TEXAS A&M UNIVERSITY
Engineering

Element Distinctness

Presenter: Yu Shen

Outline

TEXAS A&M UNIVERSITY
Engineering

- Introduction
- Quantum random walk algorithm
- Lower bound proof

Introduction

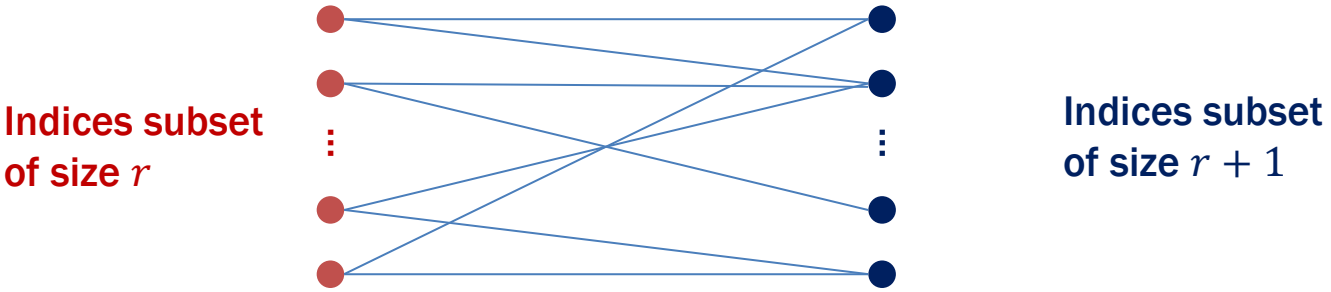
TEXAS A&M UNIVERSITY
Engineering

- Element distinctness: given a list of N numbers, are they all distinct?
- In classical computer…
  - Comparison based: $\Omega(N \log N)$
  - General model: $\Omega(N)$
- Application: finding triangles in graph; searching 2D grid, …

Quantum random walk algorithm

TEXAS A&M UNIVERSITY
Engineering

- The intuitive quantum solution (simply use Grover's searching)
  - O(N) time
- A graph with $\binom{N}{r} + \binom{N}{r+1}$ vertices, vertices corresponding to a subset of indices.



- Searching this graph consumes $O\left(N^{2/3}\right) \cdot O\left(N^{1/3}\right) = O(N)$ time.

Quantum random walk algorithm

TEXAS A&M UNIVERSITY
Engineering

- Improve the time complexity by both graph searching and random walk.
- We have indices $[N]$, and value domain $[M]$, let $r = N^{2/3}$.
- Prepare 3 types of registers:
  - $|S\rangle$ stores at most $r + 1$ indices $([1,2, \dots, N])$
  - $|y\rangle$ stores one index
  - $|x\rangle$ stores values querying $x_i, i \in S$.
- Totally, it consumes $O(r(\log M + \log N))$ qubits.

Quantum random walk algorithm

TEXAS A&M UNIVERSITY
Engineering

- Step 1 Prepare uniform superposition

$$\frac{1}{\sqrt{\binom{N}{r}(N-r)}}\sum_{|S|=r, y\notin S}|S\rangle|y\rangle.$$

- Step2 Query the values in S

$$\frac{1}{\sqrt{\binom{N}{r}(N-r)}}\sum_{|S|=r, y\notin S}|S\rangle|y\rangle\bigotimes_{i\in S}|x_i\rangle.$$

- Step 3 $O(N^{1/3})$ times repeat…
  - Step 3.1 do the conditional flipping.
  - Step 3.2 Perform $O(N^{1/3})$ steps random walk (each step contains 2 queries).
- Step 4 Measure the final state, check if $|S\rangle$ contains collision (i.e., $i, j \in S \wedge x_i = x_j$).

Quantum random walk algorithm

TEXAS A&M UNIVERSITY
Engineering

- Random walk part:
- 1. Apply “diffusion transformation”, mapping $|S\rangle|y\rangle$ to

$$|S\rangle[\left(-1+\frac{2}{N-r}\right)|y\rangle+\frac{2}{N-r}\sum_{y'\notin S,y'\neq y}|y'\rangle].$$

- 2. Add y to $|S\rangle$, change $|x\rangle$ to a vector of length $k+1$.
- 3. Query x_y and insert to $|x\rangle$.
- 4. Mapping $|S\rangle|y\rangle$ to

$$|S\rangle[\left(-1+\frac{2}{r+1}\right)|y\rangle+\frac{2}{r+1}\sum_{y'\in S,y'\neq y}|y'\rangle].$$

- 5. Erase x corresponding to new y by querying for x_y.
- 6. Removing one part in $|x\rangle$ according to y, also remove y in S.

Quantum random walk algorithm

TEXAS A&M UNIVERSITY
Engineering

- Correctness
- 1. Algorithm's state always stays in a 5-dimensional subspace of H.
- 2. The eigenvalues for the unitary transformation induced by one step of the quantum restricted to this subspace.
- 3. Operations in the iteration amplifies the probability to observe desired result:
  - 3.1 Iterations can be represented by a sequence of the form $(U^2U^1)^{t_1}$ with U_1 being a conditional phase flip and U_2 being a unitary transformation whose eigenvalues have certain properties w.r.t. steps of quantum walk).
  - 3.2 Such sequence has certain properties, which implies that the algorithm finds the collision with a constant probability.

Lower bound proof

TEXAS A&M UNIVERSITY
Engineering

- Element distinctness needs $\Omega(N^{2/3})$ quantum queries.
- Collision problem: find a pair $x, y \in \{1,2,\dots,N\}$ s.t. $f(x) = f(y)$.
- Solving collision problem needs $\Omega(N^{1/3})$ quantum queries.
- Consider a reduction from collision problem to element distinctness:
  - if we solve the element distinctness problem restricted by the oracle function on a random set $\Theta(\sqrt{N})$ inputs, then with high probability we will run into a collision.
  - Birthday paradox

Lower bound proof

TEXAS A&M UNIVERSITY
Engineering

- Solving collision problem needs $\Omega(N^{1/3})$ quantum queries.
- Reduction from half-two-to-one collision to two-to-one collision.
  - Half-wo-to-one asks if half of the inputs are mapped 1-to-1, and half of the inputs are mapped 2-to-1.
  - Half-two-to-one can be solved in $\Omega(N^{1/3})$ quantum queries, this is proved by the lower bound of quantum queries with the degree of polynomials.
  - We can then use constant slow down to construct a collision algorithm with the subroutine of half-two-to-one algorithm.

Reference

TEXAS A&M UNIVERSITY
Engineering

- A. Yao, “Near-optimal time-space tradeoff for element distinctness”
- S. Aaronson and Y. Shi, “Quantum lower bounds for the collision and the element distinctness problems”
- A. Ambainis, “Quantum walk algorithm for element distinctness”
- J. Kempe, “Quantum random walks: An introductory”

TEXAS A&M UNIVERSITY

Engineering