Large family of quantum weak coin-flipping protocols

Carlos Mochon*

Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125, USA

(Received 21 February 2005; published 29 August 2005)

Each classical public-coin protocol for coin flipping is naturally associated with a quantum protocol for weak coin flipping. The quantum protocol is obtained by replacing classical randomness with quantum entanglement and by adding a cheat detection test in the last round that verifies the integrity of this entanglement. The set of such protocols defines a family which contains the protocol with bias 0.192 previously found by the author, as well as protocols with bias as low as 1/6 described herein. The family is analyzed by identifying a set of optimal protocols for every number of messages. In the end, tight lower bounds for the bias are obtained which prove that 1/6 is optimal for all protocols within the family.

DOI: 10.1103/PhysRevA.72.022341 PACS number(s): 03.67.Hk

I. INTRODUCTION

Quantum weak coin flipping is a two party quantum protocol for agreeing on a random classical bit, where Alice wants outcome zero and Bob wants outcome one. Its main constraint is that a cheating player should not be able to bias the coin in their favor by more than some parameter ϵ.

Previous work by the same author [1] has shown that there exists a quantum weak coin-flipping protocol with bias $\epsilon=0.192$, that is, such that neither player can win by cheating with a probability greater than 0.692. The protocol with bias 0.192 was a generalization of the one by Spekkens and Rudolph [2] which achieved a bias of $1/\sqrt{2}-1/2\simeq 0.207$. Both belong to a large family of quantum weak coin-flipping protocols that are based on a set of classical games involving public coins.

The purpose of this paper is to study this large family of protocols for quantum weak coin flipping. In particular, we will prove that the optimal protocol in this family has a bias of 1/6, though such a bias can only be reached in the limit of arbitrarily large messages. Because our lower bound analysis is constructive, we shall give explicit descriptions of protocols with biases that are arbitrarily close to 1/6.

The protocols with bias of $1/\sqrt{2}-1/2$ was originally described in Ref. [2] as part of a different family of protocols for quantum weak coin flipping, all of which involved three messages. Lower bounds for this family were obtained by Ambainis [3], which proved that the $\epsilon=1/\sqrt{2}-1/2$ protocol was optimal within the family. Though our family does not contain every protocol in the Spekkens and Rudolph family, it does contain its optimal protocol.

The best lower bound currently known that applies to all weak coin-flipping protocols is by Ambainis [4] and states that the number of messages must grow at least as $\Omega[\log\log(1/\epsilon)]$. Ambainis' result rules out attaining an arbitrarily small bias with a fixed number of messages, thus the importance of looking at protocols with arbitrarily large number of messages. We believe that our result is the first of its kind in lower bounding the bias of a large family of protocols that includes instances with every number of messages.

Other important work related to quantum weak coin flipping includes Refs. [5–10] among others. Also related are the results on quantum strong coin flipping (a variant where ideally neither player should be allowed to bias the coin in either direction). The best known protocol for strong coin flipping has a bias of 1/4 [4,7] whereas Kitaev [11] has proven a lower bound of $1/\sqrt{2}-1/2$ for the optimal bias.

Before proceeding we shall give a working definition of quantum weak coin flipping as a quantum communication protocol where two parties (Alice and Bob) start off unentangled and then exchange a series of sequential quantum messages after which they must each output a single classical bit. Their outputs are required to satisfy the following constraints:

(i) If Alice and Bob both follow the protocol their outputs must always agree. Furthermore, the probability that Alice wins (i.e., both parties output zero) is given by P_A whereas the probability that Bob wins (i.e., both parties output one) is given by $P_B=1-P_A$.

(ii) If Alice is honest (i.e., follows the protocol), then independent of Bob's actions, Alice will not output one with a probability greater than P_B^*.

(iii) Similarly, if Bob is honest and Alice is dishonest, Bob will not output zero with a probability greater than P_A^*.

The only security assumption for the above protocol is that a cheating player cannot directly affect the qubits in their opponent's laboratory; that is, we desire protocols with information-theoretic security.

The parameters P_A, P_A^*, and P_B^* will be used to describe a coin-flipping protocol. Obviously, we would like to make P_A^* and P_B^* as small as possible. For simplicity, the merit of a coin-flipping protocol is often quoted by specifying the bias $\epsilon=\max(P_A^*, P_B^*)-1/2$.

Note that whereas the usual definition of coin flipping requires $P_A=P_B=1/2$, we will allow in this paper any value of $P_A\in[0,1]$. This will allow us to derive a set of tradeoff curves for P_A^* versus P_B^*.

The rest of the paper is organized as follows: Section II describes some of our notation concerning tree variables, and will introduce the theorem relating classical coin games to

*Electronic address: carlosm@theory.caltech.edu

©2005 The American Physical Society

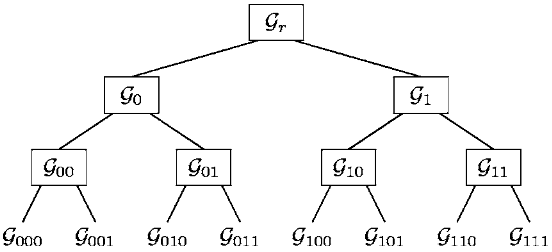

FIG. 1. A depth 3 binary tree.

quantum protocols for weak coin flipping. The theorem, which is a generalization of the work in Ref. [1], is proven in Appendix A. Though the full description of the quantum protocol is only given in the appendix, a brief description is presented at the end of Sec. II.

The main results of the paper are presented in the two subsequent sections, the proof of lower bounds for the bias in Sec. III and the description of matching protocols in Sec. IV.

We also include in Appendix B an analytic derivation of the bias $\epsilon=0.192$ of Ref. [1] which was originally found using numerical techniques. Though the result itself has been superseded by the protocols with bias $1/6$, we include the derivation because it uses a fairly different set of techniques that could potentially be useful elsewhere.

II. NOTATION

Throughout this paper we shall make ample use of binary trees. All trees henceforth will be composed exclusively of binary nodes and leaves, and the leaves will all be located at the same depth.

The nodes of a tree will be labeled by binary strings so that the leftmost node at depth k gets labeled by k zeroes, and the rest will equal one plus the binary value of the node to their left (keeping the number of digits constant). The root node will be denoted by the letter r, which will behave as the empty string so that $x=r$ implies $x0=0$ and $x1=1$. With these conventions the left descendant of node x is $x0$ and the right descendant is $x1$. We define $|x|$ as the length of the binary string x, which also corresponds to the depth of node x.

In this paper we shall use calligraphic fonts, such as $\mathcal{G}$, to denote an assignment of a number or expression to each node of a binary tree. Given an assignment $\mathcal{G}$, the value of node x will be $\mathcal{G}_x$. Most of our notation is summarized by Fig. 1. Note that, though we shall always be working with trees of fixed finite depth, we shall usually leave the depth implicit.

We define an n–coin-game as an assignment $\mathcal{G}$ to a depth n binary tree such that $\mathcal{G}_x \in [0,1]$ for all x and $\mathcal{G}_x \in \{0,1\}$ for all leaves (i.e., for all x such that $|x|=n$). To each n–coin-game, $\mathcal{G}$, we can associate a classical n-message public-coin coin-flipping protocol as follows: The state of the protocol at each step will be described by a node in the tree, and this information will be kept by both Alice and Bob. The game begins at the root node and proceeds downward until reaching a leaf node. If the current node x is a binary node of even depth, then Alice chooses which path to follow and announces the choice to Bob. This is done probabilistically, by announcing the outcome of a biased public coin, so that Alice chooses the left path with probability $\mathcal{G}_x$ and the right path with probability $1-\mathcal{G}_x$. The same mechanism occurs at odd binary nodes, except that Bob is responsible for choosing the direction and announcing it to Alice. The game ends when arriving at a leaf node x, in which case Alice wins if $\mathcal{G}_x=0$ and Bob wins if $\mathcal{G}_x=1$.

Note that we do not require that the coin-flip be fair when both Alice and Bob are honest. Given an n–coin-game $\mathcal{G}$, we can define $\mathcal{H}$ on a tree of the same depth by the equations

$$\mathcal{H}_x = \begin{cases} \mathcal{G}_x & \text{if } |x| = n, \\ \mathcal{G}_x \mathcal{H}_{x0} + (1-\mathcal{G}_x)\mathcal{H}_{x1} & \text{if } |x| < n. \end{cases} \tag{1}$$

The value of $\mathcal{H}_x$ indicates the conditional probability that Bob would win given that the game arrived at node x, assuming both players play honestly. The value of $\mathcal{H}_r$ is Bob's probability of winning for an honest game, which is clearly bounded between 0 and 1.

For each n–coin-game $\mathcal{G}$, we also define $\mathcal{A}$ and $\mathcal{B}$ on a tree of the same depth by the equations

$$\mathcal{A}_x = \begin{cases} 1-\mathcal{G}_x, & \text{for } |x| = n, \\ \mathcal{G}_x \mathcal{A}_{x0}^2 + (1-\mathcal{G}_x)\mathcal{A}_{x1}^2, & |x| \text{ even, } |x| < n, \\ \mathcal{G}_x \sqrt{\mathcal{A}_{x0}} + (1-\mathcal{G}_x)\sqrt{\mathcal{A}_{x1}}, & |x| \text{ odd, } |x| < n, \end{cases}$$

$$\mathcal{B}_x = \begin{cases} \mathcal{G}_x, & \text{for } |x| = n, \\ \mathcal{G}_x \sqrt{\mathcal{B}_{x0}} + (1-\mathcal{G}_x)\sqrt{\mathcal{B}_{x1}}, & |x| \text{ even, } |x| < n, \\ \mathcal{G}_x \mathcal{B}_{x0}^2 + (1-\mathcal{G}_x)\mathcal{B}_{x1}^2, & |x| \text{ odd, } |x| < n. \end{cases} \tag{2}$$

The importance of these quantities is given by the following theorem.

Theorem 1: *For each n–coin-game,* $\mathcal{G}$, *there exists an* $(n+1)$*-message quantum weak coin-flipping protocol such that*

$$P_A P_A^* = \mathcal{A}_r, \tag{3}$$

$$P_B P_B^* = \mathcal{B}_r^2, \tag{4}$$

and the honest probabilities of winning are

$$P_A = (1-P_B) = (1-\mathcal{H}_r), \tag{5}$$

where $\mathcal{A},\mathcal{B}$, *and* $\mathcal{H}$ *are defined in terms of* $\mathcal{G}$ *by Eqs. (1) and (2).*

The quantum protocol: We shall give a brief approximate description of the quantum protocol, which should provide the needed intuition. The full description of the protocol is contained in Appendix A along with the proof of the above theorem. A simpler version of the protocol also appears in Ref. [1].

The basic idea is to take the classical public-coin protocol associated with an n–coin-game, $\mathcal{G}$, replace the classical randomness with quantum entanglement, and then add a cheat detection step.

Classical shared randomness can be replaced by quantum entanglement using states of the form

$$\sqrt{a}|0\rangle \otimes |0\rangle + \sqrt{1-a}|1\rangle \otimes |1\rangle, \tag{6}$$

where one qubit belongs to Alice and one to Bob. The randomness can be extracted at any time by measuring both qubits in the computational basis.

In the classical protocol associated with $\mathcal{G}$ described above, Alice and Bob slowly built up a shared random string. After the first k messages they shared a random k-bit string, where string x has probability $\mathcal{P}_x$ [the formal definition of $\mathcal{P}$ is given in Eq. (A10)]. The quantum protocol is constructed so that, after k messages, Alice and Bob share the state

$$|\psi_k\rangle = \sum_{\substack{x \\ |x|=k}} \sqrt{\mathcal{P}_x}|x\rangle \otimes |x\rangle. \tag{7}$$

In the classical protocol, the sender of the message (Alice for odd messages and Bob for even messages) has control over its content and hence the ability to cheat at that step, whereas the other player has no control over the given step. In the quantum protocol the same structure is maintained. The basic step to go from a k-bit string to a $(k+1)$-bit string is for the message sender to append two qubits in the zero state, then apply a controlled unitary on the two qubits with the other k bits as control, and finally to send one of the qubits to the other player,

$$\begin{aligned}|\psi_k\rangle &\to |\psi_k\rangle \otimes |00\rangle \\ &\to \sum_{\substack{x \\ |x|=k}} \sqrt{\mathcal{P}_x}|x\rangle_A \otimes |x\rangle_B \otimes \left(\sqrt{\mathcal{G}_x}|00\rangle + \sqrt{1-\mathcal{G}_x}|11\rangle\right) \\ &\to \sum_{\substack{x \\ |x|=k}} \sum_{i\in\{0,1\}} \sqrt{\mathcal{P}_{xi}}|xi\rangle_A \otimes |xi\rangle_B = |\psi_{k+1}\rangle. \end{aligned} \tag{8}$$

After n messages, at the end of the classical protocol, Alice and Bob share an n-bit string, which determines the coin outcome based on the value of the corresponding leaf of $\mathcal{G}$. In the quantum protocol, they do the equivalent measurement, but using a two outcome POVM so that most of the entanglement is preserved after the measurement. This allows a cheat detection step to be appended to the end of the protocol as follows: the winner of the coin-flip based on the POVM must send over all of their qubits to the other player for inspection. The other player will end up with a pure state and can do a projection onto the final state and its complement. If the latter result is obtained, then cheating is detected and the losing player can declare victory, otherwise that player acknowledges defeat. In either case, the first player always declares victory.

