the single "real" game, and therefore a contradiction.

To start our analysis, we observe that if we allow Bob to not give an answer, but do not repeat the interaction upon a failure to obtain an answer, the semidefinite programming formulation in [1] tells us that the optimal probability of achieving outcome $a \in \{0, 1\}$ for Bob is given by the value of:

$$\begin{aligned} &\underline{\text{Primal problem}} \\ \text{maximize:} \quad & \langle Q_a, X \rangle \\ \text{subject to:} \quad & \mathrm{Tr}_{\mathcal{Y}}(X) \leq \mathbb{1}_{\mathcal{X}}, \\ & X \in \mathrm{Pos}\left(\mathcal{Y} \otimes \mathcal{X}\right), \end{aligned} \tag{12}$$

where Q_a is defined as in (3).

To consider the fact that the interaction is repeated whenever an answer is not received, we divide the objective function by the probability that an answer is returned. This assumes that we can ignore previous repetitions of the interaction, which is justified by the fact that the repeated interactions occur in series. Because of this, the way in which previous repetitions would be taken into account would be with an additional input for Bob corresponding to his memory after the previous rounds of the protocol. But the fact that there is no computational restriction on Bob, and he is aware of the protocol followed by Alice, means that for any possible value of that input, Bob could just simulate the procedure used to generate it, so the input is not needed, and we can ignore previous interactions.

Note that this implies that it is optimal for Bob to return an answer with nonzero probability, since we are assuming that this can win with nonzero probability.

The probability that an answer is returned is just the trace of the state after Bob returns an answer, which is a linear function of the variable X in the previous problem. In particular, the probability is given by $\langle E, X \rangle$, where

$$\begin{aligned} E = \sum_i Q_i &= \sum_i \left(\mathbb{1}_{\mathrm{L}(\mathcal{Y})} \otimes \Psi_\rho\right)(P_i) \\ &= \left(\mathbb{1}_{\mathrm{L}(\mathcal{Y})} \otimes \Psi_\rho\right) \mathbb{1}_{\mathcal{Y}\otimes\mathcal{Z}} = \mathbb{1}_{\mathcal{Y}} \otimes \mathrm{Tr}_{\mathcal{Z}}(\overline{\rho}), \end{aligned} \tag{13}$$

and the last step uses the formula

$$\Psi_\rho(Z) = \mathrm{Tr}_{\mathcal{Z}}\left[J(\Psi_\rho)\left(\mathbb{1}_{\mathcal{X}} \otimes Z^{\mathrm{T}}\right)\right]. \tag{14}$$

Note that since $\sum_i Q_i = E$, we have that $Q_a \leq E$.

We have then that the optimal probability for Bob to obtain outcome a in the model we consider is given by:

$$\begin{aligned} &\underline{\text{Primal problem}} \\ \text{maximize:} \quad & \frac{\langle Q_a, X\rangle}{\langle E, X\rangle} \\ \text{subject to:} \quad & \mathrm{Tr}_{\mathcal{Y}}(X) \leq \mathbb{1}_{\mathcal{X}}, \\ & X \in \mathrm{Pos}\left(\mathcal{Y}\otimes\mathcal{X}\right), \langle E, X\rangle \neq 0. \end{aligned} \tag{15}$$

We use now the same analysis as in [18] to obtain a more explicit form for this value. We begin by noticing that scaling a solution, X, by a nonzero constant will not change the value of the objective function. We can then get rid of the $\mathrm{Tr}_{\mathcal{Y}}(X) \leq \mathbb{1}_{\mathcal{X}}$ constraint. We achieve then the problem:

$$\begin{aligned} &\underline{\text{Primal problem}} \\ \text{maximize:} \quad & \frac{\langle Q_a, X\rangle}{\langle E, X\rangle} \\ \text{subject to:} \quad & X \in \mathrm{Pos}\left(\mathcal{Y}\otimes\mathcal{X}\right), \langle E, X\rangle \neq 0. \end{aligned} \tag{16}$$

At this point, we can additionally assume that X corresponds to a pure state. To see this, consider an X that corresponds to a mixture of two solutions, X_1 and X_2. Then, the value of the objective function will be

$$\frac{\langle Q_a, X_1\rangle + \langle Q_a, X_2\rangle}{\langle E, X_1\rangle + \langle E, X_2\rangle} \leq \max\left(\frac{\langle Q_a, X_1\rangle}{\langle E, X_1\rangle}, \frac{\langle Q_a, X_2\rangle}{\langle E, X_2\rangle}\right), \tag{17}$$

where the inequality follows from the fact that all values involved in the expression on the left hand side are positive. We then obtain the problem:

$$\begin{aligned} &\underline{\text{Primal problem}} \\ \text{maximize:} \quad & \frac{x^* Q_a x}{x^* E x} \\ \text{subject to:} \quad & x \in \mathcal{Y}\otimes\mathcal{X}, x^* E x \neq 0. \end{aligned} \tag{18}$$

Now, note that we can assume without loss of generality that a solution x is contained within the span of the support of E. Also, within this domain, (E^+) is the Moore-Penrose pseudo-inverse [15]. Therefore, we can go ahead with replacing x by $(E^+)^{1/2}x$ in the objective function, obtaining then the equivalent problem:

$$\begin{aligned} &\underline{\text{Primal problem}} \\ \text{maximize:} \quad & \frac{x^*(E^+)^{1/2} Q_a (E^+)^{1/2} x}{x^* x} \\ \text{subject to:} \quad & x \in \mathcal{Y}\otimes\mathcal{X}, x \perp \ker(E), \end{aligned} \tag{19}$$

which has the value $\|(E^+)^{1/2} Q_a (E^+)^{1/2}\|$.

