Fearful Symmetries: An Introduction to Quantum Algorithms

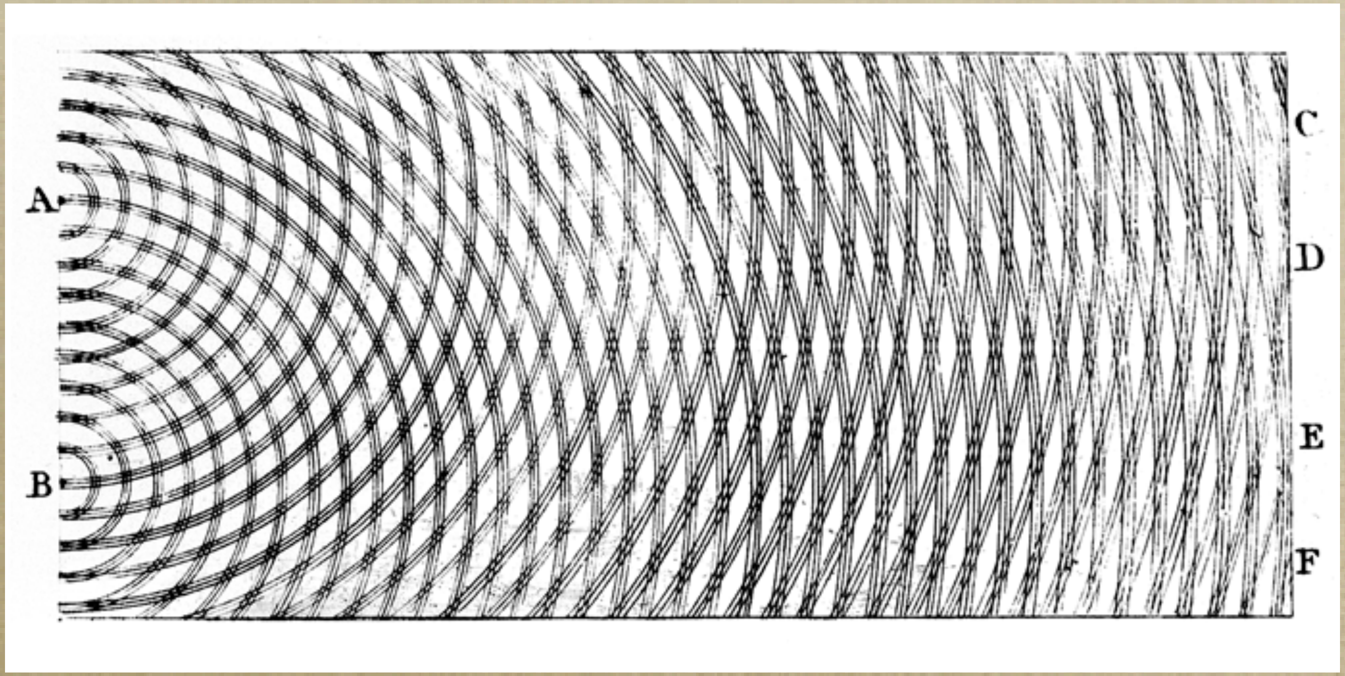
Cristopher Moore, Santa Fe Institute

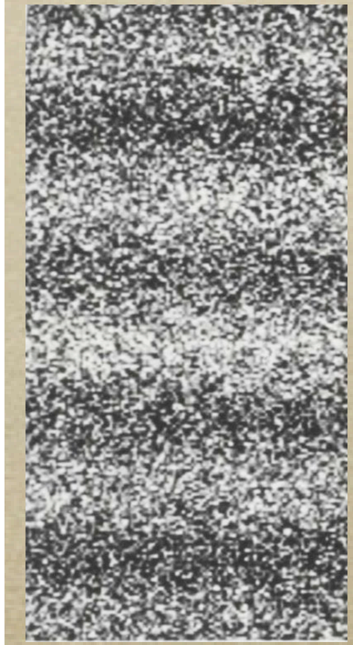
Wednesday, June 20, 2012

Physics and Computation

- Physical Church-Turing Thesis: any physical computing device is at most as powerful as a Turing machine
- Any physical system can be simulated by a standard computer
- Strong version: we can simulate a system in polynomial time (as a function of spacetime)

