Quantum Coin Hedging, and a Counter Measure*

Maor Ganz[1] and Or Sattath[2]

1 The Hebrew University, Jerusalem, Israel
maor.ganz@mail.huji.ac.il
2 The Hebrew University, Jerusalem, Israel and MIT, Cambridge, USA
sattath@cs.huji.ac.il

Abstract

A quantum board game is a multi-round protocol between a single quantum player against the quantum board. Molina and Watrous discovered quantum hedging. They gave an example for perfect quantum hedging: a board game with winning probability < 1, such that the player can win with certainty at least 1-out-of-2 quantum board games played in parallel. Here we show that perfect quantum hedging occurs in a cryptographic protocol – quantum coin flipping. For this reason, when cryptographic protocols are composed in parallel, hedging may introduce serious challenges into their analysis.

We also show that hedging cannot occur when playing two-outcome board games in sequence. This is done by showing a formula for the value of sequential two-outcome board games, which depends only on the optimal value of a single board game; this formula applies in a more general setting of possible target functions, in which hedging is only a special case.

1998 ACM Subject Classification F.1.1 Models of Computation, D.4.6. Security and Protection

Keywords and phrases Quantum hedging, Quantum coin-flipping, Quantum cryptography

Digital Object Identifier 10.4230/LIPIcs.TQC.2017.4

1 Introduction

Quantum board games

A quantum board game is a special type of an interactive quantum protocol. The protocol involves two parties: the player and the board. The board implements the rules of the game: in each round i of the protocol, the board applies some quantum operation O_i and sends a quantum message to the player; then the player applies any quantum operation it wants, and sends a quantum message back to the board. At the final round of the board game, the board applies a two outcome measurement, which determines whether the player won or lost. We assume that the player knows the rules of the board game (the length of the messages, the operations O_i and the two outcome measurement). The player has the freedom to decide on his strategy – the protocol does not specify what the player should do in each round; the only constraint posed on the player is that it must send a message of an appropriate length, as expected by the board.[1]

* This work was supported by ERC Grant 030-8301.

[1] Previous works which studied this setting did not introduce a specific term for it [22]. Other, related notions are interactive proof system, that differ from quantum board games since the verifier and prover receive an input, and from quantum games since usually we think of the players, Alice and Bob, as having symmetric roles, whereas here, the player knows that the board only implements the rules of the game, and uses its specified strategy.

Perfect hedging

Molina and Watrous showed that hedging is possible in quantum board games [22]. Perfect hedging is best explained by an example: there exists a quantum board game for which no strategy can win with certainty, but it is possible for a player to guarantee winning 1-out-of-2 independent quantum board games, which are played in parallel. A formal definition of hedging is given in Definition (3), but for now, one can think of that example. In a follow up work, Arunachalam, Molina and Russo [6] analyzed a family of quantum board games, and showed a necessary and sufficient condition so that the player can win with certainty in at least 1-out-of-n board games. As discussed later, quantum hedging is known to be a purely quantum phenomenon.

One example where Hedging becomes relevant is when reducing the error (soundness) probability of quantum interactive proof protocols such as QIP(2): since the optimal strategy for winning t-out-of-n parallel repetitions is not necessarily an independent strategy, only Markov bound (and not the Chernoff bound) can be used to show soundness [14]. These aspects resembles the behavior that occurs in the setting of Raz's (classical) parallel repetition theorem [25]; the differences are that in the classical setting there are two players who want to win all board games, whereas in our setting, there is a single player, who wants to win at least t-out-of-n board games.

Coin flipping

Quantum coin flipping is a two player cryptographic protocol which simulates a balanced coin flip. When Alice and Bob are honest, they both agree on the outcome, which is uniform on $\{0, 1\}$. Coin flipping comes in two flavors: Strong and weak. Perhaps the most intuitive one is *weak coin flipping*, in which each side has an opposite desirable outcome: 0 implies that Alice wins, and 1 implies that Bob wins. An important parameter is the optimal winning probability for a cheating player against an honest player. In weak coin flipping we denote them by P_A and P_B. We define $P^* = \max\{P_A, P_B\}$ – the maximum cheating probability of both players. In a *strong coin flipping*, a cheating player might try to bias the result to any outcome. We define P_A^0 to be the maximal winning probability of a cheating Alice who tries to bias the result to 0, and P_A^1, P_B^0, P_B^1 are defined similarly. In strong coin flipping $P^* = \max\left\{P_A^0, P_A^1, P_B^0, P_B^1\right\}$ that is P^* bounds the possible bias to any of the outcomes, by either a cheating Alice or a cheating Bob. In the classical settings, it is known that without computational assumptions, in any coin flipping protocol (either weak or strong) at least one of the players can guarantee winning with probability 1 ($P^* = 1$) [12]. Under mild computational assumption, coin flipping can be achieved classically [7]. All of the results in the rest of this paper hold information theoretically, that is, without any computational assumptions. Unconditionally secure (i.e. without computational assumptions) quantum strong coin flipping protocols with large but still non-trivial $P^* < 0.9143$ were first discovered by [3]. Kitaev then proved that in strong coin flipping, every protocol must satisfy $P_0^* \cdot P_1^* \geq \frac{1}{2}$, hence $P^* \geq \frac{\sqrt{2}}{2}$ ([16], see also [5]). Therefore, the hope to find protocols with arbitrarily small cheating probability moved to weak coin flipping. Protocols were found with decreasing P^*([26, 4] showed strong coin flipping with $P^* = \frac{3}{4}$, [19] showed weak coin flipping with $P^* = 0.692$), until it was finally proved that there are families of weak coin flipping protocols for which P^* converges to $\frac{1}{2}$ [20] (see also [2]). Following this, [9] showed how such protocol can be adopted, in order to create (arbitrarily close to) optimal strong coin flipping (so that P^* can be made arbitrarily close to $\frac{\sqrt{2}}{2}$). Although this would not be relevant for our work, analysis of coin flipping protocols was adapted, and later implemented, for experimental setups [23, 24]. There is also a strong connection between coin-flipping and bit-commitment protocols [26, 10], and to a lesser extent to oblivious transfer [8].

Is it possible to hedge in quantum coin flips? In Section 2 we give an example for perfect quantum hedging in the context of coin flipping. The result can be best explained in the context of weak coin flipping (although, a similar statement can be proved for strong coin flipping): there exists a weak coin flipping protocol where $P^* = \cos^2(\frac{\pi}{8})$ introduced by Aharonov [1] yet a cheating Bob can guarantee winning in at least 1-out-of-2 board games played in parallel.

