Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®

Information Processing Letters 89 (2004) 131–135

Information Processing Letters

www.elsevier.com/locate/ipl

Weak coin flipping with small bias

I. Kerenidis [a,*,1], A. Nayak [b,2]

[a] *Computer Science Division, University of California, Berkeley, CA 94720, USA*
[b] *The Mathematical Sciences Research Institute, 1000 Centennial Drive, Berkeley, CA 94720-5070, USA*

Received 6 December 2002; received in revised form 21 July 2003

Communicated by P.M.B. Vitányi

Abstract

This paper presents a quantum protocol that demonstrates that *weak* coin flipping with bias ≈ 0.239, less than $1/4$, is possible. A bias of $1/4$ was the smallest known, and followed from the strong coin flipping protocol of Ambainis in [33rd STOC, 2001] (also proposed by Spekkens and Rudolph [Phys. Rev. A 65 (2002) 012310]). Protocols with yet smaller bias ≈ 0.207 have independently been discovered by Ambainis (2001) and Spekkens and Rudolph [Phys. Rev. Lett. 89 (2002) 227901]. We also present an alternative strong coin flipping protocol with bias $1/4$ with analysis simpler than that of Ambainis [33rd STOC, 2001].
© 2003 Elsevier B.V. All rights reserved.

Keywords: Quantum computation; Coin flipping; Cryptography; Algorithms; Quantum communication

1. Quantum weak coin flipping

In the classic example from [5], Alice and Bob are getting a divorce, and would like to decide who gets the car. They decide to toss a coin for that purpose, but don't trust each other. In such a scenario, instead of a coin tossing protocol, they could play any fair game to decide the issue. Motivated by this, we consider the following weaker version of coin flipping.

A *weak coin flipping* protocol with bias ε, is a two-party communication game in the style of Yao [13], in which the players start with no inputs, and compute a value $c_A, c_B \in \{0,1\}$ respectively or declare that the other player is cheating. The protocol is deemed successful if Alice and Bob agree on the outcome, i.e., $c_A = c_B$. Then, the outcome 0 is identified with Alice winning, and 1 with Bob winning. The protocol satisfies the following additional properties:

(1) If both players are honest (i.e., follow the protocol), then they agree on the outcome of the protocol: $c_A = c_B$, and the game is fair: $\Pr(c_A = c_B = b) = 1/2$, for $b \in \{0,1\}$.
(2) If one of the players is honest (i.e., the other player may deviate arbitrarily from the protocol in his or

* Corresponding author.
E-mail addresses: jkeren@cs.berkeley.edu (I. Kerenidis), nayak@msri.org (A. Nayak).

[1] Supported by Charles Lee Powell Foundation, and NSF grants CCR 0049092 and EIA 0086038.

[2] Most of this work was done while the author was at California Institute of Technology, Pasadena, CA, and was supported by Charles Lee Powell Foundation, and NSF grants CCR 0049092 and EIA 0086038.

0020-0190/$ – see front matter © 2003 Elsevier B.V. All rights reserved.
doi:10.1016/j.ipl.2003.07.007

her local computation), then the other party *wins* with probability at most $1/2+\varepsilon$. In other words, if Bob is dishonest, then $\Pr(c_A = c_B = 1) \leqslant 1/2+\varepsilon$, and if Alice is dishonest, then $\Pr(c_A = c_B = 0) \leqslant 1/2+\varepsilon$.

In a strong coin flipping protocol, the goal is instead to produce a random bit which is biased away from any particular value 0 or 1. Clearly, any strong coin flipping protocol with bias ε leads to weak coin flipping with the same bias. We may also derive a strong coin-flipping protocol from a weak one. A simple way to do this is to have the winner of the game flip the coin. This results in an increase in the bias of the protocol, however: if when one player, say Alice, is dishonest, and the other (Bob) honest, the probability of Alice winning is $p_w \geqslant 1/2$, and the probability of Bob winning is p_ℓ, then the coin will have bias $p_w + (p_\ell - 1)/2$.

