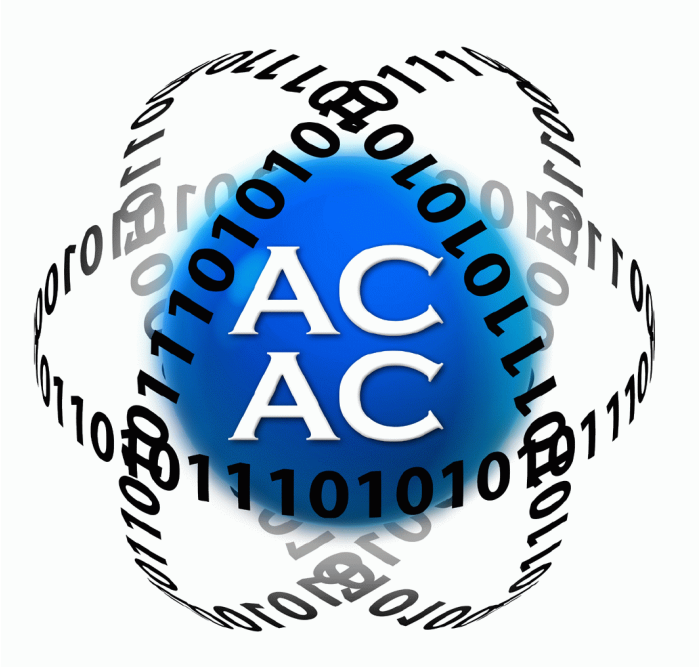
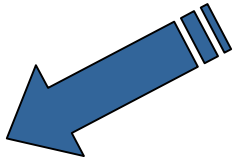
Random Walks and Quantum Walks

Stephen Bartlett, Department of Physics and Centre for Advanced Computing – Algorithms and Cryptography, Macquarie University



Random Walks and Quantum Walks

- Classical random walks have been applied to many theoretical and practical problems:
  - diffusion
  - Wiener processes
  - assessing randomized algorithms



- Quantum physics introduces new perspectives:
  - quantum diffusion
  - quantum stochastics
  - quantum walks
- **BIG QUESTION:** what do quantum walks have to say about quantum information processing?

(Classical) Random Walks

- Simplest case: walk on a 1-D lattice
  1. Let the particle start at position $k=0$ at time $t=0$
  2. For a particle at position k at time t:
     - With a 50% probability, the particle moves to position $k+1$ at time $t+1$,
     - otherwise, the particle moves to position $k-1$ at time $t+1$.
- We can think of a coin toss at every time step. If the toss gives heads, we move the particle to the right; otherwise, we move the particle to the left.

Questions for random walks

- Considering many random walks, where on average will the particle be? $\langle k \rangle = 0$ (No drift for fair coin)
- What is the variance?

  $\mathrm{Var}(k) = \sigma^2 \simeq t$ (Variance grows linearly with time)
- Is there a limiting distribution for the average of many random walks as $t \to \infty$? Normal distribution
- Consider an absorbing boundary at some k_0. What is the probability that the particle will hit this boundary after t steps? Interesting...

The Gambler's Ruin

- Consider a betting game with a 50/50 chance:
  - If you win, you get back twice your bet.
  - If you lose, you get back nothing.
- A gambler bets $1 each round of a game $\rightarrow$ random walk
- However, he starts with *X* amount of money, whereas the bank/casino has unlimited funds:
  - There is no upper bound to his winnings, but,
  - If he hits $0, he must stop playing.
- This problem is a random walk with an *absorbing boundary*
- Can also have one absorbing boundary and one reflecting boundary: *Gambler's ruin against the sheriff* (?!?!?)