Avoiding hedging through sequential repetition

Consider a cryptographic quantum protocol, which involves several uses of quantum two-outcome board games. For example, the protocol may use several occurrences of quantum coin flips played in parallel. As we have seen, the possibility of hedging makes it hard to analyze the resulting protocol, by simply analyzing each of the board games in it. In Section 3 we show that quantum hedging cannot happen when the two-outcome board games are played in sequence, even if the players are computationally unbounded.

We give a more generalized formulation for sequential board games. Suppose the player's utility for the outcome vector $a = (a_1, \ldots, a_n)$ is given by some target function $t(a)$, and the players goal is to maximize $\mathbb{E}[t(a)]$ over all possible strategies. In Theorem 10 we show that this maximal value is fully determined by the properties of each board game, and does *not* require an analysis of the entire system, which is the case when playing in parallel.

The authors are not aware of previous precise mathematical formulation proofs of that sort. It was recently brought to our attention the following intuitive discussion in [13, p. 8], and [17, p. 9] made for related models. The intuition for our proof is fairly simple and arguably not very surprising: if it is possible to hedge n games, then by simulating the board in the first game, and conditioning on some good event, allows the player to hedge $n-1$ games. But since hedging cannot occur in one game, we get a contradiction.

In Appendix B we give examples, in the classical setting, for board games and target functions, such that the sequential value of the board games is larger than the parallel value of the board games, and vice-versa.

Arunachalam, Molina and Russo [6] showed a different approach to avoid hedging: they showed that hedging is impossible in a quantum single round board game played in parallel, where the player has the possibility to force a restart of the board game.

2 Quantum coin flip hedging

In this section we will give an example for a coin flipping protocol, for which a cheater cannot guarantee a win in one flip, but one of the players can force a win in 1-out-of-2 flips:

▶ **Theorem 1.** *There exists a weak coin flipping protocol with $P^* < 1$ s.t. by playing 2 coin flips in parallel, Bob can guarantee winning in at least one of the flips.*

We will first describe the weak coin flipping protocol and its properties, and then analyze the hedging strategy of Bob. We conclude by explaining why Alice cannot hedge.

2.1 The coin flipping protocol

In this work, Aharonov's coin flipping protocol [1] will play an important role.

A quantum coin flipping protocol

Alice		**Bob**
Prepares $\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$		
	second qubit $\longrightarrow$	
		Samples $b \in_R \{0,1\}$.
	sends b $\longleftarrow$	
If $b = 1$, then apply H.		If $b = 1$, then apply H.
Measure in the standard basis		Measure in the standard basis
Alice wins if the outcome is 0		Alice wins if the outcome is 0
Bob wins if the outcome is 1		Bob wins if the outcome is 1

▶ **Theorem 2.** *The protocol above is a weak coin-flipping protocol with* $P^* = P_A = P_B = \cos^2 \frac{\pi}{8}$.

The proof is given in Appendix A. This protocol is not only a weak coin flipping with $P^* = \cos^2 \frac{\pi}{8}$, but also a strong coin flipping protocol with the same value of P^*. The proof is essentially the same. We state the result this way because it provides a natural interpretation for statements such as "Bob wins in 1 out of 2 flips". Of course, similar statements can be made for strong coin flipping, but are omitted for the sake of readability.

2.2 Coin hedging is possible

Assume a cheating Bob plays two coin flips in parallel with an honest Alice (it does not matter if he plays against the same person twice, or against two different players, since they behave the same – because they are honest). We want to know the maximum probability for a cheating Bob to win at least one coin flip. Surprisingly, this is equal to 1 in the protocol we previously described. This is impossible if Bob were to play the two coin flips sequentially (see Theorem 5).

We saw that for one coin flipping, $P_A = P_B = \cos^2 \frac{\pi}{8} \approx 0.853$. By cheating each coin flip independently, the best Bob can get is

$$\Pr\left(\text{Bob wins at-least one game}\right) = 1 - (1 - P_B)^2 = 1 - \left(1 - \cos^2 \frac{\pi}{8}\right)^2 \approx 0.978.$$

We will now show Bob's perfect hedging strategy (which is not independent), in which he wins exactly one out of the two coin flips w.p. 1, which completes the proof of Theorem 2. Alice's initial state is

$$\frac{1}{2} \sum_{i_1, i_2 \in \{0,1\}} |i_1, i_2\rangle |i_1, i_2\rangle = \frac{1}{2} \sum_{i=0}^{3} |\alpha_i\rangle |\alpha_i\rangle, \tag{1}$$

where[2]

$$
\begin{aligned}
|\alpha_0\rangle &= |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) \\
|\alpha_1\rangle &= |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\alpha_2\rangle &= \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle - |\Psi^-\rangle\right) = \frac{1}{\sqrt{2}}(|0-\rangle + |1+\rangle) \\
|\alpha_3\rangle &= \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle + |\Psi^-\rangle\right) = \frac{1}{\sqrt{2}}(|-0\rangle + |+1\rangle)\,. \qquad (2)
\end{aligned}
$$

Eq. (1) can be justified by a direct calculation, or by using the Choi–Jamiołkowski isomorphism [11, 15], see also [27], and noting that the associated matrix for the l.h.s. and the r.h.s. are equal (both are proportional to the identity matrix). Bob is given the right register of the state above. Bob applies the unitary transformation $U = \sum_i |\gamma_i\rangle\langle\alpha_i|$, where $|\gamma_0\rangle = |11\rangle, |\gamma_1\rangle = |00\rangle, |\gamma_2\rangle = |01\rangle, |\gamma_3\rangle = |10\rangle$, so that the overall state becomes $\frac{1}{2}\sum_{i=0}^{3}|\alpha_i\rangle|\gamma_i\rangle$, and sends the right register back to Alice. Alice measures the right register in the standard basis (of course, Bob could have done this just before sending the right register, if he is restricted to sending classical information). The results of those measurements determines the basis in which she measures the left register. This strategy guarantees that Bob wins in exactly one coin flip: for example, if Alice measures the qubits $|\gamma_0\rangle = |11\rangle$ then the left register collapses to $|\alpha_0\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle)$, and since in this case Alice measures both of the left register qubits in the Hadamard basis, Bob will win in exactly one out of the two coin flips. The right-most expressions in Eq. (2) are presented in this form so that it is easy to see the similar behavior in the 3 other cases.