The primitive of quantum strong coin flipping has been studied extensively, e.g., in [7,8,1,2,11]. The best known protocol, with bias $1/4 = 0.25$, is due to Ambainis [2], also independently proposed by Spekkens and Rudolph [11]. This note presents a protocol that demonstrates that *weak* coin flipping with bias ≈ 0.239, less than $1/4$, is possible. Our protocol is obtained by modifying the protocol of [2] especially so that the *winning* party is checked for cheating. We also describe a related strong coin flipping protocol with bias $1/4$ that has the advantage over [2] that the analysis is considerably simpler. A similar analysis for a class of cheating strategies has been given by [11].

Since the discovery of the above mentioned protocol, we have learnt of several exciting developments. Kitaev [6] has shown that in any protocol for *strong* coin flipping, the product of the probabilities with which each of the players can achieve outcome (say) 0, has to be at least $1/2$. Hence the protocols with arbitrarily small bias are not possible; the bias is always at least $1/\sqrt{2} - 1/2 \approx 0.207$. (Previous lower bounds applied only to certain kinds of protocol [2, 11,9].) Furthermore, Ambainis [4] and Spekkens and Rudolph [12] have constructed a family of protocols for *weak* coin flipping, where the product of the winning probabilities is exactly $1/2$. By making the winning probabilities equal, they get protocols in which each player wins with probability at most $1/\sqrt{2}$, and hence the bias is $1/\sqrt{2} - 1/2 \approx 0.207$. Subsequently, Ambainis [3] proved a lower bound of $1/2$ for the product of the winning probabilities for the specific class of protocols considered in [12]. We note that the lower bound of Kitaev for strong coin flipping does not apply here and hence quantum games of the weaker variety with even smaller bias may be possible.

The paper is organized as follows: In Section 2, we describe and analyze a weak coin flipping protocol with small bias. In Section 3, we present an alternative strong coin flipping protocol with bias $1/4$ and simpler analysis. For an introduction to Quantum Computation we refer the reader to [10].

2. A game with small bias

Below, we describe a weak coin flipping game that has bias less than $1/4$. The game is derived from the protocol of [2], which achieves the previously best known bias of $1/4$.

The protocol is parametrized by $\alpha \in [0,1]$, which we will optimize over later. For $x \in \{0,1\}$, define the state $|\psi_x\rangle = |\psi_x(\alpha)\rangle$ in a Hilbert space $\mathcal{H}_s \otimes \mathcal{H}_t = \mathbb{C}^3 \otimes \mathbb{C}^3$ as:

$$|\psi_x\rangle = \sqrt{\alpha}|xx\rangle + \sqrt{1-\alpha}|22\rangle. \tag{1}$$

The protocol has the following rounds:

(1) Alice picks $a \in_R \{0,1\}$, prepares the state $|\psi_a\rangle$ in $\mathcal{H}_s \otimes \mathcal{H}_t$ (i.e., over a pair of qutrits) and sends Bob the $\mathcal{H}_t$ qutrit.
(2) Bob picks $b \in_R \{0,1\}$ and sends it to Alice.
(3) Alice then reveals the bit a to Bob. Let $c = a \oplus b$. If $c = 0$, then $c_A \leftarrow 0$ and she sends the other part of the state $|\psi_a\rangle$ (the $\mathcal{H}_s$ qutrit). Bob checks that the qutrit pair he received in the first and the current rounds are indeed in state $|\psi_a\rangle$ by measuring according to the orthogonal projection operators $P_a = |\psi_a\rangle\langle\psi_a|$ and $I - P_a$. If the test is passed, Alice wins ($c_B \leftarrow 0$ as well), else Bob concludes that Alice has deviated from the protocol, and aborts.
(4) If, on the other hand, $c = a \oplus b = 1$, then $c_B \leftarrow 1$, and Bob returns the qutrit he received in round 1. Alice checks that her qutrits are in state $|\psi_a\rangle$ by measuring according to $\{P_a, I - P_a\}$. If the test is passed, Bob wins the game ($c_A \leftarrow 1$), else, Alice

concludes that Bob has tampered with her qutrit to bias the game, and aborts.

If the two players follow this protocol, the game is fair. We now analyze the situation where one of the players cheats.

Lemma 2.1. *If Bob is honest, then the probability that Alice wins* $\Pr(c_B = 0) \leqslant 1 - \alpha/2$.

