Quantum walk algorithms: element distinctness and spatial search

Andris Ambainis
Institute for Advanced Study, Princeton

Today's talk

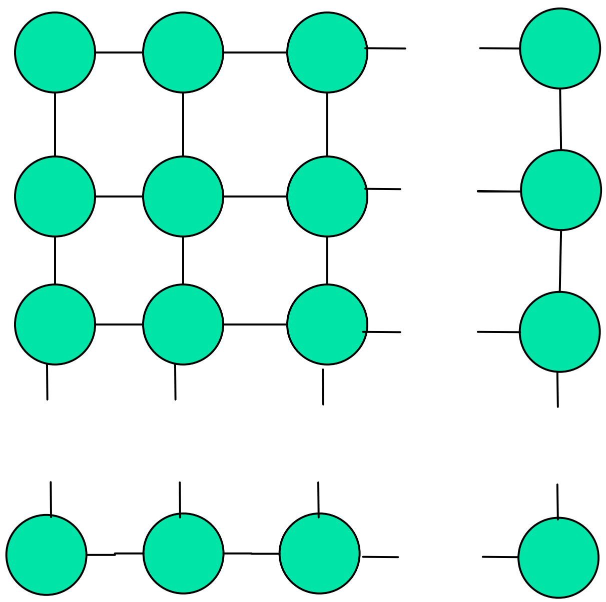
- New technique for quantum algorithms.
- Quantum walks (q. counterparts of random walks).
- Element distinctness.
- Spatial search.

Element distinctness

0	1	0	⋯	0
x_1	x_2	x_3		x_n

- Determine if $x_1, x_2, \ldots, x_N$ contains two equal numbers.
- Classically: N questions.
- Quantum: $O(N^{2/3})$.

Spatial search



- N items on $\sqrt{N}*\sqrt{N}$ grid.
- Some items marked.
- Find marked item.
- Grover: $\Omega(N)$.
- $O(\sqrt{N} \log N)$ time in 2D.
- $O(\sqrt{N})$ time in 3D.

Random walk on line

…	-2	-1	0	1	2	…

- Start in location 0.
- In every step, move left with probability ½, move right with probability ½.

Random walk on line

…	-2	-1	0	1	2	…

- State (x, d), x –location, d-direction.
- At each step,
  - Let d=left with prob. ½, d=right w. prob. ½.
  - (x, left) => (x-1, left);
  - (x, right) => (x+1, right).

Quantum walk on line

…	-2	-1	0	1	2	…

- States |x, d⟩, x –location, d-direction.

"Coin flip":

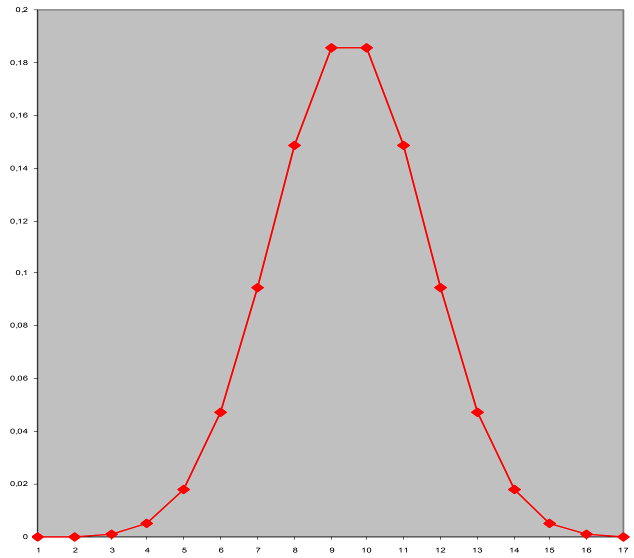
$$\begin{cases} |left> \rightarrow \frac{1}{\sqrt{2}}|left> + \frac{1}{\sqrt{2}}|right> \\ |right> \rightarrow \frac{1}{\sqrt{2}}|left> - \frac{1}{\sqrt{2}}|right> \end{cases}$$

