Quantum walks

Ashley Montanaro

Centre for Quantum Information and Foundations,
Department of Applied Mathematics and Theoretical Physics,
University of Cambridge

November 29, 2011

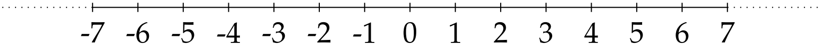
Quantum walks

- This lecture is about a generalisation of the fundamental concept of random walks (aka Markov chains) to quantum computation.

- We start with the most basic random walk possible: a walk on the line.

Walk on the line

- Take the real line

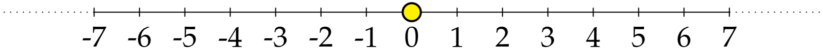


  and put a particle on the line, initially at position 0.

- At each step, toss a fair coin and move distance 1 either to the right or to the left.

Walk on the line

- Take the real line

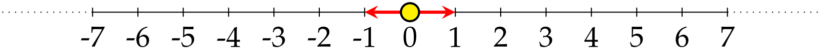


  and put a particle on the line, initially at position 0.

- At each step, toss a fair coin and move distance 1 either to the right or to the left.

Walk on the line

- Take the real line

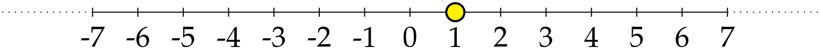


and put a particle on the line, initially at position 0.

- At each step, toss a fair coin and move distance 1 either to the right or to the left.

Walk on the line

- Take the real line

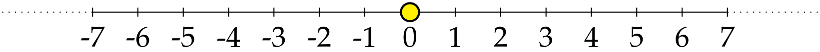


  and put a particle on the line, initially at position 0.

- At each step, toss a fair coin and move distance 1 either to the right or to the left.

Walk on the line

- Take the real line

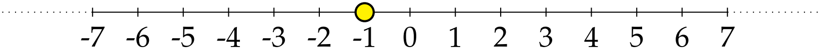


and put a particle on the line, initially at position 0.

- At each step, toss a fair coin and move distance 1 either to the right or to the left.

Walk on the line

- Take the real line

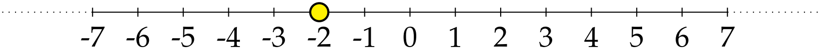


  and put a particle on the line, initially at position 0.

- At each step, toss a fair coin and move distance 1 either to the right or to the left.

Walk on the line

- Take the real line

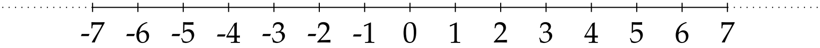


and put a particle on the line, initially at position 0.

- At each step, toss a fair coin and move distance 1 either to the right or to the left.

Walk on the line

- Take the real line



  and put a particle on the line, initially at position 0.

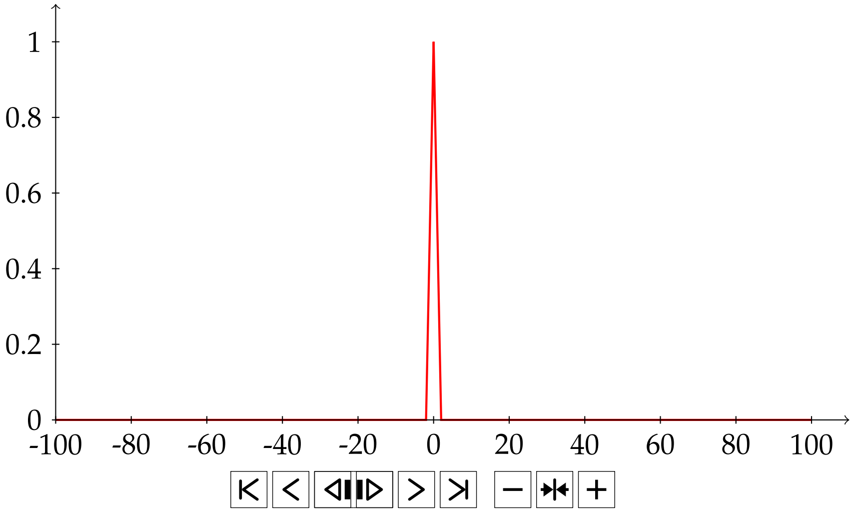
- At each step, toss a fair coin and move distance 1 either to the right or to the left.

