Element Distinctness by Quantum Walk Algorithm

Ming-Tso Wei, Yuqi Yun

May 1, 2017

Outline

- Problem Statement
- Quantum Walk Algorithm
- Element Distinctness using Quantum Walk
- Results
  - Simulation for k=2 case
  - Circuit Implementation
- Conclusion

Problem Statement

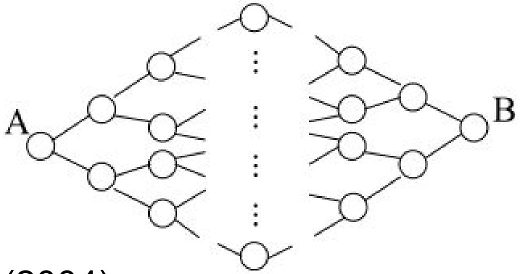
- Given a set S with N elements, are all the elements distinct?
- Element k-distinctness or k collision:
  - A subset of k equal elements: $x_{i1}=...=x_{ik}$
- Element Distinctness:
  - Finding two equal elements: k=2

Element Distinctness (k=2): Classical vs Quantum

- Classical: $\Omega(N)$ for query and $O(N\log N)$ for sorting
- Quantum:
  - Buhrman et al. (2004): $O(N^{3/4})$ queries
  - Aaronson & Shi (2004): lower bound $O(N^{2/3})$
  - Ambainis (2007): $O(N^{2/3})$ by quantum walk

Quantum Walk Algorithm

- Classical: random walk on a graph
- Quantum Walk: superposition nature→ randomness
- Quantum Walk Search on a graph
  - General: quadratically faster than classical search
  - Some special graph (ex: Glued tree): exponentially faster

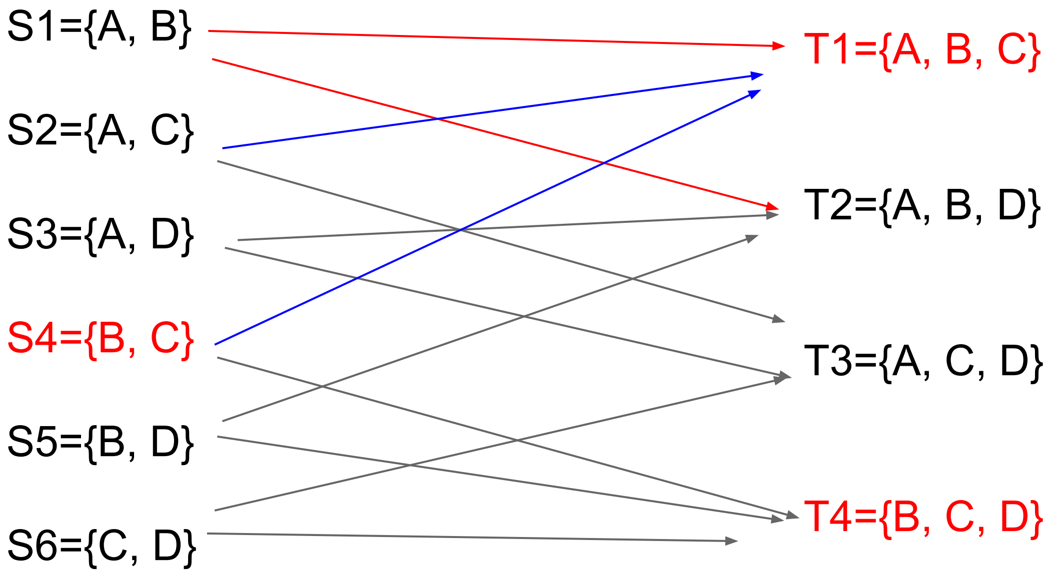


Ambainis, arXiv (2004)

Element Distinctness using Quantum Walk

$x=(x_A, x_B, x_C, x_D)$

Total number of queries: M+r



N=4
r=2
k=2

Element Distinctness (Step 1 and 2)

