Quantum Leader Election or The Computational Power of the W State

Prakash Panangaden

joint work with

Ellie D'Hondt

McGill University

Free University Brussels

+ < >

Leader Election

- A system of autonomous *agents* have to choose a special distinguished agent for the purposes of some task.

+ < >

Leader Election

- A system of autonomous *agents* have to choose a special distinguished agent for the purposes of some task.
- Paradigmatic of *distributed* decision making.

+ < >

Leader Election

- A system of autonomous *agents* have to choose a special distinguished agent for the purposes of some task.
- Paradigmatic of *distributed* decision making.
- That's easy: designate a leader when the system is set up.

+ < >

Leader Election

- A system of autonomous *agents* have to choose a special distinguished agent for the purposes of some task.
- Paradigmatic of *distributed* decision making.
- That's easy: designate a leader when the system is set up.
- Not always appropriate: what happens if the designated leader crashes?

+ < >

Leader Election

- A system of autonomous *agents* have to choose a special distinguished agent for the purposes of some task.
- Paradigmatic of *distributed* decision making.
- That’s easy: designate a leader when the system is set up.
- Not always appropriate: what happens if the designated leader crashes?
- Designate a backup ...

Leader Election

- A system of autonomous *agents* have to choose a special distinguished agent for the purposes of some task.
- Paradigmatic of *distributed* decision making.
- That’s easy: designate a leader when the system is set up.
- Not always appropriate: what happens if the designated leader crashes?
- Designate a backup ...
- What if membership in the group changes dynamically?

+ < >

Anonymous Systems

- We work in a system where all the agents execute the same program and start in the same initial state.

+ < >

Anonymous Systems

- We work in a system where all the agents execute the same program and start in the same initial state.
- We assume that agents cannot be *named*.

+ < >

Anonymous Systems

- We work in a system where all the agents execute the same program and start in the same initial state.
- We assume that agents cannot be *named*.
- We want all agents to have an equal chance of being the leader.

+ < >

Anonymous Systems

- We work in a system where all the agents execute the same program and start in the same initial state.
- We assume that agents cannot be *named*.
- We want all agents to have an equal chance of being the leader.
- We assume that communication takes place in rounds and that all agents communicate with all other agents in every step: broadcast.

+ < >

The Classical Situation

- Leader election cannot be solved: Angluin 1980.

+ < >

The Classical Situation

- Leader election cannot be solved: Angluin 1980.
- The initial state is symmetric and there is no mechanism to break the symmetry.

+ < >

The Classical Situation

- Leader election cannot be solved: Angluin 1980.
- The initial state is symmetric and there is no mechanism to break the symmetry.
- Much effort in "almost" anonymous situations, special patterns of interconnectivity and **probabilistic solutions**.

+ < >

Using Probability

- If two processes have coins they can elect a leader by tossing their coins. The one who gets “heads” is the leader.

+ < >

Using Probability

- If two processes have coins they can elect a leader by tossing their coins. The one who gets “heads” is the leader.
- If both get “heads” or both get “tails” they toss again.

+ < >

Using Probability

- If two processes have coins they can elect a leader by tossing their coins. The one who gets “heads” is the leader.
- If both get “heads” or both get “tails” they toss again.
- They are not guaranteed to terminate though they will terminate with probability 1.

+ < >

Using Probability

- If two processes have coins they can elect a leader by tossing their coins. The one who gets "heads" is the leader.
- If both get "heads" or both get "tails" they toss again.
- They are not guaranteed to terminate though they will terminate with probability 1.
- Expected number of rounds is just 2.

+ < >

What Can be Done With Quantum Resources?

- We can obviously mimic the probabilistic solutions.

+ < >

What Can be Done With Quantum Resources?

- We can obviously mimic the probabilistic solutions.
- Can we come up with a technique that is *guaranteed* to terminate after some fixed number of rounds?

+ < >

What Can be Done With Quantum Resources?

