A Note on "The Impossibility of Efficient Quantum Weak Coin Flipping"

Yusuf Alnawakhtha
University of Maryland, College Park
nawaktha@cs.umd.edu

Carl A. Miller
National Institute of Standards and Technology
University of Maryland, College Park
camiller@umd.edu

Abstract

In (STOC 2020, pp. 916–929), Miller showed that any protocol for quantum weak coin flipping with bias ϵ must use at least $\exp(\Omega(1/\sqrt{\epsilon}))$ rounds of communication. In this note, we augment the calculations from (STOC 2020, pp. 916–929) to derive explicit lower bounds on the number of rounds of communication for quantum weak coin flipping.

1 Introduction

The weak coin flipping problem consists of two players, Alice and Bob, that are trying to flip a coin (that is, to agree on a random bit). Alice wins if the outcome is 0 and Bob wins if the outcome is 1. We say that a protocol is an ϵ bias weak coin flipping protocol if an honest player can be certain that the other player did not bias the outcome by more than ϵ in their favor. In the setting of quantum weak coin flipping, Alice and Bob each possess quantum memory registers (denoted $\mathcal{A}$ and $\mathcal{B}$, respectively) and there is also a quantum message register $\mathcal{M}$ which is passed back and forth between them during the protocol. We denote by n the number of rounds of communication in the protocol (that is, the number of times that $\mathcal{M}$ is transmitted from one party to another).

In [1], it was shown that the parameter n must be at least $\exp(\Omega(1/\sqrt{\epsilon}))$. Therefore, n must grow rapidly as ϵ grows smaller. However, the results in [1] were only phrased in an asymptotic form. The purpose of this note is to provide explicit functions that lower bound the parameter n in terms of ϵ. We find, in particular, that n must be at least 10^6 for ϵ smaller than 10^{-7}. Our results are given in Table 1.

2 Preliminaries

2.1 Protocols for Quantum Weak Coin Flipping

A formal definition of quantum weak coin flipping protocol is provided below. (The theory we use for for weak coin-flipping in this note is based primarily on [2, 3].)

Definition 2.1 (n-round quantum weak coin flipping with bias ϵ)**.** *The protocol is described by the following:*

- *Three finite dimensional Hilbert spaces $\mathcal{A}, \mathcal{B}, \mathcal{M}$ (Alice's, Bob's, and the message system respectively).*
- *An initial state $|\psi_0\rangle = |\psi_{A,0}\rangle \otimes |\psi_{M,0}\rangle \otimes |\psi_{B,0}\rangle$.*
- *A set of unitrary operators $\{U_1, ..., U_n\}$ where U_i operate over $\mathcal{AM}$ for odd i and $\mathcal{MB}$ for even i*
- *A set of Hermitian projection operators $\{E_1, ..., E_n\}$ where E_i operate over $\mathcal{AM}$ for odd i and $\mathcal{MB}$ for even i, and*

$$E_i(U_i U_{i-1} \cdots U_1 |\psi_0\rangle) = U_i U_{i-1} \cdots U_1 |\psi_0\rangle . \tag{1}$$

- *Final projective measurements $\{\Pi_A^0, \Pi_A^1\}$ and $\{\Pi_B^0, \Pi_B^1\}$ on Alice's and Bob's systems respectively.*

  The protocol proceeds as follows:

1. *Alice and Bob hold the states $|\psi_{A,0}\rangle \otimes |\psi_{M,0}\rangle$ and $|\psi_{B,0}\rangle$ respectively.*
2. *The player holding the message state proceeds to act. For $i = 1$ to n,*
   (a) *If i is odd, Alice applies U_i to the product state she holds and then measures using $\{E_i, \mathbb{I}_{\mathcal{AM}} - E_i\}$. If the post measurement state is not in Supp E_i, then Alice suspects Bob of cheating and will return 0. Otherwise, she sends the message state to Bob.*
   (b) *If i is even, Bob applies U_i to the product state she holds and then measures using $\{E_i, \mathbb{I}_{\mathcal{MB}} - E_i\}$. If the post measurement state is not in Supp E_i, then Bob suspects Alice of cheating and will return 1. Otherwise, he sends the message state to Alice.*
3. *Alice and Bob measure their states using $\{\Pi_A^0, \Pi_A^1\}$ and $\{\Pi_B^0, \Pi_B^1\}$ respectively and report their outcome.*

Let P_A^* be the probability of Alice getting her desired outcome if she acts dishonestly and Bob acts honestly and let P_B^* be the probability of Bob getting his desired outcome if he acts dishonestly and Alice acts honestly. Then, we say that the protocol has bias ϵ if $max\{P_A^*, P_B^*\} - 1/2 \leq \epsilon$.

