Improving the security of device-independent weak coin flipping

Atul Singh Arora[1], Jamie Sikora[2], and Thomas Van Himbeeck[3,4]

[1] *California Institute of Technology, USA*
[2] *Virginia Polytechnic Institute and State University, USA*
[3] *University of Toronto, Canada*
[4] *Institute of Quantum Computing, University of Waterloo, Canada*

May 11, 2021

Abstract

Weak coin flipping is the cryptographic task where Alice and Bob remotely flip a coin but want opposite outcomes. This work studies this task in the device-independent regime where Alice and Bob neither trust each other, nor their quantum devices. The best protocol was devised ten years ago by Silman, Chailloux, Aharon, Kerenidis, Pironio, and Massar with bias $\epsilon \leq 0.33664$, where the bias is a commonly adopted security measure for coin flipping protocols. This work presents some techniques to lower the bias of device-independent weak coin flipping protocols, namely self-testing and abort-phobic compositions. By applying these techniques to the SCAKPM '11 protocol above, we are able to lower the bias to $\epsilon \approx 0.29104$. In our analysis, we examine rigidity bounds for the GHZ game for our setting and the continuity of semidefinite programs, which may be of independent interest.

Contents

1 Introduction

Coin-flipping is the two-party cryptographic primitive where two parties, henceforth called Alice and Bob, wish to flip a coin, but where, to make things interesting, they do not trust each other. This primitive was introduced by Blum [Blu83] who also introduced the first (classical) protocol. In this work, we concentrate on *weak* coin flipping (WCF) protocols where Alice and Bob desire opposite outcomes. Since then, a series of quantum protocols were introduced which kept improving the security. Mochon finally settled the question about the limits of the security in the quantum regime by proving the existence of quantum protocols with security approaching the ideal limit [Moc07]. Mochon's work was based on the notion of point games, a concept introduced by Kitaev. Since then, a sequence of works have continued the study of point games. In particular, the proof has been simplified [ACG+14] and made explicit [ARW, ARW19, ARV]. Interestingly, Miller [Mil20] used Mochon's proof to show that protocols approaching the ideal limit must have an exponentially increasing number of messages. We note that all of this work is in the *device-dependent* setting where *Alice and Bob trust their quantum devices*. In this work, we consider *revised* security definitions where a cheating player is allowed to control an honest player's quantum devices, opening up a plethora of new cheating strategies that were not considered in the previously mentioned references.

The prefix *weak* in weak coin flipping refers to the situation where Alice and Bob desire opposite outcomes of the coin. (We have occasion to discuss *strong* coin flipping protocols, where Alice or Bob could try to bias the coin towards either outcome, but it is not the focus of this work.) When designing weak coin flipping protocols, the security goals are as follows.

Correctness for honest parties:	If Alice and Bob are honest, then they share the same outcome of a protocol $c \in \{0, 1\}$, and c is generated uniformly at random by the protocol.
Soundness against cheating Bob:	If Alice is honest, then a dishonest (i.e., cheating) Bob cannot force the outcome $c = 1$.
Soundness against cheating Alice:	If Bob is honest, then a dishonest (i.e., cheating) Alice cannot force the outcome $c = 0$.

The commonly adopted goal of two-party protocol design is to assume perfect correctness and then minimize the effects of a cheating party, i.e., to make it as sound as possible. This way, if no parties cheats, then the protocol at least does what it is meant to still. With this in mind, we need a means to quantify the effects of a cheating party. It is often convenient to have a single measure to determine if one protocol is better than another. For this purpose, we use *cheating probabilities* (denoted p_B^* and p_A^*) and *bias* (denoted ϵ), defined as follows.

- p_B^*: The maximum probability with which a dishonest Bob can force an honest Alice to accept the outcome $c = 1$.
- p_A^*: The maximum probability with which a dishonest Alice can force an honest Bob to accept the outcome $c = 0$.
- ϵ: The maximum amount with which a dishonest party can bias the probability of the outcome away from uniform. Explicitly, $\epsilon = \max\{p_B^*, p_A^*\} - 1/2$.

These definitions are not complete in the sense that we have not yet specified what a cheating Alice or a cheating Bob are allowed to do, or of their capabilities. In this work, we study *information theoretic security*—Alice and Bob are only bounded by the laws of quantum mechanics. For example, they are not bounded by polynomial-time quantum computations. In addition to this, we study the security in the *device-independent* regime where we assume Alice and Bob have complete control over the quantum devices when they decide to "cheat".

When studying device-independent (DI) protocols, one should first consider whether or not secure classical protocols are known (since these are not affected by the DI assumption). It was proved that every classical WCF protocol[1] has bias $\epsilon = 1/2$, which is the worst possible value (see [Kit03, HW11]). Thus, it makes sense to study quantum WCF protocols in the DI setting, especially if one with bias $\epsilon < 1/2$ can be found. Indeed, Silman, Chailloux, Aharon, Kerenidis, Pironio, and Massar presented a protocol (see Protocol S) in [SCA+11] with $p_A^* = \cos^2(\pi/8) \approx 0.853$ and $p_B^* = 3/4$. We briefly discuss this protocol because we build on this result but defer the details. Their protocol begins with Alice possessing two *boxes*—physical devices that accept classical inputs and yield classical outputs—and Bob possessing one box which are together supposed to contain the GHZ state and measurements.[2] As the protocol proceeds, they, in addition to exchanging classical information, operate these boxes and exchange them.[3] As is, Protocol S has bias $\epsilon \approx 0.353$ but in [SCA+11], Protocol S is composed many times to lower the bias to $\epsilon \leq 0.33664$.

In this work, we provide two techniques for lowering the bias of weak coin flipping protocols and apply them to Protocol S, mentioned above.

2 Results

We state the main result of our work.

Theorem 1. *There exist device-independent weak coin flipping protocols with bias, ϵ, approaching* 0.29104.

We now discuss the key ideas that go into the proof of our main theorem, above. Protocol S was, in fact, a strong coin flipping protocol and we begin by turning it into a weak coin flipping protocol—Protocol W—in a routine manner. Again, we defer the explicit description of the protocol and informally describe the basic idea: since weak coin flipping has the notion of a "winner" (if $c = 0$ Alice wins and if $c = 1$ Bob wins) we have the party who does not win, conduct a test.

Our first technique is to add a pre-processing step to Protocol W which *self-tests* the boxes shared by Alice and Bob at the start of the protocol. Our second technique is to compose and analyse the resulting protocols in a new way,[4] which we call *abort-phobic* composition.

2.1 First technique: Self-testing

In the original Protocol S and it's WCF variant, Protocol W, a cheating party may control what measurement is performed in the boxes of the other party and how the state of the boxes is correlated to its own quantum memory. This is more general than *device-dependent* protocols, where for instance, the measurements are known to the honest player. However, we employ the concept of self-testing to stop Bob (or Alice) from applying such a strategy.[5] Intuitively, self testing is a powerful property which allows one to, just from certain input-output behaviours of given devices (satisfying minimal assumptions), conclude uniquely which quantum states and measurements constitute the devices (up to relabelling). The GHZ state which was used in Protocols S and W can be self-tested. Clearly, this property has the potential to improve their security.[6]

We define two variants of Protocol W: Protocol P, where Alice self-tests Bob before executing Protocol W, and Protocol Q, where Bob self-tests Alice instead. Skipping the details, the basic construction is almost trivial. Alice and Bob start with n triples of boxes and, for instance when Alice self-tests, Alice asks Bob to send all but one randomly selected triple and tests if the GHZ test passes for these. If so, the remaining triple is used for the actual protocol. If n is chosen large enough, then this forces a dishonest Bob to not tamper with the boxes too much, as suggested above. Indeed, this step already allows us to reduce the cheating probabilities.

Lemma 2 (Informal. See Lemma 10 for a formal statement)**.** *For Protocol P, i.e. where Alice self tests Bob, the cheating probabilities, in the limit of large n, are*

$$p_A^* = \cos^2(\pi/8) \approx 0.85355 \quad \textit{and} \quad p_B^* \approx 0.6667. \tag{1}$$

[1] also holds for strong coin flipping

[2] A GHZ state is a non-local quantum state; we review this in Section 3.

[3] any protocol described using boxes is readily converted into one where Alice and Bob communicate over an insecure quantum channel; see Section 3

[4] The composition in [SCA+11] may also be seen as "abort-phobic" but their analysis doesn't rely on the "abort" probability; their bound essentially neglects the abort event.

[5] The authors of [SCA+11] noted that for Protocol S, the optimal cheating strategy can be implemented using the "honest" devices and thus self-testing does not make the protocol more secure.

[6] In [SCA+11], it was noted that self-testing doesn't help improve the security of Protocol S. Alternatively stated, Protocol S has the curious property that its device dependent variant has the same security as it (the device dependent variant).

For comparison, recall that for Protocol S (it turns out, also for Protocol W), $p_A^* = \cos^2(\pi/8)$ and $p_B^* = 3/4$. We prove this lemma in two stages. In the *first* stage (see Section 5), we assume perfect self-testing—the self-testing step results in exactly specifying (up to a relabelling) the state and measurements governing Alice's boxes. This may be seen as taking $n \longrightarrow \infty$ in the self-testing step. It is known that for device-dependent protocols, where Alice and Bob trust their devices, the cheating probabilities can be cast as values of semidefinite programs (SDPs) [Kit03, Moc07]. Perfect self-testing allows us to, therefore, express Bob's cheating probabilities as an SDP. Its numerical evaluation yields the quoted value. Analysis for Alice's cheating probability is unchanged from Protocol W. In the *second* stage (see Section 6), we take n to be finite and show that for large n, the analysis converges to that of the first stage. This step is more technical but we outline the key challenges before proceeding to the second technique.

Self-testing in a cryptographic setting. Self-testing results can be made *robust*, i.e. in particular, if the success probability in a GHZ test is close to unity, then the states and measurements can be shown to be close to GHZ states and measurements (up to a relabelling), in say trace distance. Robust self-testing results are, however, usually stated in terms of expected success probabilities in tests. This implicitly assumes that multiple identical boxes are available.[7] In our cryptographic setting, such an assumption is unwarranted. Hence, we estimate this expected success probability, by measuring $n-1$ boxes. This estimate requires, to the best of our knowledge, a novel analysis which we discuss in Section 6.1.

Continuity argument. We argued above that under the perfect self-testing assumption, the analysis can be cast as an SDP. However, when the success probability is less than one (which will be the case in any realistic scenario), one cannot even bound the dimensions of the operators over which the optimisation problem is defined, making the analysis significantly harder. In the absence of such an analysis, the security guarantee of the ideal case are rendered hollow. Unless, for instance, a continuity argument can be provided which asserts that the value of the realistic optimization problem approaches that of the aforementioned SDP. These concerns are addressed in Section 6.5.

Remark. Both of these technical steps may find use in independent applications. In particular, the continuity of semidefinite programs section is written for general semidefinite programs for the most part.

2.2 Second technique: abort-phobic composition

It can happen, that for a given WCF protocol, $p_B^* \neq p_A^*$, in which case we say the protocol is *polarised*. As we saw earlier, it is known (e.g. [SCA+11]) that composing a polarised protocol with itself (or other protocols) can effectively reduce the bias. Our second improvement is a modified way of composing protocols, when there is a positive probability that the honest player catches the cheating player. Let us start by recalling the standard way of composing protocols.

Standard composition. For a protocol with cheating probabilities p_B^* and p_A^*, we say that it has polarity towards Alice when it satisfies $p_A^* > p_B^*$. Similarly, we say that it has polarity towards Bob when $p_B^* > p_A^*$. Given a polarized protocol $\mathcal{R}$, we may switch the roles of Alice and Bob since the definition of coin-flipping is symmetric. To make the polarity explicit, we define $\mathcal{R}_A$ to be the version of the protocol with $p_A^* > p_B^*$ and $\mathcal{R}_B$ to be the version with $p_B^* > p_A^*$. With this in mind, we can now define a simple composition.