We have obtained a closed formula for the optimal probability of winning for Bob in a single interaction. Consider now then the case when Bob wants to be successful in at least one of two parallel interactions where Alice acts independently. In this case, the same calculation that we did before gives us that this optimal probability is:

$$\begin{aligned} \Big\| \left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)(Q_{1-a}\otimes Q_a + Q_a \otimes \\ Q_{1-a} + Q_a \otimes Q_a)\left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)\Big\|. \end{aligned} \tag{20}$$

This can also be written as

$$\begin{aligned} \Big\| \left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)(E\otimes E - Q_{1-a}\otimes Q_{1-a}) \\ \left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)\Big\|. \end{aligned} \tag{21}$$

Since the quantity inside of the norm in equation (21) appears frequently in our analysis, we denote this quantity as

$$\begin{aligned} \Lambda = \left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)(E\otimes E - Q_{1-a}\otimes Q_{1-a}) \\ \left((E^+)^{1/2}\otimes(E^+)^{1/2}\right). \end{aligned} \tag{22}$$

throughout the rest of this section.

Note that one can assume that the initial state ρ corresponds to a pure state. The reason is because given a protocol with an initial state ρ, we can easily modify it so that Alice prepares a purification of that state instead, and just ignores the added qubits when performing the final measurement. Using this, one can derive an interesting fact about this model, which is that at least whenever one restricts Bob to perform a rank-one measurement, the optimal success probability for Bob does not depend on the Schmidt coefficients of the starting state.

This can be proved by letting the initial state that Alice holds be given by $\sum_i \sqrt{p_i} a_i \otimes b_i$, and the state corresponding to Bob's projection by $\sum_i \sqrt{q_i} c_i \otimes d_i$. Then, if one performs the correspond algebraic manipulations it is possible to obtain that the optimal probability of winning for Bob in a single parallel repetition is:

$$\Big\| \sum_{i,j,k,l} \sqrt{q_j q_l}\, b_i^* d_l d_j^* b_k \overline{a_i a_k}^* \otimes c_j c_l^* \Big\|$$

which has no dependence on the p_i.

This suggests that the example we gave at the beginning of this section might capture all the additional power Bob has in this model. In particular, it suggests that an optimal strategy for Bob might always consist of performing an orthogonal measurement on the qubits he is given, and then refusing to give an answer except when he obtains the "best" outcome.

As for our main subject of concern here (quantum hedging), it turns out that in the model we just described it is not possible for quantum hedging to exist. We will proceed to illustrate a simple proof of this in two particular cases, and then finish with a general proof .

1. Absence of hedging for the protocol in [1]

It is easy to establish that in a generalization of the example considered in [1], the hedging behavior *disappears* once Bob can avoid returning an answer. This generalization corresponds to the set of protocols where the initial quantum state shared between Alice and Bob is a pure state, ψ, such that $\mathrm{Tr}_{\mathcal{X}}(\psi\psi^*) = \mathbb{1}_{\mathcal{Z}}/\dim(\mathcal{Z})$. It suffices to prove this for one of such states, as the other ones can be obtained from it by Bob applying a unitary. In particular, we will prove it for the pure state

$$\psi = \frac{1}{\sqrt{\dim(\mathcal{X})}} \sum_i x_i \otimes x_i, \tag{23}$$

with $\dim(\mathcal{X}) = \dim(\mathcal{Z})$, and x_i being the computational basis for $\mathcal{X}$.

The reason no hedging behavior is possible is because in this situation, it is always possible for Bob to make sure he obtains the desired outcome. To see this, notice that the operator that we apply to get Q_a from P_a is the identity divided by $\dim(\mathcal{X})$. Similarly, $E = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}}/\dim(\mathcal{X})$. Therefore, $(E^+)^{1/2}Q_a(E^+)^{1/2} = P_a$. As this is a projector into a non-empty space (from the assumption that Bob has a nonzero probability of obtaining the desired outcome), the norm of this operator is 1.

2. Absence of hedging in the classical case

We look now at the behavior where the information exchanged between Alice and Bob is classical. This is reflected in the operators we consider in our model being diagonal. In particular, ρ and P_a are diagonal matrices. As ρ is a diagonal matrix, then Ψ_ρ maps diagonal matrices to diagonal matrices, and it is not hard to see that E is a diagonal matrix, and so are the Q_a.

Then, if we denote by $\Omega(E)$ the matrix that has a one in a position whenever the corresponding entry of E is nonzero, and a zero otherwise, we have that:

$$\begin{aligned}\|\Lambda\| = \Big\|\Omega(E)\otimes\Omega(E) - \Big((E^+)^{1/2}\otimes(E^+)^{1/2}\Big) \\ (Q_{1-a}\otimes Q_{1-a})\Big((E^+)^{1/2}\otimes(E^+)^{1/2}\Big)\Big\|.\end{aligned} \tag{24}$$

Now, whenever $\Omega(E)$ has a zero entry, $\left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)(Q_{1-a}\otimes Q_{1-a})\left((E^+)^{1/2}\otimes(E^+)^{1/2}\right)$ has a zero entry as well in that position, as $Q_{1-a} \leq E$. We define now $\lambda_E(X)$ as the minimum entry of a diagonal matrix X, restricted to the positions where E has a nonzero entry. We have then that the value of the game of the game when Bob is trying to win one out of two parallel repetitions is given by:

$$\begin{aligned}1 - \lambda_E\Big((Q_{1-a}\otimes Q_{1-a})\Big((E^+)^{1/2}\otimes(E^+)^{1/2}\Big) \\ \Big(Q_{1-a}\otimes Q_{1-a}\Big)\Big) = 1 - \lambda_E\left((E^+)^{1/2}Q_{1-a}(E^+)^{1/2}\right)^2.\end{aligned} \tag{25}$$

Since we have that

$$\begin{aligned}\Omega(E) &= (E^+)^{1/2}E(E^+)^{1/2} \\ &= (E^+)^{1/2}(Q_a + Q_{1-a})(E^+)^{1/2} \\ &= (E^+)^{1/2}Q_{1-a}(E^+)^{1/2} + (E^+)^{1/2}Q_a(E^+)^{1/2}\end{aligned} \tag{26}$$

we have then that the value of the game when Bob is trying to win one out of two parallel repetitions is given by:

$$\lambda_E = 1 - \|(E^+)^{1/2}Q_a(E^+)^{1/2}\|. \tag{27}$$

Therefore, there is no hedging in the classical case.