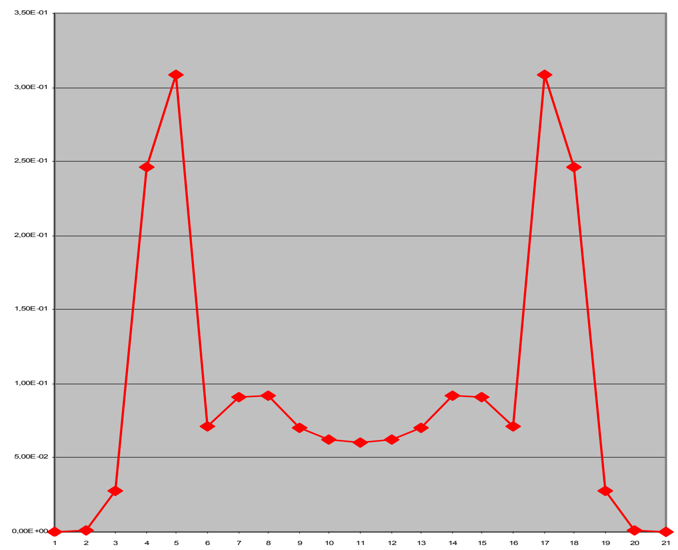
Shift:

$$\begin{cases} \left|x, left\right\rangle \rightarrow \left|x-1, left\right\rangle \\ \left|x, right\right\rangle \rightarrow \left|x+1, right\right\rangle \end{cases}$$

Classical vs. quantum

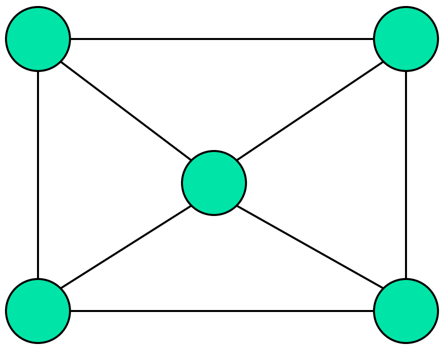
Run for t steps, measure the final location.





Distance: $\Theta(\sqrt{N})$ Distance: $\Theta(N)$

Quantum walks on general graphs



States:

$$|v\rangle|e\rangle,$$

e- edge from v.

1. Unitary "coin flip" on $|e\rangle$.
2. Shift

   $|v\rangle|e\rangle \rightarrow |u\rangle|e\rangle,$

   u – other endpoint of edge e.

Element distinctness

7	9	2	$\cdots$	1
x_1	x_2	x_3		x_N

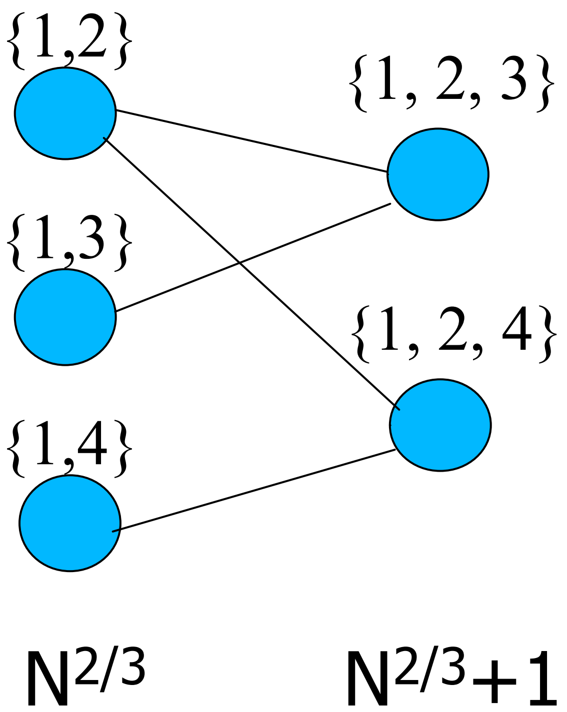
- Numbers $x_1, x_2, \ldots, x_N$.
- Determine if two of them are equal.
- Well studied problem in classical CS.
- Classically: N questions.

Element distinctness

7	9	2		1
x_1	x_2	x_3		x_N

- [Buhrman et.al., 2001]: $O(N^{3/4})$ quantum algorithm.
- [Shi, 2002]: $\Omega(N^{2/3})$ quantum lower bound.
- This talk: $O(N^{2/3})$.

