Quantum Leader Election

Maor Ganz
The Hebrew University, Jerusalem

September, 2009

Abstract

A group of \( n \) individuals \( A_1, \ldots A_n \) who do not trust each other and are located far away from each other, want to select a leader. This is the leader election problem, a natural extension of the coin flipping problem to \( n \) players. We want a protocol which will guarantee that an honest player will have at least \( \frac{1}{n} - \epsilon \) chance of winning (\( \forall \epsilon > 0 \)), regardless of what the other players do (whether they are honest, cheating alone or in groups). It is known to be impossible classically. This work gives a simple algorithm that does it, based on the weak coin flipping protocol with arbitrarily small bias recently derived by Mochon [Moc]. The protocol is quite simple to achieve if the number of rounds is linear; We provide an improvement to logarithmic number of rounds.

1 Introduction

A standard coin flipping is a game in which 2 parties, Alice and Bob, wish to flip a coin from a distance. The two parties do not trust each other, and would each like to win with probability of at least 0.5. A natural problem is to find good protocols - a protocol in which a player could not cheat and force the outcome of the game to his benefit.
There are two types of coin flipping - strong and weak. In strong coin flipping, each party might want to bias the outcome to any result. In weak coin flipping each party has a favorite outcome.

We denote the winning probability of an honest Alice as $P_A$, and similarly $P_B$ for Bob. The maximum winning probability of a cheating Alice (i.e. when she acts according to her optimal strategy, and when Bob is honest) is denoted by $P^*_A$, and similarly $P^*_B$ for Bob.

Let $\epsilon = \max(P^*_A, P^*_B) - \frac{1}{2}$ be the bias of the protocol. The bias actually tells us how good the protocol is. The smaller the bias is, the better the protocol is, because the cheating options decrease.

It is well known that without computational assumptions, coin flipping (whether weak or strong) is impossible to achieve in the classical world. That is, one of the players can always win with probability 1. In the quantum setting, the problem is far more interesting.

Quantum strong coin flipping protocols with large but still non-trivial biases were first discovered. Kitaev then proved (see for example in [ABDR03]) that in strong coin flipping, every protocol must satisfy $P^*_A \cdot P^*_B \geq \frac{1}{2}$, hence $\epsilon \geq \sqrt{2}-1$. This result raised the question of whether weak coin flipping with arbitrarily small bias is possible. Protocols were found with smaller and smaller biases, until Mochon showed in his paper [Moc] that there are families of weak coin flipping protocols whose bias converges to zero. It is also known that even in the quantum world, a perfect protocol (i.e. $\epsilon = 0$) is not possible.

If we try to expand the problem of weak coin flipping to more than 2 parties - namely $A_1, \ldots, A_n$ parties with $n$ possible outcomes, where each party $A_i$ wins if the outcome is $i$, we get the leader election problem.

As mentioned before, it is classically impossible to do a weak coin flipping with a bias < 0.5 without assumptions about the computation power. Hence, it is also impossible to solve the leader election problem in the classical setting. [Fei00] presents a classical leader election protocol (given that a player
can flip a coin by herself) that given \( \frac{(1+\delta)n}{2} \) honest players, an honest player is chosen with probability \( \Omega(\delta^{1.65}) \). In addition there is a proof that every classical protocol has a success probability of \( O(\delta^{1-\epsilon}) \), for every \( \epsilon > 0 \). Note that there are limitation on the number of cheaters.

There are many types of Leader elections. The most natural type seems to be the one we have just defined, which is \( n \) parties wanting to select one of them as a leader. We will refer to this type as the leader election problem. Another possibility is a protocol that chooses a processor randomly among \( n \) possibilities (there are no cheaters, and we want a protocol that uses minimal complexity, or one that works without knowing the number of processors. See [TKM07]). This type sometimes called fair leader election problem.

Until recently there was no quantum result regarding the leader election problem as it was defined here. However there were some results on other types, such as [ABDR03] which allow penalty for cheaters that got caught (which is obviously a weaker version of the problem).