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

2. Query all x_i for $i \in S$. This transforms the state to

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

$|\phi_{j,l}>$ $\quad |S \cap B, C| = j$ and $|y \cap B, C| = l$

$$< \phi_{j,0}|\phi_{start} >= \frac{\sqrt{\binom{k}{j}\binom{n-k}{r-j}((n-k)-(r-j))}}{\sqrt{\binom{n}{r}(n-r)}}$$

$$< \phi_{j,1}|\phi_{start} >= \frac{\sqrt{\binom{k}{j}\binom{n-k}{r-j}(k-j))}}{\sqrt{\binom{n}{r}(n-r)}}$$

$$|\phi_{0,0} >= 0$$
$$|\phi_{0,1} >= \tfrac{1}{\sqrt{2}}|AD, B > + \tfrac{1}{\sqrt{2}}|AD, C >$$
$$|\phi_{1,0} >= \tfrac{1}{2}|AB, D > + \tfrac{1}{2}|AC, D > + \tfrac{1}{2}|BD, A > + \tfrac{1}{2}|CD, A >$$
$$|\phi_{1,1} >= \tfrac{1}{2}|AB, C > + \tfrac{1}{2}|AC, B > + \tfrac{1}{2}|BD, C > + \tfrac{1}{2}|CD, B >$$
$$|\phi_{2,0} >= \tfrac{1}{\sqrt{2}}|BC, A > + \tfrac{1}{\sqrt{2}}|BC, D >$$

$$(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}})$$

Element Distinctness (Step 3 and 4)

3. $t_1 = O((N/r)^{k/2})$ times repeat:

   (a) Apply the conditional phase flip (the transformation $|S\rangle|y\rangle|x\rangle \to -|S\rangle|y\rangle|x\rangle$) for S such that $x_{i_1} = x_{i_2} = \ldots = x_{i_k}$ for k distinct $i_1, \ldots, i_k \in S$.

   (b) Perform $t_2 = O(\sqrt{r})$ steps of the quantum walk (algorithm $\boxed{1}$).

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\text{apply } (U_2U_1)^{t_2}U^{t1} \text{ to } |\phi_{start} >$$

4. Measure the final state. Check if S contains a k-collision and answer "there is a k-collision" or "there is no k-collision", according to the result.

Element Distinctness (Step 3 and 4)

3. $t_1 = O((N/r)^{k/2})$ times repeat:

   (a) Apply the conditional phase flip (the transformation $|S\rangle|y\rangle|x\rangle \rightarrow -|S\rangle|y\rangle|x\rangle$) for S such that $x_{i_1} = x_{i_2} = \ldots = x_{i_k}$ for k distinct $i_1, \ldots, i_k \in S$.

   (b) Perform $t_2 = O(\sqrt{r})$ steps of the quantum walk (algorithm $\boxed{1}$).

$$D_m = \begin{pmatrix} -1+\frac{2}{m} & \frac{2}{m} & \ldots & \frac{2}{m} \\ \frac{2}{m} & -1+\frac{2}{m} & \ldots & \frac{2}{m} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{2}{m} & \frac{2}{m} & \ldots & -1+\frac{2}{m} \end{pmatrix}$$

$$U1 = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 & 0 \\ 0 & \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{2\sqrt{2}}{3} \\ 0 & 0 & 0 & \frac{2\sqrt{2}}{3} & -\frac{1}{3} \end{bmatrix}$$

$$\text{apply } (U_2U_1)^{t_2}U^{t1} \text{ to } |\phi_{start} >$$

4. Measure the final state. Check if S contains a k-collision and answer "there is a k-collision" or "there is no k-collision", according to the result.

Simulation for arbitrary N and k=2

- Mathematica Results

$$N = 15, r = 6, t1 = 2, t2 = 2$$
$$p = (0.00256282, 0.169971, 0.00734126, 0.087622, 0.732503)$$
$$N = 500, r = 62, t1 = 8, t2 = 6$$
$$p = (0.0307232, 0.0496646, 0.0118242, 0.161007, 0.746782)$$
$$N = 234857, r = 3806, t1 = 61, t2 = 46$$
$$p = (0.0226436, 0.0108335, 0.000577899, 0.242028, 0.723917)$$

Circuit Implementation for N=4, k=2

- Initial state: $(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}})$
- Reduction to two-qubit problem
  - Invariance of $|\phi_{0,0}>$

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix} \quad U1 = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad U2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 & 0 \\ 0 & \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{2\sqrt{2}}{3} \\ 0 & 0 & 0 & \frac{2\sqrt{2}}{3} & -\frac{1}{3} \end{bmatrix}$$

5x5 matrices

Circuit Implementation for N=4, k=2

- Initial state: $(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}})$
- Reduction to two-qubit problem
  - Invariance of $|\phi_{0,0}>$

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix} \quad U1 = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad U2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 & 0 \\ 0 & \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{2\sqrt{2}}{3} \\ 0 & 0 & 0 & \frac{2\sqrt{2}}{3} & -\frac{1}{3} \end{bmatrix}$$

