Introduction to Quantum Walk

Gustavo Banegas
gustavo@cryptme.in

Department of Mathematics and Computer Science
Technische Universiteit Eindhoven

September 15, 2016

Technische Universiteit
Eindhoven
University of Technology

Content

Technische Universiteit **Eindhoven** University of Technology

What is a quantum walk?

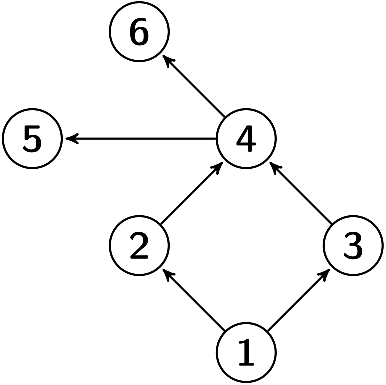
- A random walk is the simulation of random movement around a graph
- A quantum walk is similar to random walk algorithm
- Random walks are a useful model for developing classical algorithms; quantum walks provide a new way of developing quantum algorithms

Why use quantum walk?

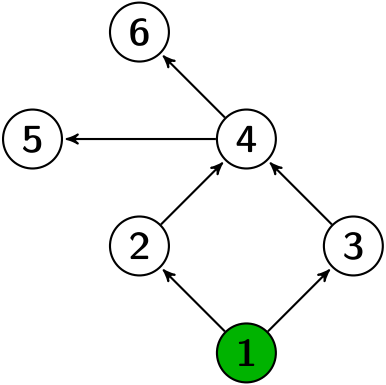
Classical Random walks used in best known classical algorithms:

- k-sat
- graph isomorphism
- approximating the permanent of a matrix

Regarding random walk on a graph

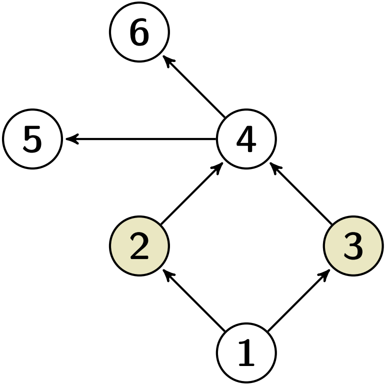


Regarding random walk on a graph



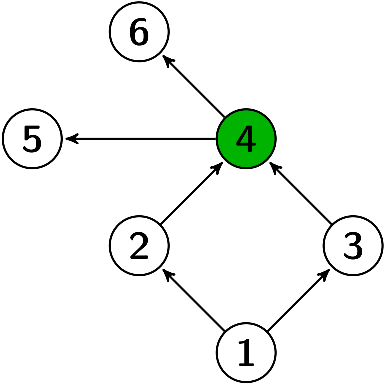
Step	Probability at vertex					
	1	2	3	4	5	6
0	1					
1						
2						
3						

Regarding random walk on a graph



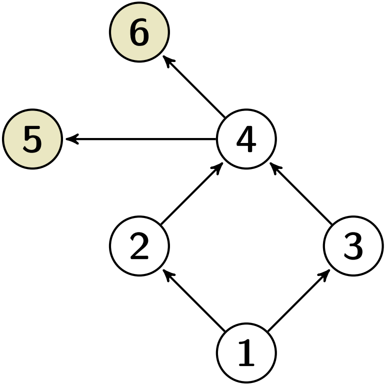
Step	Probability at vertex					
	1	2	3	4	5	6
0	1					
1		$\frac{1}{2}$	$\frac{1}{2}$			
2						
3						

Regarding random walk on a graph



Step	Probability at vertex					
	1	2	3	4	5	6
0	1					
1		$\frac{1}{2}$	$\frac{1}{2}$			
2				1		
3						

Regarding random walk on a graph



Step	Probability at vertex					
	1	2	3	4	5	6
0	1					
1		$\frac{1}{2}$	$\frac{1}{2}$			
2				1		
3					$\frac{1}{2}$	$\frac{1}{2}$

- After 3 steps we are in vertex 5 or 6 with equal probability.