In [Moc] Mochon showed the existence of a weak coin flipping protocol with an arbitrarily small bias of at most \( \epsilon \). Let us denote this protocol in \( P_\epsilon \) throughout this paper. This protocol assumes that an honest player has \( \frac{1}{2} \) chance of winning. It is also possible to build an unbalanced weak coin flipping with an arbitrarily small bias \( \epsilon \), in which one honest player will have \( q \) winning probability, and the other player will have \( 1 - q \) winning probability. We will denote this protocol as \( P_{q,\epsilon} \). In [CK09] it was shown that this is possible using repetition of \( P_\epsilon \). It is very likely that this can also be achieved by finding an appropriate families of time independent point games (see [Moc]), but this will not be done in this paper.

We will present a leader election protocol with \( n \) parties (based on Mochon’s result) in which the probability of an honest player to win converges to \( \frac{1}{n} \).

Our protocol is fairly simple and uses \( \log n \) rounds of unbalanced weak protocols \( P_{q,\epsilon} \) as will be defined later. The protocol uses at most \( \log n \)
unbalanced weak coin flip protocols. This limitation is important, because at the moment we only know how to implement an unbalanced flip using a repetition of balanced coin flip, which influences our running time complexity.

2 Leader election protocol

If \( n \) is a power of 2, then the quantum solution is easy (given a good weak coin flip protocol) - we can do a tournament (the looser quits) with \( \log(n) \) weak coin flip rounds, and the winner of the tournament will be elected as the leader. A problem arise when \( n \) is not a power of 2, then this is not possible, and putting in a dummy involves some difficulties. If the cheaters could control the dummy, they would increase their winning probability.

Our first solution (which was also discovered in [AS09], independently) is to let \( A_1 \) play \( A_2 \) and then the winner of that will play \( A_3 \) and so on, as in a tournament, except we use unbalanced weak coin flips. These are also known to be possible using the weak coin flipping protocol (see in [CK09]) but are more expensive in terms of time.

The leader will be the winner of the final \((n-1)\) step. This works, however it uses many \((n-1)\) rounds, and thus we later combine the two ideas in order to reduce the number of rounds.

We start by some standard definitions.

2.1 Definitions and requirements

By a *weak coin flipping protocol* we mean that Alice wins if the outcome is 0, and Bob wins if it is 1.

A protocol with \( P_A = q, \ P_B = 1 - q \), bias \( \epsilon \) will be denoted by \( P_{q, \epsilon} \).

A *leader election protocol* with \( n \) parties \( A_1, \ldots, A_n \) has an outcome \( t \in \{1, \ldots, n\} \). We will denote by \( P_t \) the probability that the outcome is \( t = i \).

We assume that each player has its own private space, untouchable by other players, a message space \( M \) which is common to all \( M \) can include a
We use the existence of a weak coin flinging protocol with bias at most \( \epsilon \) for every \( \epsilon > 0 \). This fact was proved in \([\text{Mo}c]\) for \( P_A = P_B = \frac{1}{2} \) and we will denote it as \( P_\epsilon \) and by \( N_\epsilon \) the number of its rounds. It seems possible to generalize it to any \( P_A, P_B \), but that was not proved yet. There is a proof that there is such a protocol for every \( P_A, P_B \) in \([\text{CK}09]\) by repetitions of \( P_\epsilon \), with \( k \cdot N_\epsilon \) rounds.

**Proposition 1.** \([\text{CK}09]\) for \( q \in [0, 1] \), \( k \in \mathbb{N} \) \( \exists P_{x,\epsilon_0} \) with \( k \cdot N_\epsilon \) rounds, such that \( |x - q| \leq 2^{-k} \) and \( \epsilon_0 \leq 2\epsilon \).

This means that if we want a protocol \( P_{q,\epsilon'} \), we can use the proposition with \( \epsilon = \frac{\epsilon'}{2} \), \( q = \frac{\epsilon}{2} \), hence \( k = 1 + \lceil \log(\frac{1}{\epsilon'}) \rceil \). This will lead to \( P_{x,\epsilon_0} \) where \( |x - q| \leq \frac{\epsilon}{2} \), \( \epsilon_0 \leq \frac{\epsilon}{2} \), and it uses \( (1 + \lceil \log(\frac{1}{\epsilon'}) \rceil) \cdot N_\epsilon = O(|N_\epsilon \cdot \log \epsilon|) \) rounds.