Note that, though it is possible for both players to declare victory at the same time, this can only occur if one of them was cheating, and in such cases we always expect the cheating player to declare victory anyway.

The rest of this paper contains the analysis of the family of protocols, which will identify the protocol with bias of 1/6 and prove that it is optimal within the family.

III. LOWER BOUNDS ON THE BIAS

In this section we shall derive lower bounds for the set of P_A^* and P_B^* that can be achieved with quantum protocols based on n–coin-games as defined in Theorem 1.

Definition 2: *For $n\in\mathbb{Z}^+$, define the set $\Lambda_n\subset\mathbb{R}^2$ so that $(A,B)\in\Lambda_n$ if and only if there exists an n–coin-game, $\mathcal{G}$, with $A=\mathcal{A}_r$ and $B=\mathcal{B}_r$, and $\mathcal{A}$ and $\mathcal{B}$ defined in terms of $\mathcal{G}$ by Eq. (2).*

For each $(A,B)\in\Lambda_n$ there exists an $(n+1)$-message quantum coin-flipping protocol such that $P_AP_A^*=A$ and $P_BP_B^*=B^2$. Furthermore, if $(P_AP_A^*,\sqrt{P_BP_B^*})\notin\Lambda_n$ then there is no protocol built out of a n–coin-game that achieves P_A, P_A^*, and P_B^*. However, it is not true that $(P_AP_A^*,\sqrt{P_BP_B^*})\in\Lambda_n$ implies the existence of a protocol with those parameters. For example, $(0.3531,\sqrt{0.3531})\in\Lambda_2$ because there exists a 3-message protocol with $P_A\simeq0.515, P_A^*\simeq0.686, P_B^*\simeq0.728$, however there are no 3-message protocols with $P_A=P_B=1/2$ and $P_A^*=P_B^*\simeq2\times0.353=0.706$. The optimal symmetric 3-message protocol is the one by Spekkens and Rudolph [2] with $P_A^*=P_B^*=1/\sqrt{2}=0.707$. Though it would be preferable to study the set of achievable triplets $(\mathcal{A}_r,\mathcal{B}_r,\mathcal{H}_r)$, the sets Λ_n are easier to analyze and in the limit $n\to\infty$ will provide us with interesting bounds.

We begin the study of the sets Λ_n by showing that they can be obtained inductively.

Lemma 3: *The set Λ_n is the convex combination of pairs of points from the set $\{(B^2,\sqrt{A})\,|\,(A,B)\in\Lambda_{n-1}\}$.*

Proof: Given an n–coin-game, $\mathcal{G}$, define the variable $\gamma\equiv\mathcal{G}_r\in[0,1]$ and the two $(n-1)$–coin-games $\mathcal{G}^{(0)}$ and $\mathcal{G}^{(1)}$ by

$$\mathcal{G}_x^{(i)} = \begin{cases} 1-\mathcal{G}_{ix} & \text{for } |x| = n-1, \\ \mathcal{G}_{ix} & \text{for } |x| < n-1, \end{cases} \tag{9}$$

for $i=0,1$. There is a natural isomorphism between $\mathcal{G}$ and the triplet $\gamma,\mathcal{G}^{(0)},\mathcal{G}^{(1)}$.

Furthermore define $\mathcal{A}^{(i)}$ and $\mathcal{B}^{(i)}$ in terms of $\mathcal{G}^{(i)}$ in the usual way. Note that $\mathcal{A}^{(i)}$ and $\mathcal{B}^{(i)}$ are not the left and right branches of $\mathcal{A}$ and $\mathcal{B}$ defined from $\mathcal{G}$ but rather $\mathcal{A}_x^{(i)}=\mathcal{B}_{ix}$ and $\mathcal{B}_x^{(i)}=\mathcal{A}_{ix}$. Therefore

$$\mathcal{A}_r = \gamma(\mathcal{B}_r^{(0)})^2 + (1-\gamma)(\mathcal{B}_r^{(1)})^2, \tag{10}$$

$$\mathcal{B}_r = \gamma\sqrt{\mathcal{A}_r^{(0)}} + (1-\gamma)\sqrt{\mathcal{A}_r^{(1)}}. \tag{11}$$

□

The set Λ_1 is fairly simple and corresponds to the convex combinations of the two points (1,0) and (0,1), which could be thought of as comprising Λ_0. Using Λ_1 and the above lemma we can prove two simple properties of the sets Λ_n,

(1) $(0,1)\in\Lambda_n$ and $(1,0)\in\Lambda_n$ for all n,

(2) $\Lambda_n\subset[0,1]\times[0,1]$ for all n.

Both properties are clearly true for Λ_1. By induction $(0,1)\in\Lambda_{n-1}$ and $(1,0)\in\Lambda_{n-1}$ implies that $(1^2,\sqrt{0})$ and $(0^2,\sqrt{1})$ are in Λ_n. Similarly, if $(A,B)\in\Lambda_{n-1}$ implies $A\in[0,1]$ and $B\in[0,1]$, then $(B^2,\sqrt{A})\in[0,1]\times[0,1]$ and so are convex combinations of such points.

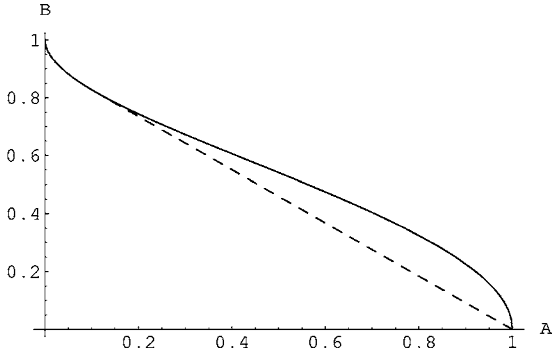

FIG. 2. The curve $(t^2, \sqrt{1-t})$ for $t \in [0,1]$. The convex hull of the curve is the region Λ_2, with the dashed line serving as lower boundary.

The first nontrivial set is Λ_2 which is the convex combination of the points on the curve $(t^2, \sqrt{1-t})$ for $t \in [0,1]$. The curve is plotted in Fig. 2. The dotted line marks the lower boundary of its convex hull which can be achieved using convex combinations of two points (the rest of the lower boundary of the convex hull is simply the curve itself).

Rather than keeping track of the sets Λ_n, it will be simpler to study exclusively their lower boundary, which will be curves connecting the points (1, 0) and (0, 1). All the optimal protocols will live on these curves, and all points below the curves will be unattainable. To formalize the notion of lower boundary we associate to every function $f(z):[0,1] \to [0,1]$ the following sets:

$$f^{+} = \{(z,w) | z \in [0,1], f(z) < w \leqslant 1\}, \qquad (12)$$

$$f^{=} = \{(z,w) | z \in [0,1], f(z) = w\}, \qquad (13)$$

$$f^{-} = \{(z,w) | z \in [0,1], f(z) > w \geqslant 0\}. \qquad (14)$$

Returning to the case of Λ_2 and Fig. 2, we see that the lower boundary follows the original curve $\sqrt{1-\sqrt{z}}$ between (1, 0) and some point which we shall call (α_2, β_2). It then turns into a straight line connecting the point (α_2, β_2) to the point (0,1). The point (α_2, β_2) can be found by calculating the slope of the line connecting each point to (0,1) and choosing the point that achieves the maximum.

In fact, all of the lower boundaries will have this form. Define for $n > 1$,

$$f_n(z) = \begin{cases} \sqrt{1 - \left(\frac{1-\beta_n^2}{\sqrt{\alpha_n}}\right)\sqrt{z}} & \text{for } z \in [0, \alpha_n], \\ \frac{\beta_n}{1-\alpha_n}(1-z) & \text{for } z \in [\alpha_n, 1], \end{cases} \qquad (15)$$

where

$$\alpha_n = \frac{n-1}{3(n+1)}, \quad \beta_n = \sqrt{\frac{n+2}{3n}}. \qquad (16)$$

For the case $n=1$ we define $f_1(z) = 1-z$, which is the limit of f_n as $n \to 1$. Because $\alpha_n \in (0,1)$ and $\beta_n \in (0,1)$ for all $n > 1$, the functions satisfy $f_n(z) \in [0,1]$ for all $z \in [0,1]$. These functions are also the lower boundaries of convex regions.

Lemma 4: *For all $n \geqslant 1$, the function f_n is strictly decreasing, and the region $f_n^{=} \cup f_n^{+}$ is convex.*

Proof: The case of $n=1$ is trivial. For $n > 1$ we have

$$f_n'(z) = \begin{cases} -\frac{1-\beta_n^2}{4\sqrt{\alpha_n}\sqrt{z} f_n(z)} & \text{for } z \in [0, \alpha_n], \\ -\frac{\beta_n}{1-\alpha_n} & \text{for } z \in [\alpha_n, 1], \end{cases} \qquad (17)$$

which is well defined and negative on (0,1]. For z near zero, $f(z) \simeq 1 - (1-\beta_n^2)/(2\sqrt{\alpha_n})\sqrt{z}$, therefore $f(z)$ is also strictly decreasing at $z=0$.

The derivative is also continuous on (0,1] because at $z = \alpha_n$ we have

$$\frac{\beta_n}{1-\alpha_n} = \frac{\sqrt{3}(n+1)}{2\sqrt{n(n+2)}} = \frac{1-\beta_n^2}{4\alpha_n\beta_n}. \qquad (18)$$

Furthermore, in the region $(0, \alpha_n)$, the second derivative is

$$f_n''(z) = f_n'(z)\left(-\frac{1}{2z} - \frac{f_n'(z)}{f_n(z)}\right) = \frac{-f_n'(z)}{4z\sqrt{\alpha_n} f_n^2(z)}\left[2\sqrt{\alpha_n} - 3(1-\beta_n^2)\sqrt{z}\right] > 0, \qquad (19)$$

where the inequality holds because $3(1-\beta_n^2) < 2$. Therefore $f_n'(z)$ is monotonically increasing on (0,1], and the region above $f_n(z)$ in this interval is convex. The point (0,1) can be included because the closure of a convex set is convex. □

We are now ready to prove the main lemma of this section.

Lemma 5: *For all $n \in \mathbb{Z}^+, \Lambda_n \subset f_n^{=} \cup f_n^{+}$ and $f_n^{=} \subset \Lambda_n$.*

Proof: The statement is clearly true for $n=1$ since $\Lambda_1 = f_1^{=}$. We will prove the rest of the cases inductively. Assume the theorem holds for Λ_n, which implies that $(z, f_n(z)) \in \Lambda_n$ for all z. By Lemma 3 we have that $(f_n^2(z), \sqrt{z}) \in \Lambda_{n+1}$ for all $z \in [0,1]$ and so are convex combinations of pairs of such points. The curve parametrized by $(f_n^2(z), \sqrt{z})$ can also be described by the points $(w, g_n(w))$ for

$$g_n(w) = \begin{cases} \sqrt{1 - \left(\frac{1-\alpha_n}{\beta_n}\right)\sqrt{w}} & \text{for } w \in [0, \beta_n^2], \\ \frac{\sqrt{\alpha_n}}{1-\beta_n^2}(1-w) & \text{for } w \in [\beta_n^2, 1]. \end{cases} \qquad (20)$$

Note how under the map $(x,y) \to (y^2, \sqrt{x})$ the straight line turns into a curve, and the curve turns into a straight line. Furthermore, because of the exchange of x and y, the straight line ends up on the right-hand side.

The pattern of points α_n and β_n, in addition to guaranteeing that the region above $f_n(z)$ is convex, also satisfies the recursion relation

$$\frac{1-\alpha_n}{\beta_n}=\frac{2\sqrt{n(n+2)}}{\sqrt{3}(n+1)}=\frac{1-\beta_{n+1}^2}{\sqrt{\alpha_{n+1}}} \tag{21}$$

and therefore $g_n(z)=f_{n+1}(z)$ in the region $[0,\alpha_{n+1}]$ (since $\alpha_{n+1}\leqslant 1/3\leqslant\beta_n^2$). Pictorially, the curve $g_n^{=}$ is like the curve $f_{n+1}^{=}$, except that the straight line intersects the curve somewhat to the right, and hence the region above $g_n^{=}$ is not convex. Its convex hull will give us the region above the curve $f_{n+1}^{=}$.

Thus far we have shown $g_n^{=}\subset\Lambda_{n+1}$, as are convex combinations of pairs of points on the curve $g_n^{=}$. Because $g_n^{=}=f_{n+1}^{=}$ in the region $[0,\alpha_{n+1}]$ we know that this segment of the curve is in Λ_{n+1}. The rest of the curve $f_{n+1}^{=}$ is simply the convex combination of the points $(\alpha_{n+1},\beta_{n+1})$ and (1,0) both of which are in $g_n^{=}$. We have therefore proven the second part of the lemma, $f_{n+1}^{=}\subset\Lambda_{n+1}$.