A Little Quantum Physics

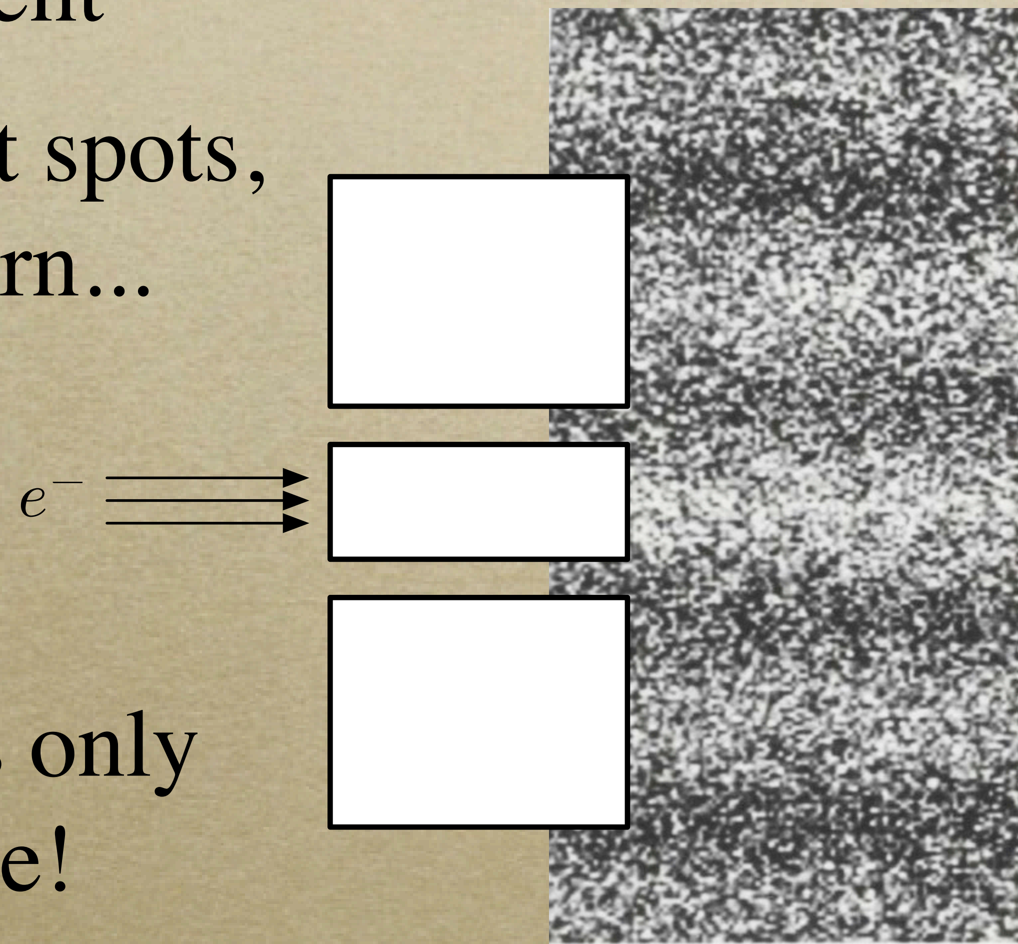




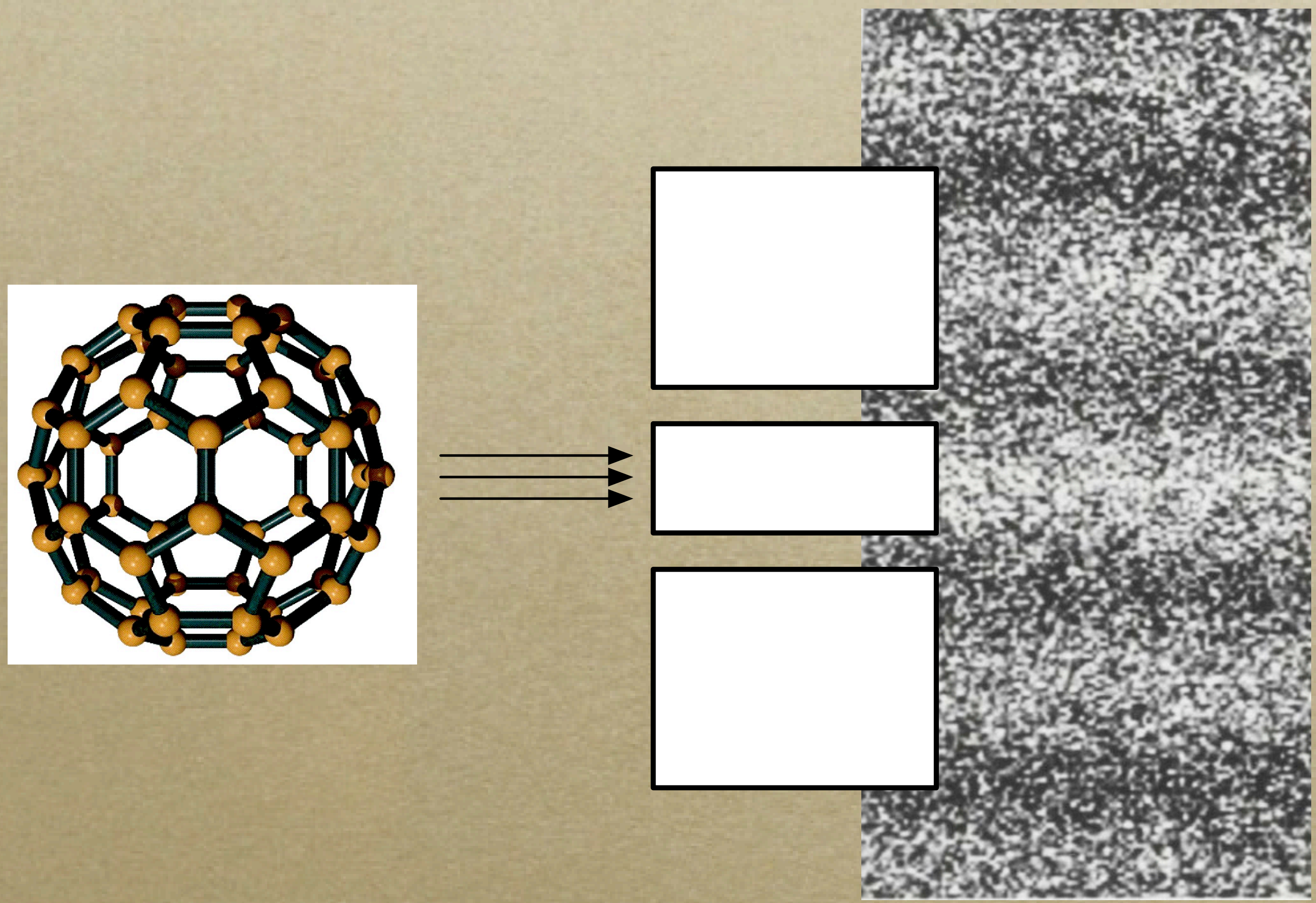
- Thomas Young, 1801: *light is possessed of opposite qualities, capable of neutralising or destroying each other.*

A Little Quantum Physics

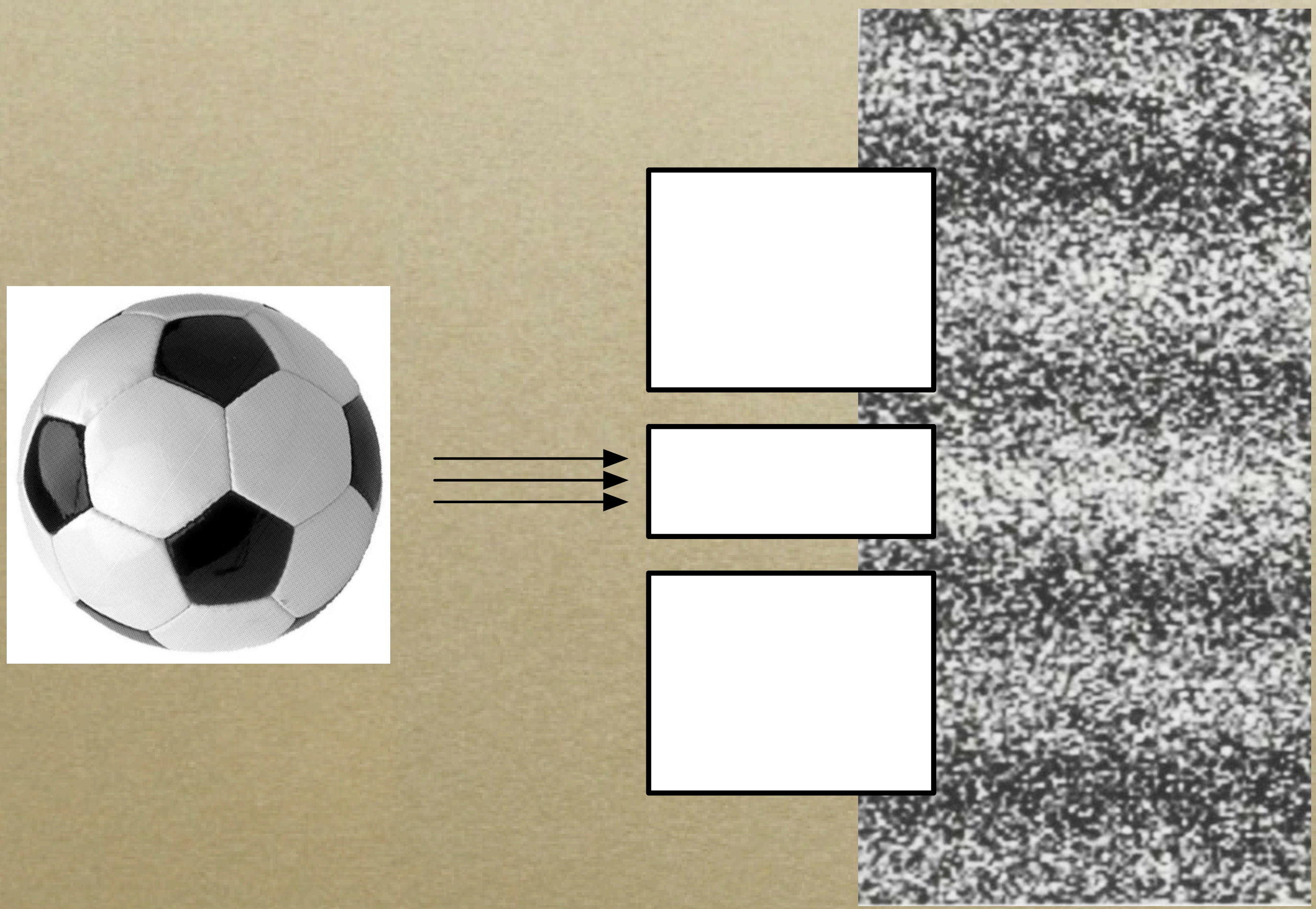
- Double-slit experiment
- Instead of two bright spots, an interference pattern...
- ...even when there is only one electron at a time!



