Quantum dice rolling: a multi-outcome generalization of quantum coin flipping

To cite this article: N Aharon and J Silman 2010 New J. Phys. 12 033027

View the article online for updates and enhancements.

Related content
- Device-independent bit commitment based on the CHSH inequality
  N Aharon, S Massar, S Pironio et al.
- Experimental quantum tossing of a single coin
  A T Nguyen, J Frison, K Phan Huy et al.
- Quantum key distribution based on orthogonal states allows secure quantum bit commitment
  Guang Ping He

Recent citations
- Quantum leader election
  Maor Ganz
- Semi-loss-tolerant strong quantum coin-flipping protocol using quantum non-demolition measurement
  Qian Yang et al
- Family of loss-tolerant quantum coin-flipping protocols
  N. Aharon et al
Quantum dice rolling: a multi-outcome generalization of quantum coin flipping

N Aharon and J Silman
School of Physics and Astronomy, Tel-Aviv University, Tel-Aviv 69978, Israel
E-mail: jsilman@ulb.ac.be

Received 12 August 2009
Published 16 March 2010
Online at http://www.njp.org/
doi:10.1088/1367-2630/12/3/033027

Abstract. The problem of quantum dice rolling (DR)—a generalization of the problem of quantum coin flipping (CF) to more than two outcomes and parties—is studied in both its weak and strong variants. We prove by construction that quantum mechanics allows for (i) weak $N$-sided DR admitting arbitrarily small bias for any $N$ and (ii) two-party strong $N$-sided DR saturating Kitaev’s bound for any $N$. To derive (ii) we also prove by construction that quantum mechanics allows for (iii) strong imbalanced CF saturating Kitaev’s bound for any degree of imbalance. Furthermore, as a corollary of (ii) we introduce a family of optimal $2m$-party strong $n^m$-sided DR protocols for any pair $m$ and $n$. 

1 Present address: Laboratoire d’Information Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium.
1. Introduction

Coin flipping (CF) is a cryptographic problem in which a pair of remote distrustful parties, usually referred to as Alice and Bob, must generate a random bit that they agree on. There are two types of CF protocols. In ‘weak’ CF, one of the parties prefers one of the outcomes and the other prefers the opposite, whereas in ‘strong’ CF each party does not know the other’s preference. The security of a CF protocol is quantified by the biases $\epsilon_A^{(i)}$ and $\epsilon_B^{(i)} (i \in \{0, 1\})$; if $P_A^{(i)}$ and $P_B^{(i)}$ are the maximal probabilities that a dishonest Alice or Bob can force the outcome $i$, then

$$\epsilon_j^{(i)} = P_j^{(i)} - \frac{1}{2}, \quad i \in \{0, 1\}, \quad j = A, B.$$  (1)

The biases tell us to what extent each of the parties can increase beyond one half their chances of obtaining each of the outcomes. For strong CF $\epsilon = \max\{\epsilon_A^{(0)}, \epsilon_A^{(1)}, \epsilon_B^{(0)}, \epsilon_B^{(1)}\}$ is usually referred to as the bias of the protocol. On the other hand, in weak CF we associate each of the outcomes with a win of one party over the other. Hence, we are not interested in bounding the maximal losing probabilities and only two of the four biases are of interest. It is from these that we compute the bias of the protocol. For example, if Alice wins when the outcome is 0, then $\epsilon = \max\{\epsilon_A^{(0)}, \epsilon_B^{(1)}\}$. Clearly, every strong CF protocol can also be used to implement a weak CF protocol, but the converse statement is generally not true.

The interest in CF arises from its being a canonical cryptographic primitive, in the sense that, like bit commitment, it can be used to implement many protocols belonging to the secure computation class, sometimes referred to as distrustful cryptography. The defining feature of this class is that the communicating parties are either adversaries or potential adversaries, and do not trust each other, as opposed to key distribution, for instance, where the communicating parties are trustful and share the same interest. CF is one of a very few examples in which
quantum mechanics improves on the security that is achievable classically, and as such has important applications in quantum cryptography; for instance, weak CF is used as a subroutine in cheat sensitive quantum bit commitment [1].

CF was first introduced by Blum in 1981, who analyzed it in classical settings [2]. It was subsequently shown that if there are no limitations on the parties’ computational power, a dishonest party can always force any outcome they desire [3]. With the publication of the quantum key-distribution protocol of Bennett and Brassard in 1984 [4], it was realized that many communication tasks that are impossible in classical settings may be possible in quantum settings. However, Mayers [5] and Lo and Chau [6] proved the impossibility of unconditionally secure bit commitment even in quantum settings and, consequently, the impossibility of the unconditional security of many other distrustful cryptographic protocols. In particular, unconditionally secure ideal quantum CF (i.e. CF protocols wherein the relative probabilities of 0 and 1 remain unchanged even in a dishonest execution) is impossible. However, since CF is strictly weaker than bit commitment [7], this leaves open the possibility of the unconditional security of non-ideal quantum CF.

In 1999 Goldenberg et al introduced a quantum gambling protocol [9], which is a problem closely related to weak CF2. The first quantum (strong) CF protocol per se was presented by Aharonov et al in 2000 [8]. The protocol achieves a bias of $\sqrt{2}/4 \simeq 0.354$ [10]. Soon afterward Spekkens and Rudolph [11], and independently Ambainis [12], devised a strong CF protocol with a bias of 1/4. On the other hand, in the same paper Ambainis showed that any CF protocol achieving a bias of $\epsilon$ requires at least $\Omega(\log \log \epsilon^{-1})$ rounds of communication. Kitaev subsequently proved an even more severe limit to the efficacy of strong CF protocols [13]: any strong CF protocol must satisfy $P_A^{(0)} \cdot P_B^{(0)} \geq 1/2$, $i \in \{0, 1\}$. As regards weak CF, in 2002 Spekkens and Rudolph introduced a family of three rounds of communication protocols in which both dishonest parties have a bias of $(\sqrt{2} - 1)/2 \simeq 0.207$ [14]. Mochon improved upon Spekkens and Rudolph’s result by constructing weak CF protocols with an infinite number of rounds [15, 16]. These efforts culminated in a proof that weak CF with an arbitrarily small bias, or unconditionally secure (non-ideal) weak CF, is possible [17]. Most recently, building upon Mochon’s latest result, Chailloux and Kerenidis devised a strong CF protocol, which saturates Kitaev’s bound in the limit of an infinite number of rounds [18].

There have also been a number of works that have analyzed cases that do not fall strictly within the original definition of CF. Mochon’s arbitrarily weak CF protocol has been generalized to cover the imbalanced case as well [18]. Quantum strong CF has been studied in the multi-party scenario [19] and the multi-outcome scenario [20, 21] (but not in both scenarios simultaneously).