- We can obviously mimic the probabilistic solutions.
- Can we come up with a technique that is *guaranteed* to terminate after some fixed number of rounds?
- Can we ensure that each one has equal chance of being the leader?

+ < >

Using a Bell pair for Leader Election

- Suppose that two agents want to choose one of themselves as a leader and they share a Bell pair.

+ < >

Using a Bell pair for Leader Election

- Suppose that two agents want to choose one of themselves as a leader and they share a Bell pair.
- They can each measure $|0\rangle\langle 0| + |1\rangle\langle 1|$; the one who gets $|1\rangle$ is the leader.

+ < >

Using a Bell pair for Leader Election

- Suppose that two agents want to choose one of themselves as a leader and they share a Bell pair.
- They can each measure $|0\rangle\langle 0| + |1\rangle\langle 1|$; the one who gets $|1\rangle$ is the leader.
- Each agent has the same chance of getting elected, the process is guaranteed to terminate in one step. Exactly what is classically impossible!

Using a Bell pair for Leader Election

- Suppose that two agents want to choose one of themselves as a leader and they share a Bell pair.
- They can each measure $|0\rangle\langle 0| + |1\rangle\langle 1|$; the one who gets $|1\rangle$ is the leader.
- Each agent has the same chance of getting elected, the process is guaranteed to terminate in one step. Exactly what is classically impossible!
- Does this generalize to more than two agents?

Networks of Agents

- A network of agents is a system in which several inter-communicating agents carry out computations concurrently.

+ < >

Networks of Agents

- A network of agents is a system in which several inter-communicating agents carry out computations concurrently.
- Synchronous: communication occurs in fixed rounds of broadcasts. Communication is classical, we send bits not qubits.

+ < >

Networks of Agents

- A network of agents is a system in which several inter-communicating agents carry out computations concurrently.
- Synchronous: communication occurs in fixed rounds of broadcasts. Communication is classical, we send bits not qubits.
- Anonymous: All agents run the same protocol and there is no mechanism for naming the agents.

+ < >

Networks of Agents

- A network of agents is a system in which several inter-communicating agents carry out computations concurrently.
- Synchronous: communication occurs in fixed rounds of broadcasts. Communication is classical, we send bits not qubits.
- Anonymous: All agents run the same protocol and there is no mechanism for naming the agents.
- All agents start in the same state.

+ < >

Networks of Agents

- A network of agents is a system in which several inter-communicating agents carry out computations concurrently.
- Synchronous: communication occurs in fixed rounds of broadcasts. Communication is classical, we send bits not qubits.
- Anonymous: All agents run the same protocol and there is no mechanism for naming the agents.
- All agents start in the same state.
- Known network size.

Networks of Agents

- A network of agents is a system in which several inter-communicating agents carry out computations concurrently.
- Synchronous: communication occurs in fixed rounds of broadcasts. Communication is classical, we send bits not qubits.
- Anonymous: All agents run the same protocol and there is no mechanism for naming the agents.
- All agents start in the same state.
- Known network size.
- No faulty or malicious agents.

+ < >

Anonymity

- All agents are completely identical: they do not carry individual names with which they can be identified.

+ < >

Anonymity

- All agents are completely identical: they do not carry individual names with which they can be identified.
- The initial network specification must be invariant under permutations of agents.

+ < >

Anonymity

- All agents are completely identical: they do not carry individual names with which they can be identified.
- The initial network specification must be invariant under permutations of agents.
- Agents start out in identical local classical states.

+ < >

Anonymity

- All agents are completely identical: they do not carry individual names with which they can be identified.
- The initial network specification must be invariant under permutations of agents.
- Agents start out in identical local classical states.
- Angluin 80: there is no solution to leader election that is guaranteed to terminate.

+ < >

Anonymity in the Quantum Setting

- Each processor must have the same “local view” of its quantum state. This can be formalized by requiring that they have the same reduced density matrix.