- It is easy to calculate that the probability of being found at position x after t steps is exactly

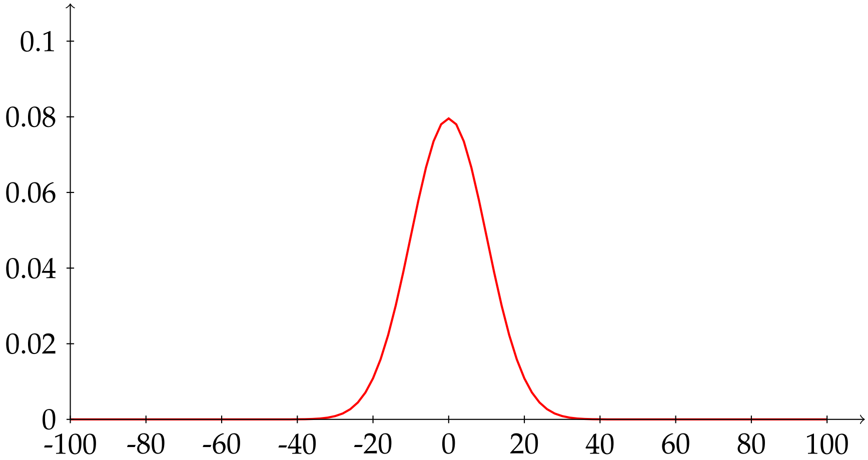
$$\frac{1}{2^t}\binom{t}{\frac{t+x}{2}},$$

  where we define $\binom{t}{r} = 0$ for non-integer r.

Random walk on the line (even times)



Random walk on the line (100 steps)



Quantum walk on the line

- Consider a quantum system with two registers $|x\rangle|c\rangle$, where the first holds an integer position x and the second holds a coin state $c \in \{L, R\}$.

Quantum walk on the line

- Consider a quantum system with two registers $|x\rangle|c\rangle$, where the first holds an integer position x and the second holds a coin state $c \in \{L, R\}$.
- Just like the classical walk, at each step our quantum walk will flip a coin and then decide which way to go.

Quantum walk on the line

- Consider a quantum system with two registers $|x\rangle|c\rangle$, where the first holds an integer position x and the second holds a coin state $c \in \{L, R\}$.
- Just like the classical walk, at each step our quantum walk will flip a coin and then decide which way to go.
- These two operations will be unitary: a coin operator C, and a shift operator S.

Quantum walk on the line

- Consider a quantum system with two registers $|x\rangle|c\rangle$, where the first holds an integer position x and the second holds a coin state $c \in \{L, R\}$.
- Just like the classical walk, at each step our quantum walk will flip a coin and then decide which way to go.
- These two operations will be unitary: a coin operator C, and a shift operator S.
- The coin operator acts solely on the coin register, and consists of a Hadamard operation:

$$C|L\rangle = \frac{1}{\sqrt{2}}\left(|L\rangle + |R\rangle\right), \quad C|R\rangle = \frac{1}{\sqrt{2}}\left(|L\rangle - |R\rangle\right).$$

Quantum walk on the line

- Consider a quantum system with two registers $|x\rangle|c\rangle$, where the first holds an integer position x and the second holds a coin state $c \in \{L, R\}$.
- Just like the classical walk, at each step our quantum walk will flip a coin and then decide which way to go.
- These two operations will be unitary: a coin operator C, and a shift operator S.
- The coin operator acts solely on the coin register, and consists of a Hadamard operation:

$$C|L\rangle = \frac{1}{\sqrt{2}}\left(|L\rangle + |R\rangle\right), \quad C|R\rangle = \frac{1}{\sqrt{2}}\left(|L\rangle - |R\rangle\right).$$

- The shift operator acts on both registers, and simply moves the walker in the direction indicated by the coin state:

$$S|x\rangle|L\rangle = |x-1\rangle|L\rangle, \quad S|x\rangle|R\rangle = |x+1\rangle|R\rangle.$$

Quantum walk on the line

- So a quantum walk on the line for t steps consists of applying the unitary operator $(S(I \otimes C))^t$ to some initial state, then measuring the position register.

Quantum walk on the line

- So a quantum walk on the line for t steps consists of applying the unitary operator $(S(I \otimes C))^t$ to some initial state, then measuring the position register.

- Note: we only measure the position at the end, not after each step.

Quantum walk on the line

- So a quantum walk on the line for t steps consists of applying the unitary operator $(S(I \otimes C))^t$ to some initial state, then measuring the position register.

- Note: we only measure the position at the end, not after each step.

- This simple process can lead to some fairly complicated results!

- Consider the first few steps of a quantum walk with initial state $|0\rangle|L\rangle$ (position 0, facing left).