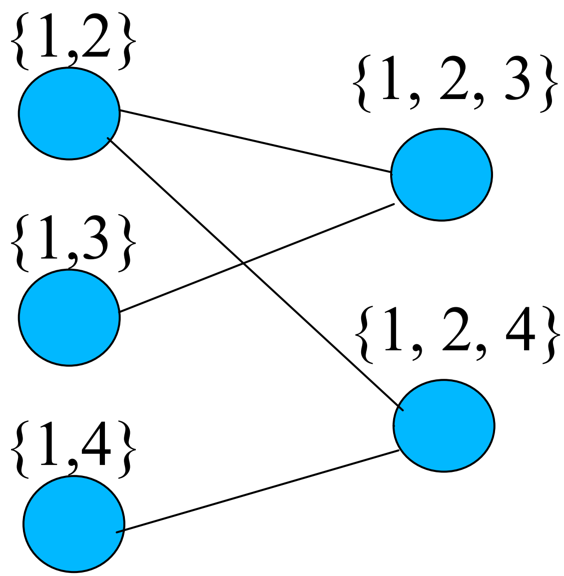
Element distinctness as search on a graph



- Vertices: $S \subseteq \{1, ..., N\}$ of size $N^{2/3}$ or $N^{2/3}+1$.
- Edges: (S,T), $T=S \cup \{i\}$.
- Marked: S contains

  $i, j, x_i=x_j$.
- In one step, we can
  - Check if vertex marked; or
  - Move to adjacent vertex.

Element distinctness as search on a graph

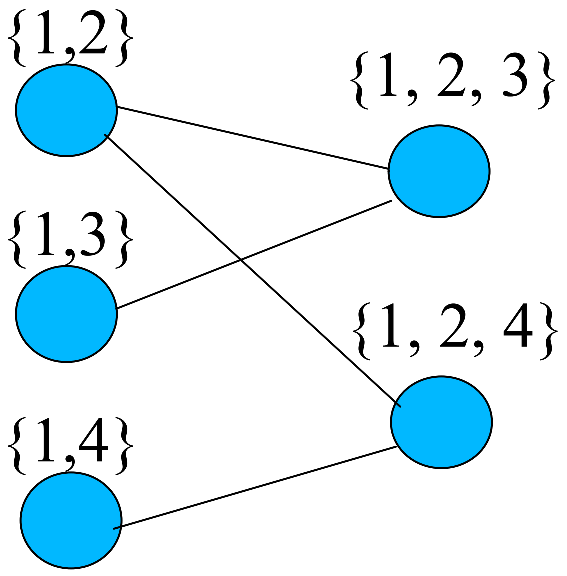


- Finding a marked vertex in M steps => element distinctness in $M+N^{2/3}$ steps.
- At the beginning, read all x_i
- Can check if vertex marked with 0 queries.
- Can move to neighbour with 1 query.

Quantum walk search [Shenvi, Kempe, Whaley, 2003]

- Start with a uniform superposition over all S.
- Apply one transition rule if S marked, another if S not marked.
- Quantum walk leads to a state in which marked S have higher amplitudes.

Walk on subsets



- States $\left|S\right\rangle\left|k\right\rangle \bigotimes_{i\in S}\left|x_i\right\rangle$

1. "Coin flip" unitary on k.
2. $|S\rangle\ |k\rangle \Rightarrow |S\cup\{k\}\rangle\ |k\rangle$, query x_k.
3. "Coin flip" unitary on k.
4. $|S\rangle\ |k\rangle \Rightarrow |S-\{k\}\rangle\ |k\rangle$, erase x_k.

Quantum "coin flip"

$$\begin{pmatrix} -1+\frac{2}{M} & \frac{2}{M} & \cdots & \frac{2}{M} \\ \frac{2}{M} & -1+\frac{2}{M} & \cdots & \frac{2}{M} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{M} & \frac{2}{M} & \cdots & -1+\frac{2}{M} \end{pmatrix}$$

Restricted to $k \in S$ or $k \notin S$

Algorithm for element distinctness

- Prepare

$$\sum_{\substack{|S|=N^{2/3},\\ k\notin S}} |S\rangle|k\rangle \otimes_{i\in S} |x_i\rangle$$

- O($N^{1/3}$) times:
  - |S> $\rightarrow$ -|S> if S contains i, j s.t. $x_i = x_j$;
  - O ($N^{1/3}$) steps of quantum walk.

Analysis of algorithm

Assume unique i, j s.t. $x_i = x_j$.