We now intend to prove that $g_n(z)\geqslant f_{n+1}(z)$ for all $z\in[0,1]$. The statement is clearly true in the region $[0,\alpha_{n+1}]$ where both are equal. In the region $[\beta_n^2,1]$ it is also true because both functions are straight lines ending in (1,0), and the starting point of the lines are $g_n(\beta_n^2)=\sqrt{\alpha_n}$ and $f_{n+1}(\beta_n^2)=\beta_{n+1}(1-\beta_n^2)/(1-\alpha_{n+1})$. The inequality $f_{n+1}(\beta_n^2)\geqslant g_n(\beta_n^2)$ can be proven by checking that $[f_{n+1}(\beta_n^2)/g_n(\beta_n^2)]^2-1=-4/[n^2(n+3)]\leqslant 0$ for $n\geqslant 1$.

Finally, in the region $[\alpha_{n+1},\beta_n^2]$ the functions $f_{n+1}(z)$ and $g_n(z)$ start off at the same point, with the same derivative, but $f''_{n+1}(z)=0$ in this region whereas $g''_n(z)$ initially is positive, and has only one zero in the region, which can be checked as in Eq. (19). If the curve g_n were to cross the curve f_{n+1} at any point in this region, then it would have to end below it. However, we already argued that $g_n(\beta_n^2)\geqslant f_{n+1}(\beta_n^2)$ and therefore the curve $g_n^{=}$ must lie above the curve $f_{n+1}^{=}$ in the middle region as well.

So far we have shown that $(g_n^{=}\cup g_n^{+})\subset(f_{n+1}^{=}\cup f_{n+1}^{+})$. By the induction assumption, $\Lambda_n\subset f_n^{=}\cup f_n^{+}$. Under the map $(x,y)\rightarrow(y^2,\sqrt{x})$, the region $f_n^{=}\cup f_n^{+}$ maps into the region to the right of the curve $g_n^{=}$, which also equals the region $g_n^{=}\cup g_n^{+}$ because $g_n(z)$ is strictly decreasing, $g_n(1)=0$ and $g_n(0)=1$. Finally, using Lemma 3 we know that Λ_{n+1} is contained in the convex combination of points in $g_n^{=}\cup g_n^{+}$. Because $(g_n^{=}\cup g_n^{+})\subset(f_{n+1}^{=}\cup f_{n+1}^{+})$, and $f_{n+1}^{=}\cup f_{n+1}^{+}$ is convex, we have $\Lambda_{n+1}\subset f_{n+1}^{=}\cup f_{n+1}^{+}$. □

Combining the previous lemma with the definition of the sets Λ_n, we have proven the following theorem.

Theorem 6: *Every $(n+1)$-message quantum weak coin-flipping protocol based on an n–coin-game satisfies*

$$P_BP_B^*\geqslant f_n^2(P_AP_A^*). \tag{22}$$

Additionally, we have the following corollary for the limit of $n\rightarrow\infty$.

Corollary 7: *All quantum weak coin-flipping protocols based on an n–coin-game (for any $n\in\mathbb{Z}^+$) satisfy*

$$P_AP_A^*\leqslant\frac{1}{3}\Rightarrow P_BP_B^*\geqslant 1-2\sqrt{\frac{P_AP_A^*}{3}}\geqslant\frac{1}{3}, \tag{23}$$

$$P_BP_B^*\leqslant\frac{1}{3}\Rightarrow P_AP_A^*\geqslant 1-2\sqrt{\frac{P_BP_B^*}{3}}\geqslant\frac{1}{3}. \tag{24}$$

In particular,

$$\max(P_AP_A^*,P_BP_B^*)\geqslant\tfrac{1}{3} \tag{25}$$

and

$$\max(P_A^*,P_B^*)\geqslant\tfrac{2}{3}\quad\text{for } P_A=P_B=\tfrac{1}{2}. \tag{26}$$

Proof: The above results use the limit

$$f_\infty(z)=\begin{cases}\sqrt{1-\frac{2}{\sqrt{3}}\sqrt{z}} & \text{for } z\in\left[0,\frac{1}{3}\right],\\ \frac{\sqrt{3}}{2}(1-z) & \text{for } z\in\left[\frac{1}{3},1\right],\end{cases} \tag{27}$$

which has the symmetry $b=f_\infty^2(a)\Rightarrow a=f_\infty^2(b)$. □

IV. OPTIMAL PROTOCOLS

In this section we will describe protocols that match the lower bounds derived in the preceding section. In a sense, most of the work has already been done since the proof of the preceding section was constructive. What remains undone is to explicitly construct the n–coin-games and to calculate from them P_A, P_A^*, and P_B^* (rather than only their products).

From the discussion of the preceding section we can see that the interesting $(n+1)$–coin-games live on the curve $f_{n+1}^{=}$. The points on the rounded part of the curve (the left segment) involve no convex combinations of points from n–coin-games and therefore are not new (i.e., they are protocols that can be described by a single n–coin-game with Alice's and Bob's role reversed). The interesting points at level $n+1$ lie on the straight segment and are the combination of the points $(\alpha_{n+1},\beta_{n+1})$ and (1, 0). To understand this segment we need to describe the n–coin-games that produce points $(\beta_{n+1}^2,\sqrt{\alpha_{n+1}})$ and (0, 1). The second point corresponds to a tree that is fairly simple, it has the value 1 at every leaf and the rest of the nodes are irrelevant. The n–coin-games for $(\beta_{n+1}^2,\sqrt{\alpha_{n+1}})$ is what we shall describe next.

Lemma 8: *For each $n\in\mathbb{Z}^+$ there is an n–coin-game, $\mathcal{G}^{(n)}$, such that*

$$\mathcal{A}_r^{(n)}=\beta_{n+1}^2=\frac{n+3}{3(n+1)}, \tag{28}$$

$$\mathcal{B}_r^{(n)}=\sqrt{\alpha_{n+1}}=\sqrt{\frac{n}{3(n+2)}}, \tag{29}$$

$$\mathcal{H}_r^{(n)}=\begin{cases}\dfrac{n}{2(n+1)}, & n \text{ even},\\[2ex] \dfrac{n+1}{2(n+2)}, & n \text{ odd}\end{cases}\quad, \tag{30}$$

with $\mathcal{A}^{(n)},\mathcal{B}^{(n)}$, and $\mathcal{H}^{(n)}$ defined in terms of $\mathcal{G}^{(n)}$ by Eqs. (1) and (2). In particular, the associated quantum weak coin-flipping protocols have

$$P_A(n)=1-\mathcal{H}_r^{(n)}=\begin{cases}\dfrac{n+2}{2(n+1)}, & n \text{ even},\\[2ex] \dfrac{n+3}{2(n+2)}, & n \text{ odd},\end{cases} \tag{31}$$

$$P_A^*(n) = \frac{\mathcal{A}_r^{(n)}}{1-\mathcal{H}_r^{(n)}} = \begin{cases} \dfrac{2(n+3)}{3(n+2)}, & n \text{ even}, \\ \dfrac{2(n+2)}{3(n+1)}, & n \text{ odd}, \end{cases} \tag{32}$$

$$P_B^*(n) = \frac{\left(\mathcal{B}_r^{(n)}\right)^2}{\mathcal{H}_r^{(n)}} = \begin{cases} \dfrac{2(n+1)}{3(n+2)}, & n \text{ even}, \\ \dfrac{2n}{3(n+1)}, & n \text{ odd}. \end{cases} \tag{33}$$

Proof: Define the parameters

$$\gamma_n = \frac{n}{n+2}, \tag{34}$$

which are the weights needed for the convex combinations. And let

$$\mathcal{G}_r^{(1)} = \gamma_1, \quad \mathcal{G}_0^{(1)} = 1, \quad \mathcal{G}_1^{(1)} = 0, \tag{35}$$

which leads to $\mathcal{A}_r^{(1)}=2/3$ and $\mathcal{B}_r^{(1)}=\mathcal{H}_r^{(1)}=1/3$. The rest of the coin games are defined inductively,

$$\mathcal{G}_r^{(n)} = \gamma_n, \tag{36}$$

$$\mathcal{G}_{0x}^{(n)} = \begin{cases} 1-\mathcal{G}_x^{(n-1)} & \text{for } |x| = n-1, \\ \mathcal{G}_x^{(n-1)} & \text{for } |x| < n-1, \end{cases} \tag{37}$$

$$\mathcal{G}_{1x}^{(n)} = \begin{cases} 0 & \text{for } |x| = n-1, \\ \mathcal{G}_x^{(n-1)} & \text{for } |x| < n-1. \end{cases} \tag{38}$$

The values of $\mathcal{G}_{1x}^{(n)}$ for $|x|<n-1$ are actually irrelevant but were chosen so that $\mathcal{G}_x^{(n)}=\gamma_{n-|x|}$ whenever $|x|<n-1$, and therefore these protocols fit into the subfamily studied in Ref. [1].

The reason for inverting the value of the leaves relates to our insistence that Alice always send the first message, which implies that the sender of the last message alternates as n is increased and correspondingly the assignments of winning and losing for the coin outcome need to be flipped.

In fact, the pattern of the leaves is fairly simple. It is chosen so that it depends on the parity of the location (from left to right) of the first 1 symbol in the string x. In the quantum protocol this translates into the first sender of a 1 qubit being the winner of the coin flip (assuming they pass the cheat detection phase).

In fact, the trees $\mathcal{G}^{(n)}$ would best be described by truncated trees of the form of Fig. 3. However, we shall continue using trees with all leaves at the same depth in order to be consistent with the preceding section.

Returning to the proof of the lemma, it is easy to see that $\mathcal{A}_{1x}^{(n)}=1$ and $\mathcal{B}_{1x}^{(n)}=\mathcal{H}_{1x}^{(n)}=0$ for all strings x. The left-hand side of the tree satisfies $\mathcal{A}_{0x}^{(n)}=\mathcal{B}_x^{(n-1)}$, $\mathcal{B}_{0x}^{(n)}=\mathcal{A}_x^{(n-1)}$, and $\mathcal{H}_{0x}^{(n)}=1-\mathcal{H}_x^{(n-1)}$ for all strings x. Therefore the root nodes are

$$\mathcal{A}_r^{(n)} = \gamma_n\left(\mathcal{B}_r^{(n-1)}\right)^2 + (1-\gamma_n)1, \tag{39}$$

$$\mathcal{B}_r^{(n)} = \gamma_n\sqrt{\mathcal{A}_r^{(n-1)}} + (1-\gamma_n)0, \tag{40}$$

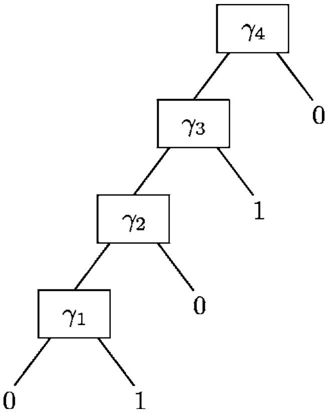

FIG. 3. A truncated tree equivalent to $\mathcal{G}^{(4)}$.

$$\mathcal{H}_r^{(n)} = \gamma_n\left(1-\mathcal{H}_r^{(n-1)}\right) + (1-\gamma_n)0. \tag{41}$$

It is then straightforward to plug in the expressions as functions of n for all the above parameters and check that Eqs. (28)–(30) are always satisfied. □

Interestingly, the sequence of protocols is such that P_A and P_B do not change when n increases from an odd integer to an even one, whereas P_A^* and P_B^* do not change when n increases from an even integer to an odd one. We offer no intuition for this property. Note, however, that for a given n, the associated protocol corresponds to a single point on the surface of optimal protocols in the three-dimensional space of triplets (P_A, P_A^*, P_B^*) that can be achieved with $n+1$ quantum messages.

For large n, the sequence of protocols converges to $P_A=P_B=1/2$ and $P_A^*=P_B^*=2/3$, yielding a protocol with bias of $1/6$. It would also be desirable to show the existence of a sequence of protocols that converges to the same point but such that $P_A=P_B=1/2$ for every protocol in the sequence. This can be easily accomplished by choosing, for each n, the point along the curve $f_n^=$ that has $\mathcal{H}_r=1/2$. In the coin-game language we need to modify the top coin $\mathcal{G}_r$, and we therefore introduce a new sequence of coin-games $\mathcal{G}'^{(n)}$ defined as

$$\mathcal{G}_x'^{(n)} = \begin{cases} 1/\left(2-2\mathcal{H}_r^{(n-1)}\right), & x=r, \\ \mathcal{G}_x^{(n)}, & \text{otherwise}. \end{cases} \tag{42}$$

For simplicity, we will concentrate on the case when n is even so that

$$\mathcal{A}_r'^{(n)} = \frac{n+1}{n+2}\left(\mathcal{B}_r^{(n-1)}\right)^2 + \frac{1}{n+2}, \tag{43}$$

$$\mathcal{B}_r'^{(n)} = \frac{n+1}{n+2}\sqrt{\mathcal{A}_r^{(n-1)}}, \tag{44}$$

$$\mathcal{H}_r'^{(n)} = \frac{n+1}{n+2}\left(1-\mathcal{H}_r^{(n-1)}\right) = \frac{1}{2}, \tag{45}$$

and the associated probabilities of winning by cheating are

$$P_A^*(n)' = 2\mathcal{A}_r'^{(n)} = \tfrac{2}{3}, \tag{46}$$

$$P_B^*(n)' = 2\left(\mathcal{B}_r'^{(n)}\right)^2 = \frac{2}{3}\frac{(n+1)^2}{n(n+2)}. \tag{47}$$

That is, we have identified a nice sequence of quantum protocols with $n+1$ messages (for n even) where $P_A=P_B=1/2$ and $P_A^*=2/3$ are all fixed and P_B^* decreases from $3/4$ to $2/3$. Of course, the case $n=2$ belongs to the family studied by Spekkens and Rudolph [2] and satisfies $P_A^*P_B^*=1/2$.