Quantum walk on the line

$$|0\rangle|L\rangle \quad \mapsto \quad \frac{1}{\sqrt{2}}\left(|-1\rangle|L\rangle + |1\rangle|R\rangle\right)$$

Quantum walk on the line

$$
\begin{aligned}
|0\rangle|L\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|-1\rangle|L\rangle + |1\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2}\left(|-2\rangle|L\rangle + |0\rangle|R\rangle + |0\rangle|L\rangle - |2\rangle|R\rangle\right)
\end{aligned}
$$

Quantum walk on the line

$$
\begin{aligned}
|0\rangle|L\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|-1\rangle|L\rangle + |1\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2}\left(|-2\rangle|L\rangle + |0\rangle|R\rangle + |0\rangle|L\rangle - |2\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2\sqrt{2}}\left(|-3\rangle|L\rangle + |-1\rangle|R\rangle + {\color{blue}2|-1\rangle|L\rangle} - |1\rangle|L\rangle + |3\rangle|R\rangle\right)
\end{aligned}
$$

Quantum walk on the line

$$\begin{aligned}
|0\rangle|L\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|-1\rangle|L\rangle + |1\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2}\left(|-2\rangle|L\rangle + |0\rangle|R\rangle + |0\rangle|L\rangle - |2\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2\sqrt{2}}\left(|-3\rangle|L\rangle + |-1\rangle|R\rangle + 2|-1\rangle|L\rangle - |1\rangle|L\rangle + |3\rangle|R\rangle\right) \\
&\mapsto \ldots
\end{aligned}$$

Quantum walk on the line

$$
\begin{aligned}
|0\rangle|L\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|-1\rangle|L\rangle + |1\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2}\left(|-2\rangle|L\rangle + |0\rangle|R\rangle + |0\rangle|L\rangle - |2\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2\sqrt{2}}\left(|-3\rangle|L\rangle + |-1\rangle|R\rangle + 2|-1\rangle|L\rangle - |1\rangle|L\rangle + |3\rangle|R\rangle\right) \\
&\mapsto \ldots
\end{aligned}
$$

- Measuring after the third step yields position -3, 1 and 3 with probability 1/8 each, and position -1 with probability 5/8.

Quantum walk on the line

$$
\begin{aligned}
|0\rangle|L\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|-1\rangle|L\rangle + |1\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2}\left(|-2\rangle|L\rangle + |0\rangle|R\rangle + |0\rangle|L\rangle - |2\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2\sqrt{2}}\left(|-3\rangle|L\rangle + |-1\rangle|R\rangle + 2|-1\rangle|L\rangle - |1\rangle|L\rangle + |3\rangle|R\rangle\right) \\
&\mapsto \ldots
\end{aligned}
$$

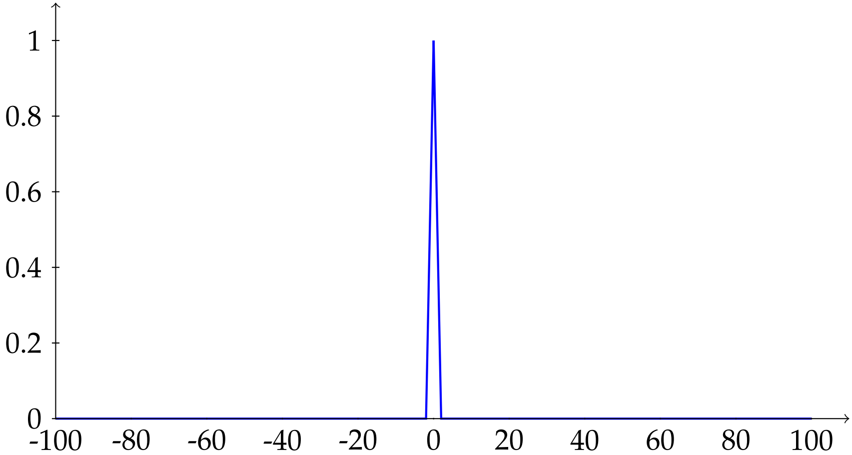
- Measuring after the third step yields position -3, 1 and 3 with probability $1/8$ each, and position -1 with probability $5/8$.
- By contrast, the classical walk is found in position -3 or 3 with probability $1/8$ each, and -1 and 1 with probability $3/8$ each.

