Quantum Leader Election via Exact Amplitude Amplification

Seiichiro Tani[*] [†]
(Joint work with Hirotada Kobayashi[‡] and Keiji Matsumoto[‡†])

* NTT Communication Science Laboratories., NTT Corporation

† Quantum Computation and Information Project, ERATO, JST

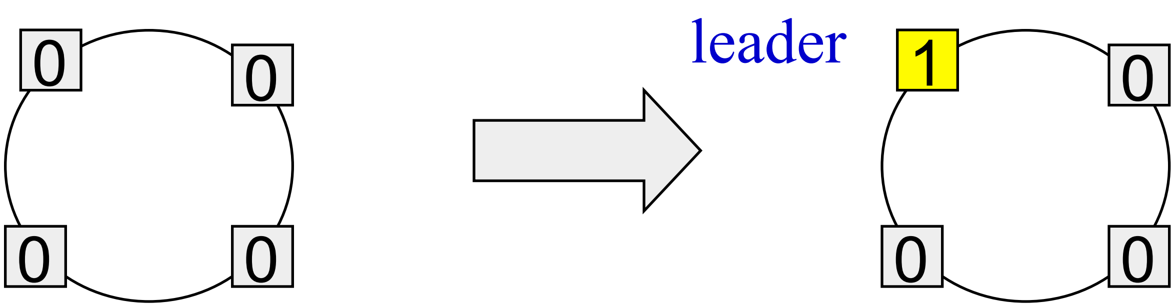
‡ Foundations of Information Research Division, NII

Anonymous Leader Election Problem (LE)

Given *n* parties connected by communication links, elect a unique leader from among *n* parties.

Under the anonymity Condition:

- Initially, all parties are in the same state.
  - ⇒Every party needs to perform the same algorithm.



Negative Results in Classical Cases

- Case 1: # of parties is given,
  No classical algorithm can solve LE exactly for many network topologies.
  ("exact" = "zero-error" and "bounded time")

- Case 2: Only the upper bound of # of parties is given,
  No classical algorithm can solve LE even with zero-error for any network topology having cycles.

Previous Quantum Results [TKM05]

For parties connected by quantum communication links:

- Case 1: n (# of parties) is given,

  LE can be solved exactly
  in poly (in n) time/communication complexity
  for any network topology.

- Case 2: Only N (the upper bound of # of parties) is given,

  LE can be solved exactly
  in poly (in N) time/communication complexity
  for any network topology.

Our Result

For given n,

- New general algorithm that solves LE
  for any network topology
  via exact amplitude amplification
  in $O(n^2)$ rounds and $O(n^4)$ communication complexity.
  (Same complexity as that of the first algorithm in [TKM05])

- Fast algorithm that solves LE
  only when n is a power of two
  in $O(n)$ rounds (faster than the algorithms in [TKM05])
  at the cost of $O(n^6 \log n)$ communication complexity.

(# Our algorithms work well
even when only the upper bound N of n is given.)

Algorithm I Overview

1. Let all parties be eligible to be the leader.
2. For $m = n$ down to 2, repeat PartyReduction(m), which works such that:
   - If m equals # of eligible parties, # of eligible parties is decreased by at least 1 (but not decreased to 0)
   - Otherwise, # of eligible parties is decreased or unchanged
3. The party still remaining eligible is the unique leader.

▼ In Step 2, always $m \geq$ (# of eligible parties)

⇒After Step 2, only one party remains eligible

▼ Even if only the upper bound of n is given, the algorithm works well by using the bound instead of n.

Consistent/inconsistent over eligible parties

Each party has *c* bits

⇒All parties share *cn*-bit string *s*.

- String *s* is inconsistent over eligible parties, if all eligible parties do not have the same *c*-bit values.
- State ϕ is inconsistent over eligible parties, If ϕ is a superposition of inconsistent strings.

Key Observation used to construct PartyReduction (m)

All eligible parties share an inconsistent state.

⇓

Eligible parties can be reduced by at least one (but cannot be reduced into 0 party) by

1. Measuring qubits.
2. Letting only eligible parties having the maximum value among eligible parties remain eligible.

PartyReduction (m)

(1) Share an inconsistent state
with prob. 1 if m equals # of eligible parties.

(2) By measurement, parties obtain an inconsistent string.

(3) Only eligible parties that have the maximum value among eligible parties remain eligible.

PartyReduction (m) meets requirements described in overview:

- if m equals # of eligible parties,
  (3) reduces # of eligible parties by at least 1
  (but not to 0).
- Otherwise # of eligible parties does not increase.

Subgoal

Share an inconsistent state among eligible parties with certainty if *k*= # of eligible parties.

(1) Each party prepares one qubits.