One may wonder how strong the effect of hedging is. In particular, can Bob guarantee fn out of n winnings, as long as $f \leq P^*$? The answer is no: by playing three coin flipping of this protocol, he cannot guarantee winning $2 = \frac{2}{3}\cdot 3$ with probability 1, even though $\frac{2}{3} \leq P^*$: we numerically calculated that Bob can only win with probability ≈ 0.986 at least 2 out of 3 coin flips. This is still higher than the optimal independent cheating that achieves a success probability of ≈ 0.94.

Fortunately for Bob, Alice can not guarantee winning in 1-out-of-2 played in parallel using this weak coin flipping protocol. In fact, she cannot do any hedging. This is true, essentially for the same reasons error reduction for QMA works in a simple manner (vis-à-vis QIP(2)). The following argument uses the definitions from Section 3.1. Recall that from Bob's perspective, he is provided with a quantum state given from Alice, and he measures it to determine whether he wins or loses. Therefore $m(a_i) = \min_{|\psi_i\rangle}\langle\psi_i|M^i_{a_i}|\psi_i\rangle$ (where $M^i_{a_i}$ is Bob's measurement operator which determines whether he gets the outcome a_i in the i^{th} game), which is equal to the smallest eigenvalue of $M^i_{a_i}$; and $m^{par}(a_1,\ldots,a_n) = \min_{|\psi\rangle}\langle\psi|M^i_{a_1}\otimes\cdots\otimes M^i_{a_n}|\psi\rangle$ which is equal to the smallest eigenvalue of $M^i_{a_1}\otimes\cdots\otimes M^i_{a_n}$. But since $M^i_{a_i}$ is a measurement operator, its eigenvalues are non-negative, and we conclude that $m^{par}(a_1,\ldots,a_n) = m(a_1)\cdot\ldots\cdot m(a_n)$.

[2] One may wonder whether the states $|\alpha_i\rangle$ are the Bell states ($|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$), written in a non-standard local basis. This is not the case: for every Bell state $|\Omega\rangle$, $SWAP|\Omega\rangle = \pm|\Omega\rangle$. This is also true if a local basis change is applied to both qubits: for $|\Omega'\rangle = U\otimes U|\Omega\rangle$, $SWAP|\Omega'\rangle = \pm|\Omega'\rangle$. Since $|\alpha_2\rangle = SWAP|\alpha_3\rangle \neq \pm|\alpha_2\rangle$, these vectors are not the Bell states written in a non-standard local basis.

3 How to circumvent hedging

Our solution to circumvent hedging is to play the board games in sequence, instead of in parallel. We will prove in Section 3.1 that in the simple scenario, in which the goal is to win at least 1-out-of-n sequential board games, hedging is not possible (i.e. the best cheating strategy is to use the optimal cheating strategy in each board game independently). We will generalize this in Section 3.2, where we will prove that the same result holds for every target function. Throughout this section, we will consider only two-outcome board games (such as coin flipping), but a generalization to any number of outcomes seems not too difficult to achieve as well.

3.1 Playing sequentially circumvents 1-out-of-n hedging

Molina and Watrous [22] defined *hedging* as the following phenomenon.[3] Suppose G_1, G_2 are two board games with multiple outcomes A_1, A_2. For $a_1 \in A_1$ let $m(a_1)$ be the minimal probability that can be achieved for the outcome a_1 in G_1, and similarly for $m(a_2)$. If the board game G is not clear from the context, we may use $m^{G_2}(a_2)$. Now suppose that two board games are played in parallel, and the goal is to minimize the probability for getting the outcome a_1 in the first board game and a_2 in the second board game, which is defined as $m^{par}(a_1, a_2)$. Since the two strategies can be played independently, clearly, $m^{par}(a_1, a_2) \leq m(a_1)\, m(a_2)$. *Parallel Hedging* for two board games is the case where this inequality is strict, that is $m^{par}(a_1, a_2) < m(a_1)\, m(a_2)$. Molina and Watrous gave an example for perfect parallel hedging in which $m^{par}(a_1, a_2) = 0$ whereas $m(a_1) = m(a_2) > 0$. This definition can be naturally generalized to more than two board games.

▶ **Definition 3** (Parallel Hedging)**.** Let $G_1, \dots, G_n$ be n quantum board games with possible outcomes $A_1, \dots, A_n$. For $a_i \in A_i$, let $m(a_i)$ be the minimal probability that can be achieved for the outcome a_i in G_i. Similarly, let $m^{par}(a_1, \dots, a_n)$ be the minimal probability that can be achieved for outcomes $(a_1, \dots, a_n)$ when playing these n board games in parallel. We say that hedging is possible in 1-out-of-n board games if there exist $a_1, \dots, a_n$ s.t.

$$m^{par}(a_1, a_2, \dots, a_n) < \prod_{i=1}^{n} m(a_i)\,. \tag{3}$$

If $m^{par}(a_1, a_2, \dots, a_n) = 0$ and $\prod_{i=1}^{n} m(a_i) > 0$, then it is called *prefect hedging*.

It is known that inequality (3) is actually an equality in the classical case for single round board games [22, 18]. We do not know whether the equality holds for multi-round classical board games. What happens when the board games are played in sequence?

▶ **Definition 4.** Given board games $\{G_i\}_{i=1}^{n}$, the protocol for playing the board games $\{G_i\}$ in order is called *sequential*, assuming the player knows the result of G_i before the start of G_{i+1} (this can be achieved by adding a last round for each board game in which the board returns the outcome).

Our next result shows that there is no sequential hedging for board games (with any number of outcomes), and the cheater cannot do better than to cheat each board game independently;

[3] Molina and Watrous restricted their definition to quantum board games with a single round of communication (the board sends an initial quantum state to the player, the player sends back another quantum state back to the board, and then the board applies a measurement to determine whether the player wins).

that is if $\{G_i\}_{i=1}^{n}$ are board games, then $m^{seq}(a_1,\ldots,a_n) = m(a_1)\cdot\ldots\cdot m(a_n)$, where $m^{seq}(a_1,\ldots,a_n)$ is defined similarly to $m^{par}(a_1,\ldots,a_n)$ for sequential board games. For simplicity and clarity, we will consider only the case where all the board games are identical and $a_i = a_j = a$ for all i,j, but the same proof will work for the general scenario as well (one will just have to add indices indicating the board game for everything).