Quantum walk on the line

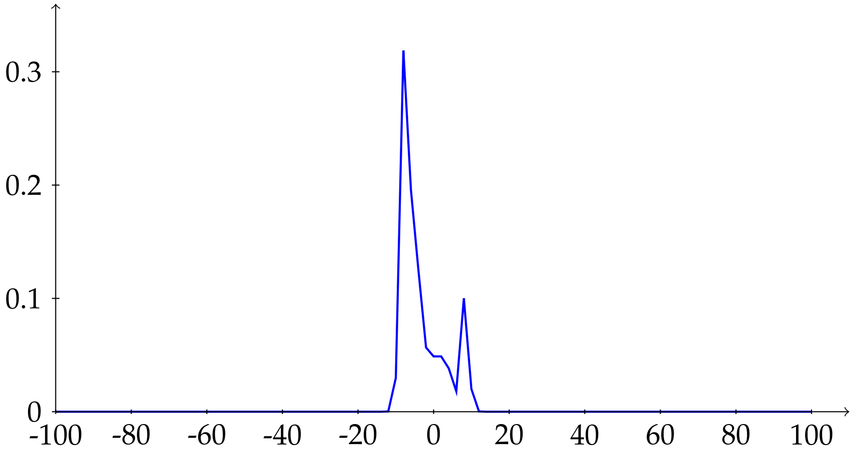
$$
\begin{aligned}
|0\rangle|L\rangle &\mapsto \frac{1}{\sqrt{2}}\left(|-1\rangle|L\rangle + |1\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2}\left(|-2\rangle|L\rangle + |0\rangle|R\rangle + |0\rangle|L\rangle - |2\rangle|R\rangle\right) \\
&\mapsto \frac{1}{2\sqrt{2}}\left(|-3\rangle|L\rangle + |-1\rangle|R\rangle + 2|-1\rangle|L\rangle - |1\rangle|L\rangle + |3\rangle|R\rangle\right) \\
&\mapsto \ldots
\end{aligned}
$$

- Measuring after the third step yields position -3, 1 and 3 with probability $1/8$ each, and position -1 with probability $5/8$.
- By contrast, the classical walk is found in position -3 or 3 with probability $1/8$ each, and -1 and 1 with probability $3/8$ each.
- The bias of the quantum walk is an effect of interference.

Hadamard walk on the line (even times 0-10)



Hadamard walk on the line (even times 12-100)



Observations

- Unlike the classical walk, the quantum walk is not symmetric about 0. This can be "fixed" by changing the initial coin state to $\frac{1}{\sqrt{2}}|0\rangle(|L\rangle + i|R\rangle)$, or using a different coin operator.

Observations

- Unlike the classical walk, the quantum walk is not symmetric about 0. This can be "fixed" by changing the initial coin state to $\frac{1}{\sqrt{2}}|0\rangle(|L\rangle + i|R\rangle)$, or using a different coin operator.

- Unlike the classical random walk, at time $t > 0$ the walker is not most likely to be found at the origin.

Observations

- Unlike the classical walk, the quantum walk is not symmetric about 0. This can be "fixed" by changing the initial coin state to $\frac{1}{\sqrt{2}}|0\rangle(|L\rangle + i|R\rangle)$, or using a different coin operator.
- Unlike the classical random walk, at time $t > 0$ the walker is not most likely to be found at the origin.
- The quantum walk seems to spread out more quickly from the origin. Classically, the variance in position after t steps is $O(t)$, but in the quantum case it turns out to be of order t^2.

Observations

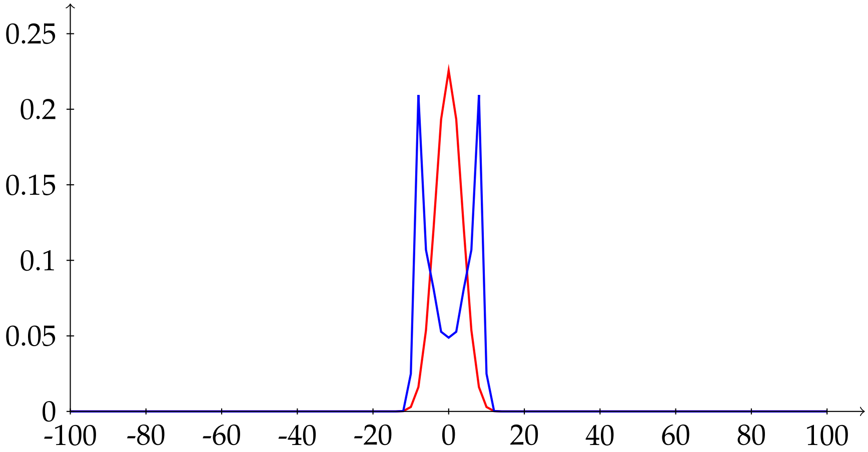
- Unlike the classical walk, the quantum walk is not symmetric about 0. This can be "fixed" by changing the initial coin state to $\frac{1}{\sqrt{2}}|0\rangle(|L\rangle + i|R\rangle)$, or using a different coin operator.