1. Simplify analysis by symmetry.
2. Analysis of 1 quantum walk step.
3. Analysis of entire algorithm.

Symmetry

- 5 types of states $|S>|k>$, $k \notin S$:
  - $\{i, j\} \cap S=0$, $k \neq i$, $k \neq j$.
  - $\{i, j\} \cap S=0$, $k=i$ or $k=j$.
  - $\{i, j\} \cap S=1$, $k \neq i$, $k \neq j$.
  - $\{i, j\} \cap S=1$, $k=i$ or $k=j$.
  - $\{i, j\} \cap S=2$.
- States of each type have equal amplitudes (symmetry, induction).

Symmetry

- For each of 5 types, take the uniform superposition of all $|S\rangle|k\rangle$.
- At any time, the state of algorithm is a superposition of $|\Psi_1\rangle$, $|\Psi_2\rangle$, $|\Psi_3\rangle$, $|\Psi_4\rangle$, $|\Psi_5\rangle$.
- Suffices to analyze 5-dimensional subspace.

Analysis of quantum walk

- One step of q. walk is described by 5*5 matrix.
- Find eigenvalues and eigenvectors of this matrix.

Analysis of quantum walk

- One eigenvector is a uniform superposition of all |S>|k>, k $\notin$ S, with eigenvalue 1.
- The other eigenvalues are $e^{i\theta_1}$, $e^{-i\theta_1}$, $e^{i\theta_2}$, $e^{-i\theta_2}$.

$$\theta_1 = \frac{C_1}{\sqrt{|S|}} = \frac{C_1}{N^{1/3}}, \quad \theta_2 = \frac{C_2}{\sqrt{|S|}} = \frac{C_2}{N^{1/3}}$$

$N^{1/3}$ steps of quantum walk

- The uniform superposition of all |S>|k>, k $\notin$ S with eigenvalue 1.
- The other eigenvalues are $e^{i\theta_1}$, $e^{-i\theta_1}$, $e^{i\theta_2}$, $e^{-i\theta_2}$.

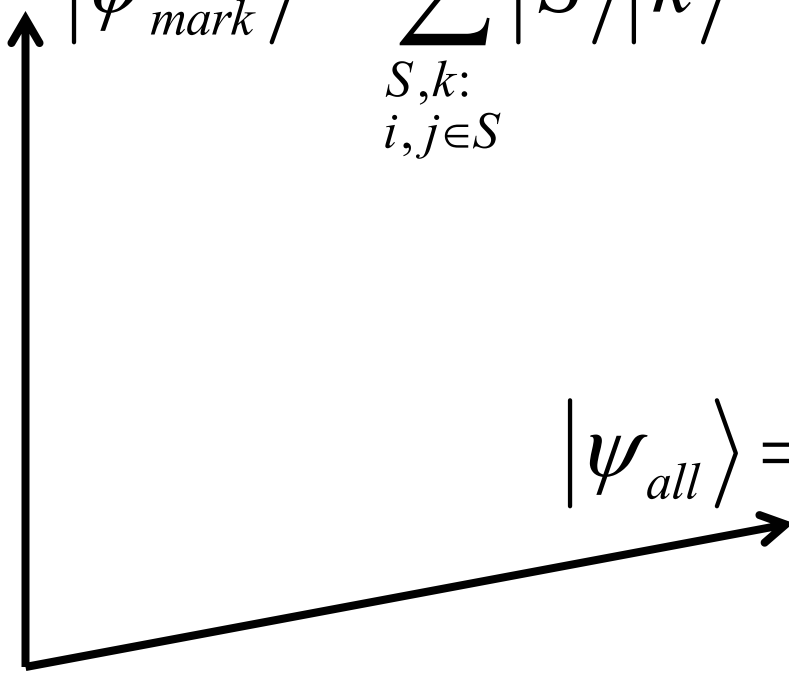
$$\theta_1 = C_1, \quad \theta_2 = C_2$$

Algorithm for element distinctness

- Prepare
$$\sum_{\substack{|S|=N^{2/3},\\ k\notin S}} |S\rangle|k\rangle \otimes_{i\in S} |x_i\rangle$$
- $O(N^{1/3})$ times:
  - $|S\rangle \rightarrow -|S\rangle$ if S contains i, j s.t. $x_i = x_j$;
  - O ($N^{1/3}$) steps of quantum walk.