Proof. We assume without loss of generality that a dishonest Alice tries to maximize her probability of winning, and therefore sends $a = b$ (so that $c = a \oplus b = 0$) in round 3. Her cheating strategy then takes the following form. Alice uses some ancillary space $\mathcal{H}$ and prepares some state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}_s \otimes \mathcal{H}_t$. She keeps the part of the state in $\mathcal{H} \otimes \mathcal{H}_s$ and sends the qutrit part in $\mathcal{H}_t$ to Bob. Let σ denote the density matrix of Bob after the first round of the protocol (i.e., of the $\mathcal{H}_t$ qutrit). Let ρ_a be the density matrix he would have if Alice had prepared the honest state $|\psi_a\rangle$:

$$\begin{aligned}\rho_a &= \mathrm{Tr}_{\mathcal{H}_s} |\psi_a\rangle\langle\psi_a| \\ &= \alpha|a\rangle\langle a| + (1-\alpha)|2\rangle\langle 2|.\end{aligned}$$

In the second round, Bob replies with a random bit b. So that she wins, Alice sends $a = b$ to Bob and subsequently tries to pass his check. For that, she performs some unitary operation U_b on her part of the state, and gets $|\tilde{\psi}_b\rangle = (U_b \otimes I)|\psi\rangle$. After that, she sends the part of the state in $\mathcal{H}_s$ to Bob. The final joint state can be written now as

$$|\tilde{\psi}_b\rangle = \sum_i \sqrt{p_i}|i\rangle|\tilde{\psi}_{i,b}\rangle.$$

As we see, at the end of the protocol Bob has the density matrix $\sigma_b = \sum_i p_i |\tilde{\psi}_{i,b}\rangle\langle\tilde{\psi}_{i,b}|$.

The probability that Alice wins the game is equal to the probability that she passes Bob's check at the end of the protocol, i.e., that Bob measures his part of the joint state and gets $|\psi_b\rangle$ as the outcome

$$\begin{aligned}&\Pr[\text{Alice wins} \mid \text{Bob sends } b] \\ &\quad= \sum_i p_i \big|\langle\psi_b|\tilde{\psi}_{i,b}\rangle\big|^2 \\ &\quad= F\big(\sigma_b, |\psi_b\rangle\langle\psi_b|\big) \\ &\quad\leqslant F\big(\mathrm{Tr}_{\mathcal{H}_s}(\sigma_b), \mathrm{Tr}_{\mathcal{H}_s}|\psi_b\rangle\langle\psi_b|\big) \\ &\quad= F(\sigma, \rho_b),\end{aligned}$$

where $F(\omega, \tau) = \|\sqrt{\omega}\sqrt{\tau}\|_{\mathrm{tr}}^2$ is the fidelity of two density matrices. Here, we have used the fact that the fidelity between two states can only increase when we trace out a part of the states. Note also that the state $\mathrm{Tr}_{\mathcal{H}_s}(\sigma_b)$ is equal to σ, which is independent of b.

Finally we have,

$$\begin{aligned}&\Pr[\text{Alice wins}] \\ &\quad\leqslant \tfrac{1}{2}\big[F(\sigma, \rho_0) + F(\sigma, \rho_1)\big] \\ &\quad\leqslant \tfrac{1}{2}\big[1 + \sqrt{F(\rho_0, \rho_1)}\big] \\ &\quad= 1 - \alpha/2.\end{aligned}$$

The second inequality is due to [11, Lemma 2], also [9, Lemma 3.2]. Moreover, $F(\rho_0, \rho_1) = (1-\alpha)^2$. This completes the proof. □

Note that the analysis above is tight in the sense that Alice can cheat with probability equal to $1 - \alpha/2$. She does this by preparing the state $|\psi_0\rangle + |\psi_1\rangle$ (normalized) and sending one qutrit to Bob in the first round. In the third round, she sends $a = b$, and the remaining qutrit from the above state.

If Bob is the dishonest player, we can show the following bound.

Lemma 2.2. *If Alice is honest, then* $\Pr(c_A = 1) \leqslant ((1-\alpha)/\sqrt{2} + \alpha)^2$.