3. General proof

We now want to obtain

$$\begin{aligned}\Big\|\Big((E^+)^{1/2}\otimes(E^+)^{1/2}\Big)(E\otimes E - Q_{1-a}\otimes Q_{1-a}) \\ \Big((E^+)^{1/2}\otimes(E^+)^{1/2}\Big)\Big\|.\end{aligned} \tag{28}$$

For simplicity, we define the following operators

$$A = (E^+)^{1/2}Q_a(E^+)^{1/2}, \tag{29}$$

$$B = (E^+)^{1/2}E(E^+)^{1/2}. \tag{30}$$

We can use the fact that $Q_{1-a} = E - Q_a$ to write the above expression in terms of A and B as

$$\Big\|A\otimes B + B\otimes A - A\otimes A\Big\| \tag{31}$$

Now, $[Q_a, (E^+)E] = 0$, and $[A, B] = 0$ as $(E^+)E$ is equal to the identity on the support of E and zero outside it, and $Q_a \leq E$, so $E^+EQ_a = Q_aE^+E = Q_a$. We have then

$$[A\otimes A, A\otimes B + B\otimes A] = 0, \tag{32}$$

Using that the infinity norm of a product of commuting Hermitian matrices is the product of infinity norms we can then write

$$\begin{aligned}\Big\|\Big((E^+)^{1/2}\otimes(E^+)^{1/2}\Big)(E\otimes E - Q_{1-a}\otimes Q_{1-a}) \\ \Big((E^+)^{1/2}\otimes(E^+)^{1/2}\Big)\Big\| = -\|A\|^2 + 2\|B\|\|A\|.\end{aligned} \tag{33}$$

As $\|B\| = 1$, the value of the SDP for playing two repetitions reduces to

$$-\|A\|^2 + 2\|A\| = 1 - (1 - \|A\|)^2, \tag{34}$$

which implies that an optimal behavior is playing each game independentely, with no hedging behavior occurring.

This proof can be easily extended to the case when Bob is trying to win k out of n games. If Bob wishes to win k out of n games, the same derivation as in (21) would lead us to

$$\left\|(\sqrt{E^+})^{\otimes n}\left(E^{\otimes n} - \sum_{t=0}^{k-1}\pi_t\left(Q_{1-a}^{\otimes n-t}\otimes Q_a^{\otimes t}\right)\right)(\sqrt{E^+})^{\otimes n}\right\| \tag{35}$$

where $\pi_t(x)$ refers to a sum over all the unique $\binom{k}{t}$ permutations of x. In the same way as for $k = 1, n = 2$, we can express Q_{1-a} as $E - Q_a$, and thus reduce the operator inside the norm in the above expression to a sum of tensor products of A and B. As $[A, B] = 0$, we reduce the above expression then to

$$\begin{aligned}
&\|B\| - \sum_{t=0}^{k-1}\binom{n}{t}\|A\|^t\sum_{r=0}^{n-t}\binom{n-t}{r}(-1)^{n-t-r}\|B\|^r\|A\|^{n-t-r} \\
&= 1 - \sum_{t=0}^{k-1}\binom{n}{t}\|A\|^t\sum_{r=0}^{n-t}\binom{n-t}{r}(-1)^{n-t-r}\|A\|^{n-t-r} \\
&= 1 - \sum_{t=0}^{k-1}\binom{n}{t}\|A\|^t(1-\|A\|)^{n-t}.
\end{aligned} \tag{36}$$

It can be seen then that in this setting no quantum advantage can be obtained by correlating Bob's strategies between several of the protocol repetitions in the presence of protocol errors.

III. DISCUSSION

In this paper, we have analyzed a specific prover-verifier interaction in which certain circumstances allow the verifier to use a hedging strategy to win one of two parallel repetitions with a higher probability than would have been possible had a classical strategy been adopted. This interesting phenomenon was originally described in [1], where the authors used a semidefinite program to describe the setup of the game, and illustrated an explicit example of hedging when two repetitions of the game were carried out. In this example it is indeed possible to achieve a perfect hedging situation, where one out of two repetitions can be won with certainty. It was previously unknown how does this perfect hedging phenomenon generalize to the case when n repetitions of the game are performed. We resolved this question, and also provided a complete closed form strategy for Bob that is optimal with respect to winning at least one out of the n parallel repetitions in this setting.

We also analyzed a variant of this setting when Bob is not obligated to return an answer back to Alice. In a practical sense, Bob's refusal to respond to Alice can be viewed in terms of an experimental setup where the lack of a response can be viewed as a protocol error in the model. This consideration led to an entirely different semidefinite program that characterized the interaction between Alice and Bob. We then used this SDP to consider our framework under a number of different settings, and asked whether or not Bob still had the ability to take advantage of the hedging behavior.