**Corollary 2.** For \( q \neq \frac{1}{2} \) the protocol \( P_{q,\epsilon} \) will use no more than \( O(|N_\epsilon \cdot \log \epsilon|) \) rounds.

There is one delicate point, that the cheaters cannot increase their winning probability in a specific protocol, by losing previous protocols (say by creating entanglements). This will be discussed in the end.

We will first present the simpler case of 3 parties, to show the basic idea. The general case is a natural generalization of this, and we will analyze it in details. Nevertheless this case captures the basic idea of the problem and solution.

2.2 Three parties: A,B,C

Alice, Bob and Charlie want to select a leader. Alice will be elected if the outcome will be 0, Bob if it will be 1 and Charlie will win on outcome 2.

Let \( \epsilon > 0 \). We will show a leader election protocol, such that if all are honest then \( P_0 = P_1 = P_2 = \frac{1}{3} \).

If party \( i \) is honest then we want that \( P_i \geq \frac{1}{3} - \epsilon \).

Let \( \epsilon' = \frac{\epsilon}{2} \) be a constant depend on \( \epsilon \).
2.2.1 Protocol

1. Alice plays Bob $P_{\frac{1}{2}, \epsilon'}$.

2. The winner plays Charlie $P_{\frac{2}{3}, \epsilon'}$.

3. The winner of that flip is declared as the leader.

2.2.2 Analysis

- If all players are honest, then $A$ (same for $B$) has $\frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}$ chance of winning. ($\frac{1}{2}$ the chance of winning $B$, and $\frac{2}{3}$ to then win $C$). $C$ has just one game, so he obviously has $\frac{1}{3}$ chance of winning.

- If $A$ is honest, we can think of it as if $A$ is the only honest player. Then the calculation is almost the same from her point of view: In the first game she has $\frac{1}{2} - \epsilon'$ winning probability, and in the second (if she won the first) she has $\frac{2}{3} - \epsilon'$ winning probability. So in the total she has $(\frac{1}{2} - \epsilon')(\frac{2}{3} - \epsilon') = \frac{1}{3} - \frac{7}{6} \epsilon' + \epsilon'^2 > \frac{1}{3} - \frac{7}{6} \epsilon' = \frac{1}{3} - \frac{7}{12} \epsilon$. Thus we have extra $\frac{5}{12} \epsilon$ to spare (the coalition $B - C$ has less than $\frac{2}{3} + \epsilon$ chance of winning).

- If $B$ is honest then the calculation is the same, just replace $A$ with $B$ and vice versa.

- If $C$ is honest - again he has only one flip, so he has at least $\frac{1}{3} - \epsilon' > \frac{1}{3} - \frac{7}{12} \epsilon$ chance of winning.
• Number of coin flips = 2.

• First coin flip is $P_{\frac{1}{2},\epsilon'}$, hence involves $N_{\epsilon'}$ rounds.
  Second coin flip is $P_{\frac{3}{5},\epsilon'}$. We have $\frac{5}{12} \epsilon > 2 \cdot \frac{1}{6}$ probability to spare. Hence by [(1)], it can be done with less than $(1 - \log(\frac{5}{6})) \cdot N_{\epsilon'} < (4 + \log \frac{1}{\epsilon}) \cdot N_{\epsilon'}$ rounds.

2.3 First try for $n$ parties

In the general case we have $n$ parties $A_1, \ldots, A_n$.

Let $\epsilon > 0$. We will show a leader election protocol, such that if all are honest then $P_i = \frac{1}{n}$.

If party $i$ is honest then we want that $P_i \geq \frac{1}{n} - \epsilon$.

Let $\epsilon' \leq \frac{\epsilon}{n}$ be a constant that depends on $\epsilon$ (the condition on $\epsilon'$ is far from tight, for convenient of the calculation).

2.3.1 Protocol:

1. Let $W = A_1$.

2. For $i = 2$ to $n$
   
   (a) $W$ plays $A_i$ a $P_{\frac{1}{2},\epsilon'}$ weak coin flipping protocol.
   
   (b) $W$ is the winner.