▶ **Theorem 5.** *Let G be a board game, played sequentially n times, then $m^{seq}(a,\ldots,a) = m(a)\cdot\ldots\cdot m(a) = m(a)^n$ for every outcome a.*

Proof. If the outcome of a single board game is a, then we say that the player *lost* that board game. We denote by "*failure*" the event in which the player gets the outcome a in all n games (i.e. loses all n rounds).

We define ℓ^* to be the probability to get the outcome a in the optimal strategy for one board game. Let ℓ_n be probability to get the outcome a over all the n-board games, in the best independent strategy. It is easy to see that

$$\ell_n = \min_{S\in\text{independent strategies}} \Pr(\text{failure} \mid S) = (\ell^*)^n \tag{4}$$

Define similarly ℓ'_n to be the minimum losing probability over all (not necessarily independent) strategies, i.e. $\ell'_n \equiv \min_{S\in\text{sequential strategies}} \Pr(\text{failure} \mid S)$. Clearly $\forall n\in\mathbb{N},\ \ell'_n \le \ell_n$ and $\ell'_1 = \ell_1$. Our goal is to show that $\forall n\in\mathbb{N},\ \ell'_n = \ell_n$. Assume towards a contradiction that this is not the case. Then there exists a minimal $n>1$ for which $\ell'_n < \ell_n$.

$$(\ell^*)^n \overset{\text{by (4)}}{=} \ell_n > \ell'_n = \ell'_{n,L}\Pr(\text{lost first round}) \ge \ell'_{n,L}\ell^*$$

where $\ell'_{n,L} := \Pr(\text{failure} \mid \text{lost first round})$. The last inequality naturally holds because $\Pr(\text{lost first round}) \ge \ell^*$, otherwise there exists a better strategy. Therefore,

$$(\ell^*)^{n-1} = \ell_{n-1} > \ell'_{n,L}$$

The strategy in which the cheater Alice (the first player) plays with Rob (Alice's imaginary friend) the first board game, and conditioned on losing, plays with Bob (the second player) the next rounds, has a losing probability $\ell'_{n,L}$.

Therefore

$$\ell_{n-1} > \ell'_{n,L} \ge \ell'_{n-1}$$

which contradicts the minimality of n. ◀

▶ **Corollary 6.** *Suppose the goal of a player is to win at least 1-out-of-n board games played sequentially. The optimal strategy is to play independently, by using the optimal cheating strategy in each of the board games.*

3.2 Playing sequentially circumvents any form of hedging

Let us consider a more general setting, in which the player's goal is to maximize the expectation of some target function; i.e., for a vector $t = (t_a\in\mathbb{R})_{a\in\{0,1\}^n}$, let

$$\mathrm{SVal}(t) \equiv \max_{S\in\text{sequential strategies}} \sum_{a\in\{0,1\}^n} t_a\cdot\Pr(a \mid S)$$

and similarly

$$\mathrm{PVal}(t) \equiv \max_{S\in\text{parallel strategies}} \sum_{a\in\{0,1\}^n} t_a\cdot\Pr(a \mid S)\,.$$

In general there are no relations between the parallel and sequential values: in Appendix B we give a classical one round board game in which $\mathrm{SVal}(t) > \mathrm{PVal}(t)$ and another in which $\mathrm{SVal}(t) < \mathrm{PVal}(t)$.

▶ **Definition 7.** Given a two-outcome board game, let q_i be the maximal probability of the player to achieve the outcome $i \in \{0,1\}$.

Note that always $q_0 \geq 1 - q_1$ and vice-versa. As we have seen before, the parallel value of a two-outcome board game heavily depends on the details of the game. In contrast, the sequential value is fully determined by q_0 and q_1.

In the following we will analyze the sequential value of the board game. For that we will define the tree value function TVal, which as the following theorem shows, is equal to the sequential value of the board game. For simplicity we will assume that for all i, $G_i = G$, but this can be easily extended for general $\{G_i\}_{i=1}^n$.

▶ **Definition 8.** For a vector $t = (t_a)_{a\in\{0,1\}^n}$ let $t_b^{\leftarrow} = t_{0b}$ and $t_b^{\rightarrow} = t_{1b}$. The tree value with parameters q_0, q_1 is defined as:

$$\mathrm{TVal}(t) \equiv \max\left\{q_0\,\mathrm{TVal}(t^{\leftarrow}) + (1-q_0)\,\mathrm{TVal}(t^{\rightarrow})\ ,\ q_1\,\mathrm{TVal}(t^{\rightarrow}) + (1-q_1)\,\mathrm{TVal}(t^{\leftarrow})\right\},$$

and for $c \in \mathbb{R}$, $\mathrm{TVal}(c) = c$.

▶ **Definition 9.** Consider a quantum board game G played n times in sequence. A strategy is said to be *pure black box* strategy if the strategy used in the i-th board game is fully determined by the outcomes of the previous board games. For a set $\mathcal{S}$ of strategies for a single board game G, an $\mathcal{S}$-black-box strategy is a pure black-box strategy in which the strategy at the i-th board game (conditioning on previous outcomes) is in $\mathcal{S}$.

▶ **Theorem 10.** *For every two-outcome board game (with parameters q_0, q_1), every n and every $t \in \mathbb{R}^{2^n}$, $\mathrm{SVal}(t) = \mathrm{TVal}(t)$.*

Furthermore, its value can be obtained by an $\{S_0, S_1\}$-black-box strategy, where S_0 (S_1) are any strategies that achieve outcomes 0 (1) with probability q_0 (q_1).

S_0 and S_1 are greedy strategies that simply try to maximize the chance of achieving the outcomes 0 and 1 respectively in the board game at hand. This theorem is in fact a generalization of Theorem 5 for 2-outcome board games: By choosing $t_a = 1 - \delta_{a,a'}$ we get that

$$\begin{aligned}\mathrm{SVal}(t) &\equiv \max_{S\in\text{sequential strategies}} \sum_{a\in\{0,1\}^n} t_a \cdot \Pr(a \mid S) = \max_{S\in\text{sequential strategies}} \sum_{a\neq a'} \Pr(a \mid S)\\ &= \max_{S\in\text{sequential strategies}} 1 - \Pr(a' \mid S)\\ &= 1 - \min_{S\in\text{sequential strategies}} \Pr(a' \mid S) = 1 - m^{seq}(a')\,. \end{aligned} \tag{5}$$

By expanding the recursion, a simple inductive argument shows that for our choice of t,

$$\mathrm{TVal}(t) = 1 - m(a_1)\cdot \ldots \cdot m(a_n). \tag{6}$$

By combining Theorem 10 and Eqs. (5) and (6), we reprove Theorem 5.