A Little Quantum Physics

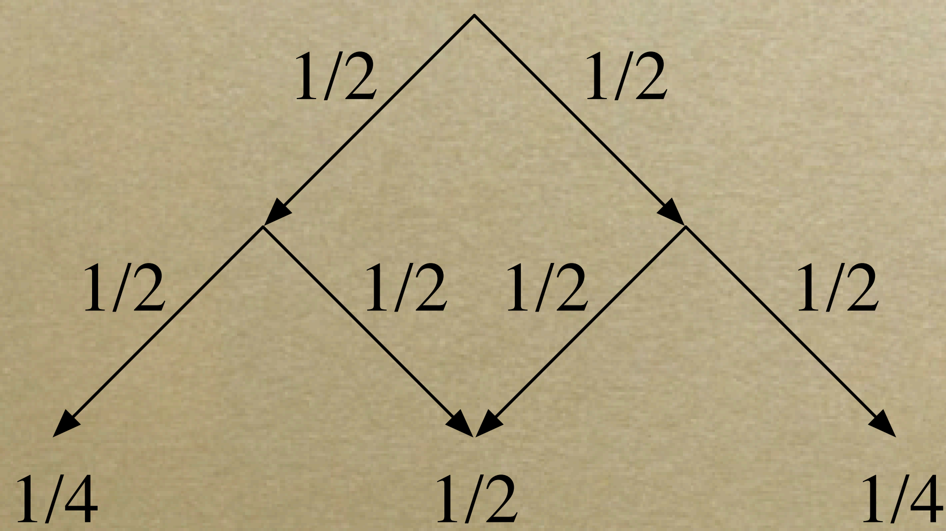


A Little Quantum Physics



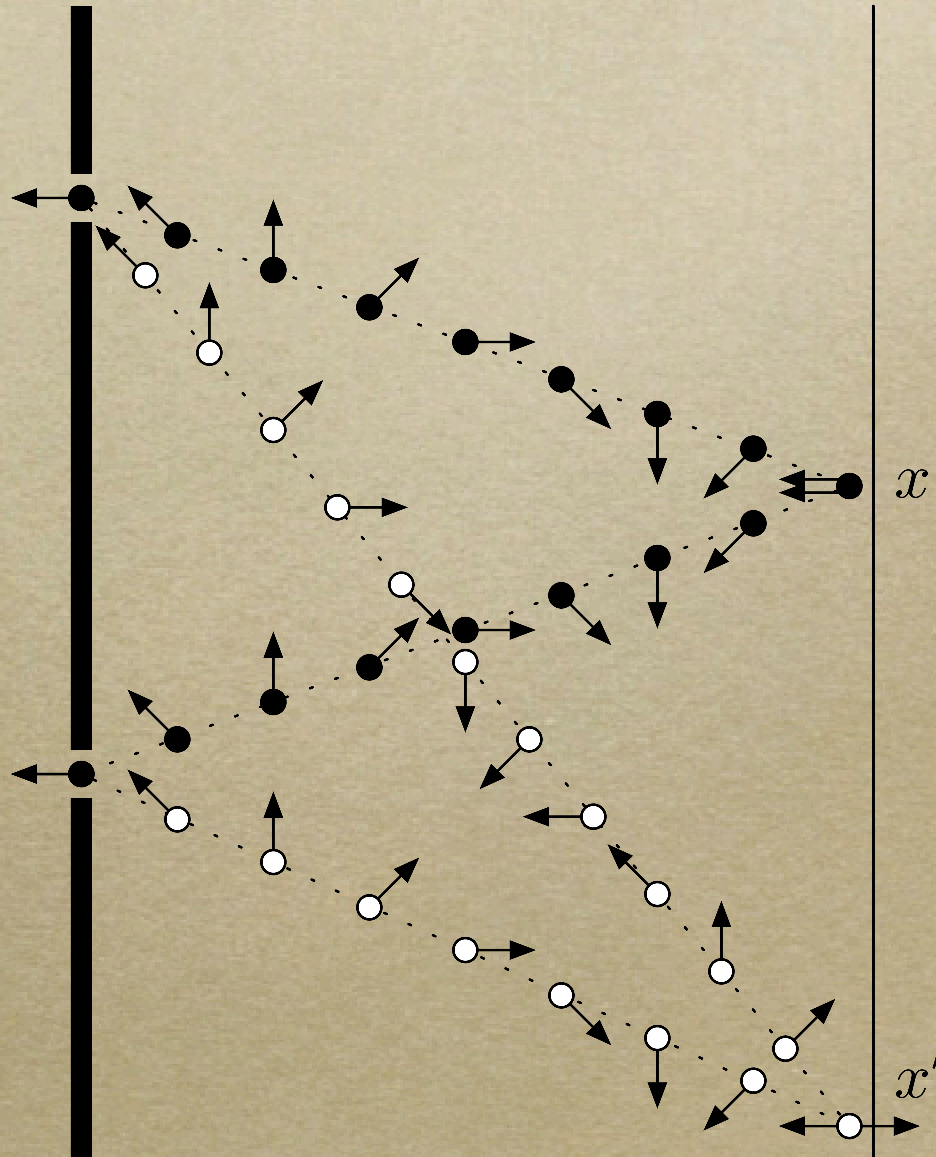
Probabilities Add

- Each path has a probability: product of probability of each step
- Total probability = sum over paths



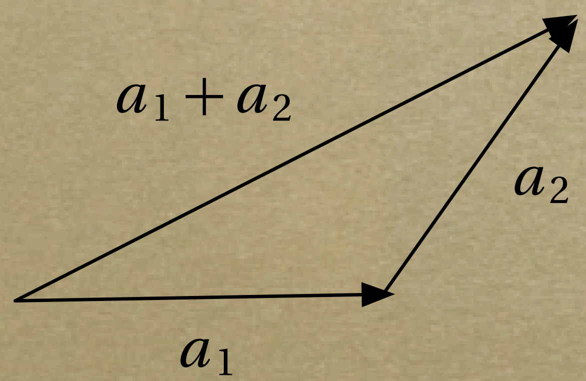
Amplitudes Interfere

- Probabilities don't add!
- Quantum states have *phases*, which can add constructively or destructively.
- Quantum algorithms: wrong answers cancel, right ones add up



Amplitudes interfere

- Each path has a complex-valued *amplitude*
- Amplitudes can add constructively or destructively
- Probability is |amplitude|^2



$$|a_1 + a_2|^2 \neq |a_1|^2 + |a_2|^2$$

Transitions

- Each step of a probabilistic algorithm is a *stochastic* matrix: columns sum to 1
- e.g. if heads, leave it alone; if tails, flip

$$\begin{pmatrix} 1 & 1/2 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1/2 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

Transitions

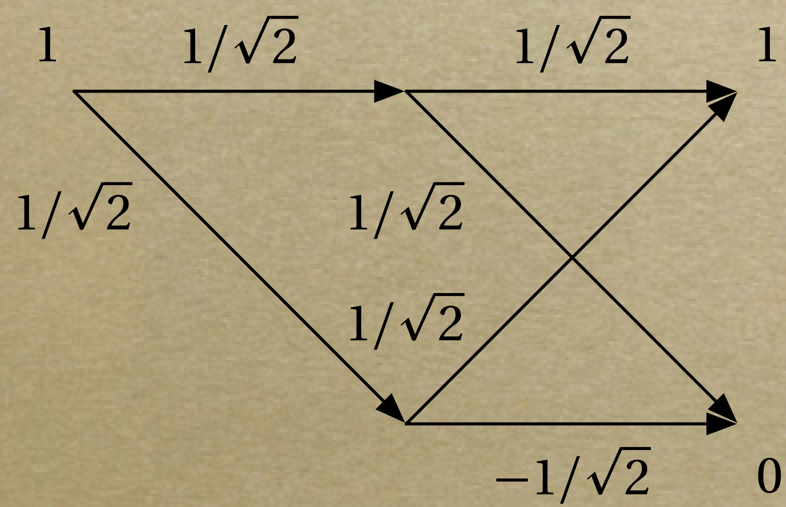
- Each step of a quantum algorithm is a *unitary* matrix: it rotates the state, preserving the Euclidean length (sum of squares)
- e.g. the Hadamard matrix produces two superpositions — which are not the same!

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \qquad \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

Transitions

- Sum over paths = matrix product

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



Entanglement

- A two-qubit system has a 4-dimensional state
- If they are independent, a tensor product:

$$a_{00} = b_0 c_0$$
$$a_{01} = b_0 c_1$$
$$a_{10} = b_1 c_0$$
$$a_{11} = b_1 c_1$$

Entanglement

- A joint state, not a product of independent ones
- Like classical correlation, except...