Protocol 3 (Winner-gets-polarity composition)**.** *Alice and Bob agree on a protocol $\mathcal{R}$.*

1. *Alice and Bob perform protocol $\mathcal{R}$.*
2. *If Alice wins, she polarizes the second protocol towards herself, i.e., they now use the protocol $\mathcal{R}_A$ to determine the final outcome.*
3. *If Bob wins, he polarizes the second protocol towards himself, i.e., they now use the protocol $\mathcal{R}_B$ to determine the final outcome.*

[7] When this iid assumption is dropped, it is usually in the context of extracting randomness or key from the observed statistics, i.e. all the devices are used/measured. In our setting, we need to leave one device unused in the pre-processing step.

The standard composition above is a sensible way to balance the cheating probabilities of a protocol. For instance, if $\mathcal{R}$ has cheating probabilities p_A^* and p_B^* with $p_A^* > p_B^*$, then the composition gets to decide "who gets to be Alice" in the second run. We can easily compute Alice's cheating probability in the composition as

$$(p_A^*)^2 + (1 - p_A^*)p_B^* < p_A^* \tag{2}$$

and Bob's as

$$p_B^* p_A^* + (1 - p_B^*)p_B^* < p_A^*. \tag{3}$$

This does indeed reduce the bias since the maximum cheating probability is now smaller.

Abort-phobic composition. The "traditional" way of considering WCF protocols is to view them as only having two outcomes "Alice wins" (when $c = 0$) or "Bob wins" ($c = 1$). This is because Alice can declare herself the winner if she catches Bob cheating. Similarly, Bob can declare himself the winner if he catches Alice cheating.[8] This is completely fine when we consider "one-shot" versions of these protocols, but we lose something when we compose them. For instance, in the simple composition used in Protocol 3, Bob should not really accept to continue onto the second protocol if he catches Alice cheating in the first. That is, if he knows Alice cheated, he can declare himself the winner of the entire protocol! In other words, the cheating probabilities (2) and (3) may get reduced even further. For purposes of this discussion, suppose Bob adopts a cheating strategy which has a probability v_B of him winning ($c = 1$), a probability v_A of him losing ($c = 0$), and a probability $v_\perp$ of Alice catching him cheating. Then his cheating probability in the (abort-phobic) version of the simple composition is now

$$v_B \cdot p_A^* + v_A \cdot p_B^* + v_\perp \cdot 0. \tag{4}$$

This quantity may be a strict improvement if $v_\perp > 0$ when $v_B = p_B^*$.

The concept of abort-phobic composition is simple. Alice and Bob keep using WCF protocols and the winner (at that round) gets to choose the polarity of the subsequent protocol. However, if either party *ever aborts*, then it is game over and the cheating player loses *the entire composite protocol*.

One may think it is tricky to analyse abort-phobic compositions, but we may do this one step at time. To this end, we introduce the concept of *cheat vectors*.

Definition 4 ($\mathbb{C}_A, \mathbb{C}_B$; Alice and Bob's cheat vectors)**.** Given a protocol $\mathcal{R}$, we say that $(v_A, v_B, v_\perp)$ is a cheat vector for (dishonest) Bob if there exists a cheating strategy where:

- v_B is the probability with which Alice accepts the outcome $c = 1$,
- v_A is the probability with which Alice accepts the outcome $c = 0$,
- $v_\perp$ is the probability with which Alice aborts.

We denote the set of cheat vectors for (dishonest) Bob by $\mathbb{C}_B(\mathcal{R})$. Cheat vectors for (dishonest) Alice and $\mathbb{C}_A(\mathcal{R})$ are analogously defined keeping the notation v_A for her winning, v_B for her losing, and $v_\perp$ for Bob aborting.

In this work, we show how to capture cheat vectors as the feasible region of a semidefinite program, from which we can optimize

$$v_B \cdot p_A^* + v_A \cdot p_B^* + v_\perp \cdot 0. \tag{5}$$

For this to work, we assume we have p_A^* and p_B^* for the protocol that comes in the second round. A simplifying observation is that once we solve for the optimal cheating probabilities in the abort-phobic composition in this way, we can then fix those probabilities and compose again. In other words, we are recursively composing the abort-phobic composition, from the *bottom up*.

By using abort-phobic compositions with Protocol P (where Alice self-tests) at the bottom, and Protocol Q (where Bob self-tests) on higher layers, we obtain composite protocls which converge onto a bias of $\epsilon \approx 0.29104$ proving the main result of this work.

[8] In doing so, we implicitly assume that the protocol has perfect correctness—when both players are honest, the probability of abort is zero.

2.3 Applications

The concept of polarity extends beyond finding WCF protocols and, as such, the "winner-gets-polarity" concept allows for WCF to be used in other compositions. Indeed, we can use it to balance the cheating probabilities in *any* polarized protocol for any symmetric two-party cryptographic task for which such notions can be properly defined.

For instance, many *strong* coin-flipping protocols can be thought of as polarized. For an example, Protocol S is indeed a polarized strong coin-flipping protocol. Thus, by balancing the cheating probabilities of that protocol using our DI WCF protocol, we get the following corollary.

Corollary 5. *There exist DI strong coin-flipping protocols where no party can cheat with probability greater than* 0.33192.

To contrast, for [SCA+11], the bound on cheating probabilities was 0.336637. There are likely more examples of protocols which can be balanced in a DI way using this idea.

2.4 Paper Organisation

TODO: complete this after everything is finalised.

3 New protocols using self-testing | First Technique

We start by recalling the DI strong coin flipping protocol introduced in [SCA+11], Protocol S, and introduce its weak coin flipping variant Protocol W. We then describe the new Protocols P and Q, where Alice and Bob respectively perform the self-testing step. We also give more formal security guarantees associated with these. Their proofs constitute Sections 5 and 6.

Notation For notational clarity, we often use single calligraphic symbols $\mathcal{S}, \mathcal{W}, \mathcal{P}$ and $\mathcal{Q}$ to refer to these protocols. When we say, for instance, consider a triple of boxes $\square^A, \square^B, \square^C$, we mean that there is a tripartite quantum state and local measurements associated with these boxes. The input to the box selects the measurement setting and the output is the measurement outcome as governed by quantum theory (see Definition 28). When we speak of Alice and Bob exchanging boxes, we understand that the description of these states and measurement settings are sent over a (possibly insecure) quantum communication channel (see Definitions 29 and 31 in Section A).

We recall the GHZ test before starting our main discussion as this is at the heart of these protocols.

Definition 6. Suppose we are given a triple of boxes, $\square^A, \square^B$ and $\square^C$, which accept binary inputs $a, b, c \in \{0, 1\}$ and produces binary output $x, y, z \in \{0, 1\}$ respectively. The boxes pass the GHZ test if $a \oplus b \oplus c = xyz \oplus 1$, given the inputs satisfy $x \oplus y \oplus z = 1$.

It is known that no classical triple of boxes can pass the GHZ test with certainty but quantum boxes can.

Claim 7. Quantum boxes pass the GHZ test with certainty (even if they cannot communicate), for the state $|\psi\rangle_{ABC} = \frac{|000\rangle_{ABC}+|111\rangle_{ABC}}{\sqrt{2}}$, and measurement[9] $\frac{\sigma_x+\mathbb{I}}{2}$ for input 0 and $\frac{\sigma_y+\mathbb{I}}{2}$ for input 1 (in the notation introduced earlier, $M^A_{0|0} = |+\rangle\langle+|, M^A_{1|0} = |-\rangle\langle-|$ and so on, where $|\pm\rangle = \frac{|0\rangle\pm|1\rangle}{\sqrt{2}}$).

The proof is easier to see in the case where the outcomes are ±1; it follows from the observations that $\sigma_y \otimes \sigma_y \otimes \sigma_y |\psi\rangle = -|\psi\rangle$, $\sigma_x \otimes \sigma_x \otimes \sigma_x |\psi\rangle = |\psi\rangle$ and the anti-commutation of σ_x and σ_y matrices, i.e. $\sigma_x\sigma_y + \sigma_y\sigma_x = 0$.

In fact a stronger property holds. If a triple of boxes passes the GHZ test with certainty, it can be shown that up to a local isometry, the state and measurements are as in Claim 7 above. While this is, manifestly, a highly idealised setting and we later, in Section 6, see how it works in practice.

Lemma 8 (TODO: cite)**.** *Let $a, b, c, x, y, z \in \{0, 1\}$. Consider a trio of quantum boxes, specified by projectors $\{M^A_{a|x}, M^B_{b|y}, M^C_{c|z}\}$ acting on finite dimensional Hilbert spaces $\mathcal{H}^A, \mathcal{H}^B$ and $\mathcal{H}^C$, and $|\psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C =: \mathcal{H}^{ABC}$. If the trio pass the GHZ test with certainty, then there exists a local isometry*

$$\Phi = \Phi^A \otimes \Phi^B \otimes \Phi^C : \mathcal{H}^{ABC} \to \mathcal{H}^{ABC} \otimes \mathbb{C}^{2\times3}$$

[9] we added the identity so that the eigenvalues associated become 0, 1 instead of −1, 1.

such that

$$\Phi\left(|\psi\rangle\right) = |\chi\rangle \otimes |\text{junk}\rangle\,,$$
$$\Phi\left(M^D_{d|t}\,|\psi\rangle\right) = \Pi^D_{d|t}\,|\text{GHZ}\rangle \otimes |\text{junk}\rangle \quad \forall D \in \{A,B,C\},\ \textit{and}\ d,t \in \{0,1\}$$

where $|\text{GHZ}\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}} \in \mathbb{C}^{2\times 3}$, $|\text{junk}\rangle \in \mathcal{H}^{ABC}$ *is some arbitrary state and* $\{\Pi^A_{a|x}, \Pi^B_{b|y}, \Pi^C_{c|z}\}$ *are projectors corresponding to* σ_x *on the first, second and third qubit of* $|\text{GHZ}\rangle$ *respectively, for* $x = 0$ *and corresponding to* σ_y *for* $x = 1$, *as in Claim 7.*

3.1 Original protocols

Protocol S is defined as follows.

Protocol S A DI-SCF protocol with $p^*_A = \cos^2 \pi/8$ and $p^*_B = 3/4$ ([SCA+11])

Alice has one box and Bob has two boxes. Each box takes one binary input and gives one binary output and are designed to play the optimal GHZ game strategy. (Who creates and distributes the boxes is not important in the DI setting.)

1. Alice chooses a uniformly random input to her box $x \in \{0,1\}$ and obtains the outcome a. She chooses another uniformly random bit $r \in \{0,1\}$ and computes $s = a \oplus (x \cdot r)$. She sends s to Bob.

2. Bob chooses a uniformly random bit $g \in \{0,1\}$ and sends it to Alice. (We may think of g as Bob's "guess" for the value of x.)

3. Alice sends x to Bob. They both compute the output $c = x \oplus g$. This is the outcome of the protocol assuming neither Alice nor Bob abort.

4. Bob tests Alice

   Test 1: Alive sends a to Bob. Bob sees if $s = a$ or $s = a \oplus x$. If this is not the case, he aborts.

   Test 2: Bob chooses $y, z \in_R \{0,1\}$ uniformly at random such that $x \oplus y \oplus z = 1$ and then performs a GHZ using x, y, z as the inputs and a, b, c as the output from the three boxes. He aborts if this test fails.

5. If Bob does not abort, they both accept the value of c as the outcome of the protocol.

We now discuss the correctness and soundness of Protocol S. From Claim 7, it is clear that when both players follow the protocol using GHZ boxes (Definition 6), Bob never aborts and they win with equal probabilities. As for the security, [SCA+11] proved the following.

Lemma 9 (Security of SCF)**.** *[SCA+11] Let* $\mathcal{S}$ *denote the protocol corresponding to Protocol S. Then, the success probability of cheating Bob,*[10] $p^*_B(\mathcal{S}) \leq \frac{3}{4}$ *and that of cheating Alice,* $p^*_A(\mathcal{S}) \leq \cos^2(\pi/8)$.

Further, both bounds are saturated by a quantum strategy which uses a GHZ state and the honest player measures along the σ_x/σ_y *basis corresponding to input* $0/1$ *into the box. Cheating Alice measures along* $\sigma_{\hat{n}}$ *for* $\hat{n} = \frac{1}{\sqrt{2}}(\hat{x}+\hat{y})$ *while cheating Bob measures his first box along* σ_x *and second along* σ_y.

Note that both players can cheat maximally assuming they share a GHZ state and the honest player measures along the associated basis. This is why it was asserted that even though the cheating player could potentially tamper with the boxes before handing them to the honest player, exploiting this freedom does not offer any advantage to the cheating player.