While we have considered this hedging behavior in a number of settings, there are still some obvious questions remaining. As mentioned, we have characterized the setup that allows Bob to win 1 out of n repetitions in a framework that generalizes the game in [1]. However, it still remains open to determine the conditions under which Bob can perfectly hedge k out of n repetitions for some $k > 1$. It would be interesting to determine the threshold of k for which perfect hedging occurs, and to also provide a characterization in regards to the strategy that Bob uses to achieve this result. Running numerical instances for higher values of k and n using a simple formulation in cvx quickly becomes computationally infeasible, as can be observed from the software we've provided in [16]. It's possible that this code could be optimized to consider further cases, and perhaps lead to intuition regarding the characterization for k out of n repetitions. Based on our current numerical evidence, it is possible that Bob cannot perfectly hedge more than $k = n/2$ games.

One could also further consider the setting in which protocol errors are introduced into the model. Here, we've assumed that Bob is not forced to return an answer back to Alice, and in the scenarios we've presented, found that hedging does not occur. In our analysis, it's possible for Bob to delay returning an answer as long as he desires. An obvious follow-up question then is to determine whether hedging behavior is possible when this is not the case. One might restraint Bob to behaviors where on average he will return an answer within a fixed number of iterations, or introduce constraints be of the form "After X iterations, Bob's probability of having return an answer must be at least equal to Y". A special case of those constraints that might be particularly interesting is when Bob is required to return an answer within a fixed number of iterations.

It's also worth noting that the problem of conclusive state exclusion, which was recently considered in [19], bears a strong resemblance to the interaction we've analyzed in this work. In their paper, the PBR game, originally formulated in [20], was analyzed in terms of an semidefinite program. Many of the mathematical results we've shown in this work are analogous to the ones in [19], specifically equations (6) and (8) as well as the optimal probabilities in Result 5. It would be interesting to

further investigate games of this variety to determine if a more general theory of such games could be formulated.

ACKNOWLEDGMENTS

We would like to thank Devin Smith for the question that led to Section II B in this paper. A significant amount of thanks is also due to John Watrous for numerous insightful discussions and suggestions. A.S. and V.R. wish to thank Nathaniel Johnston for helpful suggestions, as well as the use of his QETLAB quantum entanglement MATLAB package [21]. Thanks is also due to Alessandro Cosentino, Gus Gutoski, and Christopher Perry for insightful discussions. This research was supported by Canada's NSERC and the US ARO.

[1] Abel Molina and John Watrous. Hedging bets with correlated quantum strategies. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 468:2614–2629, 2012. URL: http://rspa.royalsocietypublishing.org/content/early/2012/04/10/rspa.2011.0621.abstract, doi:10.1098/rspa.2011.0621.

[2] John S Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964. URL: http://philoscience.unibe.ch/documents/TexteHS10/bell1964epr.pdf.

[3] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969. URL: http://prl.aps.org/abstract/PRL/v23/i15/p880_1, doi:10.1103/PhysRevLett.23.880.

[4] N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65:3373–3376, 1990. URL: http://prl.aps.org/abstract/PRL/v65/i27/p3373_1, doi:10.1103/PhysRevLett.65.3373.

[5] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151:107–108, 1990. URL: http://www.sciencedirect.com/science/article/pii/037596019090172K, doi:10.1016/0375-9601(90)90172-K.

[6] Oded Regev. Bell violations through independent bases games. *Quantum Information & Computation*, 12(1-2):9–20, 2012. URL: http://arxiv.org/abs/1101.0576.

[7] Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004. URL: http://arxiv.org/abs/quantph/0404076.

[8] T Cooney, M Junge, C Palazuelos, and D Pérez García. Rank-one quantum games. *arXiv preprint arXiv:1112.3563*, 2011. URL: http://arxiv.org/abs/1112.3563.

[9] Patrick Hayden, Kevin Milner, and Mark M Wilde. Two-message quantum interactive proofs and the quantum separability problem. *arXiv preprint arXiv:1211.6120*, 2012. URL: http://arxiv.org/abs/1211.6120.

[10] Ran Raz. Quantum information and the PCP theorem. In *Foundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on*, pages 459–468. IEEE, 2005.

[11] Stephanie Wehner. Entanglement in interactive proof systems with binary answers. In *STACS 2006*, pages 162–171. Springer, 2006. URL: http://arxiv.org/abs/quant-ph/0508201.

[12] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 534–543. IEEE, 2009. URL: http://arxiv.org/abs/0905.1300.

[13] Gus Gutoski and John Watrous. Toward a general theory of quantum games. *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 565–574, 2007. URL: http://dl.acm.org/citation.cfm?id=1250873, doi:10.1145/1250790.1250873.

[14] Gus Gutoski. Quantum strategies and local operations. *arXiv preprint arXiv:1003.0038*, 2010. URL: http://arxiv.org/abs/1003.0038.

[15] John Watrous. Lecture notes: Theory of quantum information. 2011. URL: https://cs.uwaterloo.ca/~watrous/LectureNotes.html.

[16] Abel Molina, Srinivasan Arunachalam, and Vincent Russo. https://bitbucket.org/vprusso/quantum-hedging.

[17] Michael Grant, Stephen Boyd, and Yinyu Ye. Cvx: Matlab software for disciplined convex programming. http://cvxr.com/cvx/, 2008.

[18] Nicolas J Cerf and Jaromir Fiurasek. Optical quantum cloning-a review. *arXiv preprint quant-ph/0512172*, 2005. URL: http://arxiv.org/abs/quant-ph/0512172.

[19] Somshubhro Bandyopadhyay, Rahul Jain, Jonathan Oppenheim, and Christopher Perry. Conclusive exclusion of quantum states. *arXiv preprint arXiv:1306.4683*, 2013. URL: http://arxiv.org/abs/1306.4683.

[20] Matthew F Pusey, Jonathan Barrett, and Terry Rudolph. On the reality of the quantum state. *Nature Physics*, 8:475–478, 2012. URL: http://www.nature.com/nphys/journal/v8/n6/abs/nphys2309.html, doi:10.1038/nphys2309.