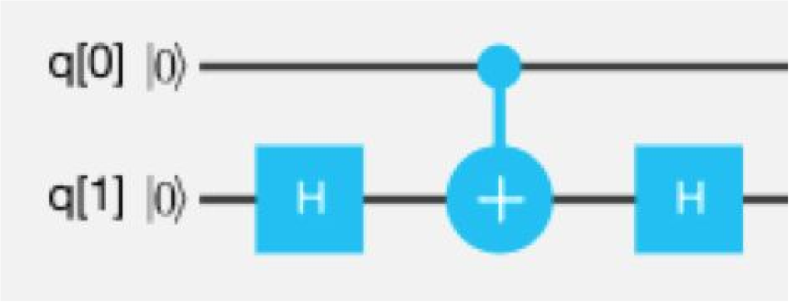
5x5 matrices → 4x4 matrices (two-qubit system)

Circuit Implementation for N=4, k=2

- Initial state: $(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}})$
- Subroutines: U, U1, U2
  - U: conditional phase flip only for $|\phi_{2,0}>$

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

A controlled-Z gate

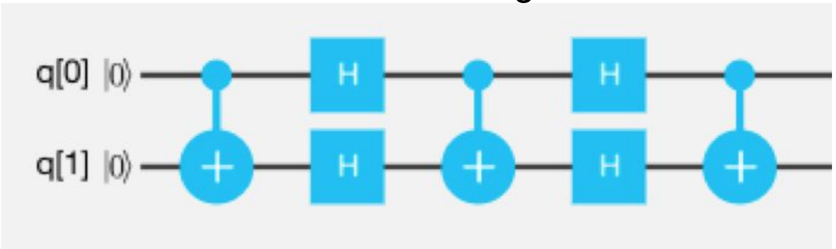


Circuit Implementation for N=4, k=2

- Initial state: $(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}})$
- Subroutines: U, U1, U2
    - U1: step 1-3 for quantum walk

$$U1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

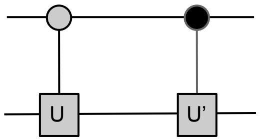
A SWAP gate



Circuit Implementation for N=4, k=2

- Initial state: $\left(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}}\right)$
- Subroutines: U, U1, U2
  - U2: step 4-6 for quantum walk

$$U2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{3} & \frac{2\sqrt{2}}{3} & 0 & 0 \\ 0 & \frac{2\sqrt{2}}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{2\sqrt{2}}{3} \\ 0 & 0 & 0 & \frac{2\sqrt{2}}{3} & -\frac{1}{3} \end{bmatrix}$$



Block diagonal → two controlled U gates

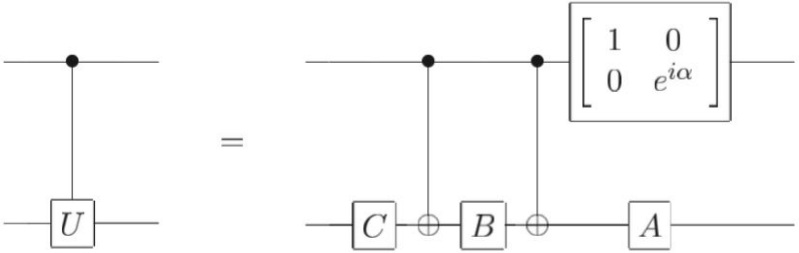
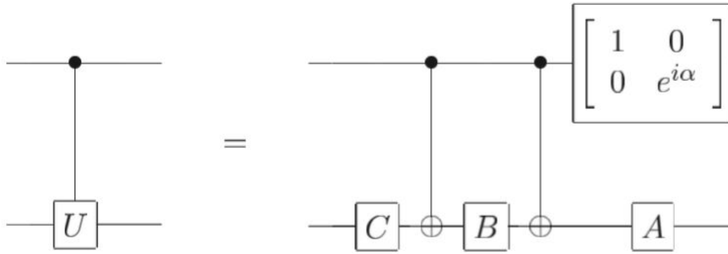
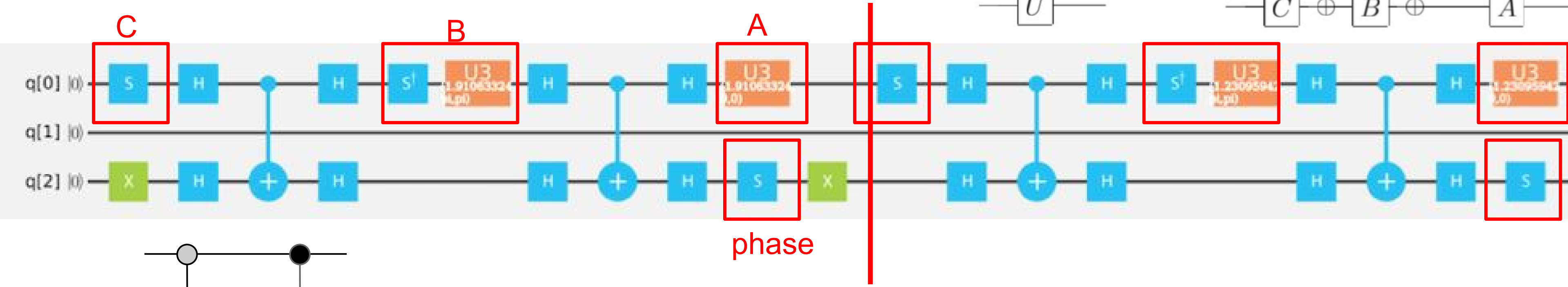