Clearly, if we take Protocol S as is and treat it like a weak coin flipping protocol, this conclusion would continue to hold. As motivated in the introduction, we consider a minor, yet crucial, modification to Protocol S. Observe that in Protocol S only Bob performs the test round, while in weak coin flipping there is a notion of Alice winning and Bob winning which may be leveraged. More precisely, if $x \oplus g = 0$, i.e. the outcome corresponding to "Alice wins",

[10] For Strong Coin Flipping, P^*_B is maxprob(Bob can force Alice to output 1),prob(Bob can force Alice to output 0); P^*_A is analogously defined.

we can imagine that Bob continues to perform the test to ensure (at least to some extend) that Alice did not cheat. However, if $x \oplus g = 1$, i.e. the outcome corresponding to "Bob wins", we can require Alice to now complete the GHZ test to ensure that Bob did not cheat. Since we analyse this protocol in detail, we state it as Protocol W, somewhat redundantly below. We have emphasised the changes compared to Protocol S in italics.

Protocol W Weak Coin Flipping version of Protocol S (Italics indicate the differences with Protocol S)

Alice has one box and Bob has two boxes. Each box takes one binary input and gives one binary output and are designed to play the optimal GHZ game strategy. (Who creates and distributes the boxes is not important in the DI setting.)

1. Alice chooses a uniformly random input to her box $x \in \{0,1\}$ and obtains the outcome a. She chooses another uniformly random bit $r \in \{0,1\}$ and computes $s = a \oplus (x \cdot r)$. She sends s to Bob.
2. Bob chooses a uniformly random bit $g \in \{0,1\}$ and sends it to Alice. (We may think of g as Bob's "guess" for the value of x.)
3. Alice sends x to Bob. They both compute the output $c = x \oplus g$. This is the outcome of the protocol assuming neither Alice nor Bob aborts.
4. Test rounds:

   (a) *If $x \oplus g = 0$,* Bob tests Alice

   Test 1: Alice sends a to Bob. Bob sees if $s = a$ or $s = a \oplus x$. If this is not the case, he aborts.

   Test 2: Bob chooses $y, z \in_R \{0,1\}$ uniformly at random such that $x \oplus y \oplus z = 1$ and then performs a GHZ using x, y, z as the inputs and a, b, c as the output from the three boxes. He aborts if this test fails.

   (b) *If $x \oplus g = 1$, Alice tests Bob*

   Test 3: Alice chooses $y, z \in_R \{0,1\}$ uniformly at random such that $x \oplus y \oplus z = 1$ and sends them to Bob. Bob inputs y, z into his boxes, obtains and sends b, c to Alice. Alice tests if x, y, z as inputs and a, b, c as outputs, satisfy the GHZ test. She aborts if this test fails.

5. If Alice and Bob do not abort, they both accept the value of c as the outcome of the protocol.

While it is not surprising that $p_A^*(\mathcal{W}) = p_A^*(\mathcal{P}) = \cos^2(\pi/8)$, it turns out that $p_B^*(\mathcal{W}) = p_B^*(\mathcal{P}) = 3/4$, despite the additional test that Alice performs i.e. P_B^* for Protocol W is not lowered. Yet, this is not quite a setback—one can show that the best cheating strategy now deviates from the GHZ state and measurements for the honest player, suggesting that a cheating player *does* benefit from tampering with the boxes. Consequently, adding a self-testing step before initiating Protocol W, may potentially improve its security and as we shall see in the following subsections, it indeed does.

A remark about the limitation of self-testing in this setting. We note that no self-testing scheme can be concocted which simultaneously self-tests Alice and Bob's boxes. More precisely, no such procedure can ensure that Alice and Bob share a GHZ state (Alice one part, Bob the other two, for instance) because this would mean perfect (or near perfect) SCF is possible which, recall, is forbidden even in the device dependent case.[11]

3.2 Alice self-tests | Protocol $\mathcal{P}$

We begin with explicitly stating Protocol P—where Alice self-tests her boxes before initiating Protocol W. In the honest implementation, the triple of boxes used in Protocol P are characterised by the GHZ setup (see Claim 7).

To state the associated security condition, we need the definition of cheat vectors from the introduction (see Definition 4).

Lemma 10. *Let $\mathcal{P}$ denote the protocol corresponding to Protocol P. Then Alice's cheating probability $p_A^*(\mathcal{P}) \leq \cos^2(\pi/8) \approx 0.852$. Further, let $c_0, c_1, c_\perp \in \mathbb{R}$, and $\mathbb{C}_B(\mathcal{P})$ be the set of cheat vectors for Bob. Then, as $N \to \infty$, the solution to the*

[11] More precisely, Kitaev [Kit03] showed that for any SCF protocol, $\epsilon \geq \frac{1}{\sqrt{2}} - \frac{1}{2}$.

Protocol P Alice self-tests

Alice starts with n boxes, indexed from 1_1 to 1_n. Bob starts with $2n$ boxes, the first half indexed by 2_1 to 2_n and the last half indexed by 3_1 to 3_n. The triple of boxes $(1_i, 2_i, 3_i)$ is meant to play the optimal GHZ game strategy.

1. Alice selects a uniformly random index $i \in \{1, \ldots, n\}$ and asks Bob to send her all the boxes *except* those indexed by 2_i and 3_i.
2. Alice performs $n-1$ GHZ tests using the $n-1$ triples of boxes she has, making sure there is no communication between any of them.[12]
3. Alice aborts if *any* of the GHZ tests fail. Otherwise, she announces to Bob that they can use the remaining boxes for Protocol W.

---

optimisation problem $\max(c_0\alpha + c_1\beta + c_\perp\gamma)$ *over* $\mathbb{C}_B(\mathcal{Q})$ *approaches that of an SDP. In particular, i.e. for* $c_0 = c_\perp = 0$ *and* $c_1 = 1$, $p_B^*(\mathcal{P}) \approx 0.667...$ *(in the limit).*

We defer the proof to Section 5.1. As remarked in the introduction, the value for $p_B^*(\mathcal{P})$ is lower than $p_B^*(\mathcal{W})$ and was obtained by numerically solving the corresponding SDP while the analysis for cheating Alice is the same as that of the original protocol. The fact that optimising linear functions in Bob's cheat vectors is an SDP becomes useful in Section 4 when we compose these protocols.

3.3 Bob self-tests | Protocol $\mathcal{Q}$

We analogously define Protocol Q—where Bob self-tests his boxes before initiating Protocol W.

Protocol Q Bob self-tests

Alice starts with n boxes, indexed from 1_1 to 1_n. Bob starts with $2n$ boxes, the first half indexed by 2_1 to 2_n and the last half indexed by 3_1 to 3_n. The triple of boxes $(1_i, 2_i, 3_i)$ is meant to play the optimal GHZ game strategy.

1. Bob selects a uniformly random index $i \in \{1, \ldots, n\}$ and asks Alice to send him all the boxes *except* those indexed by 1_i.
2. Bob performs $n-1$ GHZ tests using the $n-1$ triples of boxes he has, making sure there is no communication between any of them.
3. Bob aborts if *any* of the GHZ tests fail. Otherwise, he announces to Alice that they can use the remaining boxes for Protocol W.

Consider Protocol W and Protocol S. Suppose Bob is honest while Alice is malicious, and that at step 3, she sends an x s.t. $x \oplus g = 0$. Under these conditions, observe that Bob's actions are identical in both Protocol W and Protocol S. Since it is already known from Lemma 9 that Alice doesn't gain anything from tampering with Bob's boxes, the same conclusion holds for Protocol W. Thus, we do not expect any improvement in Bob's security, viz. $p_A^*(\mathcal{Q}) = p_A^*(\mathcal{W})$ given that Protocol Q only ensures Alice doesn't tamper with Bob's boxes. It is also immediate that $p_B^*(\mathcal{Q}) = p_B^*(\mathcal{W})$. This means that we do not see any advantage of self-testing at this stage but, analogously to Protocol P, optimisation of linear functions of Alice's cheat vectors now becomes an SDP and we reap the benefits of this simplification in the next section.

Lemma 11. *Let* $\mathcal{Q}$ *denote the protocol corresponding to Protocol Q. Then, Alice's cheating probability,* $p_A^*(\mathcal{Q}) \leq 3/4$ *and Bob's cheating probability,* $p_B^*(\mathcal{Q}) \leq \cos^2(\pi/8)$ *(which are the same as those in Lemma 9). Further, let* $c_0, c_1, c_\perp \in \mathbb{R}$*, and* $\mathbb{C}_A(\mathcal{Q})$ *be the set of cheat vectors for Alice. Then, as* $N \to \infty$*, the solution to the optimisation problem* $\max(c_0\alpha+c_1\beta+c_\perp\gamma)$ *over* $(\alpha, \beta, \gamma) \in \mathbb{C}_A(\mathcal{Q})$ *approaches that of an SDP.*

The proof is again deferred; see Section 5.2.

4 Compositions | Second Technique

Central to the discussion in this section, will be the notion of *polarity* introduced in Section 2.2 and our results will apply to polarised protocols. Note that $\mathcal{W}, \mathcal{P}$, and $\mathcal{Q}$ are all polarised. We begin by recalling that in Section 2.2, again, we had introduced a "standard composition"—the simplest implementation of the "winner gets polarity" idea. Here, we restate this composition with more precision and introduce the notation we use for the more involved cases.

4.1 Composition

Definition 12 ($C(\cdot,\cdot)$ and $C(\cdot)$)**.** Given two polarised WCF protocols, $\mathcal{X}$ and $\mathcal{Y}$, let $\mathcal{X}_A, \mathcal{X}_B$ and $\mathcal{Y}_A, \mathcal{Y}_B$ be their polarisations (see Section 2.2). Define $C(\mathcal{X}, \mathcal{Y})$ as follows:

1. Alice and Bob execute $\mathcal{X}_A$ and obtain outcome $X \in \{A, B, \perp\}$.
2. (a) If $X = A$, execute $\mathcal{Y}_A$ and obtain outcome $Y \in \{A, B, \perp\}$, else
   (b) if $X = B$, execute $\mathcal{Y}_B$ and obtain outcome $Y \in \{A, B, \perp\}$, and finally
   (c) if $X =\perp$, set $Y =\perp$.

   Output Y.

Let $\mathcal{Z}^{i+1} := C(\mathcal{X}, \mathcal{Z}^i)$ for $i \geq 1$, and $\mathcal{Z}^1 := \mathcal{X}$. Then, formally, define $C(\mathcal{X}) := \lim_{i\to\infty} \mathcal{Z}^i$.[13]

The study of such composed protocols is simplified by assuming that in an honest run, neither player outputs $\perp$ (abort), i.e. they either output A or B. We take a moment to explain this.

Consider any protocol $\mathcal{R}$ where, when both players are honest, the probability of abort is zero. The protocols we have described so far, satisfy this property, so long as we assume that honest players can prepare perfect GHZ boxes. Such protocols are readily converted into protocols where an honest player never outputs abort.

For instance, suppose that in the execution of the aforementioned protocol $\mathcal{R}$ (with no-honest-abort), Alice behaves honestly but Bob is malicious. Suppose after interacting with Bob, Alice reaches the conclusion that she must abort. Since she knows that if Bob was honest, the outcome abort could not have arisen, she concludes that Bob is cheating and declares herself the winner, i.e. she outputs A. Similarly, when Bob is honest and after the interaction, reaches the outcome abort, he knows Alice cheated and can therefore declare himself the winner, i.e. output B.

Whenever we modify a protocol so that an honest Alice (Bob) replaces the outcome abort with Alice (Bob) winning, we say Alice (Bob) is *lenient.* This is motivated by the fact that when we compose protocols, if Alice can conclude that Bob is cheating, and she still outputs A instead of aborting, she is giving Bob further opportunity to cheat—she is being lenient.

Definition 13 ($\mathcal{R}$ with lenient players)**.** Suppose $\mathcal{R}$ is a WCF protocol such that when both players are honest, the probability of outcome abort, $\perp$, is zero. Then by "*$\mathcal{R}$ with lenient Alice (Bob)*", which we denote by $\mathcal{R}^{L\perp}$ ($\mathcal{R}^{\perp L}$), we mean that Alice (Bob) follows $\mathcal{R}$ except that the outcome $\perp$ replaced with A (B). Finally, by "*lenient $\mathcal{R}$*", which we denote by $\mathcal{R}^{LL}$, we mean $\mathcal{R}$ with lenient Alice and Bob.