[21] Nathaniel Johnston. http://www.qetlab.com/.

[22] John Watrous. https://cs.uwaterloo.ca/~watrous/CS766/ProblemSets/solutions-2.pdf.

Appendix A: Proofs of theorems and lemmas

1. Proof of Lemma 3

Proof. Given that n repetitions of the test are administered, our claim states that Bob will win *at least* one out of the n tests if he adopts Φ_1 as his strategy when the projective measurement made by Alice corresponds to the parameter θ_1. A similar argument also holds for Φ_2 at the corresponding angle θ_2. We prove this explicitly for the strategy Φ_1, and the other case follows using the same argument. Before we present the proof, note that the Choi representations of the linear mappings Φ_1 and Φ_2 can be verified to refer to valid completely positive and trace preserving maps. The proof of this lemma uses a technique of preconditioning, where, given a state σ returned by Bob after applying Φ_1, we consider the resulting state after he loses a game after Alice's projective measurement, and the corresponding probability. This preconditioning has depth n since we are playing n games in parallel, and therefore have n projective measurement outcomes. To finish the proof, we set this probability to zero, and solve for θ in the resulting equation.

First, let us define the pure states:

$$\begin{aligned} |\psi_1\rangle &= \cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle\,, \quad & \left|\psi_0^1\right\rangle &= \sin(\theta)\,|00\rangle - \cos(\theta)\,|11\rangle\,, \\ \left|\psi_0^2\right\rangle &= \sin(\theta)\,|10\rangle + \cos(\theta)\,|01\rangle\,, \quad & \left|\psi_0^3\right\rangle &= \cos(\theta)\,|10\rangle - \sin(\theta)\,|01\rangle\,, \end{aligned} \tag{A1}$$

where we recall from Section II A that $v = |\psi_1\rangle \in \mathcal{Y} \otimes \mathcal{Z}$ is the state which corresponds to the winning projective measurement ($P_1 = vv^*$) outcome of Alice, and $\left|\psi_0^1\right\rangle, \left|\psi_0^2\right\rangle, \left|\psi_0^3\right\rangle \in \mathcal{Y} \otimes \mathcal{Z}$ are the states that correspond to the losing projective measurement $\left(P_0 = \left|\psi_0^1\right\rangle\left\langle\psi_0^1\right| + \left|\psi_0^2\right\rangle\left\langle\psi_0^2\right| + \left|\psi_0^3\right\rangle\left\langle\psi_0^3\right|\right)$ outcome for Bob. Bob is trying then to transform the state given by Alice to $|\psi_1\rangle$, and avoid the losing outcome.

We now explicitly run through a full instance of this test. We have that the initial state is $u^{\otimes n}$, where u is defined in equation (1), and the state after Bob applies his channel is:

$$\left|\phi_f^0\right\rangle = \left(\sum_{\vec{r}\in\{0,1\}^n} (-1)^{\wedge\vec{r}+\bigoplus\vec{r}}\,|\vec{r}\rangle\langle\vec{r}| \otimes \mathbb{1}_{\mathcal{Z}_{1\ldots n}}\right) \sum_{a\in\{0,1\}^n} \bigotimes_{i=0}^{n-1} \alpha^{1-a_i}(1-\alpha^2)^{a_i/2}\left|a_i^{\mathcal{Y}_{i+1}} a_i^{\mathcal{Z}_{i+1}}\right\rangle, \tag{A2}$$

where $a_i^{\mathcal{Y}_i}$ corresponds to the qubit returned by Bob, and $a_i^{\mathcal{Z}_i}$ corresponds to the qubit kept by Alice.

We shall condition now on Bob losing the first game, and consequently, analyze the remaining games. It should be noted that since Alice starts with the entangled state $u^{\otimes n}$ and Bob performs a unitary diagonal operation, then the states $\left|\psi_0^2\right\rangle$ or $\left|\psi_0^3\right\rangle$ in equation (A1) do not contribute to the losing projective measurement outcome. Given our preconditioning, after the first game the resulting state is a normalization of

$$\begin{aligned} \left|\phi_f^1\right\rangle &= \left(\left|\psi_0^1\right\rangle\left\langle\psi_0^1\right| \otimes \mathbb{1}_{2n-2}\right)\left|\phi_f^0\right\rangle \\ &= \left|\psi_0^1\right\rangle \otimes \left(\alpha\sin(\theta)\left(\sum_{\vec{r}\in\{0,1\}^{n-1}} (-1)^{\bigoplus\vec{r}}\,|\vec{r}\rangle\langle\vec{r}| \otimes \mathbb{1}_{\mathcal{Z}_{2\ldots n}}\right) \sum_{a\in\{0,1\}^{n-1}} \bigotimes_{i=0}^{n-1} \alpha^{1-a_j}(1-\alpha^2)^{a_j/2}\left|a_j^{\mathcal{Y}_{i+2}} a_j^{\mathcal{Z}_{i+2}}\right\rangle\right) \\ &\quad + \left|\psi_0^1\right\rangle \otimes \left(\sqrt{1-\alpha^2}\cos(\theta)\left(\sum_{\vec{r}\in\{0,1\}^{n-1}} (-1)^{\wedge\vec{r}+\bigoplus\vec{r}}\,|\vec{r}\rangle\langle\vec{r}| \otimes \mathbb{1}_{\mathcal{Z}}\right) \sum_{a\in\{0,1\}^{n-1}} \bigotimes_{i=0}^{n-1} \alpha^{1-a_j}(1-\alpha^2)^{a_j/2}\left|a_j^{\mathcal{Y}_{i+2}} a_j^{\mathcal{Z}_{i+2}}\right\rangle\right). \end{aligned} \tag{A3}$$

with the associated probability being $\mathrm{Tr}\left(\left|\phi_f^1\right\rangle\left\langle\phi_f^1\right|\right)$.

