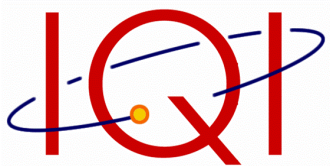
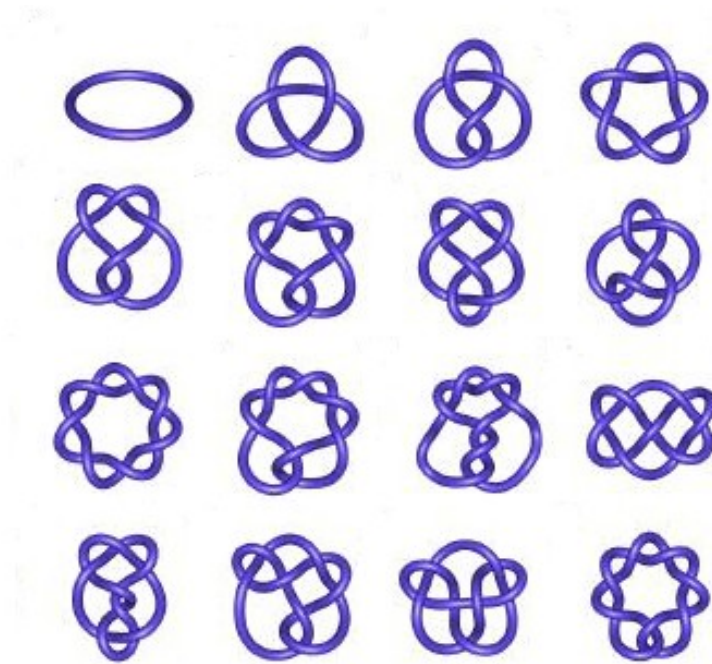


Quantum Algorithms for Topological Invariants

Stephen Jordan



NIST

Wed Feb. 3, 2010

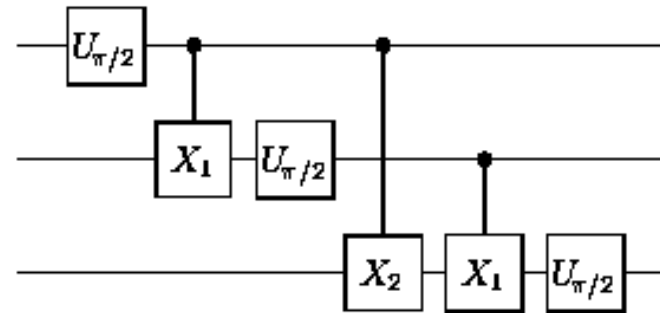
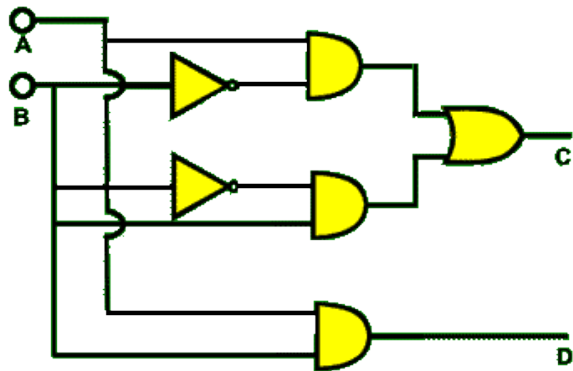
What is a quantum algorithm?

Classical

Quantum

0101101

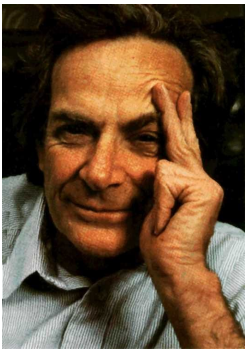
$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha(x) |x\rangle$$



$$X_n = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^n} \end{pmatrix}$$



- the rules:
 - solve problem using sequence of local quantum gates
- the goal:
 - use fewer gates than classical algorithms



R. Feynman

Simulation

$\text{poly}(n)$ quantum

$O(2^n)$ classical

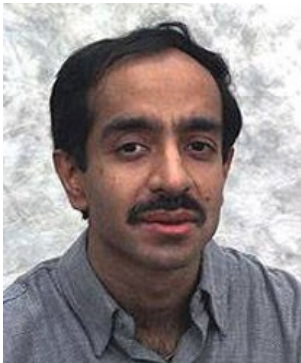


P. Shor

Factoring (1994)

$O(n^3)$ quantum

$O(2^{n^{1/3}})$ classical



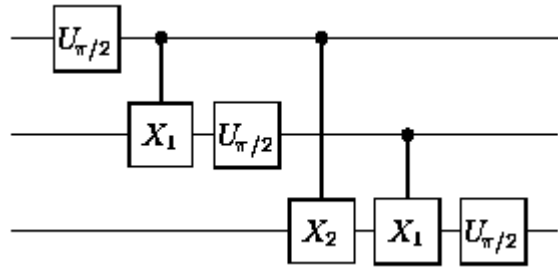
L. Grover

Search (1996)