Quantum CF is thus seen to delineate the frontier of quantum cryptography with many interesting questions still remaining open, such as what are the optimal biases achievable given a fixed number of rounds of communication. In this paper, we push the boundaries of the frontier further by generalizing the problem of quantum CF to more than two outcomes and parties, which we term dice rolling (DR). We see that DR constitutes another example of

2 Prior to Mochon’s work [17], there were serious doubts as to the possibility of weak CF with arbitrarily small bias. Quantum gambling was introduced as an example of a quantum cryptographic task, impossible in classical settings, which is nevertheless unconditionally secure. Unlike coin flipping, where both parties are supposed to follow the directions of an agreed protocol or else risk being caught cheating, quantum gambling eliminates the notion of cheating in the sense that both the casino and the player do not have to follow any prescribed set of operations, but rather are allowed to do anything to maximize their gain.
a cryptographic problem that allows for a higher level of security in quantum settings than classically, and present both weak and strong optimal DR protocols. In the process, we also obtain novel results regarding imbalanced CF and remote string-generation; in particular, since strong DR can always be used to generate a random string between any number of remote distrustful parties and vice versa, the bounds that we obtain for strong DR also apply to remote string-generation. Formally, we define the problem of DR as follows:

**Definition 1.** (weak DR). Weak \(N\)-sided DR is defined as the problem of \(N\) remote distrustful parties having to decide on a number between 1 and \(N\), such that: (i) each party is aware of any other party’s preferred outcome. In particular, no two or more parties may share the same preference. (ii) If all parties are honest the probability of each outcome is equal to \(1/N\).

Hence, in complete analogy with weak CF there is always a winner and \(N - 1\) losers.

**Definition 2.** (strong DR) \(M\)-party strong \(N\)-sided DR is defined as the problem of \(M\) remote distrustful parties having to decide on a number between 1 and \(N\), such that: (i) no party is aware of any other party’s preferred outcome. In particular, any number of parties may share the same preference. (ii) If all parties are honest the probability of each outcome is equal to \(1/N\).

(Note that these definitions reduce to those of CF in the case of two outcomes and parties.) Finally, we mention that both weak and strong DR have been extensively studied in classical settings [22], where they are commonly referred to as leader election: their importance arising from the necessity for randomization among remote parties in cryptography [23] and in fault-tolerant distributed computation [24].

The paper is organized as follows. In section 2, we prove that, using quantum resources, weak \(N\)-sided DR with arbitrarily small bias is possible for any value of \(N\). This result stands in marked contrast to the classical case, where, under certain conditions, an honest party always loses. To have some indication as to what biases are achievable with a finite number of rounds of communication, we then proceed to analyze a six-round three-sided DR protocol. In section 3, we generalize Kitaev’s bound to any number of parties, \(M\), and outcomes, \(N\), and present a family of two-party protocols that saturate it for any value of \(N\). We then make use of this family to extend this result to \(2m\)-party \(n\)-sided DR for any value of \(m\) and \(n\). In the process, we generalize Chailloux and Kerenidis’ optimal strong CF protocol to cover the imbalanced case as well. We complete our investigation of strong DR by analyzing a family of three-round two-party strong \(N\)-sided DR protocols. Finally, in section 4 we discuss the feasibility of quantum DR with current state-of-the-art technology.

### 2. Weak DR with arbitrarily small bias

The purpose of weak CF is to decide between two parties. Hence, its natural multi-outcome generalization is the problem of deciding between \(N > 2\) parties. As opposed to weak CF, in

---

\(^3\) According to Definitions I and II, weak DR is characterized by a single parameter \(N\), while strong DR is characterized by an additional parameter \(M\). The reason for this apparent discrepancy is due to the fact that if we were to carry out weak \(N\)-sided DR for \(M > N\) parties, then \(M - N\) of the outcomes would be redundant as no party would attempt to bias them. On the other hand, if we were to carry out weak \(N\)-sided DR for a number of parties \(M < N\) then at least two different parties would prefer the same outcome. The problem then effectively translates to weak imbalanced \(M\)-sided DR.
weak $N > 2$-sided DR there are many different cheating scenarios, as any number of parties $n < N$ may be dishonest. We shall be interested in the $N$ ‘worst-case’ scenarios where all but one of the parties are dishonest and, moreover, are acting in unison. That is, the dishonest parties share classical and quantum communication channels and have a joint strategy. In addition, we shall require that the protocol be ‘fair’ in the sense that the honest party’s maximum losing probability should be the same in each of these $N$ scenarios. Of course, the security of the protocol can be evaluated with respect to any other cheating scenario, but as we shall consider only fair protocols, the security of any cheating scenario is never poorer than that provided by the aforementioned $N$ worst-case scenarios.

We begin by observing that in CF, the bias has a complementary definition. Concentrating on weak CF, we could just as well define it as

$$\bar{\epsilon}_i = \bar{P}_i^* - 1/2, \quad i = A, B,$$

where $\bar{P}_i^* = P_{j\neq i}^*$ is the maximum probability that party $i$ loses. According to this definition the bias tells us to what extent party $j \neq i$ can increase party $i$’s chances of losing beyond one half. In the case of $N$ parties, the bias $\bar{\epsilon}_i$ then tells us to what extent the $N - 1$ dishonest parties can increase party $i$’s chances of losing beyond $1 - 1/N$, rather than to what extent a sole dishonest party can increase its chances of winning beyond $1/N$. We shall always use this redefinition of the bias when considering weak DR. The computation of biases in weak DR is therefore equivalent to the computation of biases in a weak imbalanced CF protocol.

2.1. Weak DR with arbitrarily small bias

**Theorem 1.** (Optimal weak $N$-sided DR). For any $0 < \delta$ a weak $N$-sided DR protocol can be formulated such that an honest party is guaranteed a $1/N - \delta$ probability of winning.

**Proof.** The proof is by construction. Consider the following $N$-party protocol. Each party is uniquely identified according to a number from 1 to $N$, with party $i$ preferring the $i$th outcome. The protocol consists of $N - 1$ stages. In stage one, parties one and two ‘weakly flip’ a balanced quantum coin. The winner and party three then weakly flip an imbalanced quantum coin in stage two, where if both parties are honest three’s winning probability equals $1/3$. And so on, the rule being that in stage $n \geq 2$ the winner of stage $n - 1$ and party $n + 1$ ‘weakly flip’ an imbalanced quantum coin, where if both parties are honest, $n + 1$’s winning probability equals $1/(n + 1)$. Thus, if all parties are honest each has the same overall winning probability of $1/N$. Using Mochon’s formalism [17], Chailloux and Kerenidis have recently proved that weak imbalanced CF with arbitrarily small bias is possible [18]. It follows that in the limit where each of the weak imbalanced CF protocols, used to implement our DR protocol, admits a vanishing bias (and $N$ is finite), any honest party’s winning probability tends to $1/N$. For a more formal proof, see appendix A. Finally, we note that since we have considered the worst-case cheating scenario, this result holds for any other cheating scenario.