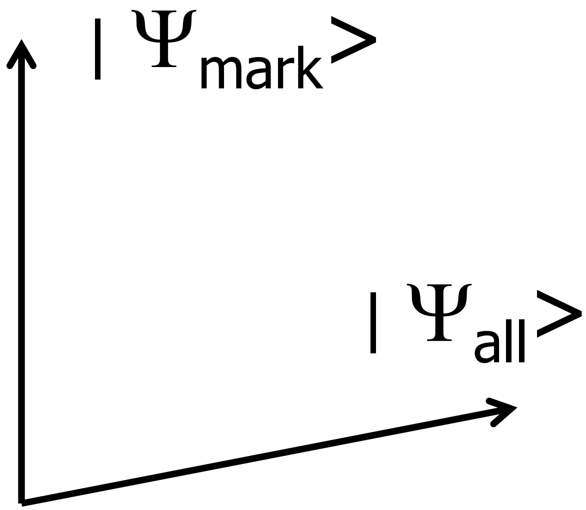
Analysis of entire algorithm

$$\left|\psi_{mark}\right\rangle = \sum_{\substack{S,k: \\ i,j\in S}} \left|S\right\rangle \left|k\right\rangle$$



$$\left|\psi_{all}\right\rangle = \sum_{S,k} \left|S\right\rangle \left|k\right\rangle$$

Analysis of entire algorithm



- Start in $|\Psi_{all}>$.
- $O(N^{1/3})$ times repeat:
  - $|\Psi_{mark}> \rightarrow -|\Psi_{mark}>$.
  - Rotate the subspace orthogonal to $|\Psi_{all}>$ by $e^{i\theta}$, $|\theta| \geq$ const.

<u>Lemma</u> The final state has a constant overlap with $|\Psi_{mark}>$.

Main lemma

Lemma The final state has a constant overlap with $|\Psi_{mark}>$.

General statement; applies to any sequence of 2 transformations.

Examples: Grover, element distinctness, other search problems?

Lemma can be used as a black box.

Handling multiple collisions

- What if multiple i, j: $x_i = x_j$?
- Sample part of x_i, $i \in \{1, 2, \ldots, N\}$ to get unique i, j: $x_i = x_j$.

Element k-distinctness

7	9	2	…	1
x_1	x_2	x_3		x_N

- Numbers $x_1, x_2, \ldots, x_N$.
- Determine if there are k equal elements.
- Similar algorithm solves the problem with $O(N^{(k-1)/k})$ queries.

Related work

- [Childs, Eisenberg, 2003, Santha 2004]: different analysis.
- [Magniez, Santha, Szegedy, 2003]: triangle finding.
- [Buhrman, Spalek, 2003]: testing matrix product.

Triangle finding [Magniez, Santha, Szegedy, 03]

- Graph G with n vertices.
- We want to know if G contains a triangle.
- $O(n^2)$ time classically.
- $O(n^{1.3})$ time quantum algorithm.
- Uses element distinctness as black box.

Testing matrix multiplication [Buhrman, Spalek 03]

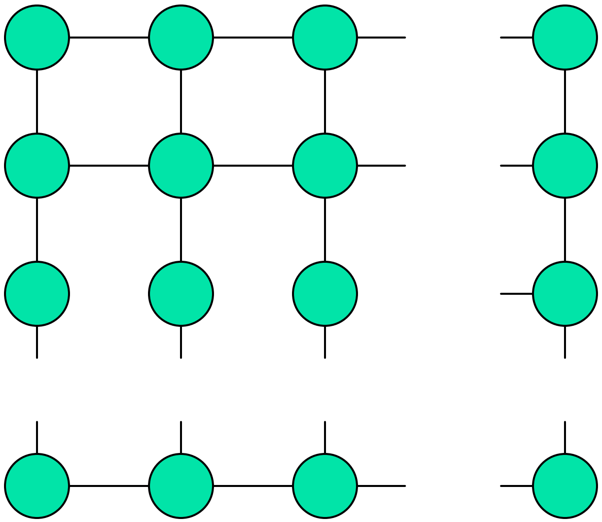
- n*n matrices A, B, C.
- Does A*B=C?
- Classically: $O(n^2)$ time.
- Quantum: $O(n^{1.67})$ time.
- Uses quantum walk on sets of columns/rows.