3. $W$ is declared as the leader.
2.3.2 Analysis

Note that player $j$ enters the game in the $j_{th}$ stage (i.e. when $i = j$ on $\#2_a$ in the protocol), when he plays coin flip with winning probability $P_i = 1 - \frac{i-1}{n} = \frac{1}{i}$ (The only exception in the protocol is $A_1$ that also plays for the first time when $i = 2$, but then also $P_1 = \frac{1}{2}$, so it is the same).

- If all are honest, then $P_i = \frac{1}{i} \cdot \frac{i}{i+1} \cdot \frac{i+1}{i+2} \cdot \ldots \cdot \frac{n-2}{n-1} \cdot \frac{n-1}{n} = \frac{1}{n}$.

- If $A_i$ is honest, $P_i = (\frac{1}{i} - \epsilon') \cdot \prod_{j=i}^{n} (\frac{j}{j+1} - \epsilon') \geq \frac{1}{n} - n\epsilon' = \frac{1}{n} - \epsilon$ (and we have more than $\epsilon$ to spare).

- Number of coin flips = $n - 1$.

  The $i_{th}$ coin flip is $P_{i-1}\epsilon'$, so it will have $(1 + \log(\epsilon)) \cdot N\epsilon'$ rounds.

2.4 Improved protocol for seven players

We mentioned in the beginning that if $n = 2^m$, we can do a tournament with $m$ rounds. In the last try we came up with a protocol of $n-1$ rounds, because each time only one couple played a coin flip. The problem with this simple solution is that it is quite inefficient in terms of number of rounds, and also
almost all the coin flips are unbalanced. We can improve this protocol by combining it with the tournament idea.

### 2.4.1 Protocol

1. The following couples play $P_{\frac{1}{2}, \epsilon'}$: $A_1 - A_2$, $A_3 - A_4$, $A_5 - A_6$.

2. The winners of $A_1 - A_2$, $A_3 - A_4$ play between them $P_{\frac{1}{2}, \epsilon'}$.

   The winner of $A_5 - A_6$ plays $A_7$ a $P_{\frac{1}{2}, \epsilon'}$.

3. The two winners of last stage play a $P_{\frac{1}{2}, \epsilon'}$.

#### 2.4.2 Analysis

- If all are honest, then $A_1 - A_4$ have the same steps, and they have winning probability of $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{4}{7} = \frac{1}{7}$.

  $A_5, A_6$ have a winning probability of $\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{7} = \frac{1}{7}$.

  $A_7$ has only two flips, so obviously $P_7 = \frac{1}{3} \cdot \frac{3}{7} = \frac{1}{7}$.

- If $A_1$ is honest he has winning probability of $(\frac{1}{2} - \epsilon')(\frac{1}{2} - \epsilon')(\frac{1}{7} - \epsilon') = \frac{1}{7} - \frac{23}{28} \epsilon' + 14 \epsilon^2 - \epsilon^3 \geq 1 - \frac{23}{28} \epsilon'$.

  Same result for $A_2 - A_4$. 


If $A_5$ (or $A_6$) is honest then he has winning probability of $(\frac{1}{2} - \epsilon')(\frac{2}{3} - \epsilon')(\frac{3}{7} - \epsilon') \geq \frac{1}{7} - \frac{35}{42} \epsilon'$.
For $A_7$ it is obviously $\geq \frac{1}{7} - \frac{16}{21} \epsilon'$.

- Number of coin flips steps $= 3$.
- We have more than $\frac{1}{7} \epsilon'$ to spare, hence we can comfortably take $\epsilon' = \frac{\epsilon}{21}$.

2.5 Final protocol

In the general case we have $n$ parties $A_1, \ldots, A_n$.

Let $\epsilon > 0$. We will show a leader election protocol, such that if all parties are honest then $P_i = \frac{1}{n}$, with $\log(n)$ coin flipping rounds.

If party $i$ is honest then we want that $P_i \geq \frac{1}{n} - \epsilon$.

Let $\epsilon' \leq \frac{\epsilon}{2 \log n}$ be a constant that depends on $\epsilon$ (the condition on $\epsilon'$ is far from tight, for convenient of the calculation).