- Unlike the classical random walk, at time $t > 0$ the walker is not most likely to be found at the origin.

- The quantum walk seems to spread out more quickly from the origin. Classically, the variance in position after t steps is $O(t)$, but in the quantum case it turns out to be of order t^2.

- This is noticeably more difficult to prove than the classical proof.

Quantum vs. classical walk on the line (even times 12-100)



Random walks on general graphs

There is a natural generalisation of the classical random walk on the line to a random walk on an arbitrary graph G with m vertices.

Random walks on general graphs

There is a natural generalisation of the classical random walk on the line to a random walk on an arbitrary graph G with m vertices.

- The walker is positioned at a vertex of G, and at each time step, it chooses an adjacent vertex to move to, uniformly at random.

- Here we will consider only undirected and regular graphs where:
  - the ability to move from A to B implies the ability to move from B to A;
  - every vertex has degree d.

Random walks on general graphs

- The probability of being at vertex j after t steps, given that the walk started at vertex i, is just $\langle j|M^t|i\rangle$ for some matrix M, where

$$M_{ij} = \begin{cases} \frac{1}{d} & \text{if } i \text{ is connected to } j \\ 0 & \text{otherwise.} \end{cases}$$

- To quantise this, we still have position and coin registers, but now the position register is m-dimensional and the coin register is d-dimensional.

Quantum walks on general graphs

- Label each vertex with a distinct integer between 1 and m. For each vertex, label its outgoing edges with distinct integers between 1 and d such that, for each i, edges labelled with i form a cycle.

Quantum walks on general graphs

- Label each vertex with a distinct integer between 1 and m. For each vertex, label its outgoing edges with distinct integers between 1 and d such that, for each i, edges labelled with i form a cycle.
- For each vertex $v \in \{1, \ldots, m\}$, let $N(v, i)$ denote the i'th neighbour of v (i.e. the vertex at the other end of the i'th edge).

Quantum walks on general graphs

- Label each vertex with a distinct integer between 1 and m. For each vertex, label its outgoing edges with distinct integers between 1 and d such that, for each i, edges labelled with i form a cycle.
- For each vertex $v \in \{1, \dots, m\}$, let $N(v, i)$ denote the i'th neighbour of v (i.e. the vertex at the other end of the i'th edge).
- Our quantum walk will once again consist of alternating shift and coin operators S and C, i.e. each step is of the form $(S(I \otimes C))$. The shift operator simply performs the map

$$S|v\rangle|i\rangle = |N(v, i)\rangle|i\rangle.$$

Quantum walks on general graphs

- Label each vertex with a distinct integer between 1 and m. For each vertex, label its outgoing edges with distinct integers between 1 and d such that, for each i, edges labelled with i form a cycle.
- For each vertex $v \in \{1, \ldots, m\}$, let $N(v, i)$ denote the i'th neighbour of v (i.e. the vertex at the other end of the i'th edge).
- Our quantum walk will once again consist of alternating shift and coin operators S and C, i.e. each step is of the form $(S(I \otimes C))$. The shift operator simply performs the map

$$S|v\rangle|i\rangle = |N(v, i)\rangle|i\rangle.$$

- As the coin register is now d-dimensional, we have many possible choices for C.

Quantum walks on general graphs

- One reasonable choice for C is the so-called *Grover* coin,

$$C = \begin{pmatrix} \frac{2}{d} - 1 & \frac{2}{d} & \dots & \frac{2}{d} \\ \frac{2}{d} & \frac{2}{d} - 1 & \dots & \frac{2}{d} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{d} & \frac{2}{d} & \dots & \frac{2}{d} - 1 \end{pmatrix}.$$

This is just the iteration used in Grover's algorithm.

Quantum walks on general graphs

- One reasonable choice for C is the so-called *Grover* coin,

$$C = \begin{pmatrix} \frac{2}{d} - 1 & \frac{2}{d} & \dots & \frac{2}{d} \\ \frac{2}{d} & \frac{2}{d} - 1 & \dots & \frac{2}{d} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{d} & \frac{2}{d} & \dots & \frac{2}{d} - 1 \end{pmatrix}.$$

  This is just the iteration used in Grover's algorithm.