For clarity and conciseness, we define C^{LL} to be compositions with lenient variants of the given protocols. We work out some examples of such protocols and analyse their security in the following section. These can be improved by considering $C^{L\perp}$ and $C^{\perp L}$—compositions where only one player is lenient. We discuss those afterwards.

Definition 14 (C^{LL}, $C^{\perp L}$ and $C^{L\perp}$)**.** Suppose a WCF protocol $\mathcal{X}$ can be transformed into its *lenient* variants (see Definition 13). Then define

$$\begin{aligned} C^{LL}(\mathcal{X}, \mathcal{Y}) &:= C(\mathcal{X}^{LL}, \mathcal{Y}), \\ C^{\perp L}(\mathcal{X}, \mathcal{Y}) &:= C(\mathcal{X}^{\perp L}, \mathcal{Y}), \quad \text{and} \\ C^{L\perp}(\mathcal{X}, \mathcal{Y}) &:= C(\mathcal{X}^{L\perp}, \mathcal{Y}). \end{aligned}$$

In words, C^{LL} is referred to as a *standard* composition, while $C^{\perp L}$ and $C^{L\perp}$ are referred to as *abort-phobic* compositions.

[13] This is just to facilitate notation. This way the cheating probabilities p_A^* and p_B^* converge and numerically this only takes a few compositions to reach in our case.

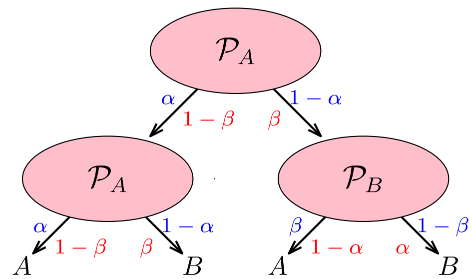

Figure 1: Standard composition of Coin flipping protocols. Subprotocols only have two outcomes depending on the coin flip. Labels indicate probabilities of outcomes for cheating Alice (blue) and cheating Bob (red)

4.2 Standard Composition | C^{LL}

We begin with the simplest case, standard composition, C^{LL}. Let us take an example. Consider protocol $\mathcal{P}$ (see Protocol P) and recall (see Lemma 10)

$$p_A^*(\mathcal{P}_A) =: \alpha \approx 0.852\ldots,$$
$$p_B^*(\mathcal{P}_A) =: \beta \approx 0.667\ldots.$$

Note that therefore $p_A^*(\mathcal{P}_B) = \beta$ and $p_B^*(\mathcal{P}_B) = \alpha$. Further, let $\mathcal{P}' := C^{LL}(\mathcal{P}, \mathcal{P})$, i.e. Alice and Bob (who are both lenient) first execute $\mathcal{P}_A$ and if the outcome is A, they execute $\mathcal{P}_A$, while if the outcome is B, they execute $\mathcal{P}_B$. This is illustrated in Figure **??** where note that the event abort doesn't appear due to the leniency assumption. This allows us to evaluate the cheating probabilities for the resulting protocol as

$$p_A^*(\mathcal{P}') = \alpha\alpha + (1-\alpha)\beta =: \alpha^{(1)}, \quad \text{and} \tag{6}$$
$$p_B^*(\mathcal{P}') = \beta\alpha + (1-\beta)\beta =: \beta^{(1)}.$$

To see this, consider Equation (6). Alice knows that if she wins the first round, her probability of winning is $\alpha > \beta$. She knows that in the first round, she can force the outcome A with probability α. From leniency, she knows that Bob would output B with the remaining probability.[14]

A side remark: one consequence of this simplified analysis is that[15] $\alpha^{(1)} > \beta^{(1)}$. Intuitively, it means that plority is preserved by the composition procedure. Proceeding similarly, i.e. defining $\mathcal{P}'' := C^{LL}(\mathcal{P}, \mathcal{P}')$, and repeating $k+1$ times overall, one obtains[16]

$$\alpha^{(k+1)} = \alpha\alpha^{(k)} + (1-\alpha)\beta^{(k)}$$
$$\beta^{(k+1)} = \beta\alpha^{(k)} + (1-\beta)\beta^{(k)}.$$

In the limit of $k \longrightarrow \infty$, one obtains

$$p_A^*(C^{LL}(\mathcal{P})) = p_B^*(C^{LL}(\mathcal{P})) = \lim_{k\to\infty} \alpha^{(k)} = \lim_{k\to\infty} \beta^{(k)} \approx 0.8199\ldots.$$

Proceeding similarly, one obtains for $X \in \{A, B\}$ and $\mathcal{X} \in \{\mathcal{I}, \mathcal{Q}\}$,

$$p_X^*(C^{LL}(\mathcal{X})) \approx 0.836\ldots$$

We thus have the following.

Theorem 15. *Let $X \in \{A, B\}$ and $\mathcal{X} \in \{\mathcal{I}, \mathcal{Q}\}$. Then $p_X^*(C^{LL}(\mathcal{P})) \approx 0.8199\ldots$ and $p_X^*(C^{LL}(\mathcal{X})) \approx 0.836\ldots$.*

[14] Without leniency, this probability could have been shared between the outcomes $\perp$ (abort) and B. Consequently, only upper bounds could be obtained on $p_A^*(\mathcal{P}')$ and $p_B^*(\mathcal{P}')$ using only α and β as security guarantees for $\mathcal{P}_A$. Upper bounds, however, would not be enough to determine the polarity of $\mathcal{P}'$ and an stymie unambiguous repetition of the composition procedure (at least as it is defined). One could nevertheless compose by hoping that the upper bounds can be used to accurately represent the polarity. This would still yield a protocol and the same calculation would yield correct bounds but the composition itself might be sub-optimal.

[15] $\alpha^{(1)} - \beta^{(1)} = (\alpha-\beta)\alpha - (\alpha-\beta)\beta = (\alpha-\beta)^2 > 0$

[16] Again, note that $\alpha^{(k+1)} - \beta^{(k+1)} = (\alpha^{(k)} - \beta^{(k)})(\alpha-\beta) > 0$.

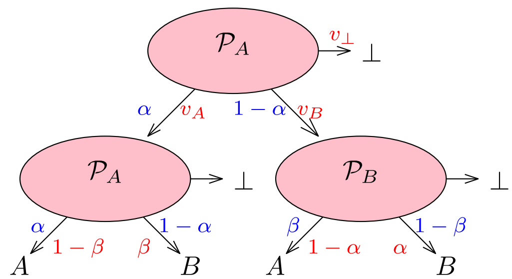

Figure 2: Abort phobic compositing for Coin flipping protocols. Subprotocols have three possible outcomes including an abort symbol. Aborting in any subprotocol directly leads to aborting the whole protocol. Labels indicate probabilities of outcomes for cheating Alice (blue) and cheating Bob (red). In the security analysis of cheating Bob, we need to optimise over the cheat vectors $(v_A, v_B, v_\perp) \in \mathbb{C}_B$.

4.3 Abort Phobic Compositions | $C^{L\perp}, C^{\perp L}$

We now look at the case of abort phobic compositions, $C^{L\perp}$ and $C^{\perp L}$. We work through essentially the same example as above and see what changes in this setting. Consider protocol $\mathcal{P}$ (see ...) and recall that as before

$$p_A^*(\mathcal{P}_A) =: \alpha \approx 0.852\ldots,$$
$$p_B^*(\mathcal{P}_A) =: \beta \approx 0.667\ldots.$$

In addition, we know from Lemma 10 that cheat vectors for Bob, $(\alpha, \beta, \gamma) \in \mathbb{C}_B(\mathcal{P}_A)$ admit a nice characterisation courtesy of the self testing step. Let $\mathcal{P}' := C^{\perp L}(\mathcal{P}, \mathcal{P})$, i.e. Alice and Bob execute $\mathcal{P}_A$ and if the outcome is A, they execute $\mathcal{P}_A$ while if the outcome is B, they execute $\mathcal{P}_B$. Bob is assumed to be lenient so an honest Bob never outputs abort, $\perp$. However, an honest Alice can output abort, $\perp$ so we keep that output in the illustration, Lemma 10. Our goal is to find $p_A^*(\mathcal{P}')$ and $p_B^*(\mathcal{P}')$. The former is the same as before because Bob is lenient:

$$p_A^*(\mathcal{P}') = \alpha \cdot \alpha + (1-\alpha) \cdot \beta.$$

Clearly, $p_B^*(\mathcal{P}') \leq \beta\alpha + (1-\beta)\beta$ but this bound may not be tight because $(1-\beta)$ is the combined probability of Alice aborting and Alice outputting A. However, we can use cheat vectors to obtain

$$p_B^*(\mathcal{P}') = \max_{(v_A, v_B, v_\perp) \in \mathbb{C}_B} v_B\alpha + v_A\beta$$

which is an SDP one can solve numerically. Unlike the previous case, the polarity of the resulting protocol, $\mathcal{P}'$, might have flipped (compared to the polarity of $\mathcal{P}$).

Repeating this procedure, one can consider $\mathcal{P}'' := C^{\perp L}(\mathcal{P}, \mathcal{P}')$ and obtain $p_A^*(\mathcal{P}'')$ directly as illustrated above and numerically solve for $p_B^*(\mathcal{P}'')$ using the cheat vectors. Numerically, we found that ten-fifteen repetitions caused the cheating probabilities to converge to approximately 0.81459. We saw that the abort probabilities associated with $\mathcal{P}$ were quite small and therefore one could hope that $\mathcal{Q}$ fares better. Proceed analogously for protocol and considering $\mathcal{Q}' := C^{L\perp}(\mathcal{Q}, \mathcal{Q})$, $\mathcal{Q}'' := C^{L\perp}(\mathcal{Q}, \mathcal{Q}')$, etc., the cheating probabilities converge to approximately 0.822655.

Theorem 16. *Let $X \in \{A, B\}$. Then*

$$p_X^*(C^{\perp L}(\mathcal{P})) \approx 0.81459$$

and

$$p_X^*(C^{L\perp}(\mathcal{Q})) \approx 0.822655$$

where the latter holds assuming Conjecture ?? is true.

While by itself $\mathcal{Q}$ doesn't seem to help, one can suppress the bias further, by noting that at the very last step, only the cheating probabilities $p_A^*(\mathcal{Q})$ and $p_B^*(\mathcal{Q})$ played a role (i.e. the fact that the cheating vectors $\mathbb{C}_A$ for $\mathcal{Q}$ had an SDP characterisation was not used). Further, we know that $p_A^*(\mathcal{P}) = p_A^*(\mathcal{Q})$ but $p_B^*(\mathcal{P}) < p_B^*(\mathcal{Q})$, i.e. using $\mathcal{P}$ at the very last step will result in a strictly better protocol.

Theorem 17. *Let $X \in \{A, B\}$,*

$$\mathcal{Z}^1 := C^{L\perp}(\mathcal{Q}, \mathcal{P}), \quad \text{and}$$
$$\mathcal{Z}^{i+1} := C^{L\perp}(\mathcal{Q}, \mathcal{Z}^i) \quad i > 1.$$

Then

$$\lim_{i\to\infty} p_X^*(\mathcal{Z}^i) \approx 0.791044\dots$$

assuming Conjecture ?? holds.

5 Security Proof | Asymptotic limit

In this section, we prove the security under the following assumption:

Assumption 18. *In protocol $\mathcal{P}$ ($\mathcal{Q}$), Alice (Bob) does not perform the box verification step and instead it is assumed that her box is (his boxes are) taken from a trio of boxes which win the GHZ game with certainty.*

Later, we drop the assumption and use the box verification step (see ..) to estimate the probability of winning the GHZ game. When the winning probability is exactly one, the states and measurements are the same as the GHZ state and σ_x, σ_y measurements, up to local isometries and this allows us to use semi definite programming. **(Atul:** I removed the lemma from here**)**

INTERNAL; (TODO: remove): Isometries can only increase dimensions (they must be injective; that is to ensure they preserve inner products of vectors). Therefore the isometry can't get rid of the $|\text{junk}\rangle$ part.