The above result stands in stark contrast to the classical case, where if the number of honest parties is not strictly greater than $N/2$, then the dishonest parties can force any outcome they desire. To see why this is so, let us consider a classical $N$-sided DR protocol and partition the parties into two groups of $m \leq [N/2]$ and $n = N - m$ parties. If both groups are honest, the probability that a party in the first (second) group wins is $m/N$ ($1 - m/N$). Therefore, any weak
DR protocol can serve as a weak imbalanced CF protocol. Suppose now that all of the parties in the second group are dishonest, and are nevertheless unable to force with certainty the outcome they choose. Clearly, this would still be the case even if they were the smaller group, i.e. $n < m \ (m > \lfloor N/2 \rfloor)$, and we obtain a contradiction, since in classical weak imbalanced CF (as in the balanced case) at least one of the parties is always able to force whichever outcome they desire.\footnote{See, for example, the proof in \cite{25} even though this proof formally covers only the balanced case, its reasoning is also applicable to the imbalanced case.}

2.2. A six-round weak three-sided DR protocol

We have just seen that weak DR with arbitrarily small bias is possible given an unlimited number of rounds of communications. The question arises as to what is the optimal bias given some finite number of rounds of communication. Unfortunately, at present this question has no answer even for CF. Nevertheless to obtain some intuition as to what biases can be obtained, we shall now analyze a six-round weak three-sided protocol following the general construction we have just presented. Different biases will be obtained depending on the biases of the weak imbalanced CF protocol employed in each stage. To this end we start by introducing a three-round weak imbalanced CF protocol based on quantum gambling.

2.2.1. A three-round weak imbalanced CF protocol. The protocol is constructed such that if both parties are honest, Alice’s winning probability equals $1 - p$. Interestingly, it turns out that this protocol coincides with the generalization of Spekkens and Rudolph’s work \cite{14} to the imbalanced case. The protocol reads as follows:

- Alice prepares a superposition of two qubits
  \[
  \ket{\psi_0} = \sqrt{1 - p - \eta} \ket{\uparrow_1 \downarrow_2} + \sqrt{p + \eta} \ket{\downarrow_1 \uparrow_2}, \quad 0 \leq \eta \leq 1 - p, \tag{3}
  \]
  where the subscripts serve to distinguish between the first and second qubit and will be omitted when the distinction is clear. She then sends the second qubit to Bob.

- Bob carries out a unitary transformation $U_\eta$ on the qubit he received and another qubit (labeled by the subscript 3) prepared in the state $\ket{\downarrow}$ such that
  \[
  \ket{\uparrow_2 \downarrow_3} \rightarrow U_\eta \ket{\uparrow_2 \downarrow_3} = \sqrt{\frac{p}{p + \eta}} \ket{\uparrow_2 \downarrow_3} + \sqrt{\frac{\eta}{p + \eta}} \ket{\downarrow_2 \uparrow_3}, \tag{4}
  \]
  and
  \[
  \ket{\downarrow_2 \uparrow_3} \rightarrow U_\eta \ket{\downarrow_2 \uparrow_3} = \sqrt{\frac{\eta}{p + \eta}} \ket{\uparrow_2 \downarrow_3} - \sqrt{\frac{p}{p + \eta}} \ket{\downarrow_2 \uparrow_3}, \tag{5}
  \]
  with $U_\eta$ acting trivially on all other states. The resulting state is then
  \[
  \ket{\psi_1} = U_\eta \ket{\psi_0} = \sqrt{1 - p - \eta} \ket{\uparrow_1 \downarrow_2 \downarrow_3} + \sqrt{p} \ket{\downarrow_1 \uparrow_2 \downarrow_3} + \sqrt{\eta} \ket{\downarrow_1 \downarrow_2 \uparrow_3}. \tag{6}
  \]
  Following this, he checks whether the second and third qubits are in the state $\ket{\uparrow_2 \downarrow_3}$.

- Bob wins if he finds the qubits in the state $\ket{\uparrow_2 \downarrow_3}$. Alice then checks whether the first qubit is in the state $\ket{\downarrow}$, in which case Bob passes the test. If Bob does not find the qubits in the
state $|\uparrow_2 \downarrow_3\rangle$, he asks Alice for the first qubit and checks whether all three qubits are in the state
\[
|\xi\rangle = \sqrt{1-p-\eta} |\uparrow_1 \downarrow_2 \downarrow_3\rangle + \sqrt{\frac{\eta}{1-p}} |\downarrow_1 \uparrow_2 \uparrow_3\rangle,
\]
in which case she passes the test.

As proved in appendix B, Alice’s maximal winning probability is given by
\[
P^*_A = \max_{\delta} \left( \sqrt{\frac{(1-p-\eta)(1-\delta)}{1-p}} + \sqrt{\frac{\eta^2 \delta}{(1-p)(p+\eta)}} \right)^2, \quad \delta \in [0, 1],
\]
while Bob’s maximal winning probability is given by
\[
P^*_B = p + \eta.
\]
In the balanced case, a protocol is fair if $P^*_A = P^*_B$. We can play with $\eta$ to make $P^*_A$ and $P^*_B$ minimal under this constraint. It is easy to show that the minimum is then obtained for $\eta = (\sqrt{2} - 1)/2$. It follows that $\epsilon_A = \epsilon_B = (\sqrt{2} - 1)/2$ and $P^*_A = P^*_B = 1/\sqrt{2}$.

2.2.2. A six-round weak three-sided DR protocol with a bias of 0.181. The protocol consists of two three-round stages. In the first stage, Alice and Bob weakly flip a balanced quantum coin. Following this, in the second stage, the winner and Claire weakly flip an imbalanced quantum coin, such that if both parties are honest Claire’s winning probability equals $1/3$. The protocol is considered ‘fair’ if $P^*_A = P^*_B = P^*_C$. Due to the protocol’s symmetry with respect to the interchange of Alice and Bob, there are only two nonequivalent worst-case scenarios, i.e. either only Alice is honest or only Claire is honest. Using the quantum gambling-based protocol, an honest Alice has a maximum chance of $1 - 1/\sqrt{2}$ of progressing to the second stage. Therefore, Alice’s maximum losing probability is given by
\[
\bar{P}^*_A = \frac{1}{\sqrt{2}} + \left(1 - \frac{1}{\sqrt{2}}\right) \bar{P}^*_{1/3},
\]
while an honest Claire’s maximum losing probability is given by
\[
\bar{P}^*_C = \bar{P}^*_{1/3},
\]
with $\bar{P}^*_{1/3}$ ($\bar{P}^*_{2/3}$) the maximum losing probability of the party with a winning probability of $1/3$ ($2/3$) when both parties are honest. Hence, we require that
\[
\bar{P}^*_{1/3} = \frac{1}{\sqrt{2}} + \left(1 - \frac{1}{\sqrt{2}}\right) \bar{P}^*_{2/3}.
\]