Proof of Theorem 10. First we show that $\mathrm{SVal}(t) \geq \mathrm{TVal}(t)$, by explicitly constructing an $\{S_0, S_1\}$-black-box strategy with the value $\mathrm{TVal}(t)$. The strategy can be best explained by defining a binary full tree with depth n. We fill the value of each node in the tree, from

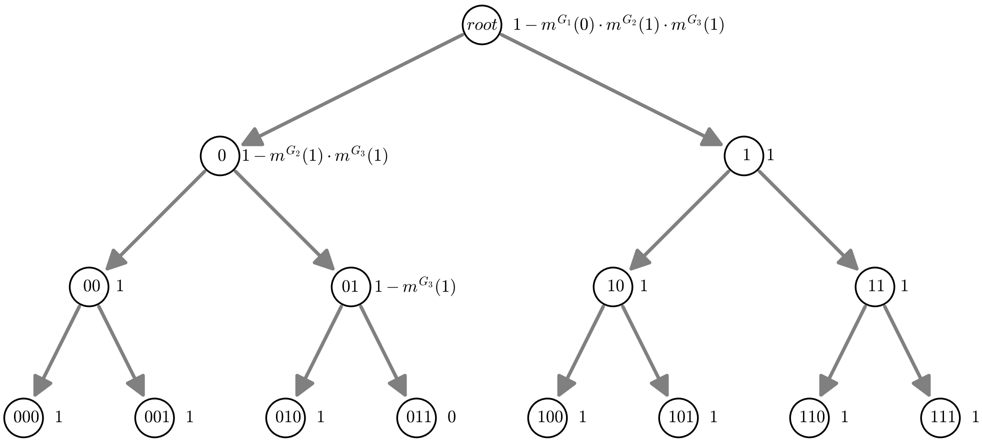

Figure 1 TVal for $t_a = 1 - \delta_{a,011}$. The labels of the leaves represent all the possible outcomes a of the values in the $n = 3$ board games, and the values on the right of each node are the TVal of that node. Indeed $t_a = 1$ for all $a \neq 011$. Note that $m(0) = 1 - q_1$ and $m(1) = 1 - q_0$, and for example $\mathrm{TVal}(01) = q_0 = 1 - m^{G_3}(1)$, and $\mathrm{TVal}(0) = q_0 + (1 - q_0) q_0 = 1 - m^{G_2}(1) + m^{G_2}(1)\left(1 - m^{G_3}(1)\right) = 1 - m^{G_2}(1) \cdot m^{G_3}(1)$.

bottom to top. The leaves of the tree will have values t_a. The values of a parent of two children with values $v^{\leftarrow}, v^{\rightarrow}$ will have the value:

$$\max\{q_0 v^{\leftarrow} + (1 - q_0) v^{\rightarrow}, q_1 v^{\rightarrow} + (1 - q_1) v^{\leftarrow}\}$$

It can be easily verified that the value of the root is $\mathrm{TVal}(t)$.

Consider the following strategy which applies S_0 if $q_0 v^{\leftarrow} + (1 - q_0) v^{\rightarrow} \geq q_1 v^{\rightarrow} + (1 - q_1) v^{\leftarrow}$ and S_1 otherwise, and continues in the same fashion with respect to the left child if the outcome is 0, and the right child if the outcome is 1. It can be proved by a simple inductive argument that the expected value of this strategy is the value of the root which is indeed $\mathrm{TVal}(t)$. Clearly, this strategy is an $\{S_0, S_1\}$ black-box strategy.

Next we show that $\mathrm{SVal}(t) \leq \mathrm{TVal}(t)$. This will be proven by induction on n – the number of board games played. Clearly, for $n = 1$, the optimal strategy has the value $\mathrm{TVal}(t)$. Let n be the minimal number, such that there exists some target t, for which there is a strategy with value greater than $\mathrm{TVal}(t)$ and denote the contradicting strategy by S. We now introduce some notation. Let $p^j = \Pr(j \text{ in first game} \mid \text{using strategy } S)$, $p^j_{\mathbf{i}} = \Pr(\mathbf{i} \text{ in the last n-1 games} \mid j \text{ in the first game, using strategy } S)$. Let $\mathcal{S}^n$ be the set of all strategies over n sequential board games.

$$\mathrm{opt} = \max_{S' \in \mathcal{S}^n} \sum_{\mathbf{i} \in 2^n} t_{\mathbf{i}} \Pr(\mathbf{i} \mid \text{ using strategy } S')$$

For $j \in \{0, 1\}$, let $\mathrm{opt}^j \equiv \max_{S' \in \mathcal{S}^{n-1}} \sum_{\mathbf{i} \in 2^{n-1}} t_{j,\mathbf{i}} \Pr(\mathbf{i} \mid \text{using strategy } S')$. Since the optimization is over board games of length $n - 1$, by the induction hypothesis, $\mathrm{opt}^0 = \mathrm{TVal}(t^{\leftarrow})$, and similarly $\mathrm{opt}^1 = \mathrm{TVal}(t^{\rightarrow})$. We know that

$$\mathrm{opt} > q_0 \cdot \mathrm{opt}^0 + (1 - q_0) \cdot \mathrm{opt}^1 \tag{7}$$

and similarly

$$\mathrm{opt} > q_1 \cdot \mathrm{opt}^1 + (1 - q_1) \cdot \mathrm{opt}^0 \tag{8}$$

otherwise, $\mathrm{opt} = \mathrm{TVal}(t)$. Assume WLOG that

$$q_0 \cdot \mathrm{opt}^0 + (1 - q_0) \cdot \mathrm{opt}^1 \geq q_1 \cdot \mathrm{opt}^1 + (1 - q_1) \cdot \mathrm{opt}^0$$

then we get that $\mathrm{opt}^0 (q_0 - 1 + q_1) \geq \mathrm{opt}^1 (q_1 - 1 + q_0)$ hence $\mathrm{opt}^0 \geq \mathrm{opt}^1$ or $(q_1 - 1 + q_0) \leq 0$, because $q_0 \geq 1 - q_1$. Since $p^j \leq q_j$ we get that $q_0 + q_1 \leq 1$ implies $p^0 = q_0$ and $p^1 = q_1$. We know that (for both the above cases)

$$\mathrm{opt} = \sum_{\mathbf{i} \in 2^{n-1}} t_{\mathbf{i}}^{\leftarrow} p^0 p_{\mathbf{i}}^0 + t_{\mathbf{i}}^{\rightarrow} p^1 p_{\mathbf{i}}^1.$$

Let us denote

$$v^0 = \sum_{\mathbf{i} \in 2^{n-1}} t_{\mathbf{i}}^{\leftarrow} p_{\mathbf{i}}^0 \ , \ v^1 = \sum_{\mathbf{i} \in 2^{n-1}} t_{\mathbf{i}}^{\rightarrow} p_{\mathbf{i}}^1$$

hence $\mathrm{opt} = p^0 v^0 + p^1 v^1$ where $p^j \leq q_j$.