+ < >

Anonymity in the Quantum Setting

- Each processor must have the same “local view” of its quantum state. This can be formalized by requiring that they have the same reduced density matrix.
- We adopt the slightly stronger assumption that the initial quantum state is invariant under permutation of the agents subspaces.

+ < >

Anonymity in the Quantum Setting

- Each processor must have the same “local view” of its quantum state. This can be formalized by requiring that they have the same reduced density matrix.
- We adopt the slightly stronger assumption that the initial quantum state is invariant under permutation of the agents subspaces.
- This rules out some states like $|0\rangle_A|0\rangle_B + e^{i\theta}|1\rangle_A|1\rangle_B$.

+ < >

Total Correctness

A *totally correct* distributed protocol is a protocol that is *terminating*, i.e. it reaches a terminal configuration in each computation, and *partially correct*, i.e. for each of the reachable terminal configurations the goal of the protocol is achieved.

+ < >

Easy Consequences

- No totally correct leader election protocol exists without prior shared entanglement.

Easy Consequences

- No totally correct leader election protocol exists without prior shared entanglement.
- Totally correct leader election algorithms for anonymous quantum networks are *fair*, i.e. each processor has equal probability of being elected leader.

+ < >

Three party states

- What kind of entangled states are there for 3 parties?

+ < >

Three party states

- What kind of entangled states are there for 3 parties?
- There are *inequivalent* enatngled states, numerical entanglement measures are inadequate.

+ < >

Three party states

- What kind of entangled states are there for 3 parties?
- There are *inequivalent* enatngled states, numerical entanglement measures are inadequate.
- $W := |100\rangle + |010\rangle + |001\rangle$ and $GHZ := |000\rangle + |111\rangle$.

+ < >

Three party states

- What kind of entangled states are there for 3 parties?
- There are *inequivalent* enatngled states, numerical entanglement measures are inadequate.
- $W := |100\rangle + |010\rangle + |001\rangle$ and $GHZ := |000\rangle + |111\rangle$.
- Both are maximally entangled but W is persistent, it requires two measurements to destroy the entanglement. GHZ becomes disentangled with just one measurement.

+ < >

Three party states

- What kind of entangled states are there for 3 parties?
- There are *inequivalent* enatngled states, numerical entanglement measures are inadequate.
- $W := |100\rangle + |010\rangle + |001\rangle$ and $GHZ := |000\rangle + |111\rangle$.
- Both are maximally entangled but W is persistent, it requires two measurements to destroy the entanglement. GHZ becomes disentangled with just one measurement.
- W_n requires $n-1$ measurements to destroy the entanglement while GHZ_n becomes disentangled with just one measurement.

+ < >

QLE with the W state

- $q \leftarrow i$th qubit of W_n
  b=0
  result=wait

+ < >

QLE with the W state

- $q \leftarrow i$th qubit of W_n
  b=0
  result=wait
- **b**:= measure q

+ < >

QLE with the W state

- $q \leftarrow i$th qubit of W_n
  b=0
  result=wait
- **b**:= measure q
- if **b** $= 1$ then **result**:= leader, else **result**:=follower.

+ < >

The Main result

If a system of n agents with a shared quantum state can solve leader election then they must have had the W_n state or its “mirror image.”

+ < >

k-symmetric moves

Suppose an n-partite state $|\psi\rangle \in \mathcal{H}^{\otimes n}$, where $\mathcal{H}$ is a 2^m-dimensional Hilbert space, is distributed over n processors. We say that there exists a k**-symmetric move** for the processors $i_1, \ldots, i_k$ with respect to $|\psi\rangle$, where $0 < k \leq n$, if for all observables $M = \sum_{j=1}^{J} \lambda_j P_j$, with $J \leq 2^m$ and all P_j projectors, we have that

$$\exists l \in \{1, \ldots, J\} : (P_l)^{\otimes k}_{i_1,\ldots,i_k} (P_{j_{k+1} \neq l})_{i_{k+1}} \ldots (P_{j_n \neq l})_{i_n} |\psi\rangle \neq 0 \tag{0}$$

+ < >

k-symmetric moves 2

The idea is that *all* measurements potentially give identical measurement results for k out of the n processors.