Results from the gambler's ruin

- Let $P^N(n)$ denote the probability that, starting with n dollars, the gambler becomes broke before winning $N > n$ dollars.
  - Solving $P^N(n) = (1/2)[\, P^N(n\text{-}1) + P^N(n\text{+}1)\,]$
  - Boundary conditions: $P^N(0) = 1$, $P^N(N) = 0$.
  - Solution: $P^N(n) = 1 - n/N$.
- Gambler's ruin against the sheriff: If $n=N$, then the gambler always loses that round (reflecting boundary).
- Let $x(n)$ be the expected number of bets before the gambler is broke, given that he has n dollars.
  - Solving $x(n) = (1/2)[\, x(n\text{+}1) + x(n\text{-}1)\,] + 1$
  - Boundary conditions: $x(N) = x(N\text{-}1) + 1$, $x(0) = 0$.
  - Solution: $x(n) = 2nN - n^2$.
  - Gambler will always become broke eventually, in $O(n^2)$ rounds

Satisfiability

- Consider *n* variables (*literals*) $\{x_i\}$, which can each take the value TRUE or FALSE
- A *clause* with *k* literals has the form, e.g.,

  $x_a \vee (\neg x_b) \vee (\neg x_c) \vee x_d \vee \ldots \vee (\neg x_y) \vee x_z$ with *k* literals

  and is TRUE if any of its individual elements is TRUE
- Now consider a formula with a lot of clauses

  $(\text{clause}_1) \wedge (\text{clause}_2) \wedge \ldots \wedge (\text{clause}_N)$
- Each clause must be TRUE in order for the whole expression to be TRUE. Might not be possible with any assignment
- Satisfiability (SAT): Is there an assignment of the literals $\{x_i\}$ that will give a TRUE expression?
- kSAT: special case where all clauses have exactly *k* literals.

SAT, kSAT and 2SAT

- We know that SAT is NP-complete (Cook's Theorem)
- 3SAT is NP-complete (or any kSAT for $k \geq 3$)
- However, 2SAT is in P. There is a randomized algorithm for 2SAT that is $O(n^2)$, where n is the number of literals
- **2SAT Randomized Algorithm**

  (C. Papadimitriou, *Computational Complexity*, 1994):
  - Start with any assignment of the n literals $\{x_i\}$, and repeat:
    - If there is no unsatisfied clause: then HALT. Formula is satisfiable.
    - Otherwise: Take any unsatisfied clause, and randomly change one of its literals
  - After r repetitions, HALT. Formula is probably not satisfiable.
- We find that $r = O(n^2)$ to get probability of answer very high.

2SAT alg. realizes a random walk

- In 2SAT, an unsatisfied clause has two literals, e.g.,

  $(x_i \vee x_j)$ or $(x_i \vee \neg x_j)$ or $(\neg x_i \vee \neg x_j)$

- For a correct assignment, one of them has to change. We have at least a 50/50 chance of improving things by flipping one at random. (Maybe better... maybe both are wrong!)
- Let *t(i)* be the expected number of repetitions of the flipping step before we get a *particular* satisfying answer, where *i* is the number of incorrect assignments in our current guess.
- We have the inequality

  $t(i) \leq (1/2)[\, t(i\text{-}1) + t(i\text{+}1)] + 1$

- We also have $t(0) = 0$ and $t(n) \leq t(n\text{-}1) + 1$.

2SAT realizes a random walk

- A bound can be found by considering equality.

  $$x(i) = (1/2)[x(i\text{-}1) + x(i\text{+}1)] + 1$$

  Same boundary conditions: $x(0) = 0$, $x(n) = x(n\text{-}1) + 1$.

  Then $x(i) \geq t(i)$ for all i.
- Gambler's ruin against the sheriff!
- Equation for a 1-D random walk with a reflecting boundary ($i=n$) and an absorbing boundary ($i=0$).
- Worse case scenario: start with $i=n$. Solve: $x(n) = n^2$.
- The expected number of repetitions $t(i)$ satisfies:

  $$t(i) \leq x(i) \leq x(n) = n^2$$
- Random walk provides a bound that allows us to determine the complexity of the 2SAT problem.

Quantizing the random walk

- Can we create a quantum version of the random walk? YES
- Basic idea: eliminate randomness by using a quantum coin, which can exist in a superposition of heads and tails
- Different "Feynman paths" can interfere in the quantum case:
  - Classical case: probabilities add
  - Quantum case: probability amplitudes add and interfere
- Must be careful when we consider absorbing boundaries:
  - Does a measurement occur?
  - What type of measurement?
- Quantum walks exhibit drastically different behaviour than their classical counterparts. Can we use it?