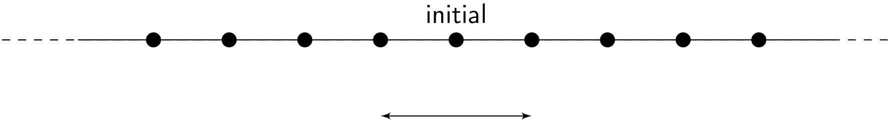
Definition of random walk

- Express a classical random walk as a matrix A of transition probabilities
- Express a position as a column vector v
- Performing a step of the walk corresponds to a left multiplication v by A
- Performing n steps of the walk corresponds to a left multiplication v by A^n

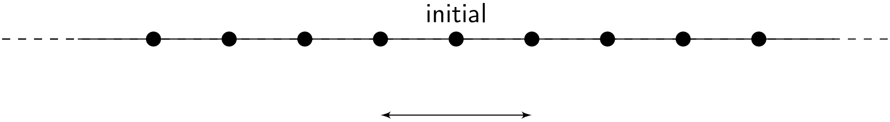
Definition of quantum walk

- Probabilities combine differently (sum of the amplitudes squared must be 1)
- Transition matrix must be unitary
- This will not in general be the case, but maybe it is needed to modify the structure of the graph (Adding a coin space)

Walking on the line



Walking on the line



n / t	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					1/2		1/2				
2				1/4		1/2		1/4			
3			1/8		3/8		3/8		1/8		
4		1/16		1/4		3/8		1/4		1/16	
5	1/32		5/32		5/16		5/16		5/32		1/32

Quantum walking on the line

- Walker's position n should be a vector in Hilbert space $\mathcal{H}_P$; Computational basis is $\{|n\rangle : n \in \mathbb{Z}\}$
- The movement, called evolution, of the walk depend on a quantum "coin":
  - "heads" the next step will be $|n+1\rangle$
  - "tails" the next step will be $|n-1\rangle$
- The Hilbert space of the system should be $\mathcal{H} = \mathcal{H}_C \otimes \mathcal{H}_P$; where $\mathcal{H}_C$ has computational basis $\{|0\rangle, |1\rangle\}$.

Quantum walking on the line

- In fact, the "coin" is any unitary matrix C with dimension 2, which acts on the vectors in Hilbert space $\mathcal{H}_C$.
- The shift from $|n\rangle$ to $|n+1\rangle$ or $|n-1\rangle$ must be described by a unitary operator called **shift operator** S. Also, it should operate as:
  - $S|0\rangle|n\rangle = |0\rangle|n+1\rangle$
  - $S|1\rangle|n\rangle = |1\rangle|n-1\rangle$
- A step of quantum walk is SC.

Quantum walking on the line

If we know the action of S on the computational basis of $\mathcal{H}$, it is possible to have a complete description of this linear operator. In the case, we can deduce that:

$$S = |0\rangle\langle 0| \otimes \sum_{n=-\infty}^{\infty} |n+1\rangle\langle n| + |1\rangle\langle 1| \otimes \sum_{n=-\infty}^{\infty} |n-1\rangle\langle n|$$

Quantum walking on the line

Let us take the initial stat at the origin $|n = 0\rangle$ and the coin state with $|0\rangle$. So, we have:

$$|\psi(0)\rangle = |0\rangle\,|n = 0\rangle$$

Applying the state of the coin, i.e $H \otimes I$, followed by application of shift operator S:

$$|0\rangle \otimes |0\rangle \xrightarrow{H\otimes I} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle \xrightarrow{S} \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |-1\rangle)$$

Quantum walking on the line

The quantum walk consists in applying the unitary operator:

$$U = S(H \otimes I)$$

So, we have: $|\psi(t)\rangle = U^t |\psi(0)\rangle$

$$|\psi(1)\rangle = \frac{1}{\sqrt{2}}(|1\rangle |-1\rangle + |0\rangle |1\rangle)$$