Proof. A cheating Bob tries to infer the value of the bit a that Alice picked from the qutrit he receives in round 1 so that he can send $b = \bar{a} = 1 \oplus a$. However, he has to minimize the disturbance caused to the over all state $|\psi_a\rangle$. Suppose that Bob applies the unitary transformation U on $\mathcal{H}_t \otimes \mathcal{H} \otimes \mathbb{C}^2$ to the qutrit he receives from Alice, some ancillary qubits initialised to $|\bar{0}\rangle$, and a qubit reserved for his reply, and that:

$$U : |i\rangle|\bar{0}\rangle|0\rangle \mapsto |\phi_{i,0}\rangle|0\rangle + |\phi_{i,1}\rangle|1\rangle. \tag{2}$$

He measures the last qubit, and sends that across in round 2. If he wins, i.e., if the XOR of the bit he sent and the one that Alice picked is 1 ($b = \bar{a}$), in round 4 he sends one qutrit (the $\mathcal{H}_t$ part) from the above state across to Alice. (Note that any transformation he may do after learning that he won, i.e., after round 3, may be incorporated into U.)

Assume that Alice had picked the bit $a \in \{0, 1\}$ in round 1. Then, the joint state under the above cheating strategy before Bob measures his reply for round 2 is:

$$\sqrt{\alpha}|a\rangle\big(|\phi_{a,0}\rangle|0\rangle + |\phi_{a,1}\rangle|1\rangle\big) + \sqrt{1-\alpha}|2\rangle\big(|\phi_{2,0}\rangle|0\rangle + |\phi_{2,1}\rangle|1\rangle\big).$$

The unnormalized residual state when the outcome of his measurement is $\bar{a}$ is thus:

$$\sqrt{\alpha}|a\rangle|\phi_{a,\bar{a}}\rangle + \sqrt{1-\alpha}|2\rangle|\phi_{2,\bar{a}}\rangle.$$

Then Bob sends to Alice the $\mathcal{H}_t$ part of his state. (The states $|\phi_{a,\bar{a}}\rangle$, $|\phi_{2,\bar{a}}\rangle$ are in $\mathcal{H}_t \otimes \mathcal{H}$.) After round 4 their joint state is in $\mathcal{H}_s \otimes \mathcal{H}_t \otimes \mathcal{H}$, where the $\mathcal{H}_s \otimes \mathcal{H}_t$ part is with Alice and the $\mathcal{H}$ part is with Bob.

So Bob's probability of winning, given that Alice's bit is a, may be bounded as:

$$\begin{aligned}
&\big\|(P_a \otimes I)\big(\sqrt{\alpha}|a\rangle|\phi_{a,\bar{a}}\rangle + \sqrt{1-\alpha}|2\rangle|\phi_{2,\bar{a}}\rangle\big)\big\|^2 \\
&\quad = \big\|\alpha\big(\langle a| \otimes I\big)|\phi_{a,\bar{a}}\rangle + (1-\alpha)\big(\langle 2| \otimes I\big)|\phi_{2,\bar{a}}\rangle\big\|^2 \\
&\quad \leqslant \big(\alpha\|\phi_{a,\bar{a}}\| + (1-\alpha)\|\phi_{2,\bar{a}}\|\big)^2 \\
&\quad \leqslant \big(\alpha + (1-\alpha)\|\phi_{2,\bar{a}}\|\big)^2.
\end{aligned}$$

Now, consider Pr[Bob wins], which is the average of the above expression over $a \in \{0,1\}$. This is maximized when $\|\phi_{2,0}\| = \|\phi_{2,1}\| = 1/\sqrt{2}$ (recall from Eq. (2) that $\|\phi_{2,0}\|^2 + \|\phi_{2,1}\|^2 = 1$). Thus, the probability of Bob winning is bounded by

$$\left(\frac{1-\alpha}{\sqrt{2}} + \alpha\right)^2,$$

as claimed. □

There is a cheating strategy for Bob that achieves the above probability of success. Bob can use the following transformation on the qutrit he receives and an ancillary qubit:

$$|2\rangle|0\rangle \mapsto |2\rangle \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big), \quad \text{and}$$
$$|x\rangle|0\rangle \mapsto |x\rangle|x\rangle, \quad \text{for } x \in \{0,1\}.$$

He then measures the ancilla to get the bit b he is supposed to send in the second round.