Quantum coin toss

- Replace the coin with a quantum two-level system

$|\text{heads}\rangle$

$|\text{tails}\rangle$

- Quantum coin toss: Hadamard transformation creates a superposition

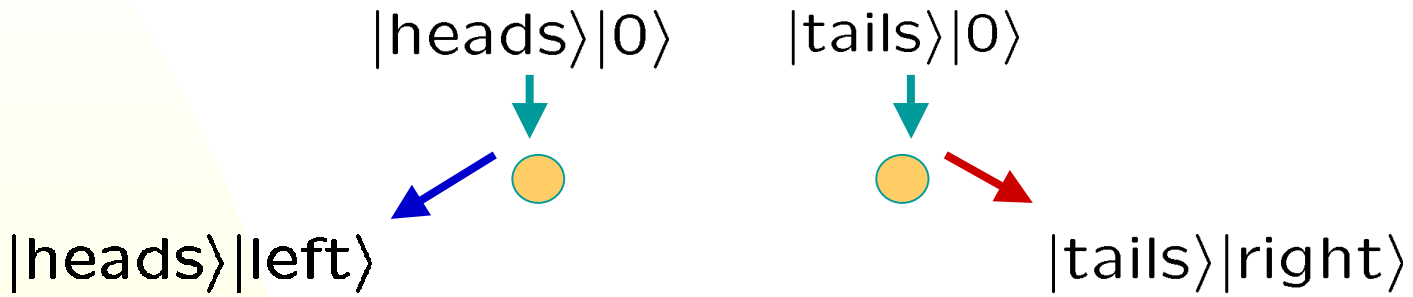
$$|\text{heads}\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|\text{heads}\rangle + |\text{tails}\rangle\right)$$

$$|\text{tails}\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|\text{heads}\rangle - |\text{tails}\rangle\right)$$

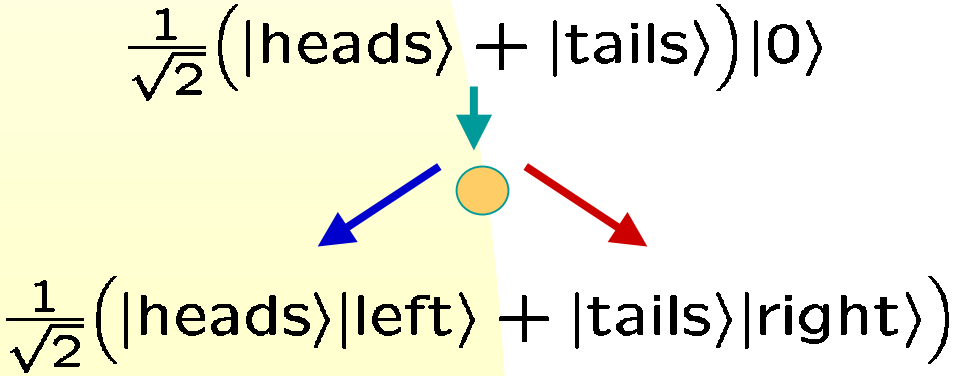
- No randomness: unitary, reversible operation

Quantum walk

- Heads goes left, tails goes right



- Quantum superpositions with coin flip:



Superposition of heads and tails goes to superposition of left and right

Quantum walk

- Coin Hilbert space is one qubit: $H_c = \text{span}\{ |+\rangle, |-\rangle \}$
- Spatial Hilbert space is n qubits:

  $H_s = \text{span}\{ |i\rangle, i \in Z_d \}$, where $d=2^n$.
- Note that our lattice "wraps around": quantum walk on a circle
- Quantum walk consists of two alternating unitary transformations:
  - Hadamard H performs the quantum coin toss