As discussed in the introduction to the preceding section, the above protocols are optimal in the following sense: to decrease one of P_A^* or P_B^* while keeping the number of messages fixed, we would have to increase the other parameter. However, the protocols are not optimal in the sense that they minimize the bias $\epsilon=\max(P_A^*,P_B^*)-1/2$ for a fixed number of messages. Only in the limit of infinite messages is the bias of the above protocols optimal.

Thus far, we have identified the point $(1/3,\sqrt{1/3})\in f_\infty^{=}$ as a protocol with $P_A=1/2$ and $P_A^*=P_B^*=2/3$. The other points on the curve $f_\infty^{=}$ can be found using the same trick of modifying the top coin $\mathcal{G}_r$. That is, let $\mathcal{G}'^{(n)}$ be as above but with $\mathcal{G}_r'^{(n)}=t$, where $t\in[0,1]$ is a parameter we can choose freely. In the limit of $n\to\infty$ we find

$$\mathcal{A}_r'^{(\infty)}(t) = t\tfrac{1}{3} + (1-t), \tag{48}$$

$$\mathcal{B}_r'^{(\infty)}(t) = t\sqrt{\tfrac{1}{3}}, \tag{49}$$

$$\mathcal{H}_r'^{(\infty)}(t) = t\tfrac{1}{2}. \tag{50}$$

The associated quantum weak coin-flipping parameters are

$$P_A(t) = 1 - \frac{t}{2}, \tag{51}$$

$$P_A^*(t) = \frac{2}{3}\frac{3-2t}{2-t}, \tag{52}$$

$$P_B^*(t) = \tfrac{2}{3}t. \tag{53}$$

These protocols correspond to the right half of the curve $f_\infty^{=}$ [i.e., the points $(z,f_\infty(z))$] for $z\in[1/3,1]$). The other half of the curve can be obtained by symmetry between Alice and Bob. In the coin-game formalism this symmetry arises by creating a new $(n+1)$–coin-game, $\mathcal{G}'$, out of given n–coin-game, $\mathcal{G}$, by the rules $\mathcal{G}_r'=1,\mathcal{G}_{0x}'=\mathcal{G}_{1x}'=\mathcal{G}_x$ for $|x|<n$ and $\mathcal{G}_{0x}'=\mathcal{G}_{1x}'=1-\mathcal{G}_x$ for $|x|=n$. In the language of protocols, we are forcing Alice's first message to have no content, which is equivalent to allowing Bob to begin the game.

The results can be best summarized by eliminating the variable t from Eqs. (51)–(53), which proves this section's main theorem.

Theorem 9: *There exist quantum weak coin-flipping protocols that asymptotically approach the curve*

$$P_A^* + P_B^* - \tfrac{3}{4}P_A^*P_B^* = 1 \tag{54}$$

in the limit of large number of messages. The corresponding probabilities of winning when the game is played honestly are

$$P_A = \tfrac{3}{4}P_A^* \quad \text{when } P_A^* \leqslant P_B^*, \tag{55}$$

$$P_B = \tfrac{3}{4}P_B^* \quad \text{when } P_A^* \geqslant P_B^*. \tag{56}$$

Implementing the optimal protocols: Surprisingly, the optimal protocols identified above are significantly easier to describe and implement than a generic protocol associated with a random n-coin-game. Here we shall present a brief description of the simplified protocol associated with the coin games from Eqs. (42)–(47).

We begin by fixing a security parameter n, which will lead to an $n+2$ message quantum protocol. For simplicity we assume that n is even.

The first n messages of the quantum protocol each involve one player preparing a two qubit entangled state and sending one of the two qubits to the other player. The two qubit states can be written as

$$\sqrt{a_i}|00\rangle + \sqrt{1-a_i}|11\rangle \tag{57}$$

for $i=1,\ldots,n$, where

$$a_i = \begin{cases} \dfrac{n+1}{n+2}, & i=1, \\ \dfrac{n-i+1}{n-i+3}, & i\neq 1. \end{cases} \tag{58}$$

As usual Alice is in charge of sending the odd messages (and hence preparing the odd numbered states) whereas Bob sends the even numbered messages.

At the end of the above procedure Alice and Bob should each have n qubits, which can be expressed in a basis of n-bit strings with the most significant bit corresponding to the first qubit sent or received. They now each perform a two-outcome measurement which can be described as follows: let S be the set of all n-bit strings such that the first occurrence of the digit one, when the bits are examined from left to right, appears at an even location, again counting from left to right (i.e., for $n=4$ we have $S=\{0001,0100,0101,0110,0111\}$). The two outcome measurement is given by the POVM elements

$$E_0 = I - E_1, \quad E_1 = \sum_{x\in S}|x\rangle\langle x|. \tag{59}$$

As usual Alice wins on outcome zero and Bob wins on outcome one. Note that, in essence, the first person to send a qubit in the "one" state is the winner at this stage. However, the following cheat detection step will be powerful enough to dissuade against the obvious cheating strategy.

Before outputting the final answer the party who won sends all their qubits over to the losing party who then does an extra cheat-detecting two-outcome measurement to verify that the $2n$ qubit state now in their possession is the correct one (i.e., they project onto the state and its complement). Unfortunately, this final step is likely to be very fairly difficult with current technology for any $n>2$.

In the end, the resulting protocol goes to a bias of $1/6$ as n is taken to infinity. For $n=4$ Bob's probability of winning by cheating is $P_B^*=0.694$ whereas for $n=6$ we get $P_B^*=0.681$. Furthermore, Alice's cheating is always restricted at

$P_A^*=2/3$. Protocols with more symmetry between Alice and Bob can also be described as above by changing the coefficients $\{a_i\}$.

V. CONCLUSIONS

We have identified a large family of quantum protocols for weak coin flipping, that are based on classical public-coin games. The family contains protocols approaching the curve $P_A^*+P_B^*-\frac{3}{4}P_A^*P_B^*=1$, which can be reached asymptotically in the limit of large number of messages. The most important of these protocols is symmetric between Alice and Bob and achieves $P_A=P_B=1/2$ and $P_A^*=P_B^*=2/3$, that is, it has a bias of $1/6$.

Furthermore, we have proven lower bounds for the bias achievable by protocols in this family. In particular, $\max(P_A^*,P_B^*)\geqslant 2/3$ or equivalently $\epsilon\geqslant 1/6$. These lower bounds show that the protocols found above are optimal within their family.

Our lower bounds also establish a strict hierarchy among coin-flipping protocols in our family with different number of messages. Admittedly, the hierarchy is of little practical interest since a small number of messages suffices in all cases to construct protocols that are reasonably close to optimal.

Though the question of optimal bias for a general quantum weak coin-flipping protocol remains open, we speculate that it might be possible to show that every protocol is equivalent to one contained in the family analyzed in this paper. Future work will be needed to verify this conjecture.

ACKNOWLEDGMENTS

The author would like to thank Graeme Smith for reading this paper. This work was supported in part by the National Science Foundation under Grant No. EIA-0086038 and by the Department of Energy under Grant No. DE-FG03-92-ER40701.

APPENDIX A: THE PROTOCOL

The purpose of this appendix is to describe the $(n+1)$-message quantum weak coin-flipping protocol associated to each n–coin-game. For each protocol we shall also derive matching upper and lower bounds on the amount that each party can cheat and thereby prove Theorem 1.

All the general ideas needed in this section have appeared previously in Ref. [1], though in a somewhat different notation. The new elements of this appendix are as follows.

(1) Ref. [1] was restricted to n–coin-games where all the binary nodes at the same depth had the same value (i.e, $\mathcal{G}_x=\mathcal{G}_{x'}$ if $|x|=|x'|<n$). These variables were given the name a_i so that $\mathcal{G}_x=a_{|x|+1}$. In this section we lift the restriction and consider general n–coin-games.

(2) An upper bound on P_A^* and P_B^* was derived in Ref. [1] but was not proven optimal. In this section we shall derive a matching lower bound.

Because most of the ideas here have been published elsewhere, we shall simply prove the necessary facts in this section without providing the intuition or motivation behind the constructions. For a more pedagogical approach we refer the reader to Ref. [1].

We begin by fixing an n–coin-game $\mathcal{G}$, which will be used throughout this section. We also fix $\mathcal{H},\mathcal{A}$, and $\mathcal{B}$ as given by Eqs. (1) and (2). Because optimal protocols with $\mathcal{H}_r=0$ and $\mathcal{H}_r=1$ are easy to construct even classically, for what follows we shall assume that $0<\mathcal{H}_r<1$.

To describe the quantum protocol associated with $\mathcal{G}$ we employ the standard quantum communication model involving the Hilbert space decomposition $H_A\otimes H_M\otimes H_B$, where H_A is Alice's private space, H_B is Bob's private space, and H_M is the space used for passing messages. We further subdivide these spaces as follows:

$$H_A = H_a \otimes H_{a'} \otimes H_{ac}, \tag{A1}$$

$$H_B = H_b \otimes H_{b'} \otimes H_{bc}, \tag{A2}$$

$$H_M = H_m \otimes H_{mn}. \tag{A3}$$

The spaces H_a and H_b each consists of n qubits and will be used to store a binary string x corresponding to a node in $\mathcal{G}$. The individual qubits comprising each space will be referred to as a_1 through a_n, and b_1 though b_n, respectively. The one-qubit space H_m will be the primary means of communication between Alice and Bob, and will be referred to as qubit m.

The rest of the spaces will only be used in the last pair of messages. The spaces $H_{a'},H_{b'}$, and H_{mn} each involve n qubits whereas H_{ac} and H_{bc} each contain one qubit.

Before describing the protocol we need to define a set of unitaries on $H_A\otimes H_M$. We begin with the controlled rotations $R_{A,k}$ defined for $k=1,\ldots,n$ by

$$R_{A,k} = \sum_{\substack{x\\ |x|=k-1}} |x\rangle\langle x|_{a_1,\ldots,a_{k-1}} \otimes U(\mathcal{G}_x)_{a_k,m}, \tag{A4}$$

where

$$U(z) = \begin{pmatrix} \sqrt{z} & 0 & 0 & -\sqrt{1-z} \\ 0 & \sqrt{z} & -\sqrt{1-z} & 0 \\ 0 & \sqrt{1-z} & \sqrt{z} & 0 \\ \sqrt{1-z} & 0 & 0 & \sqrt{z} \end{pmatrix}. \tag{A5}$$

The subscripts on the operators and matrices indicate what qubits they act on, and $R_{A,k}$ acts trivially on all qubits of $H_A\otimes H_M$ not explicitly mentioned. For the case $k=1$ the operator is not a controlled rotation but rather a regular rotation using parameter $\mathcal{G}_r$.

We shall also need the controlled rotation

$$R_{A,E} = \sum_{\substack{x\\ |x|=n}} |x\rangle\langle x|_{a_1,\ldots,a_n} \otimes \begin{pmatrix} 1-\mathcal{G}_x & -\mathcal{G}_x \\ \mathcal{G}_x & 1-\mathcal{G}_x \end{pmatrix}_{ac}, \tag{A6}$$

which is unitary because $\mathcal{G}_x\in\{0,1\}$ for $|x|=n$. The gate is simply a controlled-X applied to the qubit in space H_{ac}, where the control depends on a function of the qubits in H_a.

Note that $R_{A,E}$ can also be defined as an operator acting purely on H_A rather than $H_A \otimes H_M$.

Finally, define $S_{A,k}$ for $k=1,\ldots,n$ to swap qubit a_k with qubit m,

$$S_{A,k} = \mathrm{SWAP}(a_k,m). \tag{A7}$$

We also need $T_{A,0}$ which swaps H_a with H_{mn} conditioned on qubit ac being zero, and $T_{A,1}$ which swaps the space $H_{a'}$ with the space H_{nm} conditioned on qubit ac being one,

$$T_{A,0} = |0\rangle\langle 0|_{ac} \otimes \mathrm{SWAP}(H_a,H_{mn}) + |1\rangle\langle 1|_{ac} \otimes I, \tag{A8}$$

$$T_{A,1} = |1\rangle\langle 1|_{ac} \otimes \mathrm{SWAP}(H_{mn},H_{a'}) + |0\rangle\langle 0|_{ac} \otimes I. \tag{A9}$$

The first one is used to send the qubits in H_a when Alice wins, whereas the second one is used to receive Bob's qubits and set them in $H_{a'}$ when Alice loses.