5.1 SDP when Alice self-tests

Asymptotic proof of Lemma 10. We prove Lemma 10 under Assumption 18. We begin by making two observations.

First, note that in the protocol, if Alice applies an isometry on her box *after* she has inputted x, obtained the outcome a (and has noted it somewhere), the security of the resulting protocol is unchanged because the rest of the protocol only depends on x and a, and Alice's isometry only amounts to relabelling of the post measurement state. This freedom allows us to simplify the analysis.

Second, in the analysis, we cannot model Alice's random choice, say for x, as a mixed state because Bob can always hold a purification and thus know x. Therefore, we model the randomness using pure states and measure them in the end.

Notation: Other than PQR, all other registers store qubits.

We proceed step by step.

1. We can model (justified below) Alice's act of inputting a random x and obtaining an outcome a from her box through the state
$$|\Psi_0\rangle := \frac{1}{2}\sum_{x,a\in\{0,1\}} |xa\rangle_{XA}\, |\Phi(x,a)\rangle_{IJ} \tag{7}$$
where X represents the random input and A the output. Here, $|\Phi(x,a)\rangle_{IJ}$ are Bell states (see Equation (9)) and the registers IJ are held by Bob. Alice's act of choosing r at random, computing $s = a \oplus x.r$ is modelled as
$$|\Psi_1\rangle := \frac{1}{2\sqrt{2}}\sum_{x,a,r\in\{0,1\}} |xa\rangle_{XA}\, |\Phi(x,a)\rangle_{IJ}\, |r\rangle_R\, |a\oplus x.r\rangle_S\,. \tag{8}$$
Finally, Alice's act of sending s is modelled as Alice starting with the state
$$\mathrm{tr}_{IJS}\left[|\Psi_1\rangle\langle\Psi_1|\right] \in XAR.$$
(Tom: Can we call this state ρ_1 ?**)**

   Justification for starting with $|\Psi_0\rangle$.
   To see why we start with the state $|\Psi_0\rangle$, model Alice's choice of x as $|+\rangle_X$, suppose her measurement result is stored in $|0\rangle_A$, the state of the boxes before measurement is $|\psi\rangle_{PQR}$ and Alice holds P, i.e.
$$\left|\Psi_0'\right\rangle := |+\rangle_X\, |0\rangle_A\, |\psi\rangle_{PQR}\,.$$

Let $\{M^P_{a|x}\}$ be the measurement operators corresponding to Alice's box. The measurement process is unitarily modelled as

$$\left|\Psi_1'\right\rangle := U_{\text{measure}}\left|\Psi_0'\right\rangle = \frac{1}{\sqrt{2}}\sum_{x,a\in\{0,1\}}|x\rangle_X\,|a\rangle_A\,M^P_{a|x}\,|\psi\rangle_{PQR}$$

where

$$U_{\text{measure}} = \sum_{x\in\{0,1\}}|x\rangle\langle x|_X\otimes\left[\mathbb{I}_A\otimes M^P_{0|x}+X_X\otimes M^P_{1|x}\right]\otimes\mathbb{I}_{QR}.$$

Now we harness the freedom of applying an isometry to the post measured state (as observed above). We choose the local isometry in Lemma 8. Without loss of generality, we can assume that Bob had already applied his part of the isometry before sending the boxes (because he can always reverse it when it is his turn). We thus have,

$$\begin{aligned}\left|\Psi_2'\right\rangle := \Phi_{PQR}\left|\Psi_1'\right\rangle &= \frac{1}{\sqrt{2}}\sum_{x,a\in\{0,1\}}|x\rangle_X\,|a\rangle_A\,\Pi^H_{x|a}\,|\mathrm{GHZ}\rangle_{HIJ}\otimes|\mathrm{junk}\rangle_{PQR}\\ &= \frac{1}{2}\sum_{x,a\in\{0,1\}}|x\rangle_X\,|a\rangle_A\,U^H(x,a)\,|0\rangle_H\,|\Phi(x,a)\rangle_{IJ}\otimes|\mathrm{junk}\rangle_{PQR}\end{aligned}$$

where

$$|\Phi(x,a)\rangle_{IJ} = \frac{|00\rangle+(-1)^a(i)^x\,|11\rangle}{\sqrt{2}} \tag{9}$$

and $U^H(x,a)\,|0\rangle_H$ is $\frac{|0\rangle+(-1)^a(i)^x|1\rangle}{\sqrt{2}}$. Since the state of register H is completely determined by registers X and A, we can drop it from the analysis without loss of generality. Finally, since $|\mathrm{junk}\rangle_{PQR}$ is completely tensored out, we can drop it too without affecting the security. Formally, we can assume that Alice gives Bob the register P at this point.

2. Bob sending g is modelled by introducing $\rho_2\in XARG$ satisfying $\mathrm{tr}_{IJS}\left[|\Psi_1\rangle\langle\Psi_1|\right]=\mathrm{tr}_G(\rho_2)$.

3. At this point, either $x\oplus g$ is zero, in which case Alice's output is fixed or $x\oplus g$ is one, and in that case Bob will already know x because he knows g (he sent it) and Alice will proceed to testing Bob. Formally, therefore, we needn't do anything at this step.

4. Assuming $x\oplus g=1$, Alice sends y,z to Bob such that $x\oplus y\oplus z=1$. However, since Bob already knows x, he can deduce z from y. We thus only need to model Alice sending y and Bob responding with $d=b\oplus c$ (because Alice will only use $b\oplus c$ to test the GHZ game, so it suffices for Bob to send d). This amounts to introducing $\rho_3\in XARGYD$ satisfying $\rho_2\otimes\frac{\mathbb{I}_Y}{2}=\mathrm{tr}_D(\rho_3)$.

5. Since we postponed the measurements to the end, we add this last step. Alice now measures ρ_3 to determine $x\oplus g$ and if it is one, whether the GHZ test passed. Let

$$\Pi_i := \sum_{x,y\in\{0,1\}:x\oplus g=i}|xg\rangle\langle xg|_{XG}\otimes\mathbb{I}_{ARYD}, \tag{10}$$

$$\Pi^{\mathrm{GHZ}} := \sum_{\substack{x,y\in\{0,1\},\\ a,d\in\{0,1\}:a\oplus d\oplus 1=xy\cdot(1\oplus x\oplus y)}}|xyad\rangle\langle xyad|_{XYAD}\otimes\mathbb{I}_{RG}. \tag{11}$$

Then, we can write the cheat vector for Alice, i.e. the tuple of probabilities that Alice outputs 0, 1 and abort (see Definition 4), as

$$(\alpha,\beta,\gamma) = (\mathrm{tr}(\Pi_0\rho_3),\mathrm{tr}(\Pi_1\Pi^{\mathrm{GHZ}}\rho_3),\mathrm{tr}(\Pi_1\bar{\Pi}^{\mathrm{GHZ}}\rho_3))$$

where $\bar{\Pi}:=\mathbb{I}-\Pi$.

To summarise, the final SDP is as follows: let $|\Psi_1\rangle\in XAIJRS$ be as given in Equation (8), $\rho_2\in XARG$ and $\rho_3\in XARGYD$

$$\max\quad \mathrm{tr}([c_0\Pi_0+\Pi_1(c_1\Pi^{\mathrm{GHZ}}+c_\perp\bar{\Pi}^{\mathrm{GHZ}})]\rho_3)$$

subject to

$$\mathrm{tr}_{IJS}\left[|\Psi_1\rangle\langle\Psi_1|\right] = \mathrm{tr}_G(\rho_2)$$
$$\rho_2 \otimes \frac{\mathbb{I}_Y}{2} = \mathrm{tr}_D(\rho_3)$$

where the projectors are defined in Equation (11). □

5.2 SDP when Bob self-tests

(Tom: What is the argument to say that we do not have to consider the test by Alice when analysing cheating Alice from the point of view of Bob ?**)**

Proof of Lemma 11. Denote by $\mathcal{I}$ the protocol corresponding to Protocol **??**.

It is evident that $p_B^*(\mathcal{Q}) \le p_B^*(\mathcal{I})$ because compared to $\mathcal{I}$, in $\mathcal{Q}$ Alice performs an extra test. However, it is not hard to see that the inequality is saturated, i.e. $p_B^*(\mathcal{Q}) = p_B^*(\mathcal{I})$. Consider ... (TODO: recall/re-construct the cheating strategy for Bob that lets him win with the same 3/4 probability).

From Lemma 9, it is also clear that $p_A^*(\mathcal{Q}) = p_A^*(\mathcal{I})$ because the only difference between Bob's actions in $\mathcal{Q}$ and $\mathcal{I}$ is that Bob self-tests to ensure his boxes are indeed GHZ. However, the optimal cheating strategy for $\mathcal{I}$ can be implemented using GHZ boxes.

This establishes the first part of the lemma. For the second part, i.e. establishing that optimising $c_0\alpha + c_1\beta + c_\perp\gamma$ over $(\alpha,\beta,\gamma) \in \mathbb{C}_A$ is an SDP, we proceed as follows. Suppose Assumption 18 holds. Then we can assume that Bob starts with the state

$$\rho_0 := \mathrm{tr}_H(|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_{HIJ}) \tag{12}$$

and the effect of measuring the two boxes can be represented by the application of projectors of pauli operators X and Z.

The justification is similar to that given in the former proof. Suppose Bob holds registers QR of $|\psi\rangle_{PQR}$ which is the combined state of the three boxes. Suppose his measurement operators are $\{M^Q_{b|y}, M^R_{c|z}\}$. Then using the isometry in Lemma 8, Bob can relabel his state (and without loss of generality, we can suppose Alice also relabels according to the aforementioned isometry) to get $\Phi_{PQR}|\psi\rangle_{PQR} = |\mathrm{GHZ}\rangle_{HIJ}\otimes|\mathrm{junk}\rangle_{PQR}$. Further, since $\Phi_{PQR}(M^Q_{b|y}\otimes M^R_{c|z}|\psi\rangle_{PQR}) = \Pi^I_{b|y}\Pi^J_{c|z}|\mathrm{GHZ}\rangle_{HIJ}\otimes|\mathrm{junk}\rangle_{PQR}$ Bob's act of measurement, in the new labelling, corresponds to simply measuring the GHZ state in the appropriate Pauli basis. (TODO: in the approximate case, the initial state will be close to the one mentioned and the post-measured state will similarly only be close to the one post projectors; There should be some way of showing that this can be absorbed into the initial state). **(Tom:** There is still a TODO here**)**

1. Bob receiving s from Alice is modelled by introducing $\rho_1 \in SIJ$ satisfying $\mathrm{tr}_S(\rho_1) = \rho_0$.

2. Bob sending $g \in_R \{0,1\}$ can be seen as appending a mixed state: $\rho_1 \otimes \frac{1}{2}\mathbb{I}_G$.

3. Alice sending x (and a) can be modelled as introducing $\rho_2 \in AXSIJG$ satisfying $\mathrm{tr}_A(\rho_2) = \rho_1 \otimes \frac{\mathbb{I}_G}{2}$.