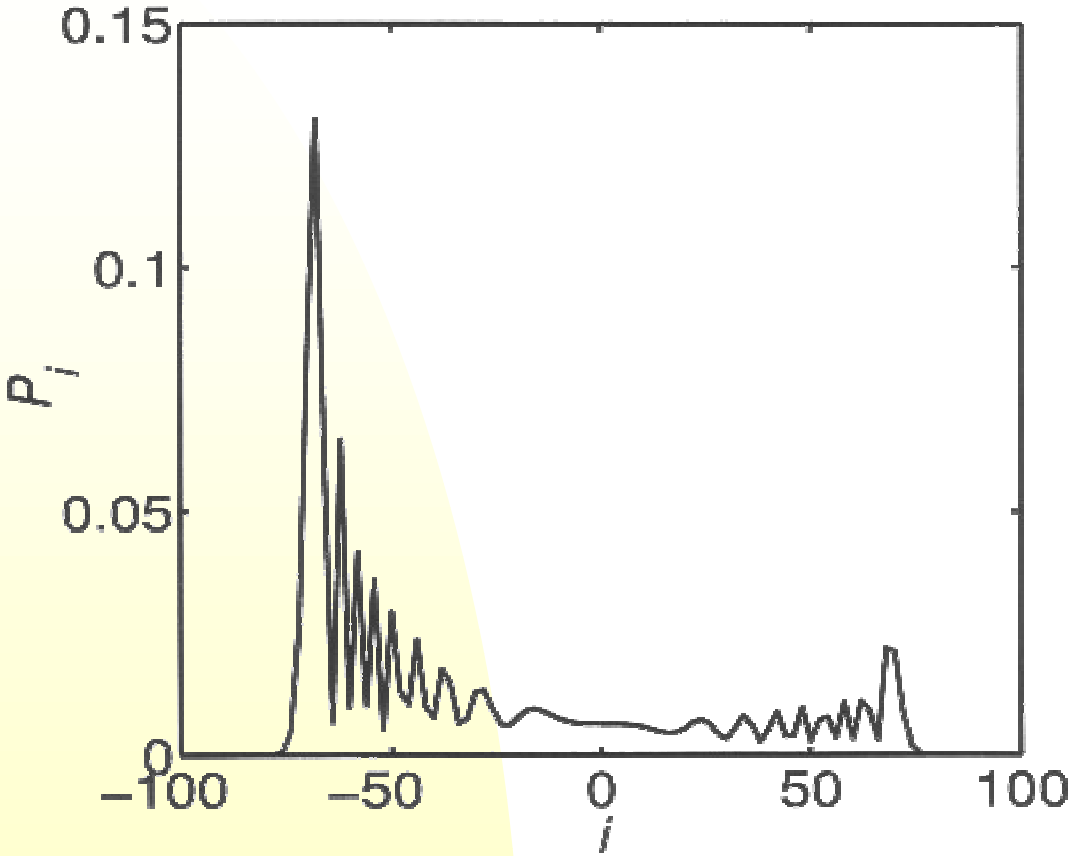
$$H : |\pm\rangle \rightarrow \frac{1}{\sqrt{2}}(|+\rangle \pm |-\rangle)$$

  - Controlled displacement:

$$F : |\pm\rangle|i\rangle \rightarrow |\pm\rangle|i \pm 1\rangle$$

- Apply $(FH)^t$ to an initial state $|+\rangle|0\rangle$

Quantum walk distribution

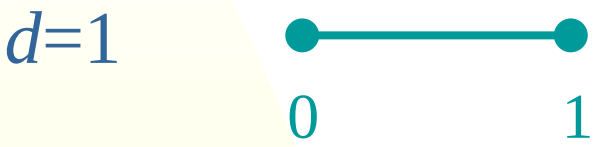


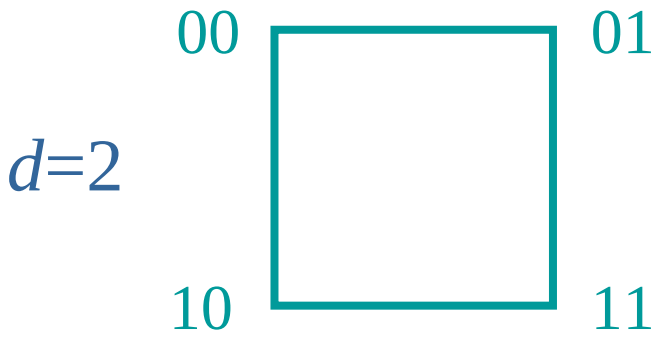
- Quantum walk does not lead to normal distribution
- Variance grows quadratically in the number of steps – faster spread than random walk