All the above operators act on Alice's Hilbert space. We can similarly define the operators $R_{B,k}, R_{B,E}, S_{B,k}$ acting in the same way on Bob's qubits. The operator $T_{B,0}$ however must be defined to swap $H_{b'}$ with H_{mn} conditioned on qubit bc being zero, whereas $T_{B,1}$ swaps H_b with H_{mn} conditioned on qubit bc being one.

To characterize the final measurements it is useful to define the probability tree $\mathcal{P}$ by

$$\mathcal{P}_x = \begin{cases} 1 & \text{if } x=r, \\ \mathcal{G}_y\mathcal{P}_y & \text{if } x=y0, \\ (1-\mathcal{G}_y)\mathcal{P}_y & \text{if } x=y1. \end{cases} \tag{A10}$$

That is, $\mathcal{P}_x$ is the probability of reaching node x when the classical coin-flipping game associated with $\mathcal{G}$ is played honestly. We can now define the two normalized states

$$|\psi_{A,1}\rangle = \frac{1}{\sqrt{\mathcal{H}_r}} \sum_{\substack{x \\ |x|=n \\ \mathcal{G}_x=1}} \sqrt{\mathcal{P}_x}|x\rangle_{H_a} \otimes |x\rangle_{H_{a'}} \otimes |1\rangle_{H_{ac}},$$

$$|\psi_{B,0}\rangle = \frac{1}{\sqrt{1-\mathcal{H}_r}} \sum_{\substack{x \\ |x|=n \\ \mathcal{G}_x=0}} \sqrt{\mathcal{P}_x}|x\rangle_{H_b} \otimes |x\rangle_{H_{b'}} \otimes |0\rangle_{H_{bc}}. \tag{A11}$$

The normalization is correct because $\mathcal{H}_r$ is the probability of arriving at a leaf x such that $\mathcal{G}_x=1$, whereas $1-\mathcal{H}_r$ is the probability of arriving at a leaf with $\mathcal{G}_x=0$. We are now ready to describe the main protocol.

Protocol 1: *Given an n–coin-game*, $\mathcal{G}$, *and the associated operators described above, define a quantum weak coin-flipping protocol by the following steps:*

(1) *Setup: Alice starts with* $H_A \otimes H_M$ *and Bob with* H_B. *They each initialize their space to the state* $|0\rangle$.

(2) *First n messages. For* $k=1$ *to* n:

(i) *If k is odd, Alice applies* $R_{A,k}$ *and sends* H_M *to Bob who applies* $S_{B,k}$.

(ii) *If k is even, Bob applies* $R_{B,k}$ *and sends* H_M *to Alice who applies* $S_{A,k}$.

(3) *Alice applies* $R_{A,E}$ *to* H_A *and Bob applies* $R_{B,E}$ *to* H_B. *No messages are needed for this step.*

(4) *If Bob has* H_M *he sends it to Alice.*

(5) *Alice applies* $T_{A,0}$ *and sends* H_M *to Bob who applies* $T_{B,0}$.

(6) *Bob applies* $T_{B,1}$ *and sends* H_M *to Alice who applies* $T_{A,1}$.

(7) *Alice measures using the two outcome POVM* $\{I - |\psi_{A,1}\rangle\langle\psi_{A,1}|, |\psi_{A,1}\rangle\langle\psi_{A,1}|\}$. *Bob measures the two outcome POVM* $\{|\psi_{B,0}\rangle\langle\psi_{B,0}|, I - |\psi_{B,0}\rangle\langle\psi_{B,0}|\}$. *They each output zero for the first outcome and one for the second.*

The basic intuition behind the protocol is that the first three steps above is a quantum implementation of the classical public-coin coin-flipping protocol associated with $\mathcal{G}$ described in Sec. II. After k messages the first k bits of H_A contain a length k string indicating the depth k node at which we are currently located. The quantum amplitude associated with each such state is $\sqrt{\mathcal{P}_x}$. Step (3) is a unitary realization of the measurement that looks at the n bit string x corresponding to a leaf, and stores the classical coin outcome in the qubit associated with H_{ac} for Alice and H_{bc} for Bob.

The rest of the steps involve cheat detection. Effectively, the winner declares victory immediately and then sends as much of their state as possible to the other party. The losing party then checks that the state is correct before accepting defeat.

Note that, as written, the above protocol takes either $n+2$ or $n+3$ messages. However, it is easy to see that the protocol can be run with only $n+1$ messages. For starters, only the space H_m needs to be sent back and forth in step (2), whereas only H_{mn} is used in steps (5) and (6). If we allow such a splitting, Alice starts with H_{mn} and step (4) is never needed. This reduces the protocol to $n+2$ messages always. But if n is odd then Alice ends up sending two messages in a row. The two messages can be combined into a single longer message and therefore the protocol only requires $n+1$ messages. We will also argue below that steps (5) and (6) can be interchanged, in which case when n is even Bob sends two messages in a row, and their merger leads again to a protocol with only $n+1$ messages.

We turn to the task of describing the evolution of the game when both players are honest. The action of $R_{A,k}$ entangles qubit a_k with qubit m, whereas $S_{B,k}$ swaps qubit m with b_k. Their combined effect is the transformation

$$\sqrt{\mathcal{P}_x}|x\rangle_{a_1,\ldots,a_{k-1}} \otimes |0\rangle_{a_k} \otimes |0\rangle_{b_k} \to \sqrt{\mathcal{P}_{x0}}|x\rangle_{a_1,\ldots,a_{k-1}} \otimes |0\rangle_{a_k} \otimes |0\rangle_{b_k} + \sqrt{\mathcal{P}_{x1}}|x\rangle_{a_1,\ldots,a_{k-1}} \otimes |1\rangle_{a_k} \otimes |1\rangle_{b_k}. \tag{A12}$$

The same effect occurs on even rounds when Alice's and Bob's actions are reversed. Therefore, the state after the first k passes through step (2) is given by

$$|\psi_k\rangle = \sum_{\substack{x \\ |x|=k}} \sqrt{\mathcal{P}_x}|x0\cdots 0\rangle_{H_a} \otimes |0\rangle_{H_{a'}\otimes H_{ac}} \otimes |x0\cdots 0\rangle_{H_b} \otimes |0\rangle_{H_{b'}\otimes H_{bc}} \otimes |0\rangle_{H_M}, \tag{A13}$$

where there are $n-k$ zeroes following each x.

Step (3) simply has the effect of setting up the fair coin outcome in H_{ac} and H_{bc},

$$|\psi_E\rangle = \sum_{\substack{x \\ |x|=n}} \sqrt{\mathcal{P}_x}|x\rangle_{H_a} \otimes |0\rangle_{H_{a'}} \otimes |\mathcal{G}_x\rangle_{H_{ac}} \otimes |x\rangle_{H_b} \otimes |0\rangle_{H_{b'}} \otimes |\mathcal{G}_x\rangle_{H_{bc}} \otimes |0\rangle_{H_M}. \tag{A14}$$

Finally, when both players are honest, step (5) has the effect of moving H_a to $H_{b'}$ conditioned on qubits ac and bc both being one. Step (6) has the effect of swapping H_b to $H_{a'}$ conditioned on ac and bc being both zero. The final state of the protocol is therefore,

$$\begin{aligned}|\psi_F\rangle &= \sum_{\substack{x \\ |x|=n \\ \mathcal{G}_x=1}} \sqrt{\mathcal{P}_x}|x\rangle_{H_a} \otimes |x\rangle_{H_{a'}} \otimes |1\rangle_{H_{ac}} \otimes |0\rangle_{H_b} \otimes |0\rangle_{H_{b'}} \\ &\quad \otimes |1\rangle_{H_{bc}} \otimes |0\rangle_{H_M} + \sum_{\substack{x \\ |x|=n \\ \mathcal{G}_x=0}} \sqrt{\mathcal{P}_x}|0\rangle_{H_a} \otimes |0\rangle_{H_{a'}} \otimes |0\rangle_{H_{ac}} \\ &\quad \otimes |x\rangle_{H_b} \otimes |x\rangle_{H_{b'}} \otimes |0\rangle_{H_{bc}} \otimes |0\rangle_{H_M} \\ &= \sqrt{\mathcal{H}_r}|\psi_{A,1}\rangle \otimes |0\rangle_{H_b\otimes H_{b'}} \otimes |1\rangle_{H_{bc}} \otimes |0\rangle_{H_M} \\ &\quad + \sqrt{1-\mathcal{H}_r}|0\rangle_{H_a\otimes H_{a'}} \otimes |0\rangle_{H_{ac}} \otimes |\psi_{B,0}\rangle \otimes |0\rangle_{H_M}.\end{aligned} \tag{A15}$$

Because $|\psi_{A,1}\rangle$ is orthogonal to any state with the value zero in register H_{ac} and $|\psi_{B,1}\rangle$ is orthogonal to any state with the value one in register H_{bc}, there are only two possible outcomes for the final measurements.

(i) Alice obtains $I-|\psi_{A,1}\rangle\langle\psi_{A,1}|$ and Bob obtains $|\psi_{B,0}\rangle\langle\psi_{B,0}|$ in which case they both output zero, that is, Alice wins. This happens with probability $1-\mathcal{H}_r$.

(ii) Alice obtains $|\psi_{A,1}\rangle\langle\psi_{A,1}|$ and Bob obtains $I-|\psi_{B,0}\rangle\langle\psi_{B,0}|$ in which case they both output one, that is, Bob wins. This happens with probability $\mathcal{H}_r$.

We have therefore proven the following lemma.

Lemma 10: *When playing Protocol 1 honestly, Alice's and Bob's outputs are perfectly correlated and satisfy*

$$P_A = 1 - \mathcal{H}_r, \quad P_B = \mathcal{H}_r. \tag{A16}$$

1. Reformulation as an SDP

We now turn to the analysis of the advantage that a cheating player can attain. Specifically, we shall focus on the case of honest Alice and cheating Bob. The case where Alice is cheating is fairly similar and will be derived at the end of the appendix from the case of cheating Bob.

When Bob is cheating we do not know exactly what operations (unitaries, measurements, or superoperators) he may be applying to his qubits. In fact, we do not even know how many qubits he may have in his laboratory. We shall therefore focus only on the evolution of the qubits under Alice's control. This approach, first advocated by Kitaev [11], will transform the maximization over Bob's cheating strategies into a semidefinite program (SDP).

Let ρ_0 be the initial state of all qubits under Alice's control, that is, it is a density operator on $H_A \otimes H_M$. Let $\rho_1,\ldots,\rho_n$ be the state of the qubits under Alice's control after each of the n passes through step (2). Note that ρ_k is a density operator for H_A when k is odd, and for $H_A \otimes H_M$ when k is even. Finally let ρ_E be the state of $H_A \otimes H_M$ at the end of step (4) and let ρ_F be the state of $H_A \otimes H_M$ at the end of step (6).

Because Alice initializes her own qubits as prescribed by the protocol without interference from Bob, their initial state is given by

$$\rho_0 = |0\rangle\langle 0|_{H_A\otimes H_M}. \tag{A17}$$

For odd k, Alice first applies the unitary $R_{A,k}$ and then sends H_M to Bob, leaving the state

$$\rho_k = \mathrm{Tr}_M[R_{A,k}\rho_{k-1}R_{A,k}^{-1}] \quad (\text{for } k \text{ odd}). \tag{A18}$$

For even k, we cannot fully characterize ρ_k in terms of ρ_{k-1} but we know that given ρ_k, if we undo the swap $S_{A,k}$ and then send back H_M we must end up with ρ_{k-1}, therefore

$$\mathrm{Tr}_M[S_{A,k}^{-1}\rho_k S_{A,k}] = \rho_{k-1} \quad (\text{for } k \text{ even}). \tag{A19}$$

Step (3) only involved the use of $R_{A,E}$, a unitary on H_A. Step (4), the recovery of H_M, is only needed when n is odd. Therefore,

$$\rho_E = R_{A,E}\rho_n R_{A,E}^{-1} \quad \text{for } n \text{ even}, \tag{A20}$$

$$\mathrm{Tr}_M\, \rho_E = R_{A,E}\rho_n R_{A,E}^{-1} \quad \text{for } n \text{ odd}. \tag{A21}$$

Finally, the state of the qubits on H_A after applying $T_{A,0}$ to ρ_E must equal the state ρ_F if we undo $T_{A,1}$ (because as usual, Bob has no effect on Alice's qubits),

$$\mathrm{Tr}_M[T_{A,1}^{-1}\rho_F T_{A,1}] = \mathrm{Tr}_M[T_{A,0}\rho_E T_{A,0}^{-1}]. \tag{A22}$$

The probability that Bob wins is given by the final measurement

$$\mathrm{Tr}[|\psi_{A,1}\rangle\langle\psi_{A,1}|\rho_F], \tag{A23}$$

where it is understood that $|\psi_{A,1}\rangle\langle\psi_{A,1}|$ can be extended to an operator on $H_A \otimes H_M$ by tensoring with the identity I_M.