4. To model the GHZ test, introduce a register Y in the state $\frac{|0\rangle_Y + |1\rangle_Y}{\sqrt{2}}$. Recall that to perform the GHZ test, we need $x\oplus y\oplus z = 1$ i.e. $z = 1\oplus y\oplus x$. Further introduce registers B and C to hold the measurement results, define

$$U := \sum_{y,x\in\{0,1\}} |y\rangle\langle y|_Y\, |x\rangle\langle x|_X \otimes (\mathbb{I}_B\otimes\Pi^I_{0|y} + X_B\otimes\Pi^I_{1|y})\otimes(\mathbb{I}_C\otimes\Pi^J_{0|(1\oplus y\oplus x)} + X_C\otimes\Pi^J_{1|(1\oplus y\oplus x)})\otimes\mathbb{I}_{ASG}. \tag{13}$$

By construction, $\rho_3 := U\left(|+\rangle\langle+|_Y\otimes|00\rangle\langle 00|_{BC}\otimes\rho_2\right)U^\dagger \in YBCAXSIJG$ models the measurement process. (TODO: this equality would become approximately true...but perhaps the noise can be absorbed in ρ_0 with some argument)

5. Since we postponed the measurements to the end, we add this step. Define

$$\Pi_i := \sum_{x,g\in\{0,1\}:x\oplus g=i} |xg\rangle\langle xg|_{XG} \otimes \mathbb{I}_{YABSIJ}$$

to determine who won. Define

$$\Pi^{\text{sTest}} := \sum_{s,a,x\in\{0,1\}:s=a\vee s=a\oplus x} |sax\rangle\langle sax|_{SAX} \otimes \mathbb{I}_{GYBCIJ}$$

to model the first test, i.e. s should either be a or $a \oplus x$. Define

$$\Pi^{\text{GHZ}} := \sum_{\substack{x,y\in\{0,1\},\\ a,b,c\in\{0,1\}:a\oplus b\oplus c\oplus 1=xy\cdot(1\oplus x\oplus y)}} |xyabc\rangle\langle xyabc|_{XYABC} \otimes \mathbb{I}_{GSIJ}$$

to model the GHZ test. Let

$$\Pi^{\text{Test}} := \Pi^{\text{GHZ}}\Pi^{\text{sTest}}, \quad \bar{\Pi}^{\text{Test}} := \mathbb{I} - \Pi^{\text{Test}}. \tag{14}$$

One can then write the cheat vector for Bob, i.e. the tuple of probabilities that Bob outputs 0, 1 and abort (see Definition 4), as

$$(\alpha, \beta, \gamma) = (\text{tr}(\Pi_0\Pi^{\text{Test}}\rho_3), \text{tr}(\Pi_1\rho_3), \text{tr}(\Pi_0\bar{\Pi}^{\text{Test}}\rho_3)).$$

(Tom: NB: Still old notation for the cheat vectors**)** To summarise, the final SDP is as follows: let $\rho_0 \in IJ$ be as defined in Equation (12), $\rho_1 \in SIJ$ and $\rho_2 \in AXSIJG$. Then,

$$\max \quad \text{tr}\left([\Pi_0(c_0\Pi^{\text{Test}} + c_\perp\bar{\Pi}^{\text{Test}}) + c_1\Pi_1]U\left(|{+00}\rangle\langle{+00}|_{YBC} \otimes \rho_2\right)U^\dagger\right)$$

subject to

$$\text{tr}_S(\rho_1) = \rho_0$$
$$\text{tr}_A(\rho_2) = \frac{1}{2}\rho_1 \otimes \mathbb{I}_G$$

where U is as defined in Equation (13) and the projectors as in Equation (14).

□

6 Security Proof | Finite n

TODO: Write the following properly

In this section, we drop Assumption ??, and estimate the GHZ winning probability from Algorithm ??. We then use the robust variant of the self-testing result to conclude that the SDP of interest must be close to the SDP we considered (with some larger space tensored to it). Finally, we show the continuity of these SDPs and thereby conclude that we converge to the asymptotic result as n is increased.

We show this for the case where Alice self-tests. We expect an analogous result to hold when Bob self-tests.

6.1 Estimation of GHZ winning probability

We assume that the $3n$ boxes are described by some joint quantum state and local measurement operators. After playing the GHZ game with $3(n-1)$ of them, and verifying that they all pass, we want to make a statement about the remaining box, whose state $\tilde{\rho}$ is conditioned on the passing of all the other test.

The expectation value of $E[X_J|J,\Omega]$ accurately describes the expected GHZ value associated to the state of the remaining boxes J, conditioned on having measuring some outcome sequence in the other boxes which passes all the GHZ tests. Note that the conditioning in J is important because otherwise we would get a bound on the GHZ averaged over all boxes, but we are only interested in the remaining box.

Protocol 5 Estimation of the GHZ value

1. Pick a box $J \in [n]$ uniformly at random.
2. For $i \in [n] \backslash J$, play the GHZ game with box i, denote outcome of game as $X_i \in \{0, 1\}$
3. If

$$\Omega: \quad X_i = 1, \text{for all } i \in [n] \backslash J \tag{15}$$

4. Then conclude that the remaining box satisfies

$$T: \quad E[X_J | J, \Omega] \geq 1 - \delta \tag{16}$$

Proposition 19 (Security of 6.1)**.** *For any implementation of the boxes and choice of $\delta > 0$ the joint probability that that the test Ω passes and that the conclusion T is false is small $\Pr[\Omega \cap \bar{T}] \leq \frac{1}{1-\delta+n\delta} \leq \frac{1}{n\delta}$, where the first upper-bound is tight.*

This is the correct form of the security statement. It is important to bound the joint distribution of Ω and $\overline{T}$, and not $\Pr[\overline{T}|\Omega]$, conditioning on passing the test Ω. Indeed in the latter case, it would not be possible to conclude anything of value about the remaining box J, as there could be some implementation of the boxes which has a very low expectation value of GHZ, but which passes the test with small but non-zero probability. The present security definition has a nice interpretation in the composable security framework of [ref]. Consider an hypothetical ideal protocol, which after having chosen J, only passes when T is true. In that case, $\Pr[\Omega \cap \overline{T}] = 0$. Then the actual protocol is equivalent the ideal one, except that if fails with probability $\epsilon = \frac{1}{1-\delta+m\delta}$, and so it is ϵ-close to the ideal algorithm.

Proof. For a given implementation of the boxes, let $p(x_1, \cdots x_n)$ denote the joint probability distribution of passing the GHZ games. Let $S = \{j | \ E[X_j | J = j, \Omega] < 1 - \delta\} \subset [n]$ be the set of boxes that have an expectation value for GHZ (conditioned on passing in the other boxes) below our target threshold and let $m = |S|$ be the number of such boxes. The value of m is unknown, so we will need to maximise over it in the end.

Let $\alpha = \Pr(\{X_i\}_i = 1)$ and $\beta_i = \Pr(\{X_i\}_{i \neq j} = 1 \cap X_j = 0)$ be respectively the probabilities of the events where all the tests pass, or they all pass except for the jth test. This allows us to rewrite $E[X_j | J = j, \Omega] = \Pr(\{X_i\}_i = 1) / \Pr(\{X_i\}_{i \neq j} = 1) = \alpha / (\alpha + \beta_j)$, and so, by definition of S, we have $\alpha/(\alpha + \beta_j) < (1 - \delta)$, for $j \in S$, which is equivalent to $\beta_j > \frac{\delta}{1-\delta}\alpha$.

The aim of the proof is to bound the probability $\Pr[\Omega \cap \overline{T}]$. If we condition and summed over the different values of J, we can rewrite it as

$$\Pr(\Omega \cap \overline{T}) = \sum_j \frac{1}{n} \Pr(\Omega \cap \overline{T} | J = j) = \sum_{j \in S} \frac{1}{n} \Pr(\{X_i\}_{i \neq j} = 1) = \frac{1}{n} \sum_{j \in S} (\alpha + \beta_i)\,, \tag{17}$$

where we have kept the round $j \in S$ ones, conditioned on which T is false. We are thus left with the optimisation problem

$$\max_{\alpha \geq 0, (\beta_i)_i \geq 0} \quad \frac{1}{n} \left(\sum_{j \in S} \alpha + \beta_j \right) \tag{18}$$

$$\text{subject to} \quad \alpha + \sum_{j \in S} \beta_j \leq 1 \tag{19}$$

$$\beta_j \geq \frac{\delta}{1-\delta}\alpha, \text{for } j \in S \tag{20}$$

This is a linear problem. Simplifying it by defining $\Sigma = \sum_{j\in S}\beta_j$, gives

$$\max_{\alpha\geq 0,\Sigma\geq 0} \quad \frac{1}{n}(m\alpha+\Sigma) \tag{21}$$
$$\text{subject to} \quad \alpha+\Sigma \leq 1 \tag{22}$$
$$\Sigma \geq m\frac{\delta}{1-\delta}\alpha \tag{23}$$

It is easily shown that the maximum is attained for $(\alpha,\Sigma) = \left(\frac{1-\delta}{1-\delta+m\delta}, \frac{m\delta}{1-\delta+m\delta}\right)$ which gives the upper-bound

$$\Pr[\Omega\cap\overline{T}] \leq \frac{1}{n}\max_m \frac{m}{1-\delta+m\delta} = \frac{1}{1-\delta+n\delta} \tag{24}$$

We note that the upper-bound is an increasing function of m and so the maximum is attained for $m=n$. This yield the desired upper-bound. From the converse statement, we note that from the present proof we can construct a probability distribution $p(x_1,\cdots x_n)$, which saturates all inequalities, and so the upper-bound $\frac{1}{1-\delta+n\delta}$ is tight. □

6.2 Robust self-testing

Lemma 20. *Let $a,b,c,x,y,z \in \{0,1\}$. Consider a trio of quantum boxes, specified by projectors $\{M^A_{a|x}, M^B_{b|y}, M^C_{c|z}\}$ acting on finite dimensional Hilbert spaces $\mathcal{H}^A, \mathcal{H}^B$ and $\mathcal{H}^C$, and $|\psi\rangle \in \mathcal{H}^A\otimes\mathcal{H}^B\otimes\mathcal{H}^C =: \mathcal{H}^{ABC}$. If the trio pass the GHZ test with probability $1-\epsilon$ (for $1>\epsilon>0$), then there exists a local isometry,*

$$\Phi = \Phi^A\otimes\Phi^B\otimes\Phi^C : \mathcal{H}^{ABC} \to \mathcal{H}^{ABC}\otimes\mathbb{C}^{2\times 3}$$

and a decreasing function of ϵ, $f(\epsilon)$ such that

$$\|\Phi(|\psi\rangle) - |\chi\rangle\otimes|\text{junk}\rangle\| \leq f(\epsilon), \tag{25}$$
$$\left\|\Phi\left(M^D_{d|t}|\psi\rangle\right) - \Pi^D_{d|t}|\text{GHZ}\rangle\otimes|\text{junk}\rangle\right\| \leq f(\epsilon) \quad \forall D\in\{A,B,C\},\ \text{and } d,t\in\{0,1\} \tag{26}$$

where $|\text{GHZ}\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}} \in \mathbb{C}^{2\times 3}$, $|\text{junk}\rangle \in \mathcal{H}^{ABC}$ is some arbitrary state and $\{\Pi^A_{a|x}, \Pi^B_{b|y}, \Pi^C_{c|z}\}$ are projectors corresponding to σ_x on the first, second and third qubit of $|\text{GHZ}\rangle$ respectively, for $x=0$ and corresponding to σ_y for $x=1$, as in Claim 7.

Proof. A proofs of robust self-testing for GHZ can be found in [MS13] and [McK14]. □

6.3 Alice self-tests

The basic idea here is to treat the state and measurements inside the boxes as variables which are optimised over, subject to the constraint that they are ϵ-close to the ideal GHZ state and measurements. This ceases to be an SDP so we relax the constraint that the post measurement states must arise from measuring some fixed state and let them be arbitrary states. The requirement that these are close to the ideal GHZ state and post measured states is still enforced. When $\epsilon=0$, we recover the asymptotic SDP (and that is no longer a relaxation). Since we only change the constant ϵ, convergence of the objective value of these SDPs is easy to show [JAMIE].

Proof. We first write exactly what is going on physically, except that we take the liberty of "renaming", i.e. applying global isometries. We treat the state $|\psi\rangle_{PQR}$ and the measurements $\{M^P_{a|x}\}$ as variables.