(2) Each eligible party initializes them to $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

Each non-eligible party initializes them to $|0\rangle$

System state: $|\phi\rangle = \left(\sum_{i=0}^{2^k - 1} |i\rangle \right) |0\rangle^{\otimes(n-k)}$

(3) Amplify the amplitude of only inconsistent states by exact amplitude amplification in O(n) rounds and $O(n^3)$ communication complexity.

Exact amplitude amplification [BHMT02]

- A: any quantum algorithm that uses no measurement to find a truth assignment for any Boolean function χ
- If the initial success probability a is $\geq 1/4$,

$$AF_0(\phi)A^{-1}F_\chi(\varphi)$$

gives a correct assignment with certainty by setting ϕ and φ ($0 \leq \phi$, $\varphi < 2\pi$) to some appropriate values depending on a, where

$$F_\chi(\varphi): |x\rangle \mapsto \begin{cases} e^{i\varphi}|x\rangle & \text{if } \chi(x)=1 \\ |x\rangle & \text{otherwise} \end{cases} \qquad F_0(\phi): |x\rangle \mapsto \begin{cases} e^{i\phi}|x\rangle & \text{if } x = 00\cdots0 \\ |x\rangle & \text{otherwise} \end{cases}$$

Requirements:

- Exact value of a needs to be known
- $a \geq 1/4$

Proof of Step (3) (1/3)

- Set A to Hadamard operator H.
- Set a to the probability of measuring inconsistent states, i.e, χ(x)=1 iff x is an inconsistent string.
  - For 2^k dimensional space,

$$a = 1 - \frac{2}{2^k} > \frac{1}{4}$$

  since all states but $|00\ldots0\rangle$ and $|11\ldots1\rangle$ are inconsistent.
- Apply exact amplitude amplification $AF_0(\phi)A^{-1}F_\chi(\varphi)$ to $A|\phi\rangle$, where
  - $F_0(\phi)$ and $F_\chi(\varphi)$ need to be performed in a distributed manner, i.e., every party needs to perform identical operations because of anonymity condition.

Proof of Step (3) (2/3)

How to Perform $F_\chi(\varphi)$ in a distributed manner?

- Suppose *n* parties share $\left|\phi\right\rangle = \left(\sum_{i=0}^{2^k-1}\left|i\right\rangle\right)\left|0\right\rangle^{\otimes(n-k)}$ in their one qubit registers R.
- Every party does the next steps.

1. Prepares an ancillary qubit in register S.
2. Check inconsistency of a string corresponding to each basis state in $O(n)$ rounds and $O(n^3)$ communication complexity as described in [TKM05].
3. Write the result "consistent" or "inconsistent" to the content of S.

Proof of Step (3) (3/3)

4. Apply the next unitary operator to the contents of R and S

$$|r\rangle|s\rangle \mapsto \begin{cases} e^{\frac{i\varphi}{n}}|r\rangle|s\rangle & \text{if } s \text{ is "inconsistent"} \\ |r\rangle|s\rangle & \text{otherwise} \end{cases}$$

where r is the content of R, and s is the content of S.

This essentially realizes $F\chi(\varphi)$ as a whole:

$$|i\rangle|s\rangle^{\otimes n} \mapsto \begin{cases} e^{i\varphi}|i\rangle|s\rangle^{\otimes n} & \text{if } s \text{ is "inconsistent"} \\ |i\rangle|s\rangle^{\otimes n} & \text{otherwise} \end{cases}$$

5. Invert every computation and communication of step 2 to disentangle S.

$F_0(\phi)$ can be performed in a similar way.

Algorithm restricted to the case where n is a power of two

Basic Proposition

Proposition

If n is a power of two,

a unique leader can be elected in O(n) rounds and $O(n^6 \log n)$ communication complexity

when there exists some value x such that the number of parties having x is odd.

Proof is by combining the results in [YK96] and [TKM05].

⇓

We'll try to make *n* parties share a superposition $|\phi_{odd}\rangle$ of only the states whose binary expression has the Hamming weight 1 (mod 2), in anonymous setting.

Sharing $|\phi_{\text{odd}}\rangle$

Every party performs the next steps.

1. Prepare $(|0\rangle + |1\rangle)/2^{1/2}$ and $|0\rangle$ in one-qubit register R and S, respectively.
2. Set to S the Hamming weight (mod 2) of the contents of all parties' s Rs.
3. Measure the qubit in S, and set the result to y.
4. If y=0, apply $U_n V$ to the qubit in R, where.

$$U_n = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\frac{\pi}{n}} \\ -e^{i\frac{\pi}{n}} & 1 \end{pmatrix}, \quad V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

5. Measure the qubit in R.

Summary

- We gave two algorithms that exactly solve LE for the given number *n* of parties.
- The first algorithm uses the exact amplitude amplification in a distributed manner in anonymous setting,

  and runs in O(n^2) rounds and O(n^4) comm. complexity for any network.
- The second one is restricted to the case where n is a power of two, and requires O(n^6log *n*) communication complexity,

  but takes only linear rounds in n.