$$a_{00} = 1/\sqrt{2} \qquad p_{00} = 1/2$$

$$a_{01} = 0 \qquad p_{01} = 0$$

$$a_{10} = 0 \qquad p_{10} = 0$$

$$a_{11} = 1/\sqrt{2} \qquad p_{11} = 1/2$$

Alice and Bob

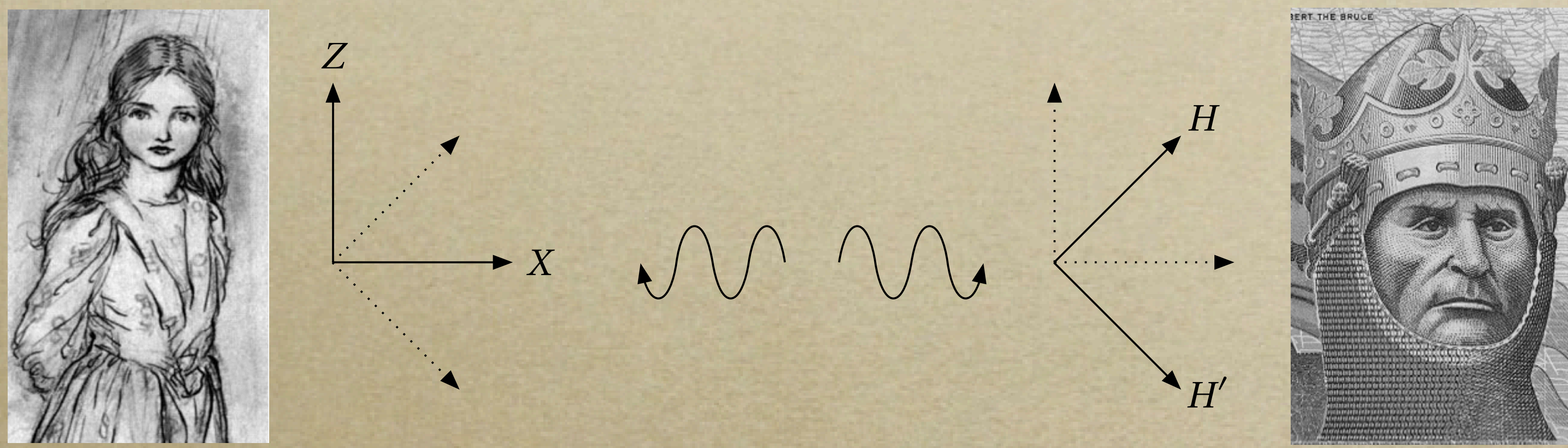
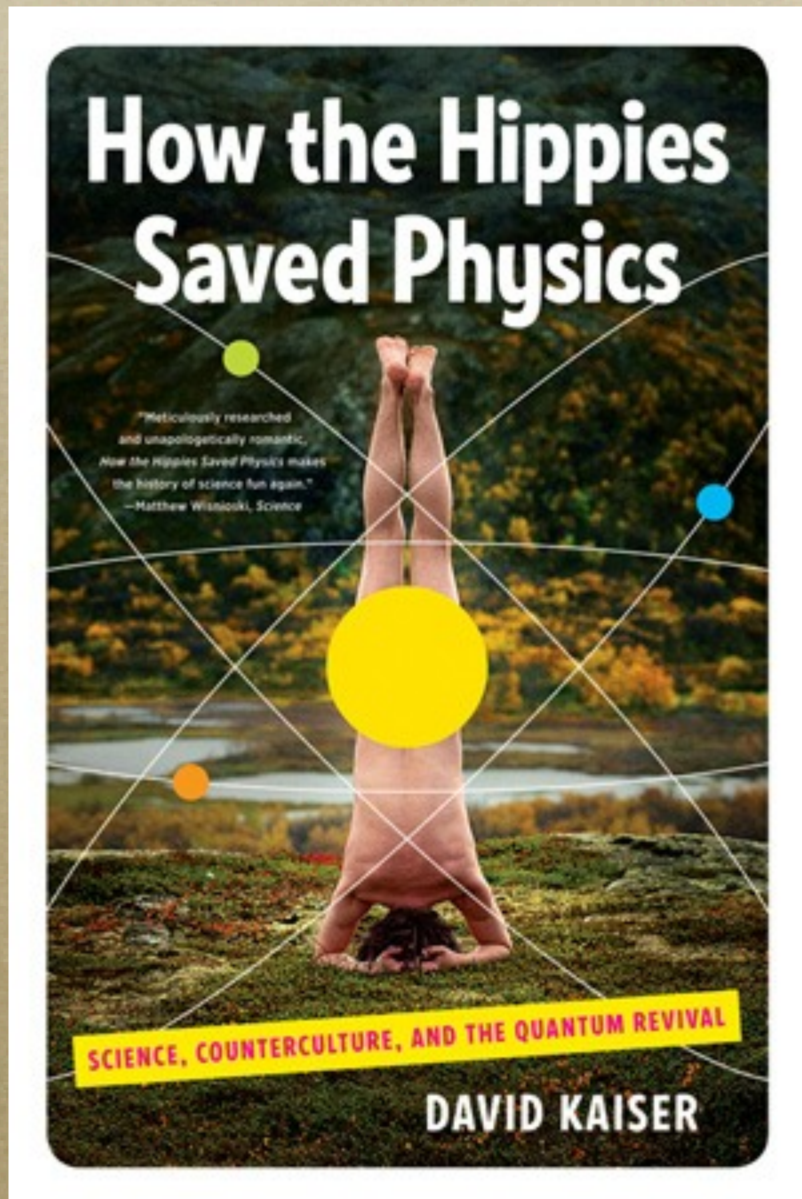


FIGURE 15.4: Alice and Bob. Alice can measure her qubit in either the Z-basis or the X-basis, and Bob can measure his in the H-basis or the H'-basis. The resulting measurements are more correlated than any classical probability distribution, correlated or not, can account for.

- But (sadly) we can't use this to communicate faster than light!

Alice and Bob and the Hippies



Physics

Fig. 1: Nature

Problems:

- come from Nature
- have solutions that are as simple, symmetric, and beautiful as possible (far more so than we have any right to expect)

Computer Science

Problems:

- are artificial
- are maliciously designed to be the worst possible
- may or may not have elegant solutions

Fig. 2: The Adversary

Beauty is Truth, Truth Beauty

In 1928, Dirac saw that the simplest, most beautiful equation for the electron has *two* solutions.

Four years later, the positron was found in the laboratory.

Conservation is Symmetry

$$\frac{dx}{dt} = \frac{\partial \mathcal{H}}{\partial p} \quad , \quad \frac{dp}{dt} = -\frac{\partial \mathcal{H}}{\partial x}$$

perhaps you are more familiar with $p = mv$ and $F = ma$; try with $\mathcal{H} = (1/2)mv^2 + V(x)$

Conservation of momentum follows from translation invariance: moving entire world by *dx* doesn't change energy

$$\frac{dp}{dt} = -\frac{\partial \mathcal{H}}{\partial x} = 0$$

Conservation is Symmetry

Noether's Theorem:
symmetry implies conservation

$$\frac{d\theta}{dt} = \frac{\partial \mathcal{H}}{\partial J} \quad , \quad \frac{dJ}{dt} = -\frac{\partial \mathcal{H}}{\partial \theta}$$

Conservation of angular momentum follows from symmetry under rotation!
In classical and quantum mechanics, *all* conservation laws are of this form.

Relativity is Symmetry

Physics is invariant under changes of coordinates to a moving frame:

$$\begin{pmatrix} x \\ ct \end{pmatrix} \to \gamma \begin{pmatrix} 1 & -v/c \\ -v/c & 1 \end{pmatrix} \begin{pmatrix} x \\ ct \end{pmatrix}$$

at small velocities, Galileo:

$$x \to x - vt \; , \; t \to t$$

Groups

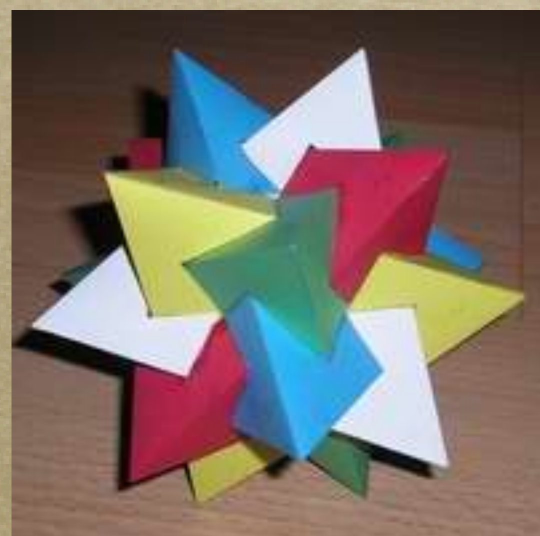
A *group* is a mathematical structure with:

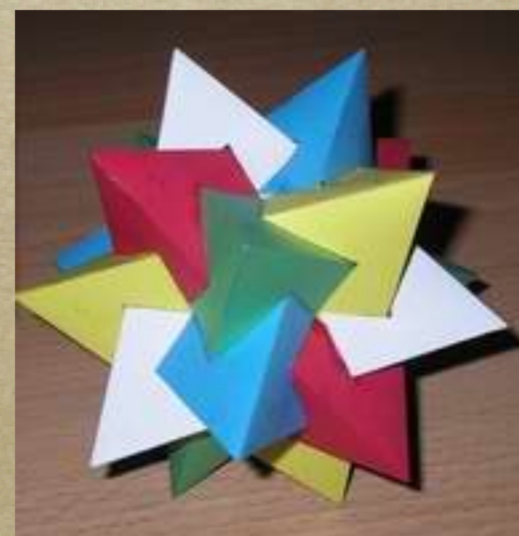
- associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- identity: $a \cdot 1 = 1 \cdot a = a$
- inverses: $a \cdot a^{-1} = a^{-1} \cdot a = 1$
- but not necessarily $a \cdot b \neq b \cdot a$

(these are *non-Abelian* groups)

Some Common Groups

- cyclic: $\mathbb{Z}_n$ (addition mod n), $\mathbb{Z}_n^*$ (multiplication)
- symmetric group (permutations): S_n, A_n
- invertible matrices
- rotations: $O(3)$
- $O(3)$ contains A_5!