The preceding arguments show that no matter what cheating strategy Bob employs, the sequence of states for Alice's qubits must satisfy the above equations, and therefore P_B^* is upper bounded by the maximum of Eq. (A23) over all assignments to the variables $\rho_0,\ldots,\rho_n,\rho_E,\rho_F$ consistent with the above equations. It is also not hard to see that Bob can achieve any set of density matrices consistent with the above equations by maintaining the purification of Alice's state. As this reduction from maximization over cheating strategies to SDP has already appeared in the literature [1,11,12] we will not belabor the point and simply state the lemma we have proven,

Lemma 11: *The maximum probability with which Bob can win by cheating in Protocol 1 is given by the solution of the SDP,*

$$P_B^* = \max \mathrm{Tr}[|\psi_{A,1}\rangle\langle\psi_{A,1}|\rho_F], \tag{A24}$$

over the positive semidefinite variables $\rho_0, \ldots, \rho_n, \rho_E, \rho_F$ *subject to the constraints of Eqs. (A17)–(A22).*

The security of the above result depends solely on the laws of quantum mechanics and the assumption that Bob cannot directly influence the qubits in Alice's laboratory. We note that we are assuming, as is usual in coin-flipping protocols, that Alice can measure the size of the Hilbert space H_M (i.e., the number of qubits sent by Bob in each message) and that if at any point she receives more or less than the required number of qubits she aborts the protocol and declares herself the winner. The optimal strategy for Bob involves sending the right number of qubits in each message and therefore is described by the above formalism.

It will be important below to know that we can exchange steps (5) and (6). This would work as follows: given ρ_E we send H_M to Bob, who is supposed to apply $T_{B,1}$ to his qubits. Upon return, Alice applies $T_{A,1}$ followed by $T_{A,0}$ ending up with state ρ'_F satisfying

$$\mathrm{Tr}_M[T_{A,1}^{-1}T_{A,0}^{-1}\rho'_F T_{A,0}T_{A,1}] = \mathrm{Tr}_M[\rho_E]. \tag{A25}$$

The final measurement can be done immediately before sending H_M to Bob because it only has support on H_A. The probability of Bob winning is

$$Tr[|\psi_{A,1}\rangle\langle\psi_{A,1}|\rho'_F]. \tag{A26}$$

However, $|\psi_{A,1}\rangle$ only has support on the space where qubit ac is one, and in this subspace $T_{A,0}$ acts trivially (and $T_{A,0}$ and $T_{A,1}$ commute). Applying projectors to both sides of the Eq. (A22) and Eq. (A25) we see that both SDPs are equivalent, and therefore steps (5) and (6) are interchangeable, at least from the perspective of honest Alice.

2. Lower bounds

To find a lower bound on P_B^* we shall describe a specific assignment of the variables ρ that satisfies the above equations, and from it calculate $\mathrm{Tr}[|\psi_{A,1}\rangle\langle\psi_{A,1}|\rho_F]$. Because P_B^* is a maximum over such assignments, this will serve as a lower bound.

Let

$$\rho_k = \begin{cases} \sigma_k \otimes |0\rangle\langle 0|_{a_{k+1},\ldots,a_n} \otimes |0\rangle\langle 0|_{H_{a'}\otimes H_{ac}} & k \text{ odd}, \\ \sigma_k \otimes |0\rangle\langle 0|_{a_{k+1},\ldots,a_n} \otimes |0\rangle\langle 0|_{H_{a'}\otimes H_{ac}\otimes H_M} & k \text{ even}, \end{cases} \tag{A27}$$

where σ_k is a density operator for qubits a_1 through a_k. The operators ρ_1 through ρ_n satisfy Eqs. (A18) and (A19) provided that

$$\sigma_k = Tr_m\Big[R_{A,k}\big(\sigma_{k-1} \otimes |0\rangle\langle 0|_{a_k,m}\big)R_{A,k}^{-1}\Big] \quad (\text{for } k \text{ odd}), \tag{A28}$$

where $\sigma_0 = 1$ is the unit, and

$$Tr_{a_k}[\sigma_k] = \sigma_{k-1} \quad (\text{for } k \text{ even}). \tag{A29}$$

The σ operators above will be defined using a tree variable $\mathcal{W}$ given by the equation

$$\mathcal{W}_x = \begin{cases} 1, & x = r, \\ \mathcal{G}_y W_y, & x = y0 \text{ and } |x| \text{ odd}, \\ (1-\mathcal{G}_y)W_y, & x = y1 \text{ and } |x| \text{ odd}, \\ \mathcal{G}_y \mathcal{B}_x^2 W_y/\mathcal{B}_y, & x = y0 \text{ and } |x| \text{ even}, \\ (1-\mathcal{G}_y)\mathcal{B}_x^2 W_y/\mathcal{B}_y, & x = y1 \text{ and } |x| \text{ even}, \end{cases} \tag{A30}$$

which is based on the weight matrix W of Ref. [1]. Note that, though it is possible for $\mathcal{B}_y$ to be zero, this can only occur if both $\mathcal{B}_{y0}$ and $\mathcal{B}_{y1}$ are zero as well, in this case we define $\mathcal{W}_{y0} = \mathcal{W}_{y1} = 0$, which resolves the potential division by zero.

Because $\mathcal{B}$ is computed bottom-up, whereas $\mathcal{W}$ is computed top-down, every node of $\mathcal{W}$ depends on the complete n–coin-game assignment $\mathcal{G}$. The appearance at every node of such global information about the protocol is crucial for optimal solutions of these SDPs and will also occur with the tree variable $\mathcal{Z}$ defined below in the section on upper bounds.

Define the σ operators as diagonal matrices with entries given by

$$\langle x|\sigma_k|x\rangle = \mathcal{W}_x \quad \text{for } |x| = k. \tag{A31}$$

The requirements of Eq. (A28) are satisfied if

$$\mathcal{W}_{y0} = \mathcal{G}_y\mathcal{W}_y \quad \text{and } \mathcal{W}_{y1} = (1-\mathcal{G}_y)\mathcal{W}_y \quad (\text{for } |y| \text{ even}), \tag{A32}$$

whereas Eq. (A29) only imposes the weaker requirement

$$\mathcal{W}_y = \mathcal{W}_{y0} + \mathcal{W}_{y1} \quad (\text{for } |y| \text{ odd}), \tag{A33}$$

both of which are clearly satisfied by $\mathcal{W}$. We have therefore outlined a valid cheating strategy for Bob through step (2).

The next two steps will follow the protocol exactly, in which case the operator ρ_E follows from ρ_n by adjusting the space H_{ac}:

$$\rho_E = \sum_x \mathcal{W}_x |x\rangle\langle x|_{H_a} \otimes |0\rangle\langle 0|_{H_{a'}} \otimes |\mathcal{G}_x\rangle\langle\mathcal{G}_x|_{H_{ac}} \otimes |0\rangle\langle 0|_{H_M}. \tag{A34}$$

Finally, in the last steps, conditioned on qubit ac being zero Alice sends her state to Bob. Conditioned on qubit ac being one, Bob returns the purification of the remaining qubits, so the final state is

$$\rho_F = |\phi_1\rangle\langle\phi_1|_{H_a\otimes H_{a'}} \otimes |1\rangle\langle 1|_{H_{ac}} \otimes |0\rangle\langle 0|_{H_M} + C_0|0\rangle\langle 0|_{H_a\otimes H_{a'}} \otimes |0\rangle\langle 0|_{H_{ac}} \otimes |0\rangle\langle 0|_{H_M}, \tag{A35}$$

where C_0 is an unimportant constant (equal to the sum of $\mathcal{W}_x$

for all x such that $\mathcal{G}_x=0$), and $|\phi_1\rangle$ is the unnormalized state given by

$$|\phi_1\rangle = \sum_{\substack{x\\|x|=n\\\mathcal{G}_x=1}} \sqrt{\mathcal{W}_x}|x\rangle_{H_a}\otimes|x\rangle_{H_{a'}}. \tag{A36}$$

Bob's probability of winning is given by

$$p = \left|\left(\langle\phi_1|_{H_a\otimes H_{a'}}\otimes\langle 1|_{H_{ac}}\right)|\psi_{A,1}\rangle\right|^2 = \left|\sum_{\substack{x\\|x|=n}} \mathcal{G}_x\sqrt{\mathcal{W}_x\mathcal{P}_x}\right|^2/\mathcal{H}_r, \tag{A37}$$

where the factor of $\mathcal{G}_x$ ensures that the sum is only taken over strings x satisfying $\mathcal{G}_x=1$.

While the expression for computing p seems rather daunting, we shall show in a moment that when properly written, it is a conserved quantity that has the same value at every depth in the tree. We begin with the following two observations: for $|y|$ even,

$$\begin{aligned}&\sqrt{\mathcal{B}_{y0}}\sqrt{\mathcal{W}_{y0}\mathcal{P}_{y0}}+\sqrt{\mathcal{B}_{y1}}\sqrt{\mathcal{W}_{y1}\mathcal{P}_{y1}}\\&\quad=(\mathcal{G}_y\sqrt{\mathcal{B}_{y0}}+(1-\mathcal{G}_y)\sqrt{\mathcal{B}_{y1}})\sqrt{\mathcal{W}_y\mathcal{P}_y}=\mathcal{B}_y\sqrt{\mathcal{W}_y\mathcal{P}_y},\end{aligned} \tag{A38}$$

whereas for $|y|$ odd we have

$$\begin{aligned}&\mathcal{B}_{y0}\sqrt{\mathcal{W}_{y0}\mathcal{P}_{y0}}+\mathcal{B}_{y1}\sqrt{\mathcal{W}_{y1}\mathcal{P}_{y1}}\\&\quad=(\mathcal{G}_y\mathcal{B}_{y0}^2+(1-\mathcal{G}_y)\mathcal{B}_{y1}^2)\sqrt{\mathcal{W}_y\mathcal{P}_y/\mathcal{B}_y}=\sqrt{\mathcal{B}_y}\sqrt{\mathcal{W}_y\mathcal{P}_y}.\end{aligned} \tag{A39}$$

For the special case when $\mathcal{B}_y=0$ the equation is also valid as it reads $0+0=0$. By induction, we can obtain the following result:

$$\mathcal{B}_r\sqrt{\mathcal{W}_r\mathcal{P}_r}=\begin{cases}\displaystyle\sum_{x;|x|=k}\mathcal{B}_x\sqrt{\mathcal{W}_x\mathcal{P}_x} & \text{for any even } k,\\ \displaystyle\sum_{x;|x|=k}\sqrt{\mathcal{B}_x}\sqrt{\mathcal{W}_x\mathcal{P}_x} & \text{for any odd } k,\end{cases} \tag{A40}$$

where as usual $0\leqslant k\leqslant n$. In particular, because for $|x|=n$ we have $\mathcal{G}_x=\mathcal{B}_x=\sqrt{\mathcal{B}_x}\in\{0,1\}$ we have shown that $p=|\mathcal{B}_r\sqrt{\mathcal{W}_r\mathcal{P}_r}|^2/\mathcal{H}_r$, which is the probability with which Bob can win the coin flip by cheating using the strategy outlined above. Since $\mathcal{W}_r=\mathcal{P}_r=1$ we have proven the desired lower bound.

Lemma 12: *For Protocol 1*,

$$P_B^*\geqslant\frac{\mathcal{B}_r^2}{\mathcal{H}_r}. \tag{A41}$$

3. Upper bounds

We shall prove an upper bound by exhibiting a solution to the dual SDP. We use the derivation of the dual in Ref. [12], though a direct derivation (as was done in Ref. [1]) would be fairly simple as well.

Our protocol can be rewritten in the notation of Ref. [12]. Let $m=\lfloor(n+1)/2\rfloor$ and define $U_{A,1}=R_{A,1}, U_{A,j}=R_{A,2j-1}S_{A,2j-2}$ for $j=2,\ldots,m, U_{A,m+1}=T_{A,0}R_{A,E}S_{A,n}$ (or if n is odd just $U_{A,m+1}=T_{A,0}R_{A,E}$) and $U_{A,m+2}=T_{A,1}$. The final measurement is $\Pi_{A,1}=|\psi_{A,1}\rangle\langle\psi_{A,1}|$. In this notation, we are looking for the maximum of $\mathrm{Tr}[\Pi_{A,1}\rho_{A,m+2}]$ over assignments of the positive semidefinite variables $\rho_{A,0},\ldots,\rho_{A,m+2}$ satisfying

$$\mathrm{Tr}_M[\rho_{A,j}]=\mathrm{Tr}_M[U_{A,j}\rho_{A,j-1}U_{A,j}^{-1}] \tag{A42}$$

for $j=1,\ldots,m+2$ and $\mathrm{Tr}_M[\rho_{A,0}]=|0\rangle\langle 0|_{H_A}$. The initial condition for $\rho_{A,0}$ (rather than the usual $\rho_{A,0}=|0\rangle\langle 0|_{H_A\otimes H_M}$) simply gives Bob a little more cheating power (i.e., to initialize H_M) but this is acceptable as we are now focusing on deriving upper bounds on P_B^* and this extra cheating power will not be helpful.