2.2 Point Games

We will give a brief description of the point game formalization, as we only need to address a few aspects of it for the purposes of this note.

Definition 2.2 (One dimensional move). *A one dimensional move is a function $\ell : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}$ with finite support. If $\ell \geq 0$ we also call ℓ a one dimensional configuration.*

Definition 2.3 (Two dimensional move). *A two dimensional move is a function $\ell : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \mapsto \mathbb{R}$ with finite support. If $\ell \geq 0$ we also call ℓ a two dimensional configuration.*

Definition 2.4 (Time-dependent point game). *A time-dependent point game is sequence of two-dimensional moves $(m_0, m_1, \ldots, m_n)$ such that for any $k \in \{0, 1, 2, \ldots, n\}$,*

$$\sum_{j=0}^{k} m_k \quad \geq \quad 0. \tag{2}$$

Next, we will build up the definition of a valid point game.

Definition 2.5 (Valid one dimensional move). *A one dimensional move l is called a valid one dimensional move if it satisfies the following two conditions*

$$\sum_x \ell(x) = 0 \tag{3}$$

$$\sum_x \left(\frac{x}{x+\lambda}\right) \ell(x) \geq 0 \qquad \forall \lambda > 0 \tag{4}$$

Definition 2.6 (Horizontally valid move). *A two dimensional move q is said to be horizontally valid if for all $y \in \mathbb{R}_{\geq 0}$, the move $x \mapsto q(x, y)$ is a one dimensional valid move.*

Similarly, we define vertically valid moves as follows:

Definition 2.7 (Vertically valid move). *A two dimensional move q is said to be vertically valid if for all $x \in \mathbb{R}_{\geq 0}$ the move $y \mapsto q(x, y)$ is a one dimensional valid move.*

Definition 2.8 (Valid time-dependent point game). *A sequence of moves (m_0, m_1, m_2) is a valid time-independent point game if all of the following hold:*

$$m_0 \quad \geq \quad 0, \tag{5}$$

$$m_0 + m_1 + m_2 \quad \geq \quad 0, \tag{6}$$

$$m_1 \textit{ is horizontally valid, and} \tag{7}$$

$$m_2 \textit{ is vertically valid.} \tag{8}$$

To relate point games with quantum weak coin flipping protocols, we import the following theorem, which is based on theory from [2]. (We quote the theorem in the particular form used in [1] for convenience.)

Theorem 2.9 (Theorem 3.11 from [1]). *Suppose that C is an n-round weak coin flipping protocol with cheating probabilities $\alpha := P_A^*$ and $\beta := P_B^*$ and suppose that $\delta > 0$. Then, there exists a valid time independent point game $R = (r_0, r_1, r_2)$ such that*

$$r_0 \;=\; \frac{1}{2}[\![0,1]\!] + \frac{1}{2}[\![1,0]\!], \tag{9}$$

$$r_0 + r_1 + r_2 = [\![\alpha+\delta, \beta+\delta]\!], \tag{10}$$

and

$$\|r_1\|_1 + \|r_2\|_1 \leq 2n. \tag{11}$$

Lastly, we will provide a definition for the two-variable profile of a move which is an essential tool for the proofs in [1]. We first state the definition of the one-variable profile function.

Definition 2.10 (Profile function). *For any non-negative x, define $P_x : [1,\infty] \mapsto \mathbb{R}$ as follows: for $x = 0$,*

$$P_0(\alpha) = \begin{cases} 1 & \textit{if } \alpha \in [1,2) \\ 0 & \textit{otherwise} \end{cases} \tag{12}$$

and for $x > 0$,

$$P_x(\alpha) = \begin{cases} 1 & \textit{if } \alpha \in [1,2) \\ (x\alpha - x)/(x+\alpha-2) & \textit{if } \alpha \in [2,\infty) \\ x & \textit{if } \alpha = \infty \end{cases} \tag{13}$$

For a two-dimensional valid move q, the profile of the move is denoted as $\hat{q} : [1,\infty]\times[1,\infty] \mapsto \mathbb{R}$ and is given by

$$\hat{q}(u,v) = \sum_{x,y} q(x,y)P_x(u)P_y(v) \tag{14}$$

2.3 Mathematical Lemmas

We restate two mathematical assertions from [1]. (In [1] these assertions are given asymptotically. We merely restate them using exact functions from their respective proofs.)