Grover search

0	1	0	…	0
x_1	x_2	x_3		x_n

- Find i for which x_i=1.
- Questions: ask i, get x_i.
- Classically, n questions.
- Quantum, O(√n) questions [Grover, 1996].

Quantum search on grids [Benioff, 2000]



- $\sqrt{n} * \sqrt{n}$ grid.
- Distance between opposite corners = $2\sqrt{n}$.
- Grover's algorithm takes

$$\sqrt{\mathbf{n}} * \sqrt{\mathbf{n}} = \mathbf{n}$$

steps.

- No quantum speedup.

Quantum search on grids

- [Aaronson, A, 2003] non-quantum walk algorithm.
- $O(\sqrt{N} \log^2 N)$ time algorithm for 2D grid.
- $O(\sqrt{N})$ time algorithm for 3 and more dimensions.

Quantum search on grids

- [Childs, Goldstone, 2003]: continuous-time quantum walk.
- $O(\sqrt{N} \log N)$ time algorithm for 4D grid.
- $O(\sqrt{N})$ time algorithm for 5 and more dimensions.

Quantum walks on grids

- This talk: discrete-time quantum walk.
- $O(\sqrt{N} \log N)$ time algorithm for 2D grid.
- $O(\sqrt{N})$ time algorithm for 3 and more dimensions.
- Improves over [Aaronson, A].
- Shows difference between discrete and continous time quantum walks.

Quantum walk on grid

- Basis states |x,y,←>, |x, y, →>, |x, y, ↑>, |x, y, ↓>.
- Coin flip on direction:

$$\begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

Quantum walk on grid

- Shift:
  - $|x, y, \leftarrow>$ $\Rightarrow$ $|x-1, y, \rightarrow>$
  - $|x, y, \rightarrow>$ $\Rightarrow$ $|x+1, y, \leftarrow>$
  - $|x, y, \uparrow>$ $\Rightarrow$ $|x, y-1, \downarrow>$
  - $|x, y, \downarrow>$ $\Rightarrow$ $|x, y+1, \uparrow>$

Search by quantum walk

- Perform a quantum walk with different "coin flip" transformation in marked locations.
- After $O\left(\sqrt{N \log N}\right)$ steps, measure the state.
- Gives marked |x, y, d> with prob. 1/log N.
- In 3 and more dimensions, O(√N) steps, constant probability.

Discrete time quantum walks

- State |x, y>|d>, with (x, y) being location, d – direction (←, ↑, →, ↓).
  - "Coin flip" on |d>;
  - Modify |x, y> dependant on |d>.
- Many possible transformations for "coin flip", with different results.

Different quantum walk

- Same coin flip

$$\begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

- Different shift

$$|x, y, \uparrow\rangle \rightarrow |x-1, y, \uparrow\rangle$$
$$|x, y, \downarrow\rangle \rightarrow |x+1, y, \downarrow\rangle$$
$$|x, y, \leftarrow\rangle \rightarrow |x, y-1, \leftarrow\rangle$$
$$|x, y, \rightarrow\rangle \rightarrow |x, y+1, \rightarrow\rangle$$

Different coin flip for marked locations

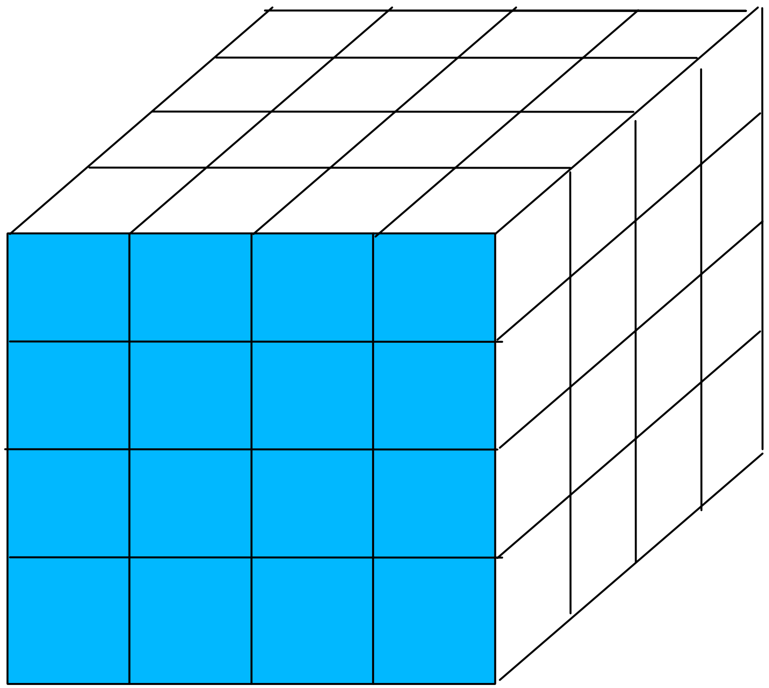
Different quantum walk

- Claim The probability of being in marked location never exceeds 2/N.