The dual SDP is given by Lemma 11 of Ref. [12] as the minimization of $\langle 0|Y_{A,0}|0\rangle$, subject to

$$Y_{A,j}\otimes I_{H_M}\geqslant U_{A,j+1}^{-1}(Y_{A,j+1}\otimes I_{H_M})U_{A,j+1} \tag{A43}$$

for $0\leqslant j\leqslant m+1$, where $Y_0,\ldots,Y_{m+1}$ are Hermitian operators on H_A and $Y_{A,m+2}\equiv\Pi_{A,1}$. Because this is the dual SDP to the original coin-flipping SDP corresponding to Protocol 1, any assignment of the variables $Y_{A,i}$ that satisfies the constraints will produce a value of $\langle 0|Y_{A,0}|0\rangle$ that is an upper bound on P_B^*. However, rather than finding a solution to the above dual SDP, we shall study a modified, but equivalent, SDP.

Lemma 13: *Let* $Z_0,\ldots,Z_{n+2}$ *be a set of Hermitian matrices, defined on* H_A, *satisfying the following equations*:

$$\begin{aligned}&Z_k\otimes I_{H_M}\geqslant R_{A,k+1}^{-1}(Z_{k+1}\otimes I_{H_M})R_{A,k+1}\quad(k\text{ even}),\\&Z_k\otimes I_{H_M}\geqslant S_{A,k+1}^{-1}(Z_{k+1}\otimes I_{H_M})S_{A,k+1}\quad(k\text{ odd}),\end{aligned} \tag{A44}$$

where $0\leqslant k<n$, *and*

$$Z_n\otimes I_{H_M}\geqslant R_{A,E}^{-1}(Z_{n+1}\otimes I_{H_M})R_{A,E}, \tag{A45}$$

$$Z_{n+1}\otimes I_{H_M}\geqslant T_{A,0}^{-1}(Z_{n+2}\otimes I_{H_M})T_{A,0}, \tag{A46}$$

$$Z_{n+2}\otimes I_{H_M}\geqslant T_{A,1}^{-1}(|\psi_{A,1}\rangle\langle\psi_{A,1}|\otimes I_{H_M})T_{A,1}, \tag{A47}$$

then $\beta\equiv\langle 0|Z_0|0\rangle$ *is an upper bound on* P_B^*.

The proof follows by noting that given a set of $Z_0,\ldots,Z_{n+2}$ satisfying the above equations, we can set $Y_0=Z_0, Y_j=Z_{2j-1}$ for $j=1,\ldots,m$ and $Y_{m+1}=Z_{n+2}$ to obtain a solution with the same minimum as the original dual SDP.

We introduce a variable, defined on a tree of depth n, which shall be used in constructing solutions of the dual SDP:

$$\mathcal{Z}_x = \begin{cases} \mathcal{B}_r^2/\mathcal{H}_r, & x=r, \\ \sqrt{\mathcal{B}_x}\mathcal{Z}_y/\mathcal{B}_y, & |x| \text{ odd}, \\ \mathcal{Z}_y, & |x| \text{ even}, \end{cases} \tag{A48}$$

where y is the parent node of x (i.e., either $x=y0$ or $x=y1$). Once again we resolve the division by zero by declaring $\mathcal{Z}_{y0}=\mathcal{Z}_{y1}=0$ whenever $\mathcal{B}_y=0$ and $|y|$ is even.

We begin the description of the solution to the dual SDP by choosing

$$Z_{n+2} = \sum_{\substack{x \\ |x|=n \\ \mathcal{G}_x=1}} \mathcal{Z}_x |x\rangle\langle x|_{H_a} \otimes I_{H_{a'}} \otimes |1\rangle\langle 1|_{H_{ac}}. \tag{A49}$$

To verify that Z_{n+2} satisfies Eq. (A47), we note that we can move the unitary operators $T_{A,1}$ to the left-hand side of the equation, where they act trivially (i.e., they exchange $I_{H_{a'}}$ with $I_{H_{mn}}$). We are left with the task of proving $Z_{n+2} \geqslant |\psi_{A,1}\rangle\langle\psi_{A,1}|$.

It is sufficient to show that

$$Z_{n+2} + \epsilon I_{H_A} \geqslant |\psi_{A,1}\rangle\langle\psi_{A,1}| \tag{A50}$$

for every $\epsilon > 0$. Because Z_{n+2} is non-negative, the left-hand-side above is positive definite. We can rescale our space by $(Z_{n+2}+\epsilon I_{H_A})^{-1/2}$ to obtain the equivalent equation

$$I \geqslant (Z_{n+2} + \epsilon I_{H_A})^{-\frac{1}{2}} |\psi_{A,1}\rangle\langle\psi_{A,1}| (Z_{n+2} + \epsilon I_{H_A})^{-\frac{1}{2}}. \tag{A51}$$

The right-hand-side of the above equation has only one non-zero eigenvalue, it is therefore sufficient to check that

$$1 \geqslant \langle\psi_{A,1}|(Z_{n+2} + \epsilon I_{H_A})^{-1}|\psi_{A,1}\rangle. \tag{A52}$$

We need to study the quantity

$$\langle\psi_{A,1}|(Z_{n+2} + \epsilon I_{H_A})^{-1}|\psi_{A,1}\rangle = \sum_{\substack{x \\ |x|=n \\ \mathcal{G}_x=1}} \frac{\mathcal{P}_x}{\mathcal{H}_r(\mathcal{Z}_x + \epsilon)} \tag{A53}$$

which once again is related to a conserved quantity at every level of the tree. However, we first note the following properties which can be checked directly from the definitions.

(i) $\mathcal{P}_x > 0$ implies $\mathcal{P}_y > 0$ for every node y that has x as a descendant.

(ii) $\mathcal{P}_x > 0$ and $\mathcal{B}_x > 0$ implies that $\mathcal{B}_y > 0$ for every node y that has x as a descendant.

(iii) $\mathcal{P}_x > 0$ and $\mathcal{B}_x > 0$ implies $\mathcal{Z}_x > 0$.

We can now remove ϵ from the above expression, because if $\mathcal{Z}_x=0$ then either $\mathcal{P}_x=0$ or $\mathcal{B}_x=0$ (which implies $\mathcal{G}_x=0$),

$$\langle\psi_{A,1}|(Z_{n+2} + \epsilon I_{H_A})^{-1}|\psi_{A,1}\rangle \leqslant \sum_{\substack{x \\ |x|=n \\ \mathcal{Z}_x>1}} \frac{\mathcal{G}_x\mathcal{P}_x}{\mathcal{H}_r\mathcal{Z}_x}, \tag{A54}$$

where the factor $\mathcal{G}_x$ imposes the condition $\mathcal{G}_x=1$, and the condition $\mathcal{Z}_x > 0$ has been moved into the sum.

If $|y|$ is odd and $\mathcal{Z}_y > 0$ we have

$$\frac{\mathcal{B}_{y0}^2\mathcal{P}_{y0}}{\mathcal{Z}_{y0}} + \frac{\mathcal{B}_{y1}^2\mathcal{P}_{y1}}{\mathcal{Z}_{y1}} = \left[\mathcal{B}_{y0}^2\mathcal{G}_y + \mathcal{B}_{y1}^2(1-\mathcal{G}_y)\right]\frac{\mathcal{P}_y}{\mathcal{Z}_y} = \frac{\mathcal{B}_y\mathcal{P}_y}{\mathcal{Z}_y}, \tag{A55}$$

where the left-hand side is well defined because $\mathcal{Z}_{y0}=\mathcal{Z}_{y1}=\mathcal{Z}_y > 0$. If $|y|$ is even we have

$$\frac{\mathcal{B}_{y0}\mathcal{P}_{y0}}{\mathcal{Z}_{y0}} + \frac{\mathcal{B}_{y1}\mathcal{P}_{y1}}{\mathcal{Z}_{y1}} = \left[\sqrt{\mathcal{B}_{y0}}\mathcal{G}_y + \sqrt{\mathcal{B}_{y1}}(1-\mathcal{G}_y)\right]\frac{\mathcal{B}_y\mathcal{P}_y}{\mathcal{Z}_y} = \frac{\mathcal{B}_y^2\mathcal{P}_y}{\mathcal{Z}_y}. \tag{A56}$$

Even if $\mathcal{Z}_y > 0$ it is possible for either $\mathcal{Z}_{y0}$ or $\mathcal{Z}_{y1}$ (or both) to be zero. If both are zero, then so is $\mathcal{B}_y\mathcal{P}_y$. If only one of them is zero (say $\mathcal{Z}_{y0}$) then the equation is still valid with the offending term removed (that is, $\mathcal{B}_{y1}\mathcal{P}_{y1}/\mathcal{Z}_{y1}=\mathcal{B}_y^2\mathcal{P}_y/\mathcal{Z}_y$). Using induction, we can prove

$$1 = \frac{\mathcal{B}_r^2\mathcal{P}_r}{\mathcal{H}_r\mathcal{Z}_r} = \begin{cases} \displaystyle\sum_{x;|x|=k;\mathcal{Z}_x>0} \frac{\mathcal{B}_x^2\mathcal{P}_x}{\mathcal{H}_r\mathcal{Z}_x} & \text{for any even k}, \\ \displaystyle\sum_{x;|x|=k;\mathcal{Z}_x>0} \frac{\mathcal{B}_x\mathcal{P}_x}{\mathcal{H}_r\mathcal{Z}_x} & \text{for any odd } k, \end{cases} \tag{A57}$$

and in particular, because $\mathcal{G}_x=\mathcal{B}_x=\mathcal{B}_x^2$ for $|x|=n$ we have shown $\langle\psi_{A,1}|(Z_{n+2}+\epsilon I_{H_A})^{-1}|\psi_{A,1}\rangle \leqslant 1$ for every $\epsilon > 0$, thus completing the proof that our choice for Z_{n+2} satisfies the requirement imposed by Eq. (A47).

The next few requirements are easier to check. Since Z_{n+2} only has support on the space in which qubit ac is one, on which $T_{A,0}$ acts trivially, we can satisfy Eq. (A46) by choosing

$$Z_{n+1} = \sum_{\substack{x \\ |x|=n}} \mathcal{Z}_x |x\rangle\langle x|_{H_a} \otimes I_{H_{a'}} \otimes |\mathcal{G}_x\rangle\langle\mathcal{G}_x|_{H_{ac}} \geqslant Z_{n+2}, \tag{A58}$$

where the inequality follows because we have simply included the (non-negative) coefficients for the states with $\mathcal{G}_x=0$.

The unitary $R_{A,E}$ operates only on the space H_A hence Eq. (A45) can be satisfied by choosing

$$Z_n = R_{A,E}^{-1} Z_{n+1} R_{A,E} = \sum_{\substack{x \\ |x|=n}} \mathcal{Z}_x |x\rangle\langle x|_{H_a} \otimes I_{H_{a'}} \otimes |0\rangle\langle 0|_{H_{ac}}. \tag{A59}$$

Finally, fix a new parameter $\epsilon' > 0$, and define

$$Z_k = \sum_{\substack{x \\ |x|=k}} \left(\mathcal{Z}_x + \frac{(n-k)\epsilon'}{n} \right) |x\rangle\langle x|_{a_1,\ldots,a_k} \otimes |0\rangle\langle 0|_{H_{a_{k+1},\ldots,a_n} \otimes H_{a'} \otimes H_{ac}} + C_k I_{a_1,\ldots,a_k} \otimes (I - |0\rangle\langle 0|)_{H_{a_{k+1},\ldots,a_n} \otimes H_{a'} \otimes H_{ac}}, \tag{A60}$$

for $k=0,\ldots,n-1$. The constants C_k will be defined recursively below, starting with C_{n-1}. For $k=0$ the above should be interpreted as

$$Z_0 = (\mathcal{Z}_r + \epsilon')|0\rangle\langle 0|_{H_A} + C_0(I - |0\rangle\langle 0|)_{H_A}. \tag{A61}$$

In order to prove that our solution to the dual SDP is valid, all that remains is to check Eq. (A44). The case of k odd is fairly simple because $\mathcal{Z}_y = \mathcal{Z}_{y0} = \mathcal{Z}_{y1}$ for $|y|$ odd, therefore qubit a_{k+1} of Z_{k+1} is unentangled with the rest of the qubits and its state is the identity density matrix (i.e., $Z_{k+1} = I_{a_{k+1}} \otimes Z'$ where Z' is an operator on the rest of the qubits). As the swap operator $S_{A,k+1}$ acts trivially on $Z_{k+1} \otimes I_{H_M}$, it is sufficient to check $Z_k \geqslant Z_{k+1}$, which is satisfied if $C_k \geqslant C_{k+1}$. For the special case of $k=n-1$ (and n even) it suffices to choose $C_k \geqslant \max \mathcal{Z}_x$ where the maximum is taken over all strings x such that $|x|=n$.