Lemma 2.11. *Let $\mathbf{A}\colon \mathbb{R}_{>0} \to \mathbb{R}$ be defined by*

$$\mathbf{A}(\delta) = \frac{3}{2}\delta + \sqrt{3\delta + \frac{9}{4}\delta^2}, \tag{15}$$

If X is any positive real-valued random variable satisfying

$$\begin{aligned} \mathbb{E}[X] &\leq 1, & (16)\\ \mathbb{E}[1/X] &\leq 1+\delta, & (17) \end{aligned}$$

then

$$\mathbb{P}(|X-1|< \mathbf{A}(\delta)) \geq \frac{2}{3}. \tag{18}$$

Proof. This follows from the proof of Lemma 6.1 in [1]. □

Proposition 2.12. *Suppose that $\delta, \nu \in (0,1)$, and let θ denote the angle of the complex number $(i+\delta)/(1+i\delta)$. Let $f\colon \mathbb{C}\cup\{\infty\} \to \mathbb{C}\cup\{\infty\}$ be a rational function whose poles are all real and lie outside of the real interval $[-1,1]$. Suppose that*

$$|f(0)|= 1, \tag{19}$$

and

$$|f(z)|\leq \nu \qquad \textit{for all } z \in [-1,1]\backslash(-\delta,\delta). \tag{20}$$

Then,

$$\max_{|z|=1}|f(z)|\geq \nu^{\frac{2\theta}{2\theta-\pi}}. \tag{21}$$

Proof. This follows from the proof of Proposition 5.3 in [1]. □

We note that in the statement of the above proposition, the angle of the complex number $i+\delta$ is $(\pi/2)-\tan^{-1}\delta$, and the angle of the complex number $(1+i\delta)$ is $\tan^{-1}\delta$, and therefore $\theta=(\pi/2)-2\tan^{-1}\delta$. Therefore we can restate Proposition 2.12 as the following corollary.

Corollary 2.12.1. *Suppose that $\delta, \nu \in (0,1)$. Let $f\colon \mathbb{C}\cup\{\infty\} \to \mathbb{C}\cup\{\infty\}$ be a rational function whose poles are all real and lie outside of the real interval $[-1,1]$. Suppose that*

$$|f(0)|= 1, \tag{22}$$

and

$$|f(z)|\leq \nu \qquad \textit{for all } z \in [-1,1]\backslash(-\delta,\delta), \tag{23}$$

Then,

$$\max_{|z|=1}|f(z)| \quad\geq\quad (1/\nu)^{\frac{\pi-4\tan^{-1}\delta}{4\tan^{-1}\delta}}. \tag{24}$$

3 Results

We proceed with explicit calculations for the main asymptotic results given in [1]. We begin with the following. If g is a two-dimensional move, then let $g^\top$ be defined by $g^\top(x,y) = g(y,x)$.

Theorem 3.1. *Let $\tau \in (0,1)$ and let g be a horizontally valid point game such that*

$$g + g^\top = 2[\![1,1]\!] - [\![2-\tau,0]\!] - [\![0,2-\tau]\!]. \tag{25}$$

Then,

$$\|g\|_1 \;\; \geq \;\; \frac{1}{24} \cdot 2^{\frac{\pi - 4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}}, \tag{26}$$

where $\mathbf{I}$ *is defined by*

$$\mathbf{I}(a) = \frac{105}{2}a + 5 \cdot \sqrt{21a + \frac{441}{4}a^2}. \tag{27}$$

Proof. Note that

$$\mathbf{I}(a) \;\; = \;\; 5\mathbf{A}(7a). \tag{28}$$

where $\mathbf{A}$ is the function defined in Lemma 2.11. Let a horizontally valid move $\mathbf{g}$ be defined by

$$\mathbf{g}(x,y) \;\; = \;\; \begin{cases} g(x,y) & \text{if } |y-4| < \mathbf{I}(\tau), \\ \\ 0 & \text{otherwise.} \end{cases} \tag{29}$$