- This operator is an appealing choice because it is permutation-symmetric (i.e. treats all edges equally), and it is far away from the identity matrix (i.e. has a large mixing effect).

Quantum walks on general graphs

- One reasonable choice for C is the so-called *Grover* coin,

$$C = \begin{pmatrix} \frac{2}{d} - 1 & \frac{2}{d} & \dots & \frac{2}{d} \\ \frac{2}{d} & \frac{2}{d} - 1 & \dots & \frac{2}{d} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{d} & \frac{2}{d} & \dots & \frac{2}{d} - 1 \end{pmatrix}.$$

  This is just the iteration used in Grover's algorithm.

- This operator is an appealing choice because it is permutation-symmetric (i.e. treats all edges equally), and it is far away from the identity matrix (i.e. has a large mixing effect).

- If $d = 2$, we would get $C = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, so in this case the coins used earlier for the walk on the line lead to more interesting behaviour.

Quantum walks on general graphs

- Note that, as the quantum walk consists only of unitary operations, the position of the walker does not tend to a limiting distribution over the vertices of G, by contrast with the classical random walk.

The hypercube

- We now focus on one particularly interesting graph: the n-dimensional hypercube (aka the Cayley graph of the group $\mathbb{Z}_2^n$).

The hypercube

- We now focus on one particularly interesting graph: the n-dimensional hypercube (aka the Cayley graph of the group $\mathbb{Z}_2^n$).

- This is the graph whose vertices are n-bit strings which are adjacent if they differ in exactly one bit.

The hypercube

- We now focus on one particularly interesting graph: the n-dimensional hypercube (aka the Cayley graph of the group $\mathbb{Z}_2^n$).

- This is the graph whose vertices are n-bit strings which are adjacent if they differ in exactly one bit.

- We will be interested in the expected time it takes for a random walk on this graph to travel from the "all zeroes" string 0^n to the "all ones" string 1^n, i.e. to traverse the graph from one extremity to the other, which is known as the hitting time from 0^n to 1^n.

Random walk on the hypercube

Classically, this time can be analysed by mapping the walk to a (biased) random walk on the line.

Random walk on the hypercube

Classically, this time can be analysed by mapping the walk to a (biased) random walk on the line.

- Imagine the walker is currently at a vertex with Hamming weight k.

Random walk on the hypercube

Classically, this time can be analysed by mapping the walk to a (biased) random walk on the line.

- Imagine the walker is currently at a vertex with Hamming weight k.
- The probability of moving to a vertex with Hamming weight $(k-1)$ is k/n, and the probability of moving to a vertex with Hamming weight $(k+1)$ is $1-k/n$.

Random walk on the hypercube

Classically, this time can be analysed by mapping the walk to a (biased) random walk on the line.

- Imagine the walker is currently at a vertex with Hamming weight k.
- The probability of moving to a vertex with Hamming weight $(k-1)$ is k/n, and the probability of moving to a vertex with Hamming weight $(k+1)$ is $1-k/n$.
- As k increases, the probability of a step leading to the Hamming weight increasing decreases, so intuitively the walker becomes "stuck" in the "middle" of the graph (i.e. near Hamming weight $n/2$).

Random walk on the hypercube

Classically, this time can be analysed by mapping the walk to a (biased) random walk on the line.

- Imagine the walker is currently at a vertex with Hamming weight k.
- The probability of moving to a vertex with Hamming weight $(k-1)$ is k/n, and the probability of moving to a vertex with Hamming weight $(k+1)$ is $1-k/n$.
- As k increases, the probability of a step leading to the Hamming weight increasing decreases, so intuitively the walker becomes "stuck" in the "middle" of the graph (i.e. near Hamming weight $n/2$).

Proposition

The hitting time from 0^n to 1^n is at least $2^n - 1$.

Quantum walk on the hypercube

Theorem

If a quantum walk on the hypercube is performed for $T \approx \frac{\pi}{2} n$ steps starting in position 0^n, and the position register is measured, the outcome 1^n is obtained with probability $1 - O(\mathrm{polylog}(n)/n)$.

Quantum walk on the hypercube

Theorem

If a quantum walk on the hypercube is performed for $T \approx \frac{\pi}{2} n$ steps starting in position 0^n, and the position register is measured, the outcome 1^n is obtained with probability $1 - O(\mathrm{polylog}(n)/n)$.