Generalizing this to Bob losing all n games, one can observe that the -1's for the $\cos(\theta)$ term in $\left|\phi_0^1\right\rangle$ cancel the $(-1)^{\bigoplus\vec{r}}$ term, and (A3) generalizes to:

$$\begin{aligned} \left|\phi_f^n\right\rangle = \left|\psi_0^1\right\rangle^{\otimes n} \Big(&\alpha^n\sin^n(\theta) + (\alpha^{n-1}\sqrt{1-\alpha^2})n\sin^{n-1}(\theta)\cos(\theta) + \ldots \\ &+ (\alpha(1-\alpha^2)^{(n-1)/2})n\cos^{n-1}(\theta)\sin(\theta) - (1-\alpha^2)^{n/2}\cos^n(\theta)\Big). \end{aligned} \tag{A4}$$

In order for Bob to ensure he wins *at least* 1 out of the n games with certainty, we require then the condition $\left\|\left|\phi_f^n\right\rangle\right\| = 0$, which implies:

$$(\alpha \sin(\theta) + \sqrt{1-\alpha^2}\cos(\theta))^n - 2(1-\alpha^2)^{n/2}\cos^n(\theta) = 0. \tag{A5}$$

This implies that for $\theta = \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(2^{1/n}-1\right)\right)$, the strategy corresponding to Φ_1 gives us a perfect hedging strategy. Following the same procedure, using the strategy corresponding to Φ_2 yields the similar condition that:

$$(\alpha \sin(\theta) + \sqrt{1-\alpha^2}\cos(\theta))^n - 2\alpha^n \sin^n(\theta) = 0, \tag{A6}$$

giving us $\theta = \tan^{-1}\left(\sqrt{\frac{1}{\alpha^2}-1}\left(\frac{1}{2^{1/n}-1}\right)\right)$. □

2. Proof of Lemma 4

Proof. As in the previous proof to win at least 1 out of n games, Bob needs to avoid the outcome corresponding to the state $\left|\psi_0^1\right\rangle^{\otimes n}$ (other states for the losing outcome can be ignored since Bob's strategy corresponds to a diagonal matrix). Let us now define a matrix

$$D = \sum_{\vec{r}\in\{0,1\}^n} (-1)^{|\vec{r}|}\sin(\theta)^{n-|\vec{r}|}\cos(\theta)^{|\vec{r}|}\left|\vec{r}\right\rangle\left\langle\vec{r}\right|, \tag{A7}$$

such that $\left|\psi_0^1\right\rangle^{\otimes n} = \mathrm{vec}\,(D)$. For convenience, we denote $\lambda = \tan(\theta)$, and rewrite D as

$$D = \cos^n(\theta)\sum_{\vec{r}\in\{0,1\}^n} (-1)^{|\vec{r}|}\lambda^{n-|\vec{r}|}\left|\vec{r}\right\rangle\left\langle\vec{r}\right|. \tag{A8}$$

We also introduce an operator

$$F = \sum_{\vec{r}\in\{0,1\}^n} (1-\alpha^2)^{|\vec{r}|/2}\alpha^{n-|\vec{r}|}\left|\vec{r}\right\rangle\left\langle\vec{r}\right|, \tag{A9}$$

such that $\mathrm{vec}\,(u^{\otimes n}) = F$, where u is again the pure state shared by Alice and Bob at the beginning of a single repetition of the protocol defined in equation (1).

From our construction the unitary U that Bob applies in Lemma 4 to his portion of the entangled state $u^{\otimes n}$ is

$$U = (-1)^n|\vec{0}\rangle\langle\vec{0}| - |\vec{1}\rangle\langle\vec{1}| + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n \\ |\vec{r}|=i}} (-1)^{n+i}k_{\vec{r}}\left|\vec{r}\right\rangle\left\langle\vec{r}\right|. \tag{A10}$$

The state that Alice holds before measurement is then $(U\otimes \mathbb{1}_{\mathcal{Z}_{1\ldots n}})u^{\otimes n}$. We analyze how successful the application of this channel would be to discriminate against $\left|\psi_0^1\right\rangle^{\otimes n}$. Upon explicit computation of the formula $\langle \mathrm{vec}\,(D)\,, (U\otimes \mathbb{1}_{\mathcal{Z}_{1\ldots n}})\mathrm{vec}\,(F)\rangle$, and using repeatedly the property $\mathrm{vec}\,(V) = (V\otimes\mathbb{1})\mathrm{vec}\,(\mathbb{1})$, we get $\langle \mathrm{vec}\,(D)\,|\mathrm{vec}\,(UF)\rangle = \langle D|UF\rangle$, resulting in the following expression:

$$
\begin{aligned}
\langle D|UF\rangle &= \mathrm{Tr}\left((-1)^n\alpha^n\lambda^n|\vec{0}\rangle\langle\vec{0}| + (1-\alpha^2)^{n/2}(-1)^{n+1}|\vec{1}\rangle\langle\vec{1}| + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}(-1)^n k_{\vec{r}}(1-\alpha^2)^{i/2}\alpha^{n-i}\lambda^{n-i}\,|\vec{r}\rangle\langle\vec{r}|\right)\\
&= (-1)^n\alpha^n\,\mathrm{Tr}\left(\lambda^n|\vec{0}\rangle\langle\vec{0}| - \left(\sqrt{\frac{1}{\alpha^2}-1}\right)^n|\vec{1}\rangle\langle\vec{1}| + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}k_{\vec{r}}\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^i\lambda^{n-i}\,|\vec{r}\rangle\langle\vec{r}|\right).\\
&= (-1)^n\alpha^n\left(\lambda^n - \left(\sqrt{\frac{1}{\alpha^2}-1}\right)^n + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}k_{\vec{r}}\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^i\lambda^{n-i}\right).\\
&= (-1)^n\alpha^n\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^n\left(\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}k_{\vec{r}}\lambda_\alpha^{n-i}\right),
\end{aligned}
\tag{A11}
$$

where $\lambda_\alpha = \lambda\left(\sqrt{\frac{1}{\alpha^2}-1}\right)^{-1}$.