▶ **Claim 11.** $v^j \leq opt^j$

Proof. The cheater can play himself (his honest self), according to his strategy, until he gets j in the first board game and then continue to play the rest $(n-1)$ of the board games against the real honest player. This is a valid strategy for $n - 1$ board games with value v^j, but since opt^j is an optimal such strategy, we get that $v^j \leq \mathrm{opt}^j$. ◀

Using the above claim,

$$\mathrm{opt} = p^0 v^0 + p^1 v^1 \leq p^0 \mathrm{opt}^0 + p^1 \mathrm{opt}^1 = p^0 \mathrm{opt}^0 + \left(1 - p^0\right) \mathrm{opt}^1. \tag{9}$$

By subtracting Eq. 9 from Eq. 7 we get that

$$0 > \mathrm{opt}^0 \left(q_0 - p^0\right) + \mathrm{opt}^1 \left(1 - q_0 - 1 + p^0\right) = \left(\mathrm{opt}^0 - \mathrm{opt}^1\right) \left(q_0 - p^0\right)$$

but either $\mathrm{opt}^0 \geq \mathrm{opt}^1$, $q_0 \geq p^0$ and we get $0 > 0$ and contradiction, or $p^0 = q_0$ hence again we get $0 > 0$ and contradiction. Altogether we now know that Eq. (7) is wrong, hence

$$\mathrm{opt} = q_0 \cdot \mathrm{opt}^0 + (1 - q_0) \cdot \mathrm{opt}^1 \tag{10}$$

and by the hypothesis assumption we get that $\mathrm{opt} = \mathrm{TVal}\,(t)$. ◀

4 Open questions

- Is there a formal connection between the setting discussed in the parallel repetition Theorem (as was discussed in the introduction) and the setting that occurs in quantum hedging?
- How general is coin hedging? Does hedging (as in Definition 3) happen in every non-trivial ($\epsilon < \frac{1}{2}$) coin flipping protocol? The same questions can be asked for perfect hedging. We conjecture that the answer for these questions is positive.
- In our example for coin hedging, we saw that the hedging player reduces the expected number of wins: The cheater could guarantee that he will win one flip out of two, thus getting an expectation 0.5 for winning, while the expectation of winning in independent cheating is ≈ 0.85. Does the expected ratio of wins in the perfect hedging of this protocol scenario increase with n? In this protocol (or, perhaps, another coin flipping protocol),

when flipping n coins in parallel and $n \to \infty$, can Bob guarantee winning $\sim nP^*$ coin flipping out of n (Of course the expected number of parallel wins cannot be higher than the expected number of independent wins (which is $\frac{1}{2}$), as was proved formally in [21])?

This property cannot hold for every protocol. The reason is essentially that P^* can be artificially increased in a way which does not help the cheating player to achieve perfect hedging. Consider some coin flipping protocol with $P^* = \frac{1}{2}$ (even though this is impossible, for $P^* > \frac{1}{2}$ a simple adaptation of the following argument applies), then a cheating Bob clearly cannot guarantee winning more than $\frac{1}{2}n$. If we now alter the protocol, such that in the last round of the protocol, with probability δ, Alice asks Bob what his outcome of the protocol was, and declares that as her outcome. This changes P^* to $P^{*\prime} = \frac{1}{2} + \frac{\delta}{2}$, but with probability δ^n these protocols coincide, and Bob cannot guarantee more than $\frac{1}{2}n$ wins, which is less than $P^{*\prime}n$ as required by the statement above.

- Can one define and show hedging for bit-commitment?

Acknowledgments. We thank Dorit Aharonov for the weak coin flipping protocol which we used and other valuable discussions, and to the anonymous referees for their comments.

References

1. Dorit Aharonov. Personal communication, 2007.
2. Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. *SIAM J. Comput.*, 45(3):633–679, 2016. doi:10.1137/14096387X.
3. Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew Chi-Chih Yao. Quantum bit escrow. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 705–714. ACM, 2000. doi:10.1145/335305.335404.
4. Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, 2004. doi:10.1016/j.jcss.2003.07.010.
5. Andris Ambainis, Harry Buhrman, Yevgenity Dodis, and Hein Rörig. Multiparty quantum coin flipping. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259. IEEE Computer Society, 2004. doi:10.1109/CCC.2004.19.
6. Srinivasan Arunachalam, Abel Molina, and Vincent Russo. Quantum hedging in two-round prover-verifier interactions. *arxiv preprint arxiv:1310.7954*, 2013. arXiv:1310.7954.
7. Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, 1983. doi:10.1145/1008908.1008911.
8. André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago J. Theor. Comput. Sci.*, 2016, 2016. arXiv:1310.3262.
9. André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*, pages 527–533. IEEE Computer Society, 2009. doi:10.1109/FOCS.2009.71.
10. André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In Rafail Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 354–362. IEEE Computer Society, 2011. doi:10.1109/FOCS.2011.42.
11. Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975. doi:10.1016/0024-3795(75)90075-0.

12 Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In Juris Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 364–369. ACM, 1986. doi:10.1145/12130.12168.

13 Gus Gutoski and John Watrous. Quantum interactive proofs with competing provers. In Volker Diekert and Bruno Durand, editors, *STACS 2005, 22nd Annual Symposium on Theoretical Aspects of Computer Science, Stuttgart, Germany, February 24-26, 2005, Proceedings*, volume 3404 of *Lecture Notes in Computer Science*, pages 605–616. Springer, 2005. doi:10.1007/978-3-540-31856-9_50.

14 Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA*, pages 534–543. IEEE Computer Society, 2009. doi:10.1109/FOCS.2009.30.

15 Andrzej Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972. doi:10.1016/0034-4877(72)90011-0.

16 Alexei Kitaev. Quantum coin flipping. Talk at the 6th workshop on Quantum Information Processing, 2003.

17 Hirotada Kobayashi. General properties of quantum zero-knowledge proofs. In Ran Canetti, editor, *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008.*, volume 4948 of *Lecture Notes in Computer Science*, pages 107–124. Springer, 2008. doi:10.1007/978-3-540-78524-8_7.