If we use the weak CF protocol of the previous section to implement the second stage, then $\bar{P}^*_{1/3}$ and $\bar{P}^*_{2/3}$, and hence the $\bar{P}^*_i$, will depend on $\eta$. We then have to minimize the $\bar{P}^*_i$ with respect to $\eta$ under the constraint that they are all equal, or minimize $\bar{P}^*_{1/3}$ under the constraint equation (13). However, there are two possible implementations. Either $1 - p = 2/3$ and the second stage begins with Alice preparing the state $\sqrt{2/3 - \eta} |\uparrow_1 \downarrow_2\rangle + \sqrt{1/3 + \eta} |\downarrow_1 \uparrow_2\rangle$, or else $1 - p = 1/3$
and the second stage begins with Claire preparing the state $\sqrt{1/3 - \eta} |\uparrow_1 \downarrow_2 \rangle + \sqrt{2/3 + \eta} |\downarrow_1 \uparrow_2 \rangle$. In the first case we have to compute

$$\min \max_{\eta} \frac{1}{2} \left( \sqrt{(2 - 3\eta)} (1 - \delta) + \frac{9\eta^2 \delta}{(1 + 3\eta)} \right)^2$$

under the constraint that

$$\max_{\delta} \frac{1}{2} \left( \sqrt{(2 - 3\eta)} (1 - \delta) + \frac{9\eta^2 \delta}{(1 + 3\eta)} \right)^2 = \frac{1}{\sqrt{2}} + \left( 1 - \frac{1}{\sqrt{2}} \right) \left( \frac{1}{3} + \eta \right),$$

while in the second case we have to compute

$$\min_{\eta} \left( \frac{2}{3} + \eta \right)$$

under the constraint that

$$\left( \frac{2}{3} + \eta \right) = \frac{1}{\sqrt{2}} + \left( 1 - \frac{1}{\sqrt{2}} \right) \max_{\delta} \left( \sqrt{(1 - 3\eta)} (1 - \delta) + \sqrt{9\eta^2 \delta / (2 + 3\eta)} \right).$$

The first of these yields the lower bias $\bar{\epsilon}_A = \bar{\epsilon}_B = \bar{\epsilon}_C \simeq 0.181$ corresponding to $\bar{P}_A^* = \bar{P}_B^* = \bar{P}_C^* \simeq 0.848$. The second yields a bias of 0.199.

3. Optimal two-party strong DR and beyond

In this section, we consider the problem of $M$ remote distrustful parties having to decide on a number between 1 and $N > 2$, without any party being aware of any other’s preference. We generalize Kitaev’s bound, equation (2), to apply to this case as well, and present a protocol that saturates it for $M = 2m$ parties and $N = n^m$ outcomes for any value of $m$ and $n$. In particular, this implies the possibility of optimal two-party strong $N$-sided DR protocols for any value of $N$. To this end we also introduce a protocol that saturates Kitaev’s bound for strong imbalanced CF:

$$P_A^{(i)^*} \cdot P_B^{(i)^*} \geq P_i, \quad i \in \{0, 1\},$$

where $P_i$ is the probability of the outcome $i$ in an honest execution of the protocol.

**Theorem 2.** (Generalization of Kitaev’s bound): Denote by $\tilde{P}_j^{(i)^*}$ the probability in a strong DR-protocol for the outcome $i$ when all parties but the $j$th are dishonest and acting in unison to force it. Any $M$-party strong $N$-sided DR protocol must satisfy

$$\tilde{P}_A^{(i)^*} \cdot \tilde{P}_B^{(i)^*} \cdot \ldots \cdot \tilde{P}_M^{(i)^*} \geq \frac{1}{N^i}, \quad i \in \{1, \ldots, N\}.$$

**Proof.** It is straightforward to adapt the original proofs of Kitaev’s bound [13, 19] to cover more than two parties and outcomes. Instead, we follow a slightly different route by noting that strong DR can always be used to implement strong imbalanced CF. In particular, let us consider an $M > 2$-party strong $N$-sided DR protocol. The probability for each of the outcomes in an
honest execution is \( P_i = 1/N \). Suppose that we take the first \( N - 1 \) outcomes (last outcome) to represent \( 0 \) (1) in an \( M \)-party strong imbalanced CF protocol, such that there is an \((N - 1)/N\) probability of obtaining \( 0 \) in an honest execution. Kitaev’s bound can be generalized to cover this case as well and reads

\[
\bar{P}_i^{(1)} \cdot \bar{P}_i^{(2)} \cdots \bar{P}_i^{(M)} \geq 1/N \quad [19].
\]

It follows that this bound should apply to \( M \)-party strong \( N \)-sided DR as well (otherwise we get a contradiction). That is, equation (18) must be satisfied. In the case of a protocol that is ‘fair’, i.e. for any value of \( i \), \( j \), \( k \) and \( l \)

\[
\bar{P}_i^{(j)} = \bar{P}_k^{(l)},
\]

we then have that

\[
q \geq \left( \frac{1}{N} \right)^{1/M},
\]

where \( q \) now denotes the maximal probability of any group of \( M - 1 \) parties to bias the result to any of the outcomes. \( \square \)

To prove that the above bound can be saturated, we need to assume the existence of a strong imbalanced CF protocol saturating Kitaev’s bound, equation (17). We therefore begin by presenting such a protocol, based on Chailloux and Kerenidis’ optimal strong CF protocol.

### 3.1. Optimal strong imbalanced CF

**Theorem 3.** (Optimal strong imbalanced CF). For any \( 0 < P_0 < 1 \) and \( 0 < \delta \) a strong imbalanced CF protocol can be formulated such that in an honest execution of the protocol the probability of the outcomes 0 and 1 equals \( P_0 \) and \( 1 - P_0 \), and the probability of a dishonest party to bias the outcome to 0 and 1 is bounded from above by \( \sqrt{P_0 + \delta} \) and \( \sqrt{1 - P_0 + \delta} \).

**Proof.** Once again the proof is by construction. Consider the following protocol:

- Alice flips an imbalanced coin such that she obtains 0 with probability \( q \) and obtains 1 with probability \( 1 - q \), and sends the outcome \( o \) to Bob.
- If \( o = 0 \) Alice and Bob carry out an optimal imbalanced weak CF protocol, where if both parties are honest Alice wins with probability \( z_0 \) and Bob wins with probability \( 1 - z_0 \). If \( o = 1 \) they carry out an optimal imbalanced weak CF protocol, where if both parties are honest Alice wins with probability \( z_1 \) and Bob wins with probability \( 1 - z_1 \).
- If Alice wins the (weak) coin flip, the outcome of the (strong CF) protocol is \( o \).
- If Bob wins the coin flip, then he flips an imbalanced coin, whose degree of imbalance is dependent on \( o \). When \( o = 0 \), Bob flips an imbalanced coin such that its outcome is equal to 0 (1) with probability \( p_0 (1 - p_0) \). When \( o = 1 \), Bob flips an imbalanced coin such that its outcome equals 1 (0) with probability \( p_1 (1 - p_1) \). The outcome of this last coin flip is the outcome of the protocol. \( \square \)

Denoting by \( P_i \) the probability of the outcome \( i \) when both parties are honest, we have that

\[
P_0 = q \left( z_0 + (1 - z_0) p_0 \right) + (1 - q) \left( 1 - z_1 \right) \left( 1 - p_1 \right)
\]

and \( P_1 = 1 - P_0 \). This protocol differs from Chailloux and Kerenidis’ protocol in that in the first round Alice performs an imbalanced coin flip rather than a balanced one and, dependent on its
outcome, she and Bob carry out different weak imbalanced CF protocols. In addition, if Bob wins, dependent on the value of \( o \), he flips one of two different coins. Thus, instead of two free parameters we now have five. It is this extra freedom that allows the generalization to any degree of imbalance.