Note that for the range of θ we are considering, it holds that $2^{1/n}-1 \le \lambda_\alpha \le \frac{1}{2^{1/n}-1}$. Note as well that from our choice of $k_{\vec{r}}$, for all i we have that $\mathrm{Im}\left(\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}k_{\vec{r}}\lambda_\alpha^{n-i}\right) = 0$, and therefore the imaginary part of (A11) is equal to 0. It then suffices to prove that for any choice of λ_a and n, there exists an $s\in[-1,1]$ such that when plugged into the definition of $k_{\vec{r}}$ in the statement of 4, we have

$$
\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}\mathrm{Re}\left(k_{\vec{r}}\right)\lambda_\alpha^{n-i} = 0. \tag{A12}
$$

Now, as A12 is an affine function of s with a positive linear coefficient, to prove the existence of such an s it suffices to prove that A12 ≤ 0 when $s=-1$, and A12 ≥ 0 when $s=1$.

We look first into the case when $s=-1$. Then, when $1\le\lambda_\alpha\le\frac{1}{2^{1/n}-1}$ it holds that:

$$
\begin{aligned}
\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}\mathrm{Re}\left(k_{\vec{r}}\right)\lambda_\alpha^{n-i} &= \lambda_\alpha^n - 1 - \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}\binom{n}{n-i}\lambda_\alpha^{n-i}\\
&= 2\lambda_\alpha^n - \lambda_\alpha^n - 1 - \sum_{i=1}^{n-1}\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}\binom{n}{n-i}\lambda_\alpha^{n-i}\\
&= 2\lambda_\alpha^n - (1+\lambda_\alpha)^n,
\end{aligned}
\tag{A13}
$$

which is ≤ 0 whenever $\lambda_\alpha \le \frac{1}{2^{1/n}-1}$. When $2^{1/n}-1\le\lambda_\alpha<1$, A12 ≤ 0 follows from two simple facts. First, the fact that $\lambda_\alpha^n<1$. Second, the fact that for each $\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}\mathrm{Re}\left(k_{\vec{r}}\right)\lambda_\alpha^{n-i}$ term, $\sum_{\substack{\vec{r}\in\{0,1\}^n\\|\vec{r}|=i}}\mathrm{Re}\left(k_{\vec{r}}\right)\le -\binom{n}{i}+1$.

We look now into the case when $s=1$. Then, when $2^{1/n}-1\le\lambda_\alpha<1$ it holds that:

$$\begin{aligned}\lambda_\alpha^n - 1 + \sum_{i=1}^{n-1} \sum_{\substack{\vec{r}\in\{0,1\}^n \\ |\vec{r}|=i}} \mathrm{Re}\left(k_{\vec{r}}\right) \lambda_\alpha^{n-i} &= \lambda_\alpha^n - 1 + \sum_{i=1}^{n-1} \sum_{\substack{\vec{r}\in\{0,1\}^n \\ |\vec{r}|=i}} \binom{n}{n-i} \lambda_\alpha^{n-i} \\ &= -2 + \lambda_\alpha^n + 1 + \sum_{i=1}^{n-1} \sum_{\substack{\vec{r}\in\{0,1\}^n \\ |\vec{r}|=i}} \binom{n}{n-i} \lambda_\alpha^{n-i} \\ &= -2 + (1+\lambda_\alpha)^n,\end{aligned} \tag{A14}$$

which is ≥ 0 whenever $\lambda_\alpha \geq 2^{1/n} - 1$. When $1 \leq \lambda_\alpha \leq \dfrac{1}{2^{1/n}-1}$, A12 ≥ 0 follows from two simple facts. First, the fact that $\lambda_\alpha^n \geq 1$. Second, the fact that for each $\sum_{\substack{\vec{r}\in\{0,1\}^n \\ |\vec{r}|=i}} \mathrm{Re}\left(k_{\vec{r}}\right) \lambda_\alpha^{n-i}$ term, $\sum_{\substack{\vec{r}\in\{0,1\}^n \\ |\vec{r}|=i}} \mathrm{Re}\left(k_{\vec{r}}\right) \geq \binom{n}{i} - 1$.

□

3. Approach for Result 5

We use an observation of Watrous [22] to reduce a question about optimality of an operator for the primal problem to a question about feasibility of an operator for the dual problem. In particular, we use the observation that if for a feasible solution X to equation (4) , $\mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}(Q_0^{\otimes n} X)$ represents a feasible solution to (5), then X represents an optimal solution for (4) (this is in fact an if and only if relation, but we only need one of the implications for our purpose). This observation follows from strong duality for semidefinite programming, and the fact that $\mathrm{Tr}\left(\mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}(Q_0^{\otimes n} X)\right) = \mathrm{Tr}(Q_0^{\otimes n} X) = \left\langle Q_0^{\otimes n}, X \right\rangle$.