Application: set disjointness

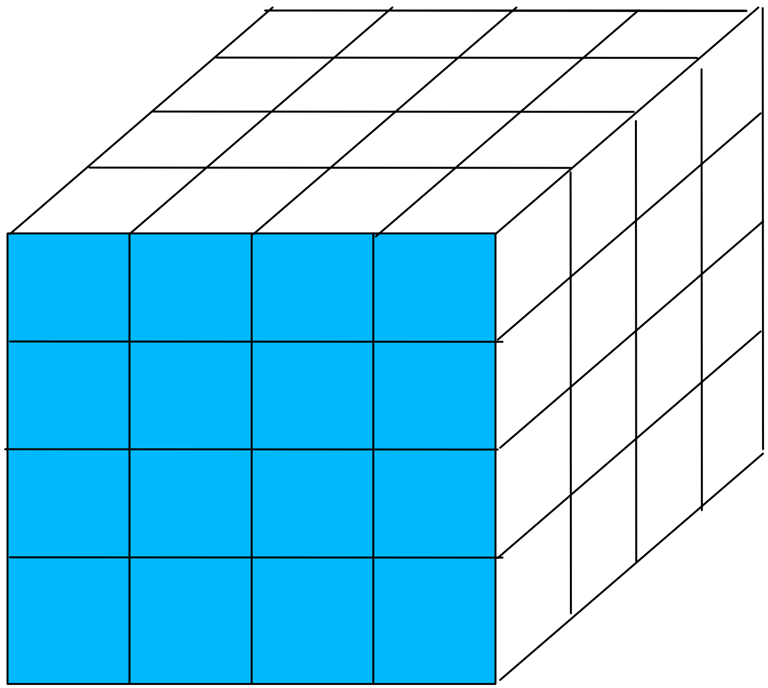
- Alice has set $A \subseteq \{1, 2, ..., N\}$, Bob has $B \subseteq \{1, 2, ..., N\}$.
- They want to know if there is i: $i \in A$, $i \in B$.
- How many qubits of communication?
- [Buhrman et.al., 97]: $O(\sqrt{N} \log N)$.
- [Hoyer, de Wolf 02]: $O(\sqrt{N}\, c^{\log^* N})$.
- [Razborov 02]: $\Omega(\sqrt{N})$.
- [Aaronson, A, 03]: $O(\sqrt{N})$.

Set disjointness



- Cube of volume N.
- Divide in N subcubes.
- Alice writes 1 in i^{th} subcube if $i \in A$.
- Bob writes 1 in i^{th} subcube if $i \in B$.

Set disjointness



- Is there a location where both Alice and Bob have 1?
- Alice and Bob run $O(\sqrt{N})$ algorithm for 3D search.
- Each step - 5 qubit communication.

More information

- Element distinctness – A, quant-ph/0311001.
- Search on grid – A, Kempe, Rivosh, Shenvi, coming soon.

Open problems

- What is the complexity of finding if there are k equal items $x_{i_1} = \ldots = x_{i_k}$?
- Algorithm: $O(N^{(k-1)/k})$.
- Lower bound: $\Omega(N^{2/3})$.

Open problems

- Our element distinctness algorithm uses $O(N^{2/3})$ space.
- Algorithm with less space?
- Space restricted to M items:
  - Quantum: $O(N/\sqrt{M})$ queries.
  - Classical: $O(N^2/M)$ queries.
- Quantum speeds up time but not space.
- Quantum lower bounds on space?

Open problems

- On 2-D grid, why one coin succeeds and the other fails? Any correspondence to physics?
- How to handle multiple marked states in quantum walk algorithms?
- Can we speed up classical Markov chain algorithms (approximating permanent)?