Applying $|\psi(2)\rangle = U |\psi(1)\rangle$

$$|\psi(2)\rangle = \frac{1}{2}(- |1\rangle |-2\rangle + (|0\rangle + |1\rangle) |0\rangle + |0\rangle |2\rangle)$$

Quantum walking on the line

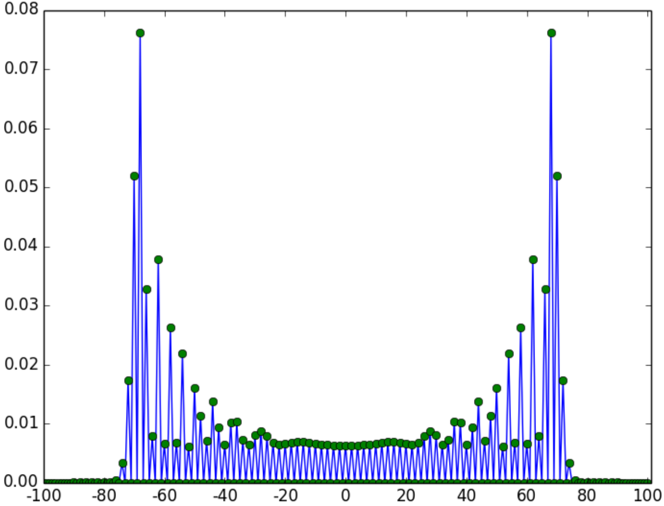
t \ n	-5	-4	-3	-2	-1	0	1	2	3	4	5
0						1					
1					1/2		1/2				
2				1/4		1/2		1/4			
3			1/8		1/8		5/8		1/8		
4		1/16		1/8		1/8		5/8		1/16	
5	1/32		5/32		1/8		1/8		17/32		1/32

Quantum walking on the line

- The superposition should not cancel terms before the calculation of the probability distribution
- The trick is to multiply the imaginary complex number i to the second initial contindition

$$|\psi(0)\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}\,|n=0\rangle$$

Quantum walking on the line



Quantum query algorithms

Considering a computation of a Boolean function $f(x_1, \ldots, x_N) : \{0,1\}^N \rightarrow \{0,1\}$. In the quantum query model, you evaluate the function accessing the oracle O by queries and the complexity is measured in the numbers of calls to O.

Quantum query algorithms

A quantum computation with T queries is just a sequence of unitary transformations:

$$U_0 \to O \to U_1 \to O \to \ldots \to U_{T-1} \to O \to U_T.$$

Element Distinctness

Definition:
Given numbers $x_1, \ldots, x_N \in [S]$, are all distinct?
Are there some x_i, x_j such as $i \neq j$ and $x_i = x_j$?
Does a set S of N elements contain any duplicate elements?

Element Distinctness

Solving classical:

The best way to solve is by sorting, which requires $\Omega(N)$.

Solving quantum:

It is possible to solve using $O(N^{2/3})$ queries. We are going to see how it works very briefly.

Element Distinctness

Example

- We use a quantum walk on a graph where the vertices are subsets of S containing either M or $M+1$ elements for some $M < N$
- Two vertices are connected if they differ in exactly one element

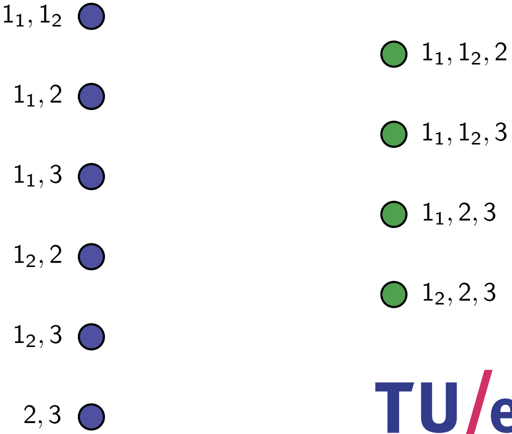
Let define an graph that encodes the set $\{1_1, 1_2, 2, 3\}$ for $M = 2$.