In our case, we have that Q_0 is given by $\left|\psi_0^1\right\rangle\left\langle\psi_0^1\right| + \left|\psi_0^2\right\rangle\left\langle\psi_0^2\right| + \left|\psi_0^3\right\rangle\left\langle\psi_0^3\right|$, where the $\psi_0^i \in \mathcal{X} \otimes \mathcal{Y}$ are defined as

$$\begin{aligned}\left|\psi_0^1\right\rangle &= \alpha \sin(\theta) \left|00\right\rangle - \sqrt{1-\alpha^2} \cos(\theta) \left|11\right\rangle, \\ \left|\psi_0^2\right\rangle &= \alpha \sin(\theta) \left|01\right\rangle + \sqrt{1-\alpha^2} \cos(\theta) \left|10\right\rangle, \\ \left|\psi_0^3\right\rangle &= \alpha \cos(\theta) \left|01\right\rangle - \sqrt{1-\alpha^2} \sin(\theta) \left|10\right\rangle.\end{aligned} \tag{A15}$$

This can be seen by considering the definition of P_0 given by the states in (A15), and observing that the operator Ψ_ρ such that $J(\Psi_\rho) = \overline{uu^*}$ maps a state $\gamma \in \mathrm{D}\left(\mathcal{Z}\right)$ to $\left(\alpha\left|0\right\rangle\left\langle 0\right| + \sqrt{1-\alpha^2}\left|1\right\rangle\left\langle 1\right|\right)\gamma\left(\alpha\left|0\right\rangle\left\langle 0\right| + \sqrt{1-\alpha^2}\left|1\right\rangle\left\langle 1\right|\right)$.

Similarly, for Φ_1 we have that the corresponding solution to the primal problem in (4) is given by

$$X = \sum_{\vec{i},\vec{j}\in\{0,1\}^n} \left|ii\right\rangle\left\langle jj\right| (-1)^{\wedge\vec{i} + \bigoplus \vec{i} + \wedge\vec{j} + \bigoplus \vec{j}}$$

$$
\begin{aligned}
\mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}(Q_0^{\otimes n}X) &= \mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}\left(\left|\psi_0^1\right\rangle\left\langle\psi_0^1\right|^{\otimes n}X\right)\\
&= \mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}\Big(\sum_{\vec{i},\vec{k}\in\{0,1\}^n}(-\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{i}|}(\alpha\sin(\theta))^{n-|\vec{i}|}(-\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{k}|}(\alpha\sin(\theta))^{n-|\vec{k}|}\left|ii\right\rangle\left\langle kk\right|\\
&\qquad\sum_{\vec{l},\vec{j}\in\{0,1\}^n}\left|ll\right\rangle\left\langle jj\right|(-1)^{\wedge\vec{l}+\bigoplus\vec{l}+\wedge\vec{j}+\bigoplus\vec{j}}\Big)\\
&= \mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}\Big(\sum_{\vec{k}\in\{0,1\}^n}(-\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{k}|}(\alpha\sin(\theta))^{n-|\vec{k}|}(-1)^{\wedge\vec{k}+\bigoplus\vec{k}}\\
&\qquad\sum_{\vec{i},\vec{j}\in\{0,1\}^n}(-\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{i}|}(\alpha\sin(\theta))^{n-|\vec{i}|}(-1)^{\wedge\vec{j}+\bigoplus\vec{j}}\left|ii\right\rangle\left\langle jj\right|\Big)\\
&= \sum_{\vec{k}\in\{0,1\}^n}(-\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{k}|}(\alpha\sin(\theta))^{n-|\vec{k}|}(-1)^{\wedge\vec{k}+\bigoplus\vec{k}}\\
&\qquad\Big(\sum_{\vec{i},\vec{j}\in\{0,1\}^n}(-\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{i}|}(\alpha\sin(\theta))^{n-|\vec{i}|}(-1)^{\wedge\vec{i}+\bigoplus\vec{i}}\left|i\right\rangle\left\langle i\right|\Big)\\
&= \sum_{\vec{k}\in\{0,1\}^n}(\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{k}|}(\alpha\sin(\theta))^{n-|\vec{k}|}(-1)^{\wedge\vec{k}}\\
&\qquad\Big(\sum_{\vec{i}\in\{0,1\}^n}(\sqrt{1-\alpha^2}\cos(\theta))^{|\vec{i}|}(\alpha\sin(\theta))^{n-|\vec{i}|}(-1)^{\wedge\vec{i}}\left|i\right\rangle\left\langle i\right|\Big).
\end{aligned}
\tag{A16}
$$

To verify feasibility of this operator for the dual problem, it would suffice then to check that $\mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}(Q_0^{\otimes n}X)\otimes\mathbb{1}_{\mathcal{Y}_{1\cdots n}}$ satisfies the $\leq$ relationship when compared to

$$
Q_0^{\otimes n} = \Big((\alpha\sin(\theta)\left|00\right\rangle - \sqrt{1-\alpha^2}\cos(\theta)\left|11\right\rangle)(\alpha\sin(\theta)\left\langle 00\right| - \sqrt{1-\alpha^2}\cos(\theta)\left\langle 11\right|) + \alpha^2\left|01\right\rangle\left\langle 01\right| + (1-\alpha^2)\left|10\right\rangle\left\langle 10\right|\Big)^{\otimes n}.
\tag{A17}
$$

In order to do this, it might be helpful to consider the fact that we can rewrite $\mathrm{Tr}_{\mathcal{Y}_{1\cdots n}}(Q_0^{\otimes n}X)$ as

$$
\begin{aligned}
&\Big((\sqrt{1-\alpha^2}\cos(\theta)+\alpha\sin(\theta))^n - 2(\sqrt{1-\alpha^2}\cos(\theta))^n\Big) *\\
&\Big((\alpha\sin(\theta)\left|0\right\rangle\left\langle 0\right| + \sqrt{1-\alpha^2}\cos(\theta)\left|1\right\rangle\left\langle 1\right|)^{\otimes n} - 2(\sqrt{1-\alpha^2}\cos(\theta)\left|1\right\rangle\left\langle 1\right|)^{\otimes n}\Big).
\end{aligned}
\tag{A18}
$$