18 Rajat Mittal and Mario Szegedy. Product rules in semidefinite programming. In Erzsébet Csuhaj-Varjú and Zoltán Ésik, editors, *Fundamentals of Computation Theory, 16th International Symposium, FCT 2007, Budapest, Hungary, August 27-30, 2007, Proceedings*, volume 4639 of *Lecture Notes in Computer Science*, pages 435–445. Springer, 2007. doi:10.1007/978-3-540-74240-1_38.

19 Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 2–11. IEEE Computer Society, 2004. doi:10.1109/FOCS.2004.55.

20 Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. *arxiv preprint arxiv:0711.4114*, 2007. arXiv:0711.4114.

21 Abel Molina. Parallel repetition of prover-verifier quantum interactions. *Arxiv preprint arXiv:1203.4885*, 2012.

22 Abel Molina and John Watrous. Hedging bets with correlated quantum strategies. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, pages 2614–2629, 2012. doi:10.1098/rspa.2011.0621.

23 Anna Pappa, André Chailloux, Eleni Diamanti, and Iordanis Kerenidis. Practical quantum coin flipping. *Phys. Rev. A*, 84:052305, 2011. doi:10.1103/PhysRevA.84.052305.

24 Anna Pappa, Paul Jouguet, Thomas Lawson, André Chailloux, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis, and Eleni Diamanti. Experimental plug and play quantum coin flipping. *Nature Communications*, 5, 2014. Article. doi:10.1038/ncomms4717.

25 Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, 1998. doi:10.1137/S0097539795280895.

26 Robert W. Spekkens and Terry Rudolph. Degrees of concealments and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(01):012310, 2001. doi:10.1103/PhysRevA.65.012310.

27 John Watrous. *Theory of quantum information.* Available online, 2011. URL: https://cs.uwaterloo.ca/~watrous/TQI/.

A Proof of Theorem 2

We will use the same method we use in other sections, which is based on semi-definite programming (SDP). See, for example, [5]. We will follow the notations used in [2, 20]. We will prove that the maximal cheating probability for both players is $P^* = P_A = P_B = \cos^2 \frac{\pi}{8}$.

If Alice is the cheater, a cheating strategy is described entirely by the one qubit state ρ which she sends to Bob. Her winning probability is given by

$$\Pr(\text{Alice wins}) = \frac{1}{2}\operatorname{Tr}\left(\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)\rho\right).$$

Since

$$\begin{aligned}\max_{\rho\succeq 0, \operatorname{Tr}\rho=1} \frac{1}{2}\operatorname{Tr}\left(\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)\rho\right) &= \max_{|\psi\rangle} \frac{\left\langle\psi\left|\frac{1}{2}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)\right|\psi\right\rangle}{\langle\psi\mid\psi\rangle} \\ &= \lambda_{max}\left(\frac{1}{2}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right)\right) \\ &= \cos^2\frac{\pi}{8},\end{aligned}$$

the maximal cheating probability is $P_A = \cos^2 \frac{\pi}{8}$.

Let us look at a cheating Bob (and an honest Alice). The initial density matrix is $\rho_0^{\mathcal{AM}} = |\phi^+\rangle\langle\phi^+|$ on Alice and the message registers $\mathcal{A}\otimes\mathcal{M}$. Then, Bob applies an operation to the $\mathcal{M}$ qubit. Alice's reduced density matrix cannot be changed due to Bob's operation. Hence our condition is $\operatorname{Tr}_{\mathcal{M}}\rho_1^{\mathcal{AM}} = \rho_1^{\mathcal{A}} = \rho_0^{\mathcal{A}} = \frac{1}{2}I$. Bob's maximal cheating probability is given by:

$$\begin{aligned}\text{maximize}\quad & \operatorname{Tr}\left[\left(|1\rangle\langle 1|\otimes|0\rangle\langle 0| + |-\rangle\langle -|\otimes|1\rangle\langle 1|\right)\cdot\rho_1^{\mathcal{AM}}\right] \\ \text{subject to}\quad & \rho_1^{\mathcal{AM}}\succeq 0 \\ & \rho_0^{\mathcal{AM}} = \left|\Phi^+\right\rangle\left\langle\Phi^+\right| \\ & \operatorname{Tr}_{\mathcal{M}}\rho_1^{\mathcal{AM}} = \rho_0^{\mathcal{A}}\end{aligned} \tag{11}$$

The maximization is justified because if the message qubit is 0, Alice measures her qubit in the computational basis, and Bob wins if her outcome is 1; if the message qubit is 1, Alice measures her qubit in the Hadamard basis, and Bob wins if her outcome is $|-\rangle$.

Solving this SDP gives

$$\rho_1^{\mathcal{AM}} = \begin{pmatrix} 0.0732 & 0 & 0.1768 & 0 \\ 0 & 0.4268 & 0 & -0.1768 \\ 0.1768 & 0 & 0.4268 & 0 \\ 0 & -0.1768 & 0 & 0.0732 \end{pmatrix}$$

with a maximum value of ≈ 0.8536.

It is possible to verify that indeed the value of the SDP is not only close, but is exactly equal to $\cos^2\frac{\pi}{8} \approx 0.8536$: One can see that $P_B \le \cos^2\frac{\pi}{8}$, via Kitaev's formalism to find the Z matrix that bounds ρ (see [20, 2] for details). Alternatively, we can use the SDP formulation of games as described in [22], which applies to the coin-flipping protocol (with Bob as the player): the matrix $Y = \frac{1}{8}\begin{pmatrix} 3+\sqrt{2} & 1 \\ 1 & 1+\sqrt{2}\end{pmatrix}$ is dual-feasible, hence its trace $\operatorname{Tr}[Y] = \frac{1}{4}\left(2+\sqrt{2}\right) = \cos^2\frac{\pi}{8}$ gives the correct bound.