Element Distinctness

Example

- We use a quantum walk on a graph where the vertices are subsets of S containing either M or $M+1$ elements for some $M < N$

Our set is $\{1_1, 1_2, 2, 3\}$ and $M = 2$

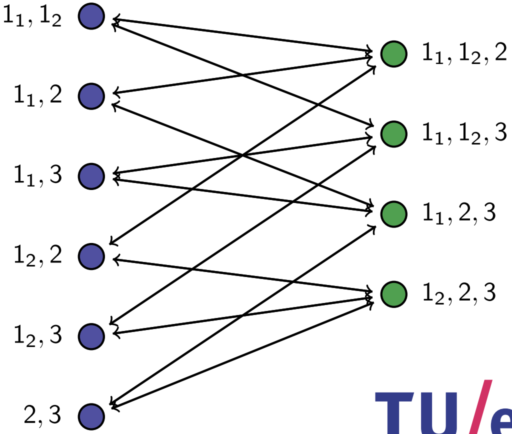


Element Distinctness

Example

- Two vertices are connected if they differ in exactly one element

Our set is $\{1_1, 1_2, 2, 3\}$ and $M = 2$



Element Distinctness

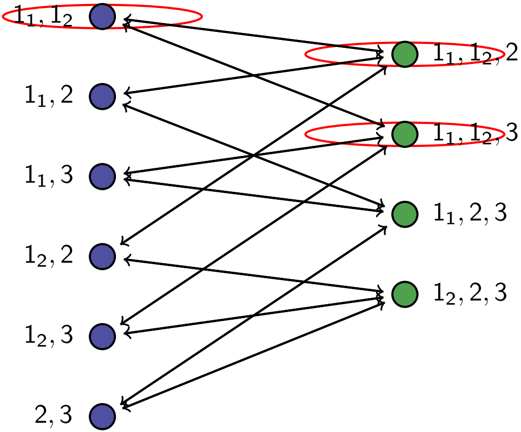
Basic walk algorithm:

1. Start with some subset $S' \subseteq S$ (where $|S'| = M$)
2. check whether S' contains any duplicates (needs $O(M)$ queries)
3. if not, change to a different subset S'' that differs in exactly one element
4. check S'' for duplicates (needs 1 query)
5. repeat steps 3 and 4 until a duplicate is found

Because this is a quantum walk, we can start with a superposition of all $M-$subsets

Element Distinctness

Example



Technische Universiteit
Eindhoven
University of Technology

Element Distinctness

Analysis of quantum walk:

- In total, we need $(M + r)$ queries, where:
  - M is the number of elements in the initial subset
  - r is the number of steps of the quantum walk
- If we pick $M = N^{2/3}$, then a solution can be found with high probability in $r = N^{1/3}$ steps of the walk
- It is needed a significant amount of space (It is $O(N^{2/3}$ elements))

Other uses of Quantum Walk

Applications of quantum walks

1. Quantum network routing
   Kempe, 2002
2. Quantum walk search algorithm
   Shenvi, Kempe, Whaley, 2002
3. Element distinctness
   Ambainis, 2004
4. Applications of element distinctness
   Magniez, Santha, Szegedy, 2003
   Buhrmann, Spalek, 2004
5. Quantum algorithms for the subset-sum problem
   Daniel J. Bernstein, Stacey Jeffery, Tanja Lange, Alexander Meurer, 2013

Open Problems

- Exponential speedup for natural problems
- Improving k-distinctness, triangle and k-clique algorithms
- Other applications for quantum walk search

Questions

Thank You!!

¿Questions?
https://www.cryptme.in/slides