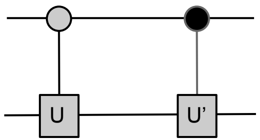
Fig. 4.6 Nielsen & Chuang (2001)

Circuit Implementation for N=4, k=2

- Initial state: $\left(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}}\right)$
- Subroutines: U, U1, U2
  - U2: step 4-6 for quantum walk



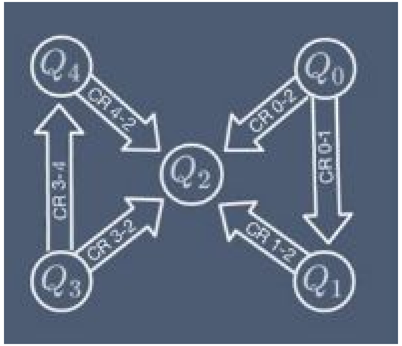




Circuit Implementation for N=4, k=2

- Apply $U_2U_1UU_2U_1U$ on $\left(0, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}}\right)$
- Real topology
  - We chose Q0 and Q2

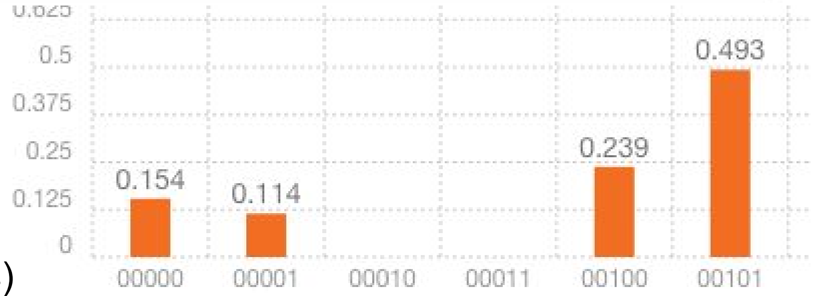
approximated by $\left\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right\}$



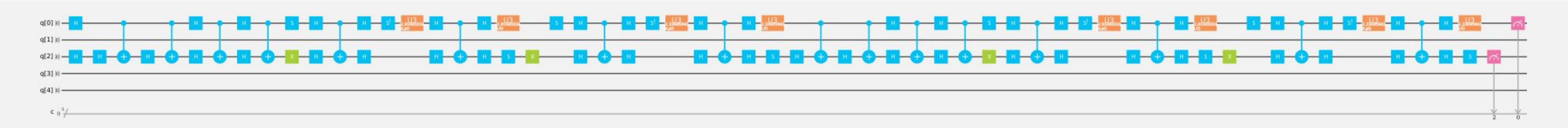
Implementation on IBM Q

	$P(\|\phi_{0,1}>)$	$P(\|\phi_{1,0}>)$	$P(\|\phi_{1,1}>)$	$P(\|\phi_{2,0}>)$
Numerical (Mathematica)	0.100823	0.102881	0.201646	0.59465
IBM Simulator (100 shots)	0.210	0.010	0.220	0.560
IBM Simulator (8192 shots)	0.148	0.031	0.155	0.666
IBM real processor (1024 shots)	0.176	0.093	0.231	0.500
IBM real processor (8192 shots)	0.154	0.114	0.239	0.493

- P~0.6



Real machine (8192 shots)



Discussion

- Limited number of gates on the IBM simulator
  - Not accessible for N>4 cases. $t_1 = O((N/r)^{k/2})$
- Generalization to k-distinctness is challenging
  - Translate 2k+1 by 2k+1 matrices to quantum circuits

Questions?

Thank you!