We now show an explicit strategy with winning probability $\cos^2\frac{\pi}{8}$, which shows that $P_B \geq \cos^2\frac{\pi}{8}$, which completes the proof. Bob applies a $-\frac{3\pi}{8}$ rotation

$$U = \begin{pmatrix} \cos -\frac{3\pi}{8} & -\sin -\frac{3\pi}{8} \\ \sin -\frac{3\pi}{8} & \cos -\frac{3\pi}{8} \end{pmatrix} = \begin{pmatrix} \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \\ -\cos\frac{\pi}{8} & \sin\frac{\pi}{8} \end{pmatrix}$$

on the $\mathcal{M}$ qubit, which transforms the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to:

$$\begin{aligned} |\zeta\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \left(\sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle\right) + |1\rangle \otimes \left(\sin\frac{\pi}{8}|1\rangle + \cos\frac{\pi}{8}|0\rangle\right)\right) \\ &= \frac{1}{\sqrt{2}}\left(\left(\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\right) \otimes |0\rangle\right) + \\ &\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(\left(\sin\frac{\pi}{8} - \cos\frac{\pi}{8}\right)|+\rangle - \left(\cos\frac{\pi}{8} + \sin\frac{\pi}{8}\right)|-\rangle\right) \otimes |1\rangle\right) \end{aligned}$$

We simplify

$$\frac{1}{\sqrt{2}}\left(\sin\frac{\pi}{8} + \cos\frac{\pi}{8}\right) = \frac{1}{\sqrt{2}}\sqrt{\frac{1}{2}\left(2+\sqrt{2}\right)} = \frac{\sqrt{2+\sqrt{2}}}{2} = \cos\frac{\pi}{8}$$

and similarly, $\frac{1}{\sqrt{2}}\left(\cos\frac{\pi}{8} - \sin\frac{\pi}{8}\right) = \frac{\sqrt{2-\sqrt{2}}}{2} = \sin\frac{\pi}{8}$. Hence,

$$|\zeta\rangle = \frac{1}{\sqrt{2}}\left(\left(\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\right)|0\rangle - \left(\sin\frac{\pi}{8}|+\rangle + \cos\frac{\pi}{8}|-\rangle\right)|1\rangle\right).$$

Bob measures the r.h.s. qubit in the computational basis, and sends the classical result to Alice. His winning probability is thus $\cos^2\frac{\pi}{8}$. This completes the proof that $P_A = P_B = P^* = \cos^2\frac{\pi}{8}$.

B Relations between parallel and sequential board games

Here we show that the value of the sequential board games can be larger than the parallel board games and vice-versa, depending on the target function, even in the classical setting. Out standard example for a sequential superiority uses the target function: "must win *exactly* 1-out-of-2 board games". This of course, gives the sequential run an advantage over the parallel run, of knowing the outcomes of the previous board games. For that we define a very simple one-round board game: the player chooses a bit b, which is sent to the board.

- If $b = 0$, the player loses (with probability 1).
- If $b = 1$, the player wins with probability $\frac{1}{2}$.

▶ **Lemma 12.** *In the above board game,* $\mathrm{SVal}(t) \geq \frac{3}{4} > \frac{1}{2} = \mathrm{PVal}(t)$.

Proof. The optimal winning probability in a single board game for an honest player is $\frac{1}{2}$ by always sending $b = 1$. Also note, that the player can force a loss with probability 1, by sending $b = 0$. Assume that we are now playing two board games. If the board games are played in sequence, then the optimal strategy will be to try and win the first board game by sending $b_1 = 1$. With probability $\frac{1}{2}$ he will win, then he can lose the second board game by sending $b_2 = 0$. If the player lost the first board game, he will try to win the second board game by sending $b_2 = 1$. Altogether, this strategy wins exactly once with probability $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$, proving the first inequality.

Let us look at the four deterministic possibilities for the player when the two board games are played in parallel. If he sends $b_0 = b_1 = 0$, he then loses with probability 1. If he sends $b_0 \neq b_1$, i.e. loses one of the board games and tries to win the other, then his winning probability of exactly one board game is $\frac{1}{2}$. If he sends $b_0 = b_1 = 1$, i.e. trying to win both, then his winning probability of exactly one board game is again $\frac{1}{2}$ (because no matter what the outcome of the first board game is, the second outcome must be different, and this happens with probability $\frac{1}{2}$). Since every random strategy is a convex combination of these deterministic strategies, every classical strategy will also have a winning probability of at most $\frac{1}{2}$, which is inferior to the winning probability in the sequential setting. Naturally, giving the player quantum powers, does not help him in this classical simple board game, to achieve anything better. ◀

In the other direction, we give an example for a classical board game in which the parallel setting, achieves better value than the classical one. Define a board game, in which the board sends a bit a equally distributed, and then the player returns a bit b. If $a = 0$, then the player loses if $b = 0$, and if $b = 1$ then the player wins with probability p. If $a = 1$, then the player wins if $b = 0$, and if $b = 1$ then the player loses with probability p. We think of p to be of a parameter $p < \frac{3}{4}$. Our target function is the same as before – win *exactly* 1-out-of-2 board games.

▶ **Lemma 13.** *In the above board game,* $\mathrm{PVal}(t) \geq \frac{1}{2} + 2p\,(1-p) > \frac{1}{2} + \frac{1}{2}p = \mathrm{SVal}(t)$*.*

Proof. In the parallel settings, the player gets the a_1, a_2 and only then sends b_1, b_2, which gives him the edge. If $a_1 \neq a_2$, his strategy is to send $b_1 = 0, b_2 = 0$ and he will win exactly one board game out of the two. If $a_1 = a_2$ then he will send $b_1 = b_2 = 1$ and he will win exactly one of the board games with probability $p\,(1-p)$. Overall we see that $\mathrm{PVal}(t) \geq \frac{1}{2} + 2p\,(1-p)$. In the sequential setting, it does not matter what happened in the first board game, as the second board game will determine the result (the outcome of the second board game must be different than the first). With probability $\frac{1}{2}$ the board will send a good a_2, resulting in the player winning with certainty exactly 1 out of the 2 board games if they send $b_2 = 0$. With probability $\frac{1}{2}$ the board will send a bad a_2, resulting in the player winning with probability p exactly 1 out of the 2 board games if they send $b_2 = 1$, and doing so with probability 0 otherwise. In total we get that $\mathrm{SVal}(t) = \frac{1}{2} + \frac{1}{2}p$. By taking $p < \frac{3}{4}$, we will get that $P^*_{seq} < P^*_{par}$ (because then $\frac{1}{2} + 2p\,(1-p) > \frac{1}{2} + \frac{1}{2}p$). ◀

In the quantum setting, we already saw that parallel can achieve better value, in our coin flipping example in section 2. We conclude that there is no general connection between the value of the parallel setting and the sequential setting. In parallel, you know the rest of the questions before giving an answer to question 1, while in sequence you know the outcomes of all previous games before you have to give an answer. Either one might be beneficial, depending on the situation.