1. We begin as before with $|\Psi'_0\rangle$,

$$|\Psi'_0\rangle := |+\rangle_X|0\rangle_A|\psi\rangle_{PQR'}$$

   and[17] obtain the "post measurement state" as

$$|\Psi'_1\rangle = \frac{1}{2}\sum_{x,a\in\{0,1\}}|x\rangle_X|a\rangle_A M^P_{a|x}|\psi\rangle_{PQR'}.$$

[17](we put R' because we already used R for the random register)

Since we are allowed to "rename" (without changing the value of the SDP), we have

$$\left|\Psi_2'\right\rangle = \frac{1}{2}\sum_{x,a\in\{0,1\}} |x\rangle_X |a\rangle_A \Phi_{PQR}M^P_{a|x}|\psi\rangle_{PQR'}. \tag{27}$$

At this point, in the asymptotic case, we could directly apply the self-testing result and replace $\Phi_{PQR'}M^P_{a|x}|\psi\rangle_{PQR'}$ with $\Pi^H_{x|a}|\text{GHZ}\rangle_{HIJ}\otimes|\text{junk}\rangle_{PQR'}$. Now, instead, we require

$$\left\|\Phi_{PQR'}M^P_{a|x}|\psi\rangle_{PQR'} - \Pi^H_{x|a}|\text{GHZ}\rangle_{HIJ}\otimes|\text{junk}\rangle_{PQR'}\right\| \le \epsilon \quad \forall a,x\in\{0,1\}$$

[EDIT: here the norm is just the vector norm but we can impose it as density matrices; there we use the trace norm; the remark shows how to convert that into an SDP]where the norm[18] here is the trace norm $\|.\|$ (see Remark 21) and ϵ' is a function ϵ which vanishes as ϵ vanishes (ϵ comes from the self testing step). One could, henceforth, continue as in the asymptotic case. More precisely, one could start with $|\Psi_0\rangle := \left|\Psi_2'\right\rangle$, model the classical computation step as

$$\begin{aligned}|\Psi_1\rangle &= U_{\text{comp}}|\Psi_0\rangle|00\rangle_{RS}\\ &= \frac{1}{2\sqrt{2}}\sum_{x,a,r\in\{0,1\}}|xa\rangle_{XA}|r\rangle_R|a\oplus x.r\rangle_S\Phi_{PQR}M^P_{a|x}|\psi\rangle_{PQR'}\end{aligned}$$

where U_{comp} is implicitly defined to yield the stated state. Then, the act of sending s (which is the first communication step) is modelled as

$$\text{tr}_{IJSPQR'}(|\Psi_1\rangle\langle\Psi_1|)\in XARH.$$

2. The remaining steps are unchanged except that Alice additionally, always holds the register H now.

The final optimisation problem is defined on the variables $|\psi\rangle\in PQR'$, $M^P_{a|x}$ projectors (or POVMs) acting on PQR, $\Phi_{PQR'}$ a local isometry[19] from $PQR'\to HIJPQR'$, $|\text{junk}\rangle\in PQR'$, $\rho_2\in XARGH$ and $\rho_3\in XARGYDH$. The problem is:

$$\max \quad \text{tr}([c_0\Pi_0 + \Pi_1(c_1\Pi^{\text{GHZ}} + c_\perp\bar{\Pi}^{\text{GHZ}})]\rho_3)$$

subject to

$$\begin{aligned}\left\|\Phi_{PQR'}M^P_{a|x}|\psi\rangle_{PQR'} - \Pi^H_{x|a}|\text{GHZ}\rangle_{HIJ}\otimes|\text{junk}\rangle_{PQR'}\right\| &\le \epsilon \quad \forall a,x\in\{0,1\}\\ |\Psi_1\rangle &:= U_{\text{comp}}|\Psi_0\rangle|00\rangle_{RS}\\ \text{tr}_{IJSPQR'}\left[|\Psi_1\rangle\langle\Psi_1|\right] &= \text{tr}_G(\rho_2)\\ \rho_2\otimes\frac{\mathbb{I}_Y}{2} &= \text{tr}_D(\rho_3)\end{aligned} \tag{28}$$

where $|\Psi_0\rangle$ is as defined above (see Equation (27) and recall that $|\Psi_0\rangle = \left|\Psi_2'\right\rangle$). This, as it is stated, is not an SDP. However, it is clear that when $\epsilon = 0$, we recover the asymptotic case (many variables can be dropped because they either are fixed (and no longer variable, e.g. $|\Psi_0\rangle$) or become redundant, e.g. register H). Let $v(\epsilon,d)$ be the value of the optimization program above where d encodes the dimension of systems PQR. We now relax the constraints to obtain an SDP. Let $v'(\epsilon,d)$ be its value. We want the relaxation to be such that $v'(0,d)=v(0,d)$. Additionally, because it is a relaxation, we know $v(\epsilon,d)\le v'(\epsilon,d)$. It then suffices to show the continuity of the relaxation (the SDP), to establish the convergence of $v(\epsilon,d)$ to $v(0,d)$ as $\epsilon\to 0$ [JAMIE double-check!].

There are two steps to the relaxation. First, we relax the Equation (28) as in Remark 21. This is straightforward. Second, we remove the variables $|\psi\rangle, M^P_{a|x}$ and $\Phi_{PQR'}$ and instead introduce variables $|\xi^{a,x}\rangle\in HIJPQR'$ for $a,x\in\{0,1\}$. We substitute[20] $|\psi\rangle$ with $|\xi\rangle$ and $M^P_{a|x}|\psi\rangle$ with $|\xi^{a,x}\rangle$ in the definition of $|\Psi_0\rangle$ and in the constraint Equation (28). This is evidently a relaxation (because one can represent any choice of $|\psi\rangle, M^P_{a|x}$ and $\Phi_{PQR'}$ using $|\xi\rangle$ and $|\xi_{a,x}\rangle$ in

[18]We could have used other norms but they would be a relaxation of the constraints.

[19]by local we mean it has the form $\Phi_P\otimes\Phi_Q\otimes\Phi_R$ where, for instance, $\Phi_P: P\to HP$.

[20]we can drop the pure state requirement; we use it for notational simplicity

the optimisation problem). Relaxing further to mixed states, the SDP is then defined on $\xi^{aa',xx'} \in \mathrm{L}(HIJPQR')$ for $a, a', x, x' \in \{0,1\}$, $\rho_{\text{junk}} \in \mathrm{PSD}(PQR')$, $\rho_2 \in \mathrm{PSD}(XARGH)$ and $\rho_3 \in \mathrm{PSD}(XARGYDH)$ as

$$\max \quad \mathrm{tr}([c_0\Pi_0 + \Pi_1(c_1\Pi^{\mathrm{GHZ}} + c_\perp\bar{\Pi}^{\mathrm{GHZ}})]\rho_3)$$

subject to

$$\left\| \xi^{aa',xx'} - \Pi^H_{a|x} \left|\mathrm{GHZ}\right\rangle\left\langle\mathrm{GHZ}\right|_{HIJ} \Pi^H_{a'|x'} \otimes \rho_{\text{junk}} \right\| \le \epsilon'' \quad \forall a, a', x, x' \in \{0,1\}$$
$$\bar{\Psi}_1 := U_{\text{comp}}\bar{\Psi}_0 \otimes \left|00\right\rangle\left\langle 00\right|_{RS} U^\dagger_{\text{comp}}$$
$$\mathrm{tr}_{IJSPQR'}\left[\bar{\Psi}_1\right] = \mathrm{tr}_G(\rho_2)$$
$$\rho_2 \otimes \frac{\mathbb{I}_Y}{2} = \mathrm{tr}_D(\rho_3)$$

where

$$\bar{\Psi}_0 := \frac{1}{4}\sum_{x,x',a,a' \in \{0,1\}} \left|xa\right\rangle\left\langle x'a'\right|_{XA} \xi^{aa',xx'}_{HIJPQR'}$$

and ϵ'' is a function of ϵ which vanishes as ϵ vanishes. Clearly, when $\epsilon = 0$, we recover the asymptotic SDP and by construction, the SDP is a relaxation of the optimisation problem we started with. Recall that $v'(\epsilon, d)$ is the value of this SDP. It is easy [for JAMIE! please help] that $v'(\epsilon, d)$ is continuous as a function of ϵ (at least for small ϵ?); my guess would be that we are slowly enlarging the feasible region so won't expect any jumps. □

Remark 21. It is straightforward to show that $\| |\rho\rangle - |\sigma\rangle \| \le \epsilon \implies \mathrm{tr}\,|\rho - \sigma| \le \epsilon'$ where $\epsilon' = 2\sqrt{1-(1-\epsilon)}$.

For many norms (including the trace norm), we have $\|X\| \le \epsilon \implies |\lambda_{\max}(X)| \le \epsilon'$ where ϵ' vanishes as ϵ vanishes. It is easy to bound $\lambda_{\max}(X) \le \epsilon$ as

$$\begin{pmatrix} X - \epsilon\mathbb{I} & 0 \\ 0 & \epsilon\mathbb{I} - X \end{pmatrix} \ge 0.$$

This is an SDP constraint because we can define some $\begin{pmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{pmatrix} \ge 0$ and then set the linear constraint $Y_{11} = X - \epsilon\mathbb{I}$ and $Y_{22} = \epsilon\mathbb{I} - X$.

[EDIT When X is not Hermitian, we can relax it using Schur's complement as

$$\begin{pmatrix} \mathbb{I} & X \\ X^T & \epsilon''\mathbb{I} \end{pmatrix} \ge 0 \iff \epsilon''\mathbb{I} \ge X^T X$$

and if $\|X\| \le \epsilon$, then there should be some function ϵ'' of ϵ that satisfies the above (with possibly a multiplicative factor of $\dim(X)$).]

6.4 Bob self tests

For Bob's case, we work out an example which is essentially the same as what we want to prove. In this case, we are unable to find a simple SDP relaxation as above and instead rely on the NPA hierarchy for the continuity result.

Example 22. We consider three optimisation problems. The first is supposed to be the "asymptotic version", the second is supposed to by a toy model of what happens in the lab with ϵ as a parameter, and finally the third is an SDP relaxation of the second, obtained using the NPA hierarchy.

First: Let $\rho_0 := \mathrm{tr}_{HI}\left[\left|\mathrm{GHZ}\right\rangle\left\langle\mathrm{GHZ}\right|\right]_{HIJ}$. The variable is $\rho_1 \in ZJ$. The SDP program is

$$\max \quad \mathrm{tr}(\Pi_{\text{obj}}\rho_2\Pi_{\text{obj}})$$

subject to

$$\mathrm{tr}_Z(\rho_1) = \rho_0$$
$$\rho_2 = \sum_{\substack{z,z' \\ c,c'}} \left|c\right\rangle\left\langle c'\right|_C \otimes \Pi^J_{c|z} \otimes \Pi^Z_z \quad \rho_1 \quad \Pi^J_{c'|z'} \otimes \Pi^Z_{z'}$$

where Π_{obj} is an arbitrary but fixed projector which acts non-trivially on registers CZ and $\{\Pi^J_{c|z}\}$ constitute two sets of projective measurements, the setting indexed by z and outcome by c.

The main simplifications we make, compared to Bob's asymptotic SDP, are:
(1) we keep only the J register from the HIJ registers used in the GHZ test,
(2) we skipped the part where Alice first sends s, then Bob sends g and in turn Alice sends x and a which are finally used to do the test; we simply have her send z, the basis in which to measure,
(3) the action of the (appropriately adapted) unitary U is captured directly by defining ρ_3
(4) the final measurement operator is left arbitrary so long as it acts on "classical registers", CZS.

These simplifications can be undone with the main idea unchanged. We now proceed with defining the second variant which has the PQR registers as well.

Second: The variables are $\rho_0 \in HIJPQR$, $\rho_1 \in ZJR$, $\rho_{\text{junk}} \in R$ and $\{M_{0|z}, M_{1|z}\}$ are projectors acting on JR, for $z \in \{0,1\}$. The optimisation problem is

$$\max \quad \operatorname{tr}(\Pi_{\text{obj}}\rho_2\Pi_{\text{obj}})$$

subject to

$$\left\|\rho_0 - |\text{GHZ}\rangle\langle\text{GHZ}|_{HIJ} \otimes \rho_{\text{junk}}\right\| \le \epsilon_0 \tag{29}$$

$$\left\|M_{c|z}\rho_0 M_{c'|z'} - \Pi^J_{c|z}|\text{GHZ}\rangle\langle\text{GHZ}|\Pi^J_{c'|z'} \otimes \rho_{\text{junk}}\right\| \le \epsilon_1 \quad \forall \quad c, c', z, z' \in \{0,1\}. \tag{30}$$

$$\operatorname{tr}_Z(\rho_1) = \operatorname{tr}_{HIPQ}\rho_0$$

$$\rho_2 = \sum_{\substack{z,z'\\c,c'}} |c\rangle\langle c'|_C \quad \otimes \quad M_{c|z} \otimes \Pi^Z_z \quad \rho_1 \quad M_{c'|z'} \otimes \Pi^Z_{z'}$$

where ϵ_0 and ϵ_1 are functions of ϵ which vanish as ϵ vanishes.