Because anonymous networks are invariant under permutations we need not specify any particular subset of processors.

+ < >

Proof Ideas

- k-symmetric moves exist if and only if a certain form of the state holds.

+ < >

Proof Ideas

- k-symmetric moves exist if and only if a certain form of the state holds.
- If a k-symmetric move is possible this will persist in any successor state.

+ < >

Proof Ideas

- k-symmetric moves exist if and only if a certain form of the state holds.
- If a k-symmetric move is possible this will persist in any successor state.
- Any protocol for which k-symmetric branches exist with k different from 1 or $n - 1$ is not totally correct.

+ < >

Proof Ideas

- k-symmetric moves exist if and only if a certain form of the state holds.
- If a k-symmetric move is possible this will persist in any successor state.
- Any protocol for which k-symmetric branches exist with k different from 1 or $n - 1$ is not totally correct.
- From the form of the state in the first item we get the desired result.

+ < >

Proof Ideas

- k-symmetric moves exist if and only if a certain form of the state holds.
- If a k-symmetric move is possible this will persist in any successor state.
- Any protocol for which k-symmetric branches exist with k different from 1 or $n-1$ is not totally correct.
- From the form of the state in the first item we get the desired result.
- We can extend to the case where they share more than 1 qubit each.

+ < >

Without Anonymity

- Suppose that we set up the state $W_{2,n-2}$ and give each processor one qubit. Each processor measures its qubit.

+ < >

Without Anonymity

- Suppose that we set up the state $W_{2,n-2}$ and give each processor one qubit. Each processor measures its qubit.
- If it gets $|1\rangle$ it becomes a candidate otherwise it is a voter. Now we can hold an election and choose a leader, if n is odd there is a unique winner.

+ < >

Without Anonymity

- Suppose that we set up the state $W_{2,n-2}$ and give each processor one qubit. Each processor measures its qubit.
- If it gets $|1\rangle$ it becomes a candidate otherwise it is a voter. Now we can hold an election and choose a leader, if n is odd there is a unique winner.
- But how can the voters name their preference in an anonymous network?

+ < >

Using Network Structure

- If the network is a ring then each voter sends a message clockwise.

+ < >

Using Network Structure

- If the network is a ring then each voter sends a message clockwise.
- Voters pass on messages they receive, candidates count messages that they receive.

+ < >

Using Network Structure

- If the network is a ring then each voter sends a message clockwise.
- Voters pass on messages they receive, candidates count messages that they receive.
- As soon as one of them gets more than half the votes it will declare itself leader.

+ < >

Conclusions

- The leader election problem can be exactly solved with shared correlation; either with classical correlated random variables or with the W state.

+ < >

Conclusions

- The leader election problem can be exactly solved with shared correlation; either with classical correlated random variables or with the W state.
- The W state is the *only* state that has this power. It is worth studying the different kinds of entanglement and their relative power in different computational situations.

+ < >

Conclusions

- The leader election problem can be exactly solved with shared correlation; either with classical correlated random variables or with the W state.
- The W state is the *only* state that has this power. It is worth studying the different kinds of entanglement and their relative power in different computational situations.
- These kind of symmetry breaking arguments have been used to prove expressiveness theorems before (e.g. Palamidessi 2003).

+ < >

Conclusions

- The leader election problem can be exactly solved with shared correlation; either with classical correlated random variables or with the W state.
- The W state is the *only* state that has this power. It is worth studying the different kinds of entanglement and their relative power in different computational situations.
- These kind of symmetry breaking arguments have been used to prove expressiveness theorems before (e.g. Palamidessi 2003).
- A group of researchers in Japan have - independently - given a quantum algorithm for leader election. They allow qubits to be passed around.

+ < >