To obtain the biases, suppose that a dishonest Alice tries to bias the outcome to 0. There are two ways in which this can be achieved, either by announcing that she has obtained \( o = 0 \) or by announcing that she obtained \( o = 1 \). In the first case, her maximal probability of success equals

\[
P_A^{(0)^r} = z_0 + \epsilon_0 + (1 - z_0 - \epsilon_0) p_0, \tag{21}
\]

where \( \epsilon_0 \ll 1 \) is the bias of the weak imbalanced CF that is carried out when Alice inputs 0, while in the second case her maximal probability of success equals

\[
Q_A^{(0)^r} = 1 - p_1. \tag{22}
\]

Similarly, if Alice tries to bias the outcome to 1, her maximal probabilities of success equal

\[
P_A^{(1)^r} = z_1 + \epsilon_1 + (1 - z_1 - \epsilon_1) p_1, \tag{23}
\]

where \( \epsilon_1 \ll 1 \) is the bias of the weak imbalanced coin flip, which is performed whenever Alice inputs 1, and

\[
Q_A^{(1)^r} = 1 - p_0. \tag{24}
\]

Suppose now that a dishonest Bob tries to bias the outcome to 0. Given that in the first stage Alice outputs 0 (1) with probability \( q \ (1 - q) \), Bob’s maximal probability of success is given by

\[
P_B^{(0)^r} = q + (1 - q) (1 - z_1 + \epsilon_1), \tag{25}
\]

while if he tries to bias the outcome to 1, his maximal probability of success is given by

\[
P_B^{(1)^r} = 1 - q + q (1 - z_0 + \epsilon_0). \tag{26}
\]

For ideal weak imbalanced CF (i.e. \( \epsilon_0 = \epsilon_1 = 0 \)), this construction allows for Kitaev’s bound to be exactly attained. This can be seen by imposing the following four constraints:

\[
P_A^{(i)^r} = Q_A^{(i)^r}, \quad i \in \{0, 1\}, \tag{27}
\]

\[
P_A^{(i)^r} = P_B^{(i)^r}, \quad i \in \{0, 1\}. \tag{28}
\]

Solving these equations together with equation (20) we obtain

\[
q = \frac{1}{2} \left( 1 + \sqrt{P_0} - \sqrt{P_1} \right), \tag{29}
\]

\[
p_0 = 1 - \sqrt{P_1}, \quad p_1 = 1 - \sqrt{P_0}, \tag{30}
\]

\[
z_1 = 1 + \frac{\sqrt{P_0} - 1}{\sqrt{P_1}}, \quad z_2 = 1 + \frac{\sqrt{P_1} - 1}{\sqrt{P_0}}. \tag{31}
\]

Note that for \( P_i \in [0, 1] \) \( q, z_i \) and \( p_i \) are also in the required range of values, i.e. \( [0, 1] \). Substituting back into equations (21) to (26), we obtain

\[
P_A^{(0)^r} = P_B^{(0)^r} = \sqrt{P_0}, \quad P_A^{(1)^r} = P_B^{(1)^r} = \sqrt{P_1}. \tag{32}
\]
Returning to the non-ideal case, using for $q$, the $z_i$, and the $p_i$ the values just obtained, from equations (21) to (26) we have that

$$P_A^{(0)^*} = Q_A^{(0)^*} + \epsilon_0 \sqrt{P_1} = \sqrt{P_0} + \epsilon_0 \sqrt{P_1}, \quad P_A^{(1)^*} = Q_A^{(1)^*} + \epsilon_1 \sqrt{P_0} = \sqrt{P_1} + \epsilon_1 \sqrt{P_0},$$

(33)

$$P_B^{(0)^*} = \sqrt{P_0} + \frac{1}{2} \epsilon_1 (1 - \sqrt{P_0} + \sqrt{P_1}), \quad P_B^{(1)^*} = \sqrt{P_1} + \frac{1}{2} \epsilon_0 (1 + \sqrt{P_0} - \sqrt{P_1}).$$

(34)

(Note that we no longer require that the constraints given by equations (27) and (28) are satisfied.) Since the $\epsilon_i$ can be made arbitrarily small, it follows that the protocol saturates Kitaev’s bound for any degree of imbalance.

3.2. Optimal two-party strong DR

**Theorem 4.** (Optimal two-party strong DR). For any $0 < \delta$ a two-party strong $N$-sided DR protocol can be formulated such that a dishonest party’s probability of biasing any of the outcomes is bounded from above by $1/\sqrt{N} + \delta$.

**Proof.** Equipped with the above result, we proceed to prove the possibility of two-party strong $N$-sided DR saturating Kitaev’s bound for any value of $N$. Consider the following strong $N$-sided DR protocol. In the first stage the parties carry out a strong imbalanced CF protocol such that there is an $\lceil N/2 \rceil /N$ ($\lfloor N/2 \rfloor /N$) probability for the outcome 0 (1). If the outcome of the coin flip is 0 (1), then they agree that the DR protocol’s outcome is (is not) going to lie between 1 and $\lceil N/2 \rceil$. Suppose that the first coin flip results in 0. Then in the second stage they ‘strongly’ flip another coin such that there is an $\lceil \lceil N/2 \rceil /2 \rceil / \lceil N/2 \rceil$ ($\lfloor \lfloor N/2 \rfloor /2 \rfloor / \lfloor N/2 \rfloor$) probability for the outcome 0 (1). If the outcome is 0 (1), then they agree that the DR protocol’s outcome is going to lie between 1 and $\lceil \lceil N/2 \rceil /2 \rceil$ ($\lfloor \lfloor N/2 \rfloor /2 \rfloor + 1$ and $\lceil N/2 \rceil$), and so on, until they obtain a single result (see figure 1). The probability of obtaining 1 in an honest execution equals

$$\frac{\lceil N/2 \rceil}{N}, \frac{\lceil \lceil N/2 \rceil /2 \rceil}{\lceil N/2 \rceil}, \ldots, \frac{1}{\lfloor \lfloor N/2 \rfloor /2 \rfloor \cdots /2} = \frac{1}{N}.$$  

(35)

It is straightforward to verify that this probability is true of all other outcomes. Let us now consider a dishonest execution of the protocol such that the biases of the underlying strong imbalanced CF protocols are all equal to $\delta \ll 1/\log_2 N$. The probability of obtaining the outcome 1 is given by

$$\left(\sqrt{\frac{\lceil N/2 \rceil}{N}} + \delta\right) \left(\sqrt{\frac{\lceil \lceil N/2 \rceil /2 \rceil}{\lceil N/2 \rceil}} + \delta\right) \cdots \left(\sqrt{\frac{1}{\lfloor \lfloor N/2 \rfloor /2 \rfloor \cdots /2}} + \delta\right)$$

$$\simeq \frac{1}{\sqrt{N}} + c \left[ \log_2 N \right] \delta + O \left( \delta^2 \right),$$

(36)

where $c \sim \sqrt{2/\log_2 N}$. (The formal proof follows along the same lines as that given for weak DR in section 2, and so is omitted.) Similar expressions can be obtained for the probabilities of all other outcomes. Hence, we have shown that this construction saturates the generalization of Kitaev’s bound, equation (18), for $M = 2$ and any $N$.  

Figure 1. Two-party strong five-sided DR protocol saturating Kitaev’s bound. The digits inside the boxes denote the possible outcomes. Each branching represents a strong imbalanced coin flip. The fractions beside each branch give the probability for the outcomes within the box below, conditional on the outcomes in the box above. Thus, for the leftmost branch we find that the probability for outcome 1 equals $1/2 \cdot 2/3 \cdot 3/5 = 1/5$, etc.