2.5.1 Protocol

We will define the protocol recursively.

Let us call it $Leader\left(\{A_1, \ldots, A_n\}, \epsilon\right)$.

Say it returns the leader selected.

Let $k \in \mathbb{N}$ s.t. $2^k \leq n \leq 2^{k+1}$.

1. The following are done simultaneously:
   
   - $A_1, \ldots, A_{2^k}$ plays a tournament (of $k$ rounds) among themselves with $P_{\frac{1}{2}, \epsilon'}$. Denote the winner as $w_1$.
   
   - $w_2 = Leader\left(\{A_{2^k+1}, \ldots, A_n\}\right)$.

2. $w_1$ plays $w_2$ a $P_{\frac{1}{2^n}, \epsilon'}$.
   
   The winner of this is the leader.
2.5.2 Analysis

- Assume that all parties are honest.
  Look at $A_1, \ldots, A_{2^k}$. In the tournament everyone has a $\frac{1}{2^k}$ winning chance. Then they have another coin flip with $\frac{2^k}{n}$ winning chance, so in total they each have $\frac{1}{2^k} \cdot \frac{2^k}{n} = \frac{1}{n}$ winning chance.
  From induction we know each of $A_{2^k+1}, \ldots, A_n$ has a $\frac{1}{n-2^k}$ winning chance in the recursive leader procedure (to become $w_2$). Then the winner has a $1 - \frac{2^k}{n}$ winning chance in the last step, so altogether he has $\frac{1}{n-2^k} \cdot (1 - \frac{2^k}{n}) = \frac{1}{n}$.

- We have $\log(n)$ coin flipping steps, and according to (2) we will have up to $O(|N| \epsilon \log(\epsilon) \log(n))$ total rounds.

- If $A_i$ is honest, then he has a winning probability of $\prod_{i=1}^{\log(n)} (c_i - \epsilon') \geq \frac{1}{n} - \log(n)\epsilon' \ (c_i < 1)$.

- The number of unbalanced coin flips is bounded by $\log(n)$.
  In fact: $\#\text{unbalanced coin flips} = (\# \text{ of 1's in the binary representation of } n) - 1$.
  This can be proved easily by induction on $n$:
  For $n = 2, 3, 4$ it is clear.
  If $n = 2^k$ then it has 0 such. Else $2^k < n < 2^{k+1}$, and the first $2^k$ use again 0 unbalanced coin flips between them. The remaining $n - 2^k$ use from the induction hypothesis the of 1’s in its binary from - 1. When joining the two groups, we again use an unbalanced coin flip which is equivalent to the MSB 1 in the binary form of the $n$ in the $k_{th}$ bit (From the $2^k$).
3 Remarks

3.1 Consecutive coin flipping protocols

Let \( P \) be a weak coin flipping protocol, with \( P_B^* \) the maximal cheating probability of Bob.

We want to run two instances of \( P \), one after the other (not even at the same time).

We will define (see \[Moc\] for full details):

- Let \( \mathcal{H} = \mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B} \) be the Hilbert space of the system.
- \( | \psi_0 > = | \psi_{A,0} > | \psi_{M,0} > | \psi_{B,0} > \) is the initial state of the system.
- Let there be \( n \) (even) stages, \( i \) denote the current stage.
- On the odd stages \( i \), Alice will apply a unitary \( U_{A,i} \) on \( \mathcal{A} \otimes \mathcal{M} \).
- On the even stages, Bob will apply a unitary \( U_{B,i} \) on \( \mathcal{M} \otimes \mathcal{B} \).
- Let \( | \psi_i > \) be the state of the system in the \( i_{th} \) stage.
- Let \( \rho_{A,i} = Tr_{\mathcal{M} \otimes \mathcal{B}}(| \psi_i >< \psi_i |) \) be the density matrix of Alice in the \( i_{th} \) stage.
- Alice’s initial state (density matrix) is \( \rho_{A,0} = | \psi_{A,0} >< \psi_{A,0} |. \)
- For even state \( i \) we have \( \rho_{A,i} = \rho_{A,i-1}. \)
- Let \( \tilde{\rho}_{A,i} \) be the state of \( \mathcal{A} \otimes \mathcal{M} \) after Alice gets the \( i_{th} \) message.
- For odd \( i \) : \( \rho_{A,i} = Tr_{\mathcal{M}}(\tilde{\rho}_{A,i}), \rho_{A,i} = Tr_{\mathcal{M}}(U_{A,i} \tilde{\rho}_{A,i-1} U_{A,i}^\dagger). \)