We briefly justify why this optimization problem correctly captures the physical situation, modulo the simplifications listed above (which again, don't change the argument here). Let $|\psi\rangle \in HIJPQR$ be the state in the box and $M_{c|z}$ be the measurement operators for the last box. Since we're allowing Bob to optimise over $|\psi\rangle$ and $M_{c|z}$ we don't quite need to worry about the isometry in the self-testing step. We suppress the c's and z's for the moment. The self-testing statement says that $\||\psi\rangle - |\text{GHZ}\rangle \otimes |\text{junk}\rangle\| \le \epsilon$ which entails Equation (29). The self-testing statement also says that $\|M|\psi\rangle - \Pi|\text{GHZ}\rangle \otimes |\text{junk}\rangle\| \le \epsilon$. which implies Equation (30).

It is straightforward to see that for $\epsilon = 0$, this optimization problem reduces to the first one. The ρ_0 part is trivial and replacement of $M_{c|z}$ with $\Pi_{c|z}$ in ρ_2 can be made as in illustrated Example 23 below.

Third: Denote the value of the second program by $v(\epsilon, d)$. As argued, $v(0, d)$ is the value of the first program for all d (finite d). [EDIT: I realised even an NPA relaxation is not simple/obvious here] Let $w(\epsilon, d, k)$ denote the value of the NPA relaxation of the second program, to level k. The NPA hierarchy is well known and for our purposes here, it suffices to note two facts. First, the NPA relaxation is always an SDP and second, the NPA relaxation converges to, in this case, the second program as k tends to infinity. Since $v(\epsilon, d) \le w(\epsilon, d, k)$ for all k and d, the continuity result follows [JAMIE: complete the argument?].

Example 23. Let ρ_{AB} be a density matrix, Π^B, Π'^B be projectors on B and M^B, M'^B be measurement (Kraus) operators on B. Suppose $M^B\rho_{AB}M'^B = \Pi^B\rho_{AB}\Pi'^B$. Suppose

$$M^B\rho_{AB}M'^B = \Pi^B\rho_{Ab}\Pi'^B. \tag{31}$$

If σ_{AB} is another density matrix such that $\operatorname{tr}_A(\sigma_{AB}) = \operatorname{tr}_B(\rho_{AB})$, then

$$M^B\sigma_{AB}M'^B = \Pi^B\sigma_{AB}\Pi'^B. \tag{32}$$

This follows from Uhlman's theorem which guarantees that there exists a U acting on system A such that

$$(U \otimes \mathbb{I}_B)\,\sigma_{AB}\left(U^\dagger \otimes \mathbb{I}_B\right) = \rho_{AB}.$$

Thus, conjugating Equation (31) with $U \otimes \mathbb{I}_B$, we obtain Equation (32). (NB: We didn't need the fact that Π, Π' are projectors and M, M' are measurement operators)

6.5 SDP-valued functions and their continuity

A semidefinite program (SDP) is an optimization problem of the form

$$\begin{aligned} f(A,B) = \text{maximize:} \quad & \langle A, X \rangle \\ \text{subject to:} \quad & \Phi(X) = B \\ & X \geq 0. \end{aligned} \tag{33}$$

We call $f(A,B)$ the value of the semidefinite program which is the supremum of $\langle A, X \rangle$ over all X that are feasible ($X \geq 0$ and $\Phi(X) = B$). In this work we wish to view how the value of an SDP changes as you change A and/or B. Ultimately, we wish to know if the value of an SDP is continuous as a function of A and B. To this end, let us consider the function

$$h(A) = \text{maximize:} \quad \langle A, X \rangle \tag{34}$$

$$\text{subject to:} \quad X \in C \tag{35}$$

where C is a nonempty, convex set. This is a generalization of an SDP which is convenient for the upcoming analysis. Notice that when C is unbounded, it may be the case that f takes the value $+\infty$. Since we cannot count that high, we use the following definition.

Definition 24. We define the *support* of the function h, denoted as $\text{supp}(h)$, as

$$\text{supp}(h) := \{A : h(A) \text{ is finite}\}. \tag{36}$$

We now show some elementary properties of this function.

Lemma 25. *The support of h is convex and h is a convex function on its support.*

Proof. For $A_1, A_2 \in \text{supp}(h)$ and $\lambda_1, \lambda_2 \geq 0$ satisfying $\lambda_1 + \lambda_2 = 1$, we have

$$h(\lambda_1 A_1 + \lambda_2 A_2) \leq h(\lambda_1 A_1) + h(\lambda_2 A_2) \tag{37}$$

$$= \lambda_1 h(A_1) + \lambda_2 h(A_2) \tag{38}$$

$$< +\infty \tag{39}$$

where the last inequality follows from $A_1, A_2 \in \text{supp}(h)$. Thus, $\lambda_1 A_1 + \lambda_2 A_2 \in \text{supp}(h)$, proving $\text{supp}(h)$ is a convex set, and h is convex from the above inequalities. □

The following corollary follows from the fact that h is convex.

Corollary 26. *h is continuous on the interior of its support.*

Another well-known corollary is that h is continuous everywhere if C is compact. This follows from the above corollary since the support is the entire space.

Corollary 27. *If C is compact, h is continuous everywhere.*

6.5.1 SDP approximation and finite statistics

(Jamie: Continue here.**)**

(Jamie: references are incomplete. SCA+11 is missing first names. ARV missing year and journal and year. ARW is missing everything. Kit03 should probably have a link to the website. STOC references inconsistent. TQC refs inconsistent. Are ARW and ARW 19 the same?**)**

References

[ACG+14] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin, *A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias*, SIAM Journal on Computing **45** (2014), no. 3, 633–679.

[ARV] Atul Singh Arora, Jérémie Roland, and Chrysoula Vlachou, *Analytic quantum weak coin flipping protocols with arbitrarily small bias*, pp. 919–938.

[ARW] Atul Singh Arora, Jérémie Roland, and Stephan Weis, *Quantum weak coin flipping*.

[ARW19] Atul Singh Arora, Jérémie Roland, and Stephan Weis, *Quantum weak coin flipping*, Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing - STOC 2019, ACM Press, 2019.

[Blu83] Manuel Blum, *Coin flipping by telephone a protocol for solving impossible problems*, SIGACT News **15** (1983), no. 1, 23–27.

[HW11] Esther Hänggi and Jürg Wullschleger, *Tight bounds for classical and quantum coin flipping*, Theory of Cryptography (Berlin, Heidelberg) (Yuval Ishai, ed.), Springer Berlin Heidelberg, 2011, pp. 468–485.

[Kit03] Alexei Kitaev, *Quantum coin flipping*, Talk at the 6th workshop on Quantum Information Processing, 2003.

[McK14] Matthew McKague, *Self-testing graph states*, Theory of Quantum Computation, Communication, and Cryptography (Berlin, Heidelberg) (Dave Bacon, Miguel Martin-Delgado, and Martin Roetteler, eds.), Springer Berlin Heidelberg, 2014, pp. 104–120.

[Mil20] Carl A. Miller, *The impossibility of efficient quantum weak coin flipping*, Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (New York, NY, USA), STOC 2020, Association for Computing Machinery, 2020, pp. 916–929.

[Moc07] Carlos Mochon, *Quantum weak coin flipping with arbitrarily small bias*, arXiv:0711.4114 (2007).

[MS13] Carl A. Miller and Yaoyun Shi, *Optimal Robust Self-Testing by Binary Nonlocal XOR Games*, 8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013) (Dagstuhl, Germany) (Simone Severini and Fernando Brandao, eds.), Leibniz International Proceedings in Informatics (LIPIcs), vol. 22, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2013, pp. 254–262.

[SCA+11] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, *Fully distrustful quantum bit commitment and coin flipping*, Physical Review Letters **106** (2011), no. 22.

7 Acknowledgements

A Device Independence and the Box Paradigm

We describe device independent protocols as classical protocols with one modification: we assume that the two parties can exchange boxes and that the parties can shield their boxes (from the other boxes i.e. the boxes can't communicate with each other once shielded).

Definition 28 (Box)**.** A *box* is a device that takes an input $x \in \mathcal{X}$ and yields an outputs $a \in \mathcal{A}$ where $\mathcal{X}$ and $\mathcal{A}$ are finite sets. Typically, a set of n boxes, taking inputs $x_1, x_2, \dots x_n$ and yielding outputs $a_1, a_2 \dots a_n$ are *characterised* by a joint conditional probability distribution, denoted by

$$p(a_1, a_2 \dots a_n | x_1, x_2 \dots x_n).$$

Further, if $p(a_1, a_2 \dots a_n | x_1, x_2 \dots x_n) = \operatorname{tr}\left[M^1_{a_1|x_1} \otimes M^2_{a_2|x_2} \cdots \otimes M^n_{a_n|x_n} \rho\right]$ then we call the set of boxes, *quantum boxes*, where $\{M^i_{a'|x'}\}_{a' \in \mathcal{A}_i}$constitute a POVM for a fixed i and x', ρ is a density matrix and their dimensions are mutually consistent.

Henceforth, we restrict ourselves to quantum boxes.

Definition 29 (Protocol in the box formalism)**.** A generic two-party protocol in the box formalism has the following form:

1. Inputs:
   (a) Alice is given boxes $\square_1^A, \square_2^A \dots \square_p^A$ and Bob is given boxes $\square_1^B, \square_2^B, \dots \square_q^B$.
   (b) Alice is given a random string r^A and Bob is given a random string r^B (of arbitrary but finite length).
2. Structure: At each round of the protocol, the following is allowed.
   (a) Alice and Bob can locally perform arbitrary but finite time computations on a Turing Machine.
   (b) They can exchange classical strings/messages and boxes.

A protocol in the box formalism is readily expressed as a protocol which uses a (trusted) classical channel (i.e. they trust their classical devices to reliably send/receive messages), untrusted quantum devices and an untrusted quantum channel (i.e. a channel that can carry quantum states but may be controlled by the adversary).

Assumption 30 (Setup of Device Independent Two-Party Protocols)**.** *Alice and Bob*

1. *both have private sources of randomness,*
2. *can send and receive classical messages over a (trusted) classical channel,*
3. *can prevent parts of their untrusted quantum devices from communicating with each other, and*
4. *have access to an untrusted quantum channel.*

We restrict ourselves to a "measure and exchange" class of protocols—protocols where Alice and Bob start with some pre-prepared states and subsequently, only perform classical computation and quantum measurements locally in conjunction with exchanging classical and quantum messages. More precisely, we consider the following (likely restricted) class of device independent protocols.

Definition 31 (Measure and Exchange (Device Independent Two-Party) Protocols)**.** A *measure and exchange (device independent two-party) protocol* has the following form:

1. Inputs:
   (a) Alice is given quantum registers $A_1, A_2, \dots A_p$ together with POVMs[21]
   $$\{M_{a|x}^{A_1}\}_a, \{M_{a|x}^{A_2}\}_a, \dots \{M_{a|x}^{A_p}\}_a$$
   which act on them and Bob is, analogously, given quantum registers $B_1, B_2, \dots B_q$ together with POVMs
   $$\{M_{b|y}^{B_1}\}_b, \{M_{b|y}^{B_2}\}_b, \dots, \{M_{b|y}^{B_q}\}_b.$$
   Alice shields $A_1, A_2, \dots A_p$ (and the POVMs) from each other and from Bob's lab. Bob similarly shields $B_1, B_2 \dots B_q$ (and the POVMs) from each other and from Alice's lab.
   (b) Alice is given a random string r^A and Bob is given a random string r^B (of arbitrary but finite length).
2. Structure: At each round of the protocol, the following is allowed.
   (a) Alice and Bob can locally perform arbitrary but finite time computations on a Turing Machine.
   (b) They can exchange classical strings/messages.
   (c) Alice (for instance) can
      i. send a register A_l and the encoding of her POVMs $\{M_i^{A_l}\}_i$ to Bob, or
      ii. receive a register B_m and the encoding of the POVMs $\{M_i^{B_m}\}_i$.

   Analogously for Bob.

It is clear that a protocol in the box formalism (Definition 29) which uses only quantum boxes (Definition 28) can be implemented as a measure and exchange protocol (Definition 31).

[21]For concreteness, take the case of binary measurements. By $\{M_{a|x}^{A_1}\}_a$, for instance, we mean $\{M_{0|x}^{A_1}, M_{1|x}^{A_1}\}$ is a POVM for $x \in \{0, 1\}$.