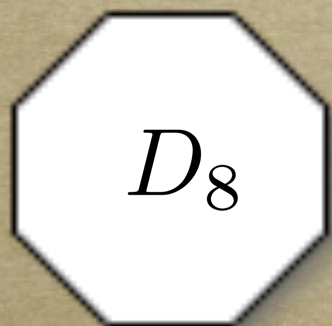




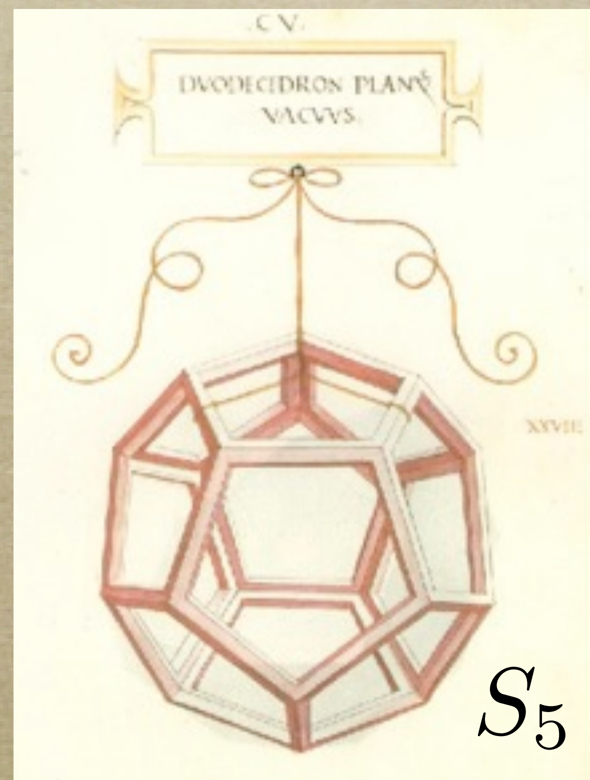
Symmetry Groups

Transformations that leave an object fixed:

$\mathbb{Z} \times \mathbb{Z}$



D_8



S_5

When Symmetry is Periodicity

- Given a function $f : \mathbb{Z}_n \rightarrow S$ we can ask for which *h* we have

$$f(x) = f(x + h)$$

for all *x*.

- These *h* are multiples of the periodicity *r*.
- The set of all such *h* forms a *subgroup*.

Periodicity Gives Factoring!

- To factor *n*, let $f(x) = c^x \bmod n$.
- Find smallest *r* such that $f(x) = f(x+r)$ i.e., $c^r \equiv 1 \bmod n$. Suppose *r* is even:

$$c^r - 1 = kn = (c^{r/2} + 1)(c^{r/2} - 1)$$

- Now take g.c.d. of *n* with both factors (easy).
- Works at least 1/2 the time with random *c*!

Factoring: An Example

- Let's factor 15. Choose c=2:

$$\begin{array}{cccccccccc} x: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2^x: & 1 & 2 & 4 & 8 & 1 & 2 & 4 & 8 & 1 \end{array}$$

$$2^4 - 1 = 15 = (2^2 - 1)(2^2 + 1) = 3 \times 5$$

- Bad news: in general r could be as large as n, exponentially big as a function of #digits.

Quantum Measurements

Measure *f(x)*, and “collapse” to a superposition

x :	0	1	**2**	3	4	5	**6**	7	8
2^x :			4				4		

This is a random *coset* of the subgroup *H*.

But, if we simply measure *x*, all we see is a random value! This is the wrong measurement.

The Fourier Transform

Periodicities are peaks in $\hat{f}$, where $(\omega = \mathrm{e}^{2\pi i/n})$

$$f(x) = \frac{1}{\sqrt{n}} \sum_k \hat{f}(k)\, \omega^{kx}\,,\;\; \hat{f}(k) = \frac{1}{\sqrt{n}} \sum_x f(x)\, \omega^{-kx}$$

Change of basis $Q_{x,k} = \frac{1}{\sqrt{n}}\, \omega^{kx}$

from *x* to *k*. This transformation is *unitary:*

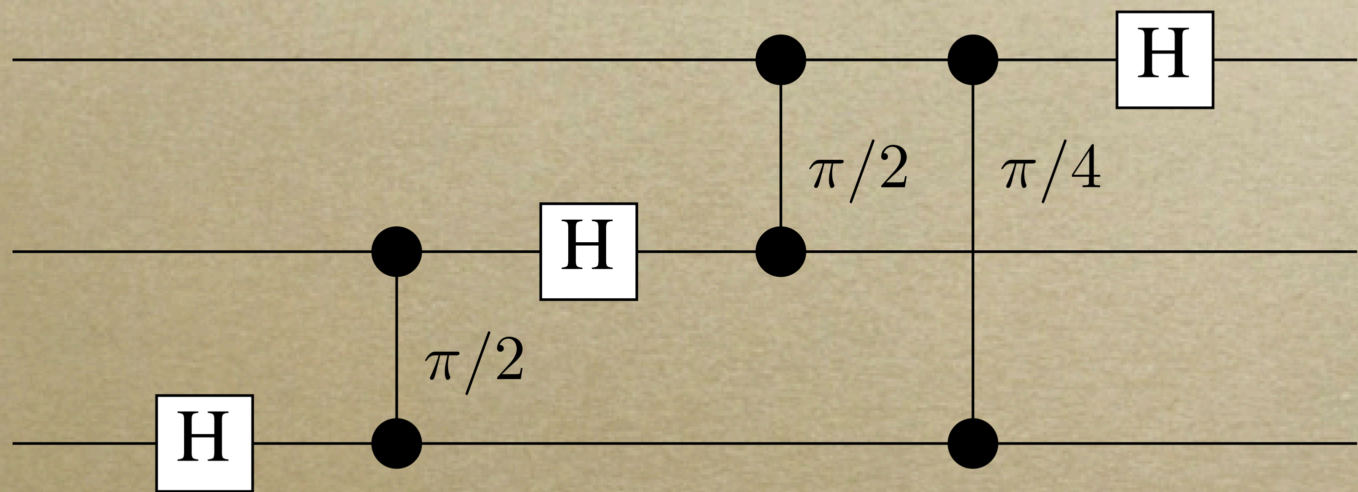
$$Q^{-1} = Q^{\dagger}$$

Shor's Algorithm

- Quantum mechanics allows us to perform unitary transformations.
- We can "do" the Fourier transform mod n with only $O(\log^2 n)$ elementary quantum operations.
- We then measure the frequency, this gives us the periodicity of $f(x)$.