3.3. A family of optimal multi-party strong DR protocols

The above construction readily allows for the introduction of a family of $2m$-party strong $n^m$-sided DR protocols saturating the generalization of Kitaev’s bound, equation (18).

**Corollary** (Optimal $2m$-party strong $n^m$-sided DR). For any $0 < \delta$ a $2m$-party strong $n^m$-sided DR protocol can be formulated such that dishonest parties’ probability of biasing any of the outcomes is bounded from above by $1/\sqrt{n^m} + \delta$.

**Proof.** The idea is to sequentially have distinct pairs of parties strongly roll a dice to eliminate some of the outcomes, until a single outcome is obtained. Thus, in the case of four parties and nine outcomes, in the first stage the first and second parties strongly roll a three-sided dice. If its outcome is 1, outcomes 4 to 9 are eliminated, while if its outcome is 2, outcomes 1 to 3 and 7 to 9 are eliminated, etc. Suppose, for example, that outcomes 1 to 6 are eliminated. Then in the second stage parties three and four strongly roll a three-sided dice, where if its outcome is 1, then the final outcome of the protocol is 7, while if its outcome is 6, then the final outcome is 8, etc. In general, for $2m$-parties and an $n^m$-sided dice, the protocol consists of $n$ stages. In each stage a different pair of parties strongly rolls an $n$-sided dice. As there are a total of $2m$ parties, each party participates in a dice roll once. In order to force the outcome they desire, the $2m - 1$ dishonest parties must bias the result of the dice roll in which the honest party participates, and since at any stage there is only a single outcome that can lead to the desired outcome, the dishonest parties can maximally bias the outcome with a probability of $(1/n)^{1/2} + \bar{\epsilon}$, which saturates the generalization of Kitaev’s bound, equation (18). \(\Box\)

It is not straightforward to generalize this scheme to any number of parties and outcomes. The problem is that we have introduced an ordering, which, dependent on it, may in general
render the protocol asymmetric in the biases, or even trivial by allowing the dishonest parties to force the outcome that they desire. This can be fixed by making use of optimal weak DR to decide the ordering. Unfortunately, this comes at the expense of optimality, i.e. equation (18) is no longer saturated. Nevertheless, protocols incorporating optimal weak and strong DR may give rise to biases remarkably close to the inherent bounds. As an example, consider the following three-party strong three-sided DR protocol. In the first round Alice, Bob and Claire weakly roll a three-sided dice. The winner then randomly selects a number \( a \in \{1, 3\} \) and informs the two losers of his/her choice. The two losers then strongly flip a coin. Denote its outcome by \( b \in \{0, 1\} \). The outcome of the protocol is \( (a + b) \mod 3 \). It is easy to verify that the maximal probability of any two parties to successfully bias any of the outcomes approximately equals 0.693 63, while from equation (19) \( q = (1/3)^{1/3} \simeq 0.693 36 \). That is, a difference of 0.027 \%. Similarly to the optimal 2\( m \)-party \( n \)-sided DR protocols described above, this protocol can be generalized to a family of 3\( n \)-party 3\( n \)-sided DR protocols, with each giving rise to the same bias.

To complete the discussion, we should mention that strong DR is nontrivial also in classical settings. Indeed, the classical biases for two-party \( N \)-sided DR are constrained by the following set of inequalities [13]:

\[
(1 - \tilde{P}_A^{(i^*)})(1 - \tilde{P}_B^{(j^*)}) \leq \frac{N - 2}{N} + \frac{1}{N^2} \delta_{i,j}, \quad i, j \in \{1, \ldots, N\}.
\]

It is straightforward to verify that these inequalities are ‘weaker’ than the corresponding Kitaev bound, and hence allow for higher biases.

3.4. A family of three-round two-party strong DR protocols

In this subsection, we introduce a family of three-round strong DR protocols, which generalizes Colbeck’s entanglement-based strong CF protocol [26] to any number of outcomes. Suppose Alice and Bob want to strongly roll an \( N \)-sided dice using the least amount of communication. They may proceed as follows. Alice prepares a pair of systems in the state \( |\psi_N\rangle \otimes |\psi_N\rangle \), where

\[
|\psi_N\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle \otimes |i\rangle,
\]

and sends the second half of each system to Bob. Bob randomly selects one of the systems to serve as the dice and informs Alice of his selection. Alice and Bob then measure their half of the selected system in the Schmidt basis. The outcome of this measurement is the outcome of the dice roll. Finally, Alice sends Bob her half of the system that was not selected, and he verifies it was indeed prepared in the state \( |\psi_N\rangle \).

Generalizing Colbeck’s proof (see appendix C), Alice’s and Bob’s maximal probabilities of biasing to any of the outcomes are given by

\[
P_A^{(i^*)} = \frac{N + 1}{2N}, \quad P_B^{(i^*)} = \frac{2N - 1}{N^2}, \quad \{i = 1, \ldots, N\}.
\]

Thus, for \( N = 3 \), \( \epsilon_A^{(i)} = P_A^{(i^*)} - 1/3 = 1/3 \) and \( \epsilon_B^{(i)} = P_B^{(i^*)} - 1/3 = 2/9 \). Interestingly, in the limit where \( N \to \infty \), \( P_A^{(i^*)} \to 1/2, \quad P_B^{(i^*)} \to 2/N \), so that \( P_A^{(i^*)} \cdot P_B^{(i^*)} \to 1/N \). Hence, in this limit Kitaev’s bound is nontrivially saturated in a finite number of rounds, albeit at the cost of a high asymmetry of the biases.
4. Discussion

Before we conclude, we would like to examine the possibility of actually implementing quantum DR in the laboratory with a view toward practical applications. DR can always be carried out via two-party imbalanced CF. Hence, the question of the feasibility of quantum DR reduces to the question of the feasibility of quantum CF. Recently, two experiments were carried out showing that quantum CF is indeed feasible in ‘realistic’ settings [27, 28]. The success of these experiments rests on having overcome the problem of losses—by far the greatest source of malfunctions in the implementation of quantum protocols requiring communication over long distances. Indeed, the protocol employed in [28], first introduced in [29], is utterly impervious to losses or ‘loss-tolerant’ and gives rise to a bias of 0.4. In particular, it is readily generalized to cover the imbalanced case as well (see appendix D), thereby allowing us to realize any weak or strong DR protocol. To obtain an intuition for the numbers involved when utilized for DR, this protocol would, for example, enable us to carry out a two-party strong four-sided DR protocol with a bias of $0.9^2 - 0.25 \simeq 0.56$. Of course, the eventual availability of feasible quantum error correction protocols should eliminate the need for loss-tolerant protocols and dramatically decrease the gap between the biases achievable in theory and in practice, leading to far more secure implementations.

To summarize, we proved by construction that quantum mechanics allows for (i) weak $N$-sided DR admitting arbitrarily small bias for any $N$ and (ii) two-party strong $N$-sided DR saturating Kitaev’s bound for any $N$. To derive this last result, we also proved by construction that quantum mechanics allows for (iii) strong imbalanced CF saturating Kitaev’s bound for any degree of imbalance. Furthermore, we used the optimal two-party strong DR result to introduce a family of optimal $2m$-party strong $n^m$-sided DR protocols for any pair $m$ and $n$. The question of whether in the general case of any number of outcomes and parties there exist strong DR protocols saturating the corresponding generalization of Kitaev’s bound remains open for now.