As we vary the parameter α from 0 to 1 Alice's cheating probability decreases from 1 to $1/2$ and Bob's cheating probability increases from $1/2$ to 1. The bias is minimized when the two probabilities are made equal:

$$1 - \alpha/2 = \left(\frac{1-\alpha}{\sqrt{2}} + \alpha\right)^2.$$

By choosing α to satisfy the above equation, we get a protocol in which no player can win the game with probability greater than 0.739. The bias is then $0.239 < 1/4$.

3. A strong coin flipping protocol

Finally, we present a variant of the strong coin flipping protocol of [2], which has the same bias, but is much more simple to analyze. The idea behind this protocol also occurs in the "purification protocol" for bit-commitment in [11]. The protocol has the following three rounds:

(1) Alice picks $a \in_R \{0,1\}$, prepares the state $|\psi_a\rangle \in \mathcal{H}_s \otimes \mathcal{H}_t$ as in Eq. (1) and sends Bob the qutrit.
(2) Bob picks $b \in_R \{0,1\}$ and sends it to Alice.
(3) Alice then reveals the bit a to Bob and sends the second half of the state $|\psi_a\rangle$. Bob checks that the qutrit pair he received are indeed in state $|\psi_a\rangle$. If the test is passed, Bob accepts the outcome $c = a \oplus b$, else Bob concludes that Alice deviated from the protocol, and aborts.

The analysis for Bob's cheating strategy is the same as in [2] and his cheating probability is at most

$$\tfrac{1}{2} + \frac{\|\rho_0 - \rho_1\|_{\mathrm{tr}}}{4} = \tfrac{1}{2}(1+\alpha).$$

The analysis for Alice's cheating strategy is the same as in Lemma 2.1 above, and the same bound of $1 - \alpha/2$ holds here as well. This analysis is considerably simpler and does not require the symmetrization in [2] for the state sent in the first round.

By making the two cheating probabilities equal

$$1 - \alpha/2 = \tfrac{1}{2}(1+\alpha),$$

we achieve the bias of $\frac{1}{4}$ for $\alpha = \frac{1}{2}$.

Acknowledgements

We thank Umesh Vazirani for helpful discussions, and Rob Spekkens and Terry Rudolph for detailed comments on the paper and bringing [11] to our attention. We also thank the anonymous referee for helpful suggestions.

References

[1] D. Aharonov, A. Ta-Shma, U. Vazirani, A. Yao, Quantum bit escrow, in: Proc. 32nd Annual ACM Symp. on Theory of Computing, 2000, pp. 705–714.
[2] A. Ambainis, A new protocol and lower bounds for quantum coin flipping, in: Proc. 33rd Annual ACM Symp. on Theory of Computing, 2001, pp. 134–142.
[3] A. Ambainis, Lower bound for a class of weak quantum coin flipping protocols, LANL Preprint quant-ph/0204063, 2002.
[4] A. Ambainis, Personal communication, 2001.
[5] M. Blum, Coin flipping by telephone: A protocol for solving impossible problems, in: Advances in Cryptology: Report on CRYPTO'81, 1981, pp. 11–15.
[6] A. Kitaev, Personal communication, 2001.
[7] H. Lo, H. Chau, Why quantum bit commitment and ideal quantum coin tossing are impossible, Physica D 120 (1998) 177–187.
[8] D. Mayers, Unconditionally secure quantum bit commitment is impossible, Phys. Rev. Lett. 78 (1997) 3414–3417.
[9] A. Nayak, P. Shor, Bit-commitment-based quantum coin flipping, Phys. Rev. A 67 (2003), article no. 012304.
[10] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[11] R.W. Spekkens, T. Rudolph, Degrees of concealment and bindingness in quantum bit commitment protocols, Phys. Rev. A 65 (2002), article no. 012310.
[12] R.W. Spekkens, T. Rudolph, A quantum protocol for cheat-sensitive weak coin flipping, Phys. Rev. Lett. 89 (2002), article no. 227901.
[13] A.C.-C. Yao, Quantum circuit complexity, in: Proc. 34th Annual Symp. on Foundations of Computer Science, 1993, pp. 352–361.