Efficient Circuits for the QFT

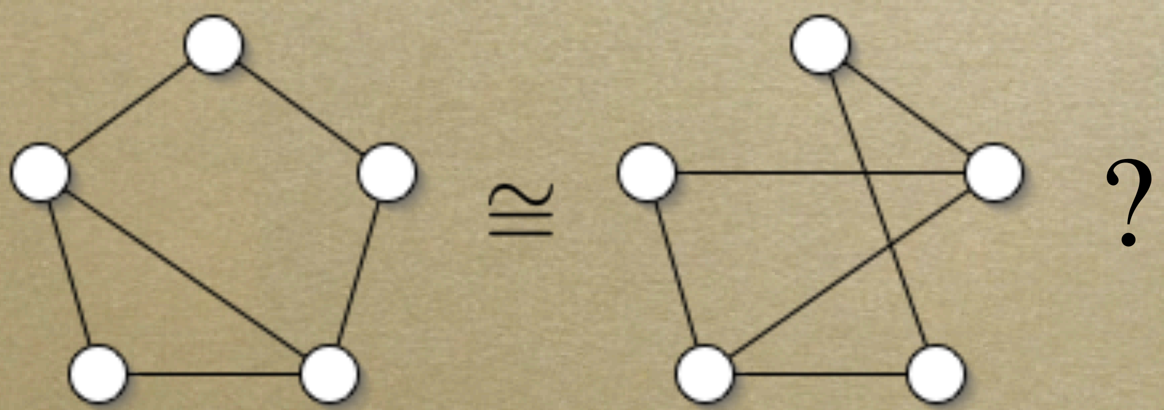
- We can break down the QFT recursively (like the FFT) into elementary gates:



- Quadratic in the number of qubits
- Thus *n* can be exponentially large!

Graph Isomorphism

- Factoring appears to be outside P, but not NP-complete. (Indeed, we believe that BQP does not contain all of NP.)
- Another candidate problem like this:



Solving with Symmetry

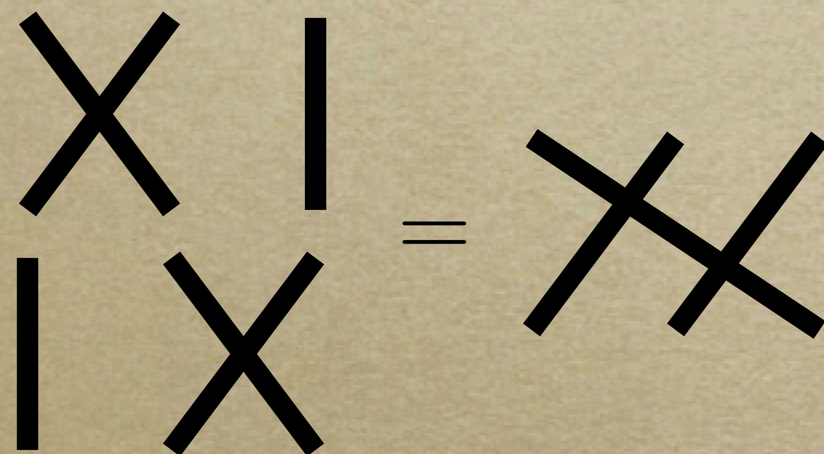
- Take the union of the two graphs. Permuting the $2n$ vertices defines a function f on S_{2n} . What is its symmetry subgroup H?
- Assume no internal symmetries. Then either f is 1-1 and $H = \{1\}$, or f is 2-1 and

$$H = \{1, m\}$$

for some m that exchanges the two graphs.

The Permutation Group

- The set of *n!* permutations of *n* things forms the permutation group S_n :



- A richly non-Abelian group ($ab \neq ba$.)

The Hidden Subgroup Problem

- We have a function $f : G \to X$
- We want to know its symmetries $H \subseteq G$
- Essentially all quantum algorithms that are exponentially faster than classical are of this form:
  - $\mathbb{Z}_n^*$ = factoring
  - S_n = Graph Isomorphism
  - D_n = some cryptographic lattice problems

Non-Abelian Fourier Transforms

- For non-Abelian G, we need *representations*:
- Geometric pictures of G in d-dimensional space

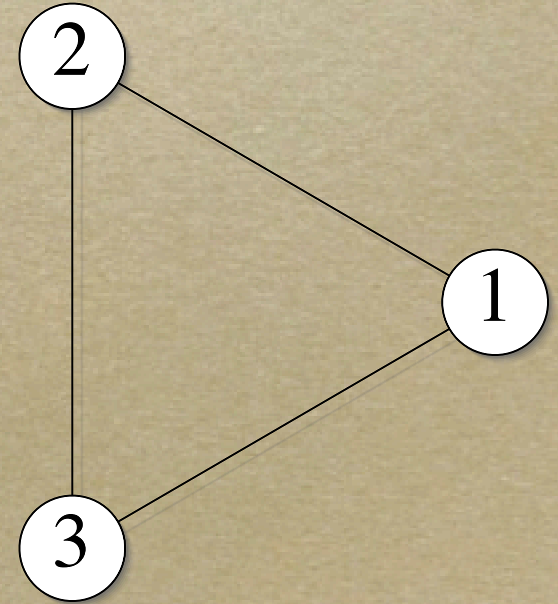
- A_5 has a three-dimensional representation: permute the colors by rotating.

Non-Abelian Fourier Transforms

- S_3 has **1** (trivial), $\pi = \pm 1$ (parity), and rotations of three points in the plane:

$$\rho((1\,2)) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; \rho((1\,2\,3)) = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}$$

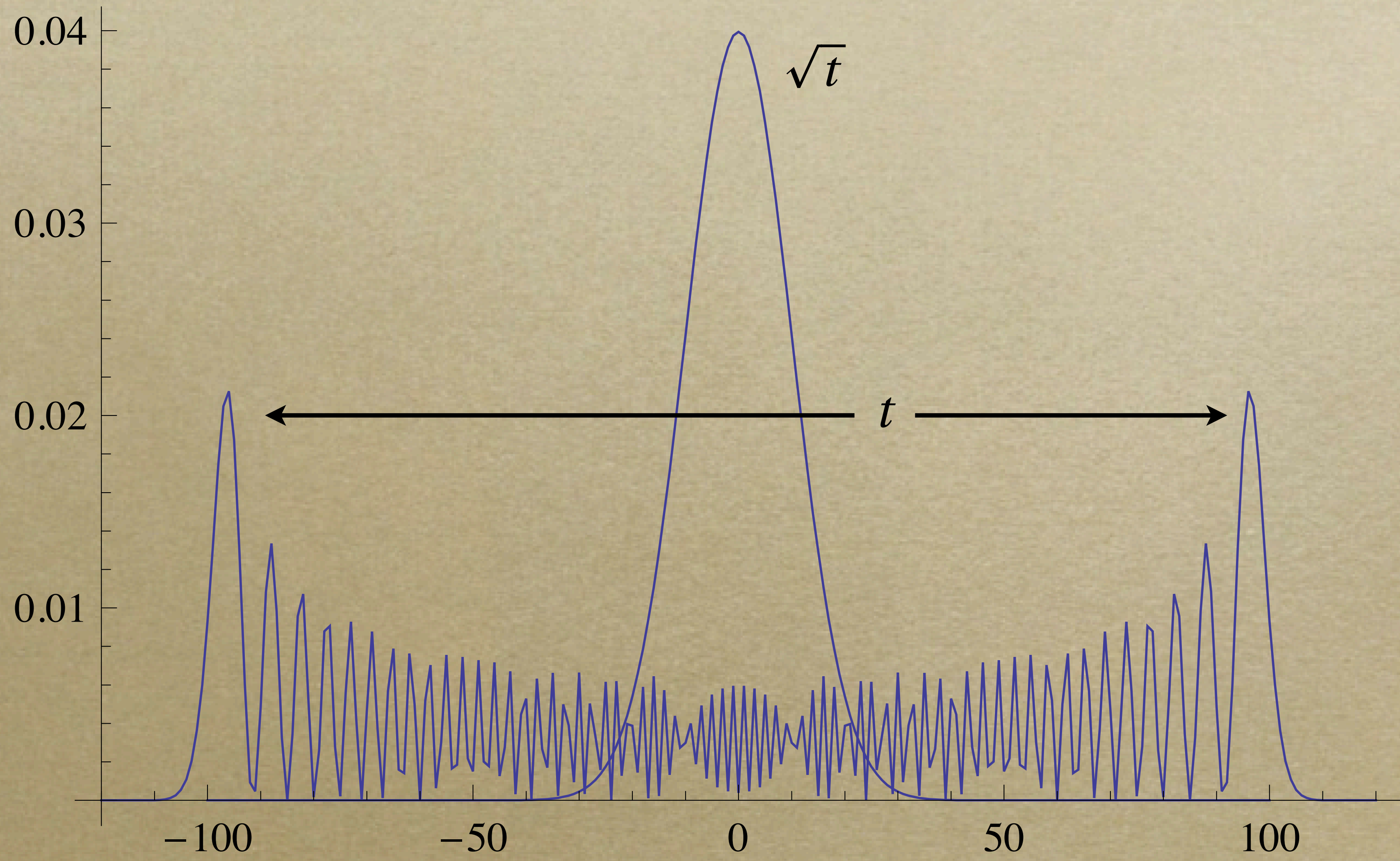
- Gives 1+1+4 = 6 "frequencies," just enough. Coincidence?