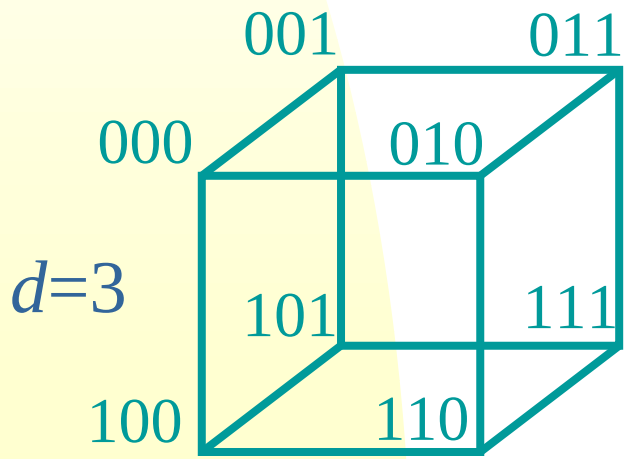
Mackay, Bartlett, Stephenson, Sanders, J. Phys. A (2002)

Random Walks on a Hypercube

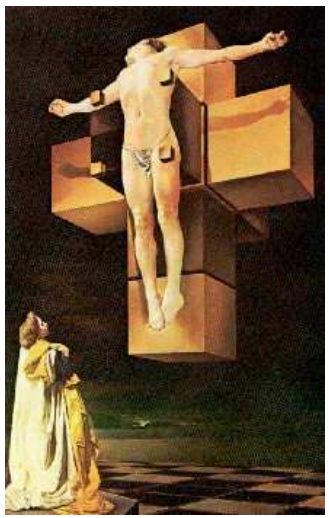
- Hypercube: in *d* dimensions, has 2^n vertices







d=4 ?



Salvador Dali: *Corpus Hypercubicus*

Random Walks on a Hypercube

- The vertices of a hypercube in d-dimensions are labelled by a d bit string

$$(b_1 b_2 b_3 ... b_d) \quad b_i \in \{0,1\}$$

- For example, (000...0) is one corner, and (111...1) is the "opposite" corner
- Random walk on a hypercube:
  1. Start with some vertex, labelled (000...0).
  2. At each step, randomly choose $s \in \{1,...,d\}$.
  3. Flip the s^{th} bit. The walk "travels" only on the edges
- Hitting time: expected number of steps to reach the opposite corner on a d-dimensional hypercube: $\geq 2^{d-1}$

Quantum Walks on a Hypercube

- Use a *d*-sided coin: $H_c = \text{span}\{ |s\rangle, s \in Z_d \}$
- Spatial states are represented by state of *d* qubits:

  $H_s = \text{span}\{ |b_1 b_2 b_3 \ldots b_d\rangle, b_i \in Z_2 \}$
- Generalized coin flip (discrete Fourier transform):

$$C : |s\rangle \rightarrow \sum_m e^{2\pi i m s/d} |m\rangle$$

- Generalized controlled displacement:

$$F : |s\rangle|b_1 b_2 \ldots b_d\rangle \rightarrow |s\rangle|b_1 b_2 \ldots (b_s + 1) \ldots b_d\rangle$$

- Alternate *C* and *F* on initial state $|0\rangle|000\ldots0\rangle$
- Quantum superpositions make the resulting behaviour different from the classical walk

Hitting times... what does that mean?

- What does it mean to say that a quantum walk has "reached" a particular point? Checking requires a measurement
- Can't measure the position of the quantum walk at each step, or we recover the (classical) random walk
- Some possibilities:
  - One-shot measurements: after some fixed time T, measure the position of the quantum walk
  - Concurrent measurements: for some fixed position $|x\rangle$, apply at each step the projection $|x\rangle\langle x|$, I-$|x\rangle\langle x|$. Such a measurement leaves the superpositions in the orthogonal space intact.
- Results: for either type of measurements, quantum walks on a hypercube can hit exponentially faster (quant-ph/0205083)

Conclusions (?)

- Random walks are useful, e.g., in assessing the complexity of some randomized (classical) algorithms
- Quantum walks have distinct behaviour from their classical counterparts
  - No randomness: all evolution is unitary
  - Variance increases quadratically faster
  - Hitting times may be exponentially faster
- Quantum walks may have many uses in quantum information processing, but we don't know enough about them or their power (yet!)