What remains to be proven is Eq. (A44) for the case of even k. Fix some even value of k and let $\alpha = Z_k \otimes I_{H_M}$ and $\beta = R_{A,k+1}^{-1}(Z_{k+1} \otimes I_{H_M})R_{A,k+1}$. There are just the left- and right-hand sides of the equation we are trying to prove: $\alpha \geqslant \beta$. Define the projector

$$\Pi = I_{a_1,\ldots,a_k} \otimes |0\rangle\langle 0|_{H_{a_{k+1},\ldots,a_n} \otimes H'_a \otimes H_{ac}} \otimes I_{H_M}. \tag{A62}$$

We shall prove in a moment $\Pi(\alpha-\beta)\Pi = (\epsilon'/n)\Pi$. It is also easy to see that $\Pi\alpha(I-\Pi) = (I-\Pi)\alpha\Pi = 0$ and $(I-\Pi)\alpha(I-\Pi) = C_k(I-\Pi)$. Under these conditions, it is always possible to choose a large enough C_k so that $\alpha \geqslant \beta$, which defines C_k in terms of C_{k+1} (except for C_{n-1} which can be defined directly from Z_n). For a proof, see for instance the proof of Lemma 3 in Ref. [1].

To prove $\Pi(\alpha-\beta)\Pi = (\epsilon'/n)\Pi$ we need to study the effect of the unitary $R_{A,k+1}$ on Z_{n+1}. The expression has the form of a sum of $|x\rangle\langle x|_{a_1,\ldots,a_k}$ tensored with

$$U(\mathcal{G}_x)^{-1}\left[\left(\mathcal{Z}_{x0}|0\rangle\langle 0|_{a_{k+1}} + \mathcal{Z}_{x1}|1\rangle\langle 1|_{a_{k+1}}\right) \otimes I_m\right]U(\mathcal{G}_x) \tag{A63}$$

for $|x|=k$, where $U(z)$ is defined by Eq. (A5). The component of the above that survives the projection Π has the form

$$\begin{aligned}
&\left(\mathcal{G}_x\mathcal{Z}_{x0} + (1-\mathcal{G}_x)\mathcal{Z}_{x1}\right)|0\rangle\langle 0|_{a_{k+1}} \otimes I_m \\
&= \left(\mathcal{G}_x\sqrt{\mathcal{B}_{x0}} + (1-\mathcal{G}_x)\sqrt{\mathcal{B}_{x1}}\right)\frac{\mathcal{Z}_x}{\mathcal{B}_x}|0\rangle\langle 0|_{a_{k+1}} \otimes I_m \\
&= \mathcal{Z}_x|0\rangle\langle 0|_{a_{k+1}} \otimes I_m.
\end{aligned} \tag{A64}$$

It is now straightforward to check that $\Pi\alpha\Pi = \Pi\beta\Pi + \epsilon'/n\Pi$, completing the proof that our choice of Z_k satisfies Eq. (A44).

Note that, while the original protocol only depends on the first column of the matrix $U(z)$, the above calculation involved the entire matrix. The reason for this is that when transforming from the SDP involving the Y variables to the SDP involving the Z variables we gave Bob a small amount of extra cheating power to set the qubits in H_M between application of $S_{A,k}$ and $R_{A,k+1}$, in which case the full matrix $U(z)$ becomes important. However, since the upper bound derived in this section matches the lower bound from the last section, it should be clear that such extra power is not useful.

The result thus far is the description of a set of variables $Z_0,\ldots,Z_{n+2}$ satisfying the equations of the dual SDP. This gives us an upper bound $P_B^* \leqslant \beta = \langle 0|Z_0|0\rangle = \mathcal{Z}_r + \epsilon'$. However, since $\epsilon' > 0$ is arbitrary, we have proven

Lemma 14: *For Protocol 1*,

$$P_B^* \leqslant \frac{\mathcal{B}_r^2}{\mathcal{H}_r}. \tag{A65}$$

4. Honest Bob vs cheating Alice

The analysis of the case of honest Bob and cheating Alice is fairly similar to the above calculations. Fortunately, we can exploit certain symmetries in the protocol to derive expressions for P_A^* from the above expressions for P_B^*.

Given an n–coin-game $\mathcal{G}$ define a new $(n+1)$–coin-game, $\mathcal{G}'$ by the rules $\mathcal{G}'_r = 1, \mathcal{G}'_{0x} = \mathcal{G}'_{1x} = \mathcal{G}_x$ for $|x| < n$ and $\mathcal{G}'_{0x} = \mathcal{G}'_{1x} = 1 - \mathcal{G}_x$ for $|x| = n$. We'd like to argue that the quantum protocol associated with $\mathcal{G}'$ is equivalent to the protocol associated with $\mathcal{G}$ but with Alice's and Bob's roles exchanged.

The basic idea is that the first message of $\mathcal{G}'$, which Alice sends to Bob is the pure state $|0\rangle$. If Bob is cheating, this state reveals no extra information about Alice's state, and if Alice is cheating, she has no incentive to reveal herself as a cheater by sending anything other than the state $|0\rangle$. The subsequent messages in $\mathcal{G}'$ correspond to those of $\mathcal{G}$ but with Alice and Bob reversed. The only potential problem with this argument is that the order of the cheat detection messages [steps (5) and (6)] needs to be switched in order to make the protocols equivalent. However, we argued after formulating the problem as an SDP that these two steps could be exchanged without increasing or decreasing P_B^*.

Therefore, Bob's maximum probability of winning by cheating in $\mathcal{G}'$, which we call $P_B^{*\prime}$ and can be calculated using the above formulas, equals P_A^*. But $\mathcal{B}'_r = \sqrt{\mathcal{A}_r}$ and $\mathcal{H}'_r = 1 - \mathcal{H}_r$, where the primed variables are calculated from $\mathcal{G}'$. The conclusion is that

$$P_A^* = P_B^{*\prime} = \frac{\mathcal{B}_r'^2}{\mathcal{H}'_r} = \frac{\mathcal{A}_r}{1-\mathcal{H}_r}. \tag{A66}$$

In particular we have proven the main result of this appendix, which is equivalent to Theorem 1.

Theorem 15: *The quantum weak coin-flipping protocol associated to an n–coin-game $\mathcal{G}$ by Protocol 1 satisfies*

$$P_A^* = \frac{\mathcal{A}_r}{1-\mathcal{H}_r}, \quad P_B^* = \frac{\mathcal{B}_r^2}{\mathcal{H}_r}, \tag{A67}$$

and $P_A = 1 - P_B = 1 - \mathcal{H}_r$, where $\mathcal{A}, \mathcal{B}$, and $\mathcal{H}$ are defined in terms of $\mathcal{G}$ by Eqs. (1) and (2).

The above result could be made more symmetric between Alice and Bob, if we were to redefine $\mathcal{A}$ and $\mathcal{B}$ by

$$\mathcal{A}_x^{(new)} = \begin{cases} \sqrt{\mathcal{A}_x}, & |x| \text{ even}, \\ \mathcal{A}_x, & |x| \text{ odd}, \end{cases} \tag{A68}$$

$$\mathcal{B}_x^{(new)} = \begin{cases} \mathcal{B}_x, & |x| \text{ even}, \\ \sqrt{\mathcal{B}_x}, & |x| \text{ odd} \end{cases} \tag{A69}$$

which could be computed bottom-up by a sequence of linear and root-mean-squared averages as in Ref. [1]. The definitions would also make the conserved quantities such as Eqs. (A40) and (A57) have the same expression at even and odd depths. However, the old definitions make manifest the convexity that was exploited in the main sections of this paper, and therefore these definitions were selected.

APPENDIX B: BIAS OF 0.192 REVISITED

In this section we shall derive an analytical expression that corresponds to the bias of 0.192 found in Ref. [1]. Since the protocol with bias 0.192 has been superseded by the results of the present work, we shall only sketch the proof. Nonetheless, we hope that the techniques used in deriving this expression, which are rather different to the approach taken in the rest of the paper, will be of use in some future applications.

The protocols that converged to a bias of 0.192 had coin games such that $\mathcal{G}_x = a_{|x|+1}$ for binary nodes. The pattern of zeros and ones on the leaves was such that, at each depth, the tree $\mathcal{A}_x$ only had two values which we can call the high value and the low value. The high value only got updated at even depths whereas the low value only got updated at odd depths. In particular, the value of the root node could be calculated using the following sequences: set $H_n = 1$ and $L_n = 0$ and define

$$H_k = \sqrt{a_{k+1}L_{k+1}^2 + (1 - a_{k+1})H_{k+1}^2}, \tag{B1}$$

$$L_k = L_{k+1}, \tag{B2}$$

for even $k \geqslant 0$, and

$$H_k = H_{k+1}, \tag{B3}$$

$$L_k = a_{k+1}H_{k+1} + (1 - a_{k+1})L_{k+1}, \tag{B4}$$

for odd $k \geqslant 0$. The value of A_r is then given by H_0^2.

The sequence is defined so that H decreases and L increases with decreasing k. At every step the condition $1 \geqslant H_k \geqslant L_k \geqslant 0$ holds. For good choices of a_k the two sequences will approach each other and H_0 will be close to L_0.

A good sequence of parameters will also have a_k small for large k. For k small, a_k can be larger as long as $a_k(H_k - L_k)$ remains small. In such a case, we can use the expansion

$$H_k \simeq H_{k+1} - a_{k+1}\frac{H_{k+1}^2 - L_{k+1}^2}{2H_{k+1}}, \tag{B5}$$

for even k.

Furthermore, if a_k is slowly varying, we can replace it with a continuous function $a(k)$, and the above computation can be approximated by the coupled differential equations

$$\frac{dH}{dk} = \frac{a(k)}{2}\frac{H^2 - L^2}{2H}, \tag{B6}$$

$$\frac{dL}{dk} = -\frac{a(k)}{2}(H - L), \tag{B7}$$

where now H and L are treated as functions of the continuous variable $k \in [0, n]$. An extra factor of $1/2$ was picked up on the right-hand side of the above equations because H and L only get updated every other integer in the discrete sequence.

Of course, we are only concerned with the convergence point where $H \simeq L$. In the limit $n \to \infty$, and for appropriate $a(k)$, the two expressions will converge to the same point $H_0 = L_0$. To study the convergence point we can study H as a function of L, which satisfies the differential equation

$$\frac{dH}{dL} = -\frac{H + L}{2H}. \tag{B8}$$

Surprisingly, the function $a(k)$ drops out of the above expression which means it only controls the rate of convergence but not the final point of convergence (assuming it satisfies the requirements discussed above). In essence, much the same behavior can be observed by choosing different γ_n sequences for the protocol with bias $1/6$ found in the main section of this paper.

The differential equation is invariant under simultaneous rescaling of H and L, and therefore becomes separable under the change of variables $H \to H/L$. Its solutions have the form

$$\ln\left(H^2 + \frac{1}{2}LH + \frac{1}{2}L^2\right) + \frac{2}{\sqrt{7}} \arctan \frac{\sqrt{7}L}{4H + L} = \text{const}. \tag{B9}$$

The initial condition for the differential equation is $H(L = 0) = 1$, which corresponds to the initial starting point when $k \to \infty$. Applying the initial condition we obtain $const = 0$. We are interested in the point where H and L converge, that is, the value L_0 such that $H(L_0) = L_0$,

$$\ln 2L_0^2 = -\frac{2}{\sqrt{7}} \arctan \frac{\sqrt{7}}{5}. \tag{B10}$$

From this value we can obtain $\mathcal{A}_r = L_0^2$. When a_k varies slowly enough and meets our other requirements we also get $P_A = 1/2$ and therefore $P_A^* = 2L_0^2$. These conditions also guarantee that $P_B^* = P_A^*$, hence

$$P_A^* = P_B^* = \exp\left[-\frac{2}{\sqrt{7}} \arctan \frac{\sqrt{7}}{5}\right] \simeq 0.692\,181\,687, \tag{B11}$$

which corresponds to the bias $\epsilon \simeq 0.192$ from Ref. [1].

[1] C. Mochon, 45th Symposium on Foundations of Computer Science (FOCS '04) (IEEE Computer Society, 2004), pp. 2–11; quant-ph/0403193 (unpublished).

[2] R. W. Spekkens and T. Rudolph, Phys. Rev. Lett. **89**, 227901 (2002).

[3] A. Ambainis, quant-ph/0204063 (unpublished).

[4] A. Ambainis, *Proceedings on 33rd Annual ACM Symposium on Theory of Computing* (ACM, New York, 2001), pp. 134–142.

[5] H.-K. Lo and H. F. Chau, Physica D **120**, 177 (1998).

[6] L. Goldenberg, L. Vaidman, and S. Wiesner, Phys. Rev. Lett. **82**, 3356 (1999).

[7] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2002).

[8] C. Mochon, Phys. Rev. A **70**, 032312 (2004).

[9] T. Rudolph and R. W. Spekkens, Phys. Rev. A **70**, 052306 (2004).

[10] I. Kerenidis and A. Nayak, Inf. Process. Lett. **89**, 131 (2004).

[11] A. Kitaev, results presented at QIP 2003 (slides and video available from MSRI).

[12] A. Ambainis, H. Buhrman, Y. Dodis, and H. Roehrig, 19th IEEE Annual Conference on Computational Complexity (IEEE Computer Society, 2004), pp. 250–259; quant-ph/0304112 (unpublished).