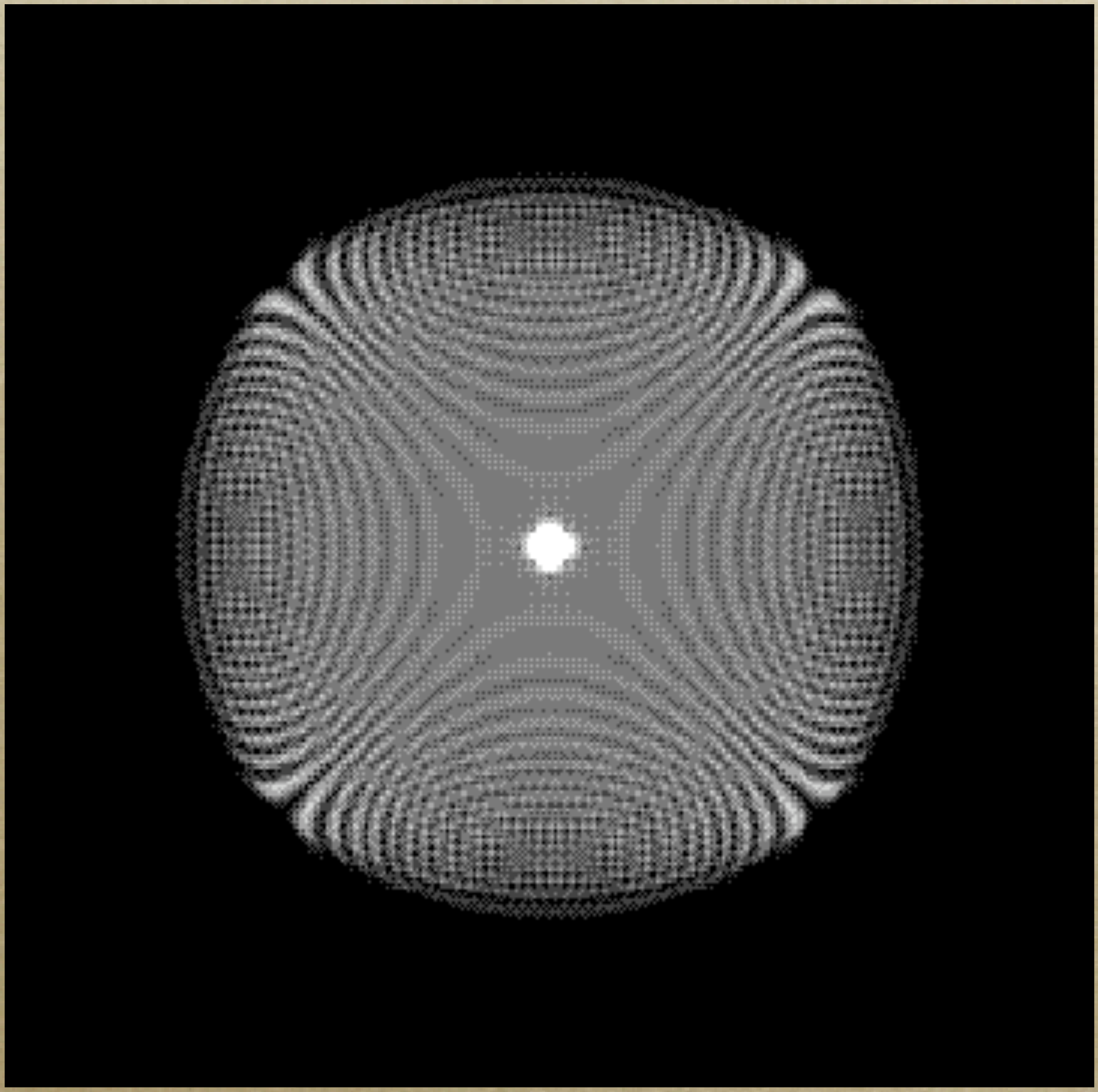
The Story So Far...

- It turns out that this naïve generalization of Shor's algorithm doesn't work: the permutation group S_n is "too non-Abelian."
- Tantalizingly, we know a *measurement* exists, but we don't know if we can do it efficiently.
- How much can quantum computing really do? How "special" is factoring?