Similarly to the classical case, we can simplify this to a walk on the line. Define a set of $2n$ states $\{|\upsilon_k, L\rangle, |\upsilon_k, R\rangle\}$ indexed by $k = 0, \ldots, n$ as follows:

$$\begin{aligned}
|\upsilon_k, L\rangle &:= \frac{1}{\sqrt{k\binom{n}{k}}} \sum_{x,|x|=k} \sum_{i,x_i=1} |x\rangle|i\rangle, \\
|\upsilon_k, R\rangle &:= \frac{1}{\sqrt{(n-k)\binom{n}{k}}} \sum_{x,|x|=k} \sum_{i,x_i=0} |x\rangle|i\rangle.
\end{aligned}$$

(The special cases $|\upsilon_0, L\rangle$ and $|\upsilon_n, R\rangle$ will not be used and are undefined.)

Quantum walk on the hypercube

- The quantum walk on the hypercube preserves tbe subspace spanned by this set of states:

$$S|\upsilon_k, L\rangle = |\upsilon_{k-1}, R\rangle,\ S|\upsilon_k, R\rangle = |\upsilon_{k+1}, L\rangle,$$

Quantum walk on the hypercube

- The quantum walk on the hypercube preserves tbe subspace spanned by this set of states:

$$S|\upsilon_k, L\rangle = |\upsilon_{k-1}, R\rangle, \; S|\upsilon_k, R\rangle = |\upsilon_{k+1}, L\rangle,$$

- and in the case of the coin operator,

$$\begin{aligned}
(I \otimes C)|\upsilon_k, L\rangle &= \left(\frac{2k}{n} - 1\right)|\upsilon_k, L\rangle + \frac{2\sqrt{k(n-k)}}{n}|\upsilon_k, R\rangle \\
(I \otimes C)|\upsilon_k, R\rangle &= \frac{2\sqrt{k(n-k)}}{n}|\upsilon_k, L\rangle + \left(1 - \frac{2k}{n}\right)|\upsilon_k, R\rangle.
\end{aligned}$$

Quantum walk on the hypercube

- The quantum walk on the hypercube preserves tbe subspace spanned by this set of states:

$$S|\upsilon_k, L\rangle = |\upsilon_{k-1}, R\rangle, \; S|\upsilon_k, R\rangle = |\upsilon_{k+1}, L\rangle,$$

- and in the case of the coin operator,

$$\begin{aligned}(I \otimes C)|\upsilon_k, L\rangle &= \left(\frac{2k}{n} - 1\right)|\upsilon_k, L\rangle + \frac{2\sqrt{k(n-k)}}{n}|\upsilon_k, R\rangle \\ (I \otimes C)|\upsilon_k, R\rangle &= \frac{2\sqrt{k(n-k)}}{n}|\upsilon_k, L\rangle + \left(1 - \frac{2k}{n}\right)|\upsilon_k, R\rangle.\end{aligned}$$

- This behaviour is similar to the quantum walk on the line, with two differences: first, the direction in which the walker is moving flips with each shift, and second, the coin is different at each position (i.e. depends on k).

Quantum walk on the hypercube

- The quantum walk on the hypercube preserves tbe subspace spanned by this set of states:

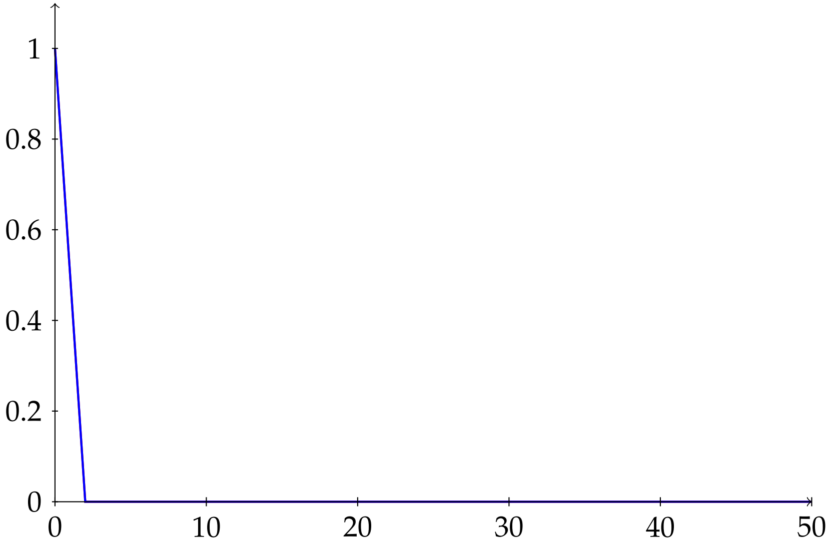
$$S|\upsilon_k, L\rangle = |\upsilon_{k-1}, R\rangle,\ S|\upsilon_k, R\rangle = |\upsilon_{k+1}, L\rangle,$$