Acknowledgments

We thank Dorit Aharonov, Oded Regev, Lev Vaidman and especially Serge Massar for useful comments. We also thank Ran Canetti for expounding to us on the importance of DR protocols in the construction of fault-tolerant distributed systems. NA acknowledges the support of the Wolfson Foundation. JS acknowledges support from the Israeli Science Foundation (grant no. 784/06) and the Inter-University Attraction Poles Programme (Belgian Science Policy) under Project IAP-P6/10 (Photonics@be). Both authors acknowledge the support of the European Commission under the Integrated Project Qubit Applications (QAP), funded by the IST Directorate (contract no. 015848).

Note added. After the publication of our results on the arXiv, an independently conceived work by Ganz appeared [30], which reproduces our weak DR result and improves upon its

---

5 As noted in [20], losses are especially problematic in quantum CF since they give rise to a finite probability of an indefinite outcome even in honest executions. The problem can be circumvented by having a protocol restarted in the event of an indefinite outcome, but this can be exploited by a dishonest party to significantly increase its bias, if not bias the outcome as it chooses. Indeed, except for [27, 29], all protocols in the literature become trivial if allowed to restart [29]. By loss-resistant we mean any protocol, which does not become trivial if allowed to restart, while by loss-tolerant we mean a protocol whose bias remains invariant when allowed to restart.
communication complexity by having some of the coin flips carried out in parallel rather than in succession. Hence, for a weak $N$-sided DR protocol where each coin flip takes $n$ rounds of communication, the communication complexity is reduced from $n(N - 1)$ to $\sim n \log N$.

Appendix A

Here we give a formal proof of Theorem 1 (section 2.1).

For any weak DR protocol, based on the weak imbalanced CF scheme of section 2, party $N > n$’s maximum chance of losing is the sum of the probabilities for losing in each of the stages $n - 1$ (the stage at which it becomes involved in the protocol) to $N - 1$ (the last stage). This probability is given by

$$\hat{P}_n^* = \hat{\Pi}_{n-1}^* + \sum_{k=n}^{N-1} \hat{\Pi}_k^* \prod_{j=0}^{k-n-1} (1 - \hat{\Pi}_{n-1+j}) = \frac{n-1}{n} + \bar{\delta}_{n-1} + \left( \frac{1}{n+1} + \delta_n \right) \left( 1 - \bar{\delta}_{n-1} \right) + \sum_{i=n+1}^{N-1} \left( 1 - \frac{1}{k+1} + \bar{\delta}_k \right) \left( 1 - \bar{\delta}_{n-1} \right) \prod_{j=1}^{k-n} \left( \frac{n+j}{n+j+1} - \bar{\delta}_{n-1+j} \right), \quad (A.1)$$

where $\hat{\Pi}_k^*$ is party $n$’s maximum chance of losing stage $k$, conditional on having made it to that round, and $\delta_k$ is the corresponding bias. Thus, each $\hat{\Pi}_k^*$ is multiplied by the probability that party $n$ has made it to stage $k$. Now the term independent of the $\bar{\delta}_k$ equals $(N - 1)/N$. Recalling that by definition $\hat{P}_n^* = (N - 1)/N + \bar{\epsilon}_n$ and letting $\bar{\delta}_{\max} = \max_k \delta_k$ and $\bar{\delta}_{\min} = \min_k \delta_k$ ($k = n - 1, \ldots, N - 2$), we find

$$\bar{\epsilon}_n \leq \bar{\delta}_{\max}(n) + \bar{\delta}_{\max}(n) \left( \frac{1}{n} - \bar{\delta}_{\min}(n) \right) - \bar{\delta}_{\min}(n) \left( \frac{1}{n+1} + \bar{\delta}_{\max}(n) \right) + \bar{\delta}_{\max}(n) \sum_{k=n+1}^{N-1} \left( \frac{1}{n} - \bar{\delta}_{\min}(n) \right) \prod_{j=1}^{k-n} \left( \frac{n+j}{n+j+1} - \bar{\delta}_{\min}(n) \right)$$

$$- \bar{\delta}_{\min}(n) \sum_{k=n+1}^{N-1} \left( \frac{1}{k+1} + \bar{\delta}_{\max}(n) \right) \prod_{j=1}^{k-n} \left( \frac{n+j}{n+j+1} - \bar{\delta}_{\min}(n) \right)$$

$$- \bar{\delta}_{\max}(n) \sum_{k=n+1}^{N-1} \left( \frac{1}{k+1} + \bar{\delta}_{\max}(n) \right) \left( \frac{1}{n} - \bar{\delta}_{\min}(n) \right) \prod_{j=m}^{k-n} \left( \frac{n+j}{n+j+1} - \bar{\delta}_{\min}(n) \right)$$

$$\leq \bar{\delta}_{\max}(n) + \bar{\delta}_{\max}(n) \frac{n}{n+1} \sum_{k=n+1}^{N-1} \frac{1}{k+1} \prod_{j=1}^{k-n} \frac{n+j}{n+j+1}$$

$$< N \bar{\delta}_{\max}(n). \quad (A.2)$$

Hence, if each of the weak imbalanced CF protocols, used to implement the DR protocol, are such that $\bar{\delta}_k \ll 1/N$, where now $k = 1, \ldots, N - 1$, an honest party’s (including party $N$) winning probability tends to $1/N$.

Appendix B

Here we give a proof of the biases, equations (8) and (9), for the weak imbalanced CF protocol discussed in section 2.2.

B.1 Alice’s maximal bias

Most generally Alice can prepare any state of the form

$$|\psi'_0\rangle = \sum_{i,j=\uparrow, \downarrow} \alpha_{ij} |ij\rangle \otimes |\Phi_{ij}\rangle,$$  

(B.1)

where the $|\Phi_{ij}\rangle$ are states of some ancillary system at her possession. After Bob applies $U_\eta$, the resulting composite state is given by

$$|\psi'_1\rangle = U_\eta |\psi'_0\rangle \otimes |\downarrow\rangle = \alpha_{\uparrow\uparrow} \left( \sqrt{\frac{p}{p+\eta}} |\uparrow\uparrow\downarrow\rangle + \sqrt{\frac{\eta}{p+\eta}} |\uparrow\downarrow\uparrow\rangle \right) \otimes |\Phi_{\uparrow\uparrow}\rangle + \alpha_{\downarrow\uparrow} \left( \sqrt{\frac{p}{p+\eta}} |\downarrow\uparrow\downarrow\rangle + \sqrt{\frac{\eta}{p+\eta}} |\downarrow\downarrow\uparrow\rangle \right) \otimes |\Phi_{\downarrow\uparrow}\rangle.$$  

(B.2)

The probability that Bob does not find the second and third qubits in the state $|\uparrow_2\downarrow_3\rangle$ is

$$\bar{P}_{\uparrow\downarrow} = 1 - P_{\uparrow\downarrow} = 1 - \frac{|\alpha_{\uparrow\uparrow}|^2 p + |\alpha_{\downarrow\uparrow}|^2 p}{p+\eta},$$  