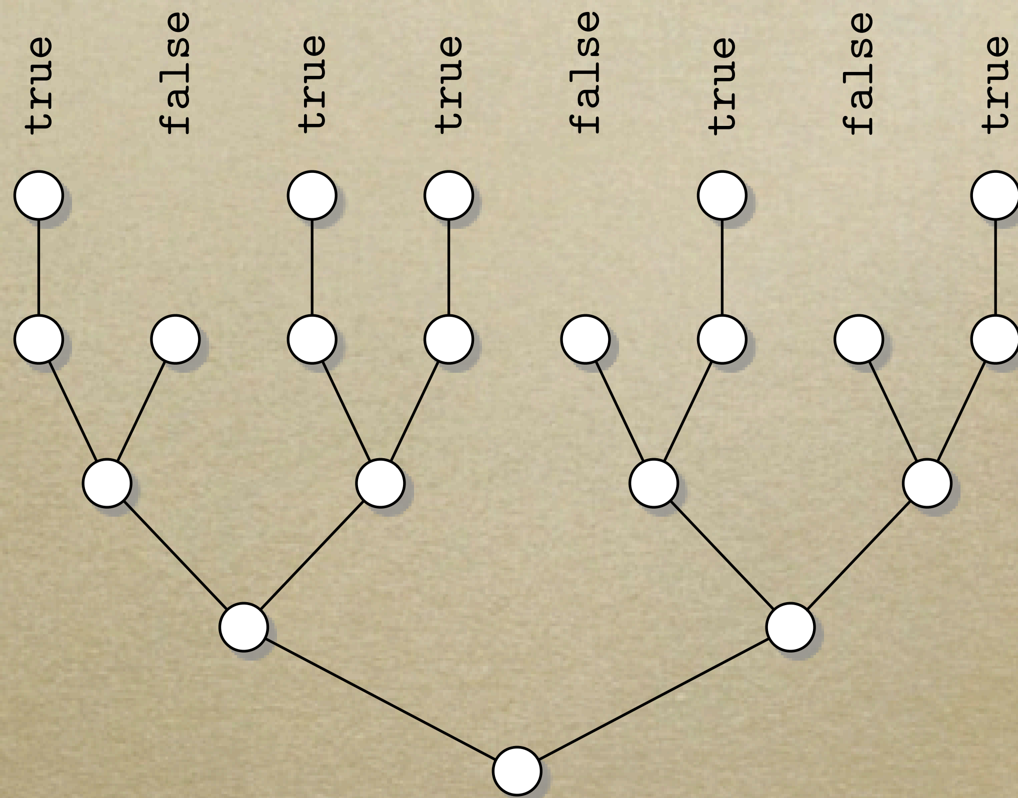
Classical and Quantum Walks



Classical and Quantum Walks

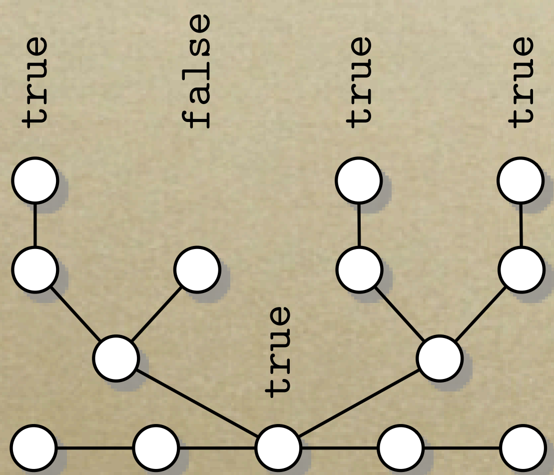


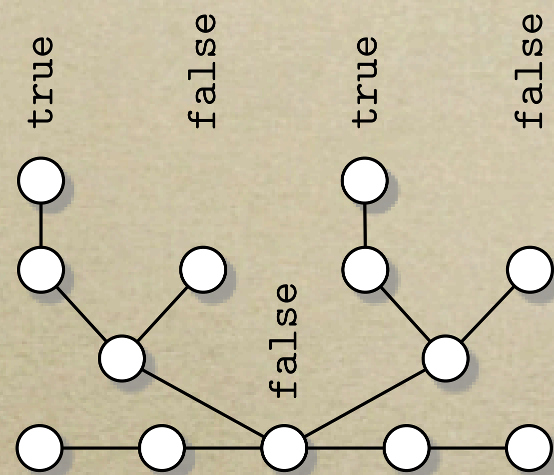
Evaluating a Game Tree

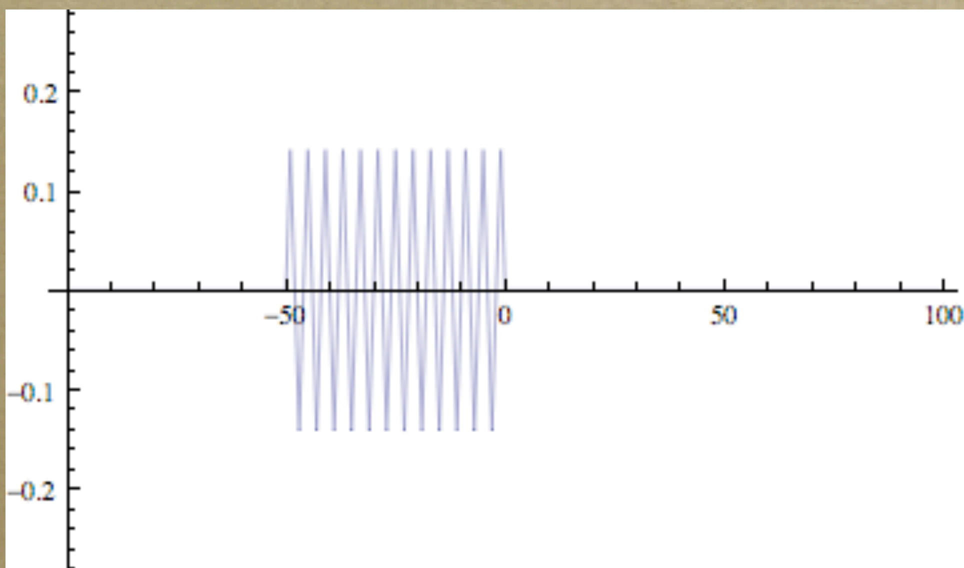


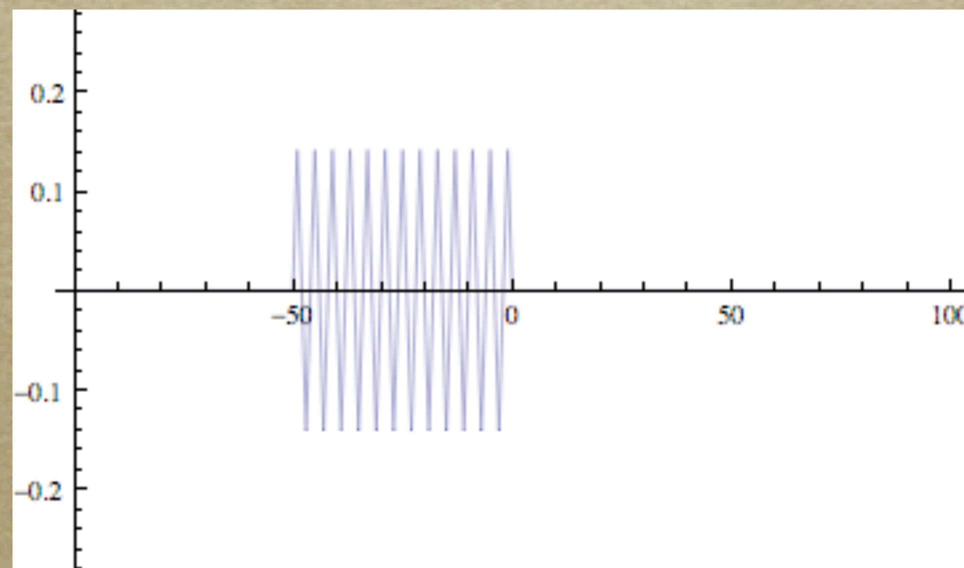
- You have a winning strategy if at least one move is a loss for your opponent: a NAND gate

Scattering Algorithms



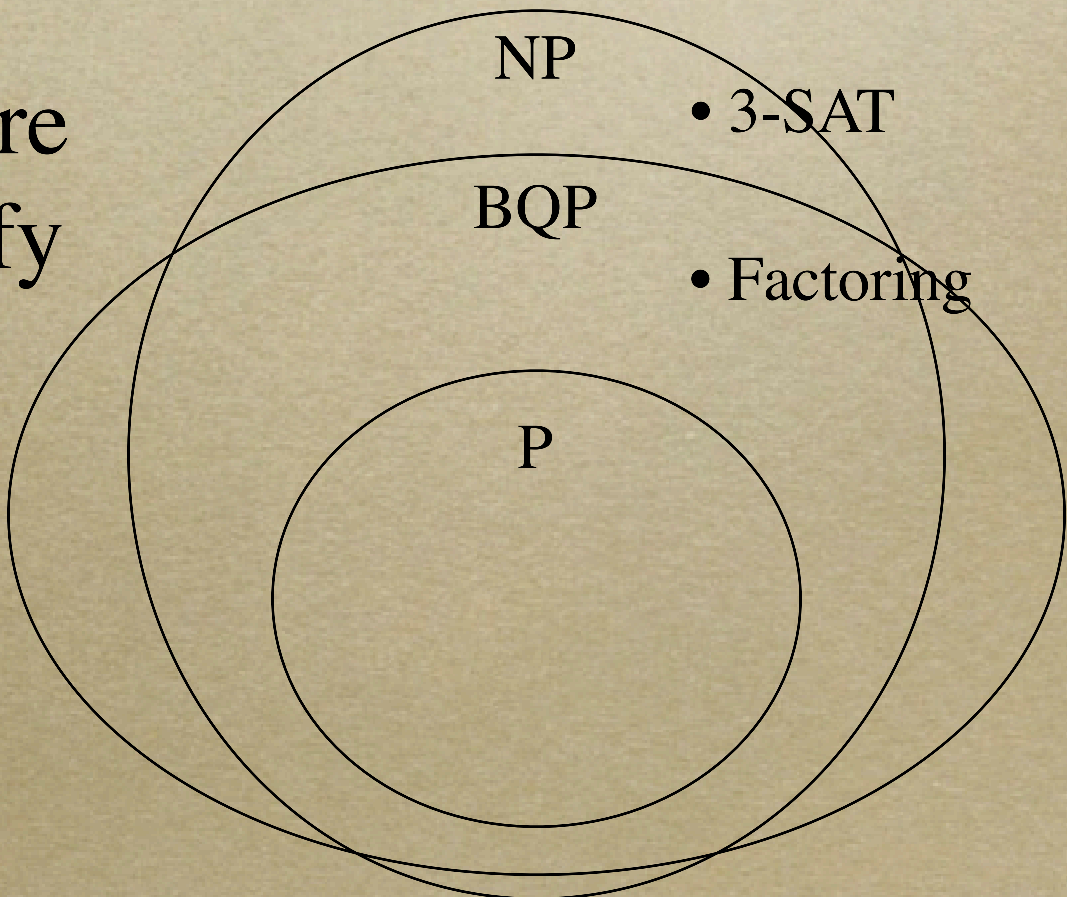






How Powerful is Quantum?

- We believe that they can't solve NP-complete problems
- But solutions can require quantum proofs to verify



Shameless Plug

This book rocks! You somehow manage to combine the fun of a popular book with the intellectual heft of a textbook.

— Scott Aaronson

A treasure trove of information on algorithms and complexity, presented in the most delightful way.

— Vijay Vazirani

A creative, insightful, and accessible introduction to the theory of computing, written with a keen eye toward the frontiers of the field and a vivid enthusiasm for the subject matter.

— Jon Kleinberg

Oxford University Press, 2011