- and in the case of the coin operator,

$$\begin{aligned}(I \otimes C)|\upsilon_k, L\rangle &= \left(\frac{2k}{n} - 1\right)|\upsilon_k, L\rangle + \frac{2\sqrt{k(n-k)}}{n}|\upsilon_k, R\rangle \\ (I \otimes C)|\upsilon_k, R\rangle &= \frac{2\sqrt{k(n-k)}}{n}|\upsilon_k, L\rangle + \left(1 - \frac{2k}{n}\right)|\upsilon_k, R\rangle.\end{aligned}$$

- This behaviour is similar to the quantum walk on the line, with two differences: first, the direction in which the walker is moving flips with each shift, and second, the coin is different at each position (i.e. depends on k).
- Based on this reduction, it is easy to plot the behaviour of this quantum walk numerically for small n.

Quantum vs. classical walk on the hypercube



Summary of quantum walks

- Quantum walks display very different behaviour from classical random walks and are an interesting technique for designing quantum algorithms.

Summary of quantum walks

- Quantum walks display very different behaviour from classical random walks and are an interesting technique for designing quantum algorithms.
- They are frequently more difficult to analyse than classical random walks...

Summary of quantum walks

- Quantum walks display very different behaviour from classical random walks and are an interesting technique for designing quantum algorithms.
- They are frequently more difficult to analyse than classical random walks...
- Importantly, quantum walks on low-degree graphs can be implemented efficiently on a quantum computer.

Summary of quantum walks

- Quantum walks display very different behaviour from classical random walks and are an interesting technique for designing quantum algorithms.
- They are frequently more difficult to analyse than classical random walks...
- Importantly, quantum walks on low-degree graphs can be implemented efficiently on a quantum computer.
- The quantum walk model is quite general: in fact, it turns out that every quantum computation can be interpreted as a quantum walk!
  - "Universal computation by quantum walk", Andrew Childs, `arXiv:0806.1972`
  - "Universal quantum computation using the discrete time quantum walk", Lovett et al, `arXiv:0910.1024`

Course summary

- Quantum computers offer new possibilities for information processing which are fundamentally impossible for computers based only on classical physics.

- Significant examples of quantum speed-ups include an efficient algorithm for integer factorisation and a provable quadratic speed-up for unstructured search.

- Quantum computers are not a panacea and one can prove limitations on their power using classical mathematical techniques.

- One of the most important early applications of quantum computers is likely to be the simulation of quantum mechanical systems.

Quantum algorithms we didn't mention

Some exponential speed-ups:

- Extracting information from solutions to linear equations.
- Solving Pell's equation ($x^2 - dy^2 = 1$) in integers.
- Approximating the Jones polynomial of knots on the complex unit circle.
- Testing equality of bit-strings using exponentially less communication.

Quantum algorithms we didn't mention

Some exponential speed-ups:

- Extracting information from solutions to linear equations.
- Solving Pell's equation ($x^2 - dy^2 = 1$) in integers.
- Approximating the Jones polynomial of knots on the complex unit circle.
- Testing equality of bit-strings using exponentially less communication.

And some polynomial speed-ups:

- Computing AND-OR trees with n variables in time $O(\sqrt{n})$.
- Determining whether a list contains duplicate elements.
- Finding triangles and other properties of graphs.

…

Open problems

Unlike many fields of mathematics, the relatively young field of quantum computing has many accessible open problems.

- We know that quantum and classical query complexity of total boolean functions can only be separated by a 6th power. Can this 6 be reduced to a 2?
- Is there any total boolean function which has an exact quantum query algorithm which uses fewer than half the number of queries than the best possible classical algorithm?
- There are exponential query complexity separations for functions with a significant promise on the input (eg. Simon's problem). What about functions with a weaker promise on the input?

Open problems

- Is there a quantum algorithm which can simulate k-local Hamiltonians using time $O(t \log(1/\epsilon))$?

- Can we harness the exponentially faster hitting of quantum walks to solve important classical problems?

- Is there an efficient quantum algorithm for the nonabelian hidden subgroup problem? Such an algorithm would solve the graph isomorphism problem.

- More generally, can we find more quantum algorithms?