(B.3)

and the resulting composite state is then

$$|\psi'_2\rangle = \mathcal{N} \left( \alpha_{\uparrow\uparrow} \sqrt{\frac{\eta}{p+\eta}} |\uparrow\uparrow\rangle \otimes |\Phi_{\uparrow\uparrow}\rangle + \alpha_{\downarrow\uparrow} |\uparrow\downarrow\rangle \otimes |\Phi_{\downarrow\uparrow}\rangle \right) + \alpha_{\downarrow\uparrow} \sqrt{\frac{\eta}{p+\eta}} |\downarrow\downarrow\rangle \otimes |\Phi_{\downarrow\uparrow}\rangle,$$  

(B.4)

where $\mathcal{N}$, the normalization, is

$$\frac{1}{\mathcal{N}^2} = 1 - \frac{p}{p+\eta} (|\alpha_{\uparrow\uparrow}|^2 + |\alpha_{\downarrow\uparrow}|^2).$$  

(B.5)

The probability that Alice passes the test is therefore given by

$$P_{\text{test}} = \| \langle \xi | \psi'_2 \rangle \|^2 = \mathcal{N}^2 \left| \alpha_{\uparrow\uparrow} \sqrt{\frac{1-p-\eta}{1-p}} |\Phi_{\uparrow\downarrow}\rangle + \alpha_{\downarrow\uparrow} \sqrt{\frac{\eta^2}{(1-p)(p+\eta)}} |\Phi_{\downarrow\downarrow}\rangle \right|^2.$$  

(B.6)

The maximum is obtained for $|\Phi_{\uparrow\downarrow}\rangle = |\Phi_{\downarrow\uparrow}\rangle$. This choice of the ancillary states does not affect the maximum of $P_{\uparrow\downarrow}$. Hence, Alice obtains no advantage by using ancillary systems, and we can eliminate them. Alice’s maximum cheating probability is then

$$P_A^* = \max_{\alpha_{ij}} \bar{P}_{\uparrow\downarrow} \cdot P_{\text{test}},$$  

(B.7)

where now

$$\bar{P}_{\uparrow\downarrow} \cdot P_{\text{test}} = \left| \alpha_{\uparrow\downarrow} \sqrt{\frac{1-p-\eta}{1-p}} + \alpha_{\downarrow\uparrow} \sqrt{\frac{\eta^2}{(1-p)(p+\eta)}} \right|^2.$$  

(B.8)
(\(P_{\uparrow\downarrow} = 1/N^2\)). Clearly, this expression is maximum when \(\alpha_{\uparrow\uparrow} = \alpha_{\downarrow\downarrow} = 0\). Therefore, to maximize her chance of successfully cheating, Alice will prepare a state of the form

\[
|\psi_0\rangle = \sqrt{1-\delta} \left| \uparrow_1 \downarrow_2 \right\rangle + \sqrt{\delta} \left| \downarrow_1 \uparrow_2 \right\rangle,
\]

where, with no loss of generality, we have set \(\alpha_{\uparrow\downarrow} = \sqrt{1-\delta}\) and \(\alpha_{\downarrow\uparrow} = \sqrt{\delta}\) so that

\[
P_A^* = \max_\delta \left( \frac{(1-p-\eta)(1-\delta)}{1-p} + \frac{\eta^2 \delta}{(1-p)(p+\eta)} \right)^2. \tag{B.10}
\]

### B.2 Bob’s maximal bias

Bob wins and passes the test whenever Alice does not find the first qubit in the state \(|\uparrow\rangle\). The probability for this is just \(p + \eta\). This gives an upper bound on Bob’s maximal cheating probability, which is attained if Bob always announces that he has won. That is,

\[
P_B^* = p + \eta. \tag{B.11}
\]

### Appendix C

Here we give a proof of the biases, equation (38), the strong DR protocol for section 3.4 given in).

#### C.1 Alice’s maximal bias

Suppose that Alice wants to bias the outcome to 1. Most generally, she will prepare a state of the form \(|\psi_N\rangle = \sum_{i=1}^N \sum_{j=1}^N a_{ij} |\phi_{ij}\rangle \otimes |i\rangle\), where the \(|i\rangle\) denote the states of the two \(N\)-level systems that she sends Bob, and the \(|\phi_{ij}\rangle\) denote the states of two \(N\)-level systems that she keeps and possible ancillary systems. Clearly, for any optimal choice of the \(a_{ij}\) and the \(|\phi_{ij}\rangle\), we can obtain another optimal choice by effecting, for example, the transformation \(a_{ij} \leftrightarrow a_{kj}\) \((i, k \neq j)\) or interchanging the two systems. Hence, with no loss of generality we may set \(a_{i1} = a_{1k} = c\) \((i, k \neq 1)\). Suppose now that Bob chooses the first \(N\)-level system to serve as the coin. Then the probability that he obtains 1 is just \((a_{11}^2 + (n-1)c^2)/N(1-p)\). Conditioned on this, the maximum probability that Alice is not caught cheating equals \((a_{11} + (N-1)c)/(N(\alpha_{11}^2 + (N-1)c^2))\). The same result applies in the case that Bob chooses the second system as the coin. Alice’s maximum winning probability is, therefore, given by \(\max_{a_{11},c}(a_{11} + (N-1)c)/N\) subject to the normalization condition \(a_{11}^2 + 2(N-1)c^2 = 1\), resulting in \((N+1)/2N\).

#### C.2 Bob’s maximal bias

Suppose that Bob wants to bias the outcome to 1. The number of terms in \(\sqrt{N} \sum_{i=1}^N |i\rangle \otimes |i\rangle\) (the maximally entangled two-qubit state prepared by Alice), in which neither of the two qubits is to be found in the state \(|1\rangle\), is \((N-1)^2\). Hence, Bob’s maximal bias is bounded from above by \(1 - (N-1)^2/N^2 = (2N-1)/N^2\).

### Appendix D

Here we give an adaptation of Berlín et al’s protocol to the imbalanced case such that the probability of 0 equals \(1 - 2p(1-p)\).
D.1 The protocol

- Alice prepares one of the states $|0_b\rangle = |\uparrow_n\rangle = |\uparrow_m\rangle$, $|0_b\rangle = |\uparrow_n\rangle = |\uparrow_m\rangle$ and $|1_b\rangle = |\downarrow_n\rangle$, $|1_b\rangle = |\downarrow_m\rangle$ with probabilities $p/2$ and $(1 - p)/2$, respectively, and sends it to Bob. Denote this state by $|s_b\rangle$ ($s = 0, 1, \hat{b} = \hat{n}, \hat{m}$).

- Bob chooses at random between the bases $\hat{n}$ and $\hat{m}$, and measures the qubit he received in the chosen basis. If he records no outcome, he asks Alice to repeat step 1; otherwise, he proceeds with the protocol.

- Bob sends Alice a classical bit $c$ having a value 0, 1 with probability $p$, $1 - p$, respectively.

- Alice reveals which state she has prepared to Bob.

- Bob aborts the protocol whenever Alice says that she has prepared a state orthogonal to the one he obtained.

- If Bob does not abort the protocol, the outcome of the coin flip is $s \oplus c$.

References