Consider the rational function

$$z \mapsto \mathbf{g}(z,z). \tag{30}$$

Let $D \colon \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ be the complex extension of this function. The proofs of Propositions 7.7 and 7.8 in [1] show that

$$D(4) \;\; \geq \;\; \frac{2}{3} \tag{31}$$

and

$$D(z) \;\; \leq \;\; \frac{1}{3} \tag{32}$$

for all $z \in [3,5] \smallsetminus (4 - 2\mathbf{I}(\tau), 4 + 2\mathbf{I}(\tau))$. If we define $D' \colon \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ by $D'(z) = D(z+4)/D(4)$, then Corollary 2.12.1 implies that there exists a unit-length complex number ζ such that

$$D'(\zeta) \;\; \geq \;\; 2^{\frac{\pi - 4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}} \tag{33}$$

and therefore

$$\begin{aligned} D(4+\zeta) &\geq D(4)\cdot 2^{\frac{\pi-4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}} \qquad (34)\\ &\geq \frac{2}{3}\cdot 2^{\frac{\pi-4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}}. \qquad (35) \end{aligned}$$

The proof of Proposition 7.9 in [1] shows that

$$D(z+\zeta) \leq 16\left\|g\right\|_1, \tag{36}$$

and therefore,

$$\left\|g\right\|_1 \geq \frac{1}{24}\cdot 2^{\frac{\pi-4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}}, \tag{37}$$

as desired. □

Now we can compute an explicit lower bound on the number of rounds for quantum weak coin-flipping. We follow the proof of Proposition 8.1 in [1]. Suppose that there is an n-round weak coin-flipping protocol that achieves bias less than ϵ. By Theorem 2.9, there is a valid time independent point game (m_0, m_1, m_2) from $\frac{1}{2}\llbracket 0,1\rrbracket + \frac{1}{2}\llbracket 1,0\rrbracket$ to $\llbracket \frac{1}{2}+\epsilon, \frac{1}{2}+\epsilon\rrbracket$ such that

$$\left\|m_1\right\|_1 + \left\|m_2\right\|_1 \leq 2n. \tag{38}$$

If we let (q_0, q_1, q_2) be the time-independent point game defined as in equation (131) in [1]:

$$q_i(x,y) = 2m_i\left(x\left(\frac{1}{2}+\epsilon\right), y\left(\frac{1}{2}+\epsilon\right)\right), \tag{39}$$

and let $q = ((q_1) + (q_2)^\top)/2$, then $(q_0, q, q^\top)$ is a valid time-independent point game from $\llbracket 2-\tau, 0\rrbracket + \llbracket 0, 2-\tau\rrbracket$ to $2\llbracket 1,1\rrbracket$, where

$$\tau = 4\epsilon/(1+2\epsilon), \tag{40}$$

and $\left\|q\right\|_1 \leq 2n$. Therefore, by Theorem 3.1,

$$\left\|q\right\|_1 \geq \frac{1}{24}\cdot 2^{\frac{\pi-4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}} \tag{41}$$

and thus

$$n \geq \frac{1}{48}\cdot 2^{\frac{\pi-4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}} \tag{42}$$

In summary, a lower bound for n in terms of ϵ can be computed via the following formulae:

$$\tau := 4\epsilon/(1+2\epsilon) \tag{43}$$

$$\mathbf{I}(\tau) := \frac{105}{2}\tau + 5 \cdot \sqrt{21\tau + \frac{441}{4}\tau^2} \tag{44}$$

$$n \geq \frac{1}{48} \cdot 2^{\frac{\pi - 4\tan^{-1}(2\mathbf{I}(\tau))}{4\tan^{-1}(2\mathbf{I}(\tau))}}. \tag{45}$$

A table of values for the expression on the righthand side of inequality (45), computed in Mathematica, is given in Table 1.

ϵ	Lower bound on n
$1 \cdot 10^{-6}$	3.915
$5 \cdot 10^{-7}$	45.6
$2 \cdot 10^{-7}$	5989
$1 \cdot 10^{-7}$	$1.46 \cdot 10^{6}$
$5 \cdot 10^{-8}$	$3.49 \cdot 10^{9}$
$1 \cdot 10^{-8}$	$6.35 \cdot 10^{23}$

Table 1: Lower bounds on the number of communication rounds (n) for a weak coin-flipping protocol with bias less than ϵ.

References

[1] Carl A Miller. The impossibility of efficient quantum weak coin flipping. In Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, pages 916–929, 2020.

[2] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. arXiv:0711.4114, 2007.

[3] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. SIAM Journal on Computing, 45(3):633–679, 2016.