We know that

\[
P_B^* \leq \max_{\rho:(1)-(4)} Tr[\Pi_{A,1} \rho_{A,n}] \tag{1}
\]

regardless of Bob’s actions (see \[Moc\] for full proof).
We conclude that Bob can not improve his winning chances in a specific round by doing something in previous rounds.

**Corollary.** If Alice plays Bob a series of weak coin flipping $P_{q_i, \epsilon_i}$, then Bob’s winning probability is bounded from above by $1 - q_i$ in the $i_{th}$ game.

Since Alice will always start the protocol with a new-empty environment (i.e. no correlations or leftovers from previous protocols), Bob cannot achieve a higher winning probability than the bound at $1$ in any way, including correlations from previous protocols. (If one could have raised his winning probability, by using a previous protocol, he could have also done it without using it).

### 3.2 The message space

When we analyze coin flipping between two players, we assume one of them is honest and analyze the scenario that the other player is cheating and we then bound his winning probability. In multiparty protocol, such as the leader election, another possibility might occur. A cheating player $A_i$ might interfere a weak coin flipping protocol between two other players $A_j$ and $A_k$ (honest or not). We claim that this should not change our computation.

**Claim.** If $A_j$ plays $A_k$ a $P_{q, \epsilon}$ coin flip, then even if $A_i$ interferes, it does not change their winning probabilities.

We can look at it from the point of view of honest $A_j$. He can assume that the rest of the players are cheaters. When he plays against $A_k$ it doesn’t matter whether $A_i$ interferes (as long as he does not change $A_j$ private space), because a cheater $A_k$ could have done the same on its own, and this scenario is included in the calculation of $P^*$. Hence leaving the winning probabilities unchanged.
3.3 Additional work

A related work was published [AS09] recently. They refer to the leader election problem as weak dice rolling, and they use the same protocol as we did (independently) in 2.3. They also extend the leader election problem to the strong scenario, under the name of strong dice rolling. Namely they consider the problem of \( M \geq 2 \) remote parties, having to decide on a number between 1 and \( N \geq 3 \), without any party being aware to any other’s preference. They generalize Kitaev’s bound to apply to this case, and get that

\[
P_{A_1}^{(i)} \cdots P_{A_M}^{(i)} \geq \frac{1}{N}, \quad i \in \{1, \ldots, M\} \quad \text{where} \quad P_{A_j}^{(i)} \quad \text{gives the probability for the outcome} \ i \ \text{when all parties but the} \ j_{th} \ \text{are dishonest and acting in unison to force the outcome} \ i.
\]

This was done by noting that strong leader election can always be used to implement strong imbalanced coin flipping. They also extend the protocol in [CK09] to \( 2 \cdot M \) parties and \( N^M \) outcomes for any \( M, N \in \mathbb{N} \).

Acknowledgments

I would like to thanks Prof. Dorit Aharonov for her support and guidance, and also thank Prof. Michael Ben-Or for his help.

References

[ABDR03] Andris Ambainis and Harry Buhrman and Yevgeniy Dodis and Hein Roehrig, Multiparty Quantum Coin Flipping, arXiv.org:0304112, 2003.

[AS09] Aharon N. and Silman J., Quantum dice rolling, arxiv.org:0908.1682, 2009.

[CK09] Andre Chailloux and Iordanis Kerenidis, Optimal quantum strong coin flipping, arXiv.org:0904.1511, 2009.
[Fei00] Uriel Feige, Noncryptographic selection protocols, http://www.wisdom.weizmann.ac.il/~feige/Others/leader.ps, 2000.

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

[TKM07] Seiichiro Tani and Hirotada Kobayashi and Keiji Matsumoto, Exact Quantum Algorithms for the Leader Election Problem, arXiv.org:0712.4213, 2007.