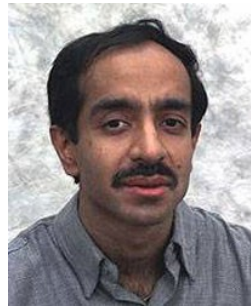
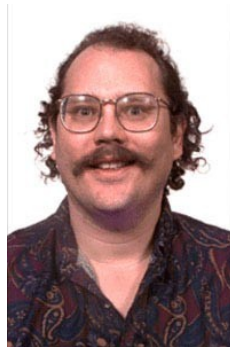
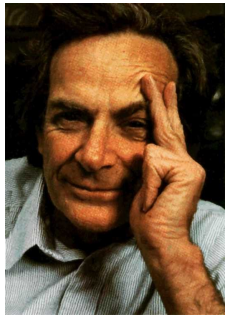
$O(\sqrt{N})$ quantum

$O(N)$ classical

Despite simple rules



and some early successes



the game is hard.



We need heuristics.



Alonzo Church



Alan Turing

Church-Turing Thesis

Everything computable is computable by a Turing machine.

Modern form:

Every physical system can be efficiently simulated by a standard quantum computer.

Heuristic:

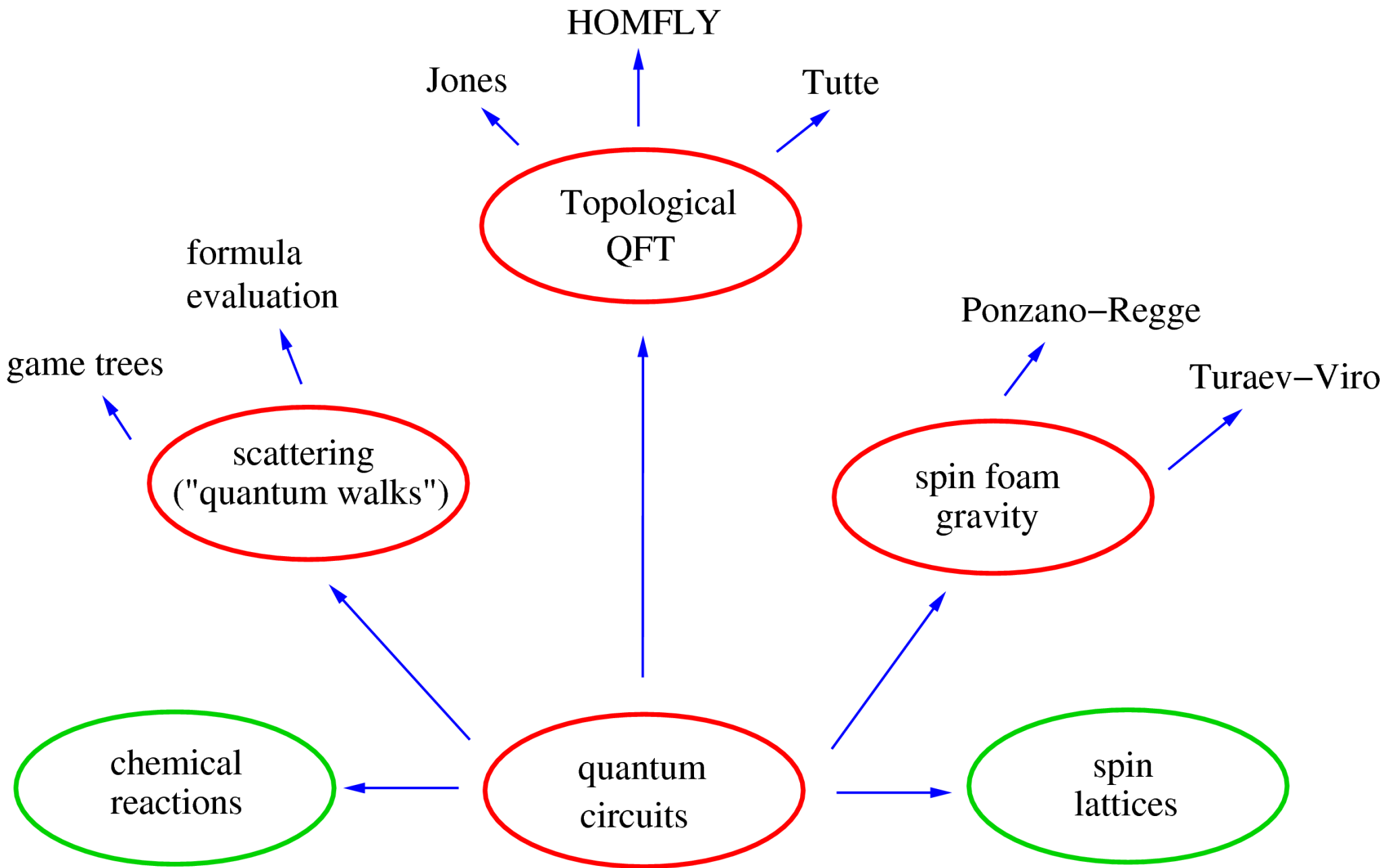
Find quantum algorithms by simulating physical systems.

Every physical system can be efficiently simulated by a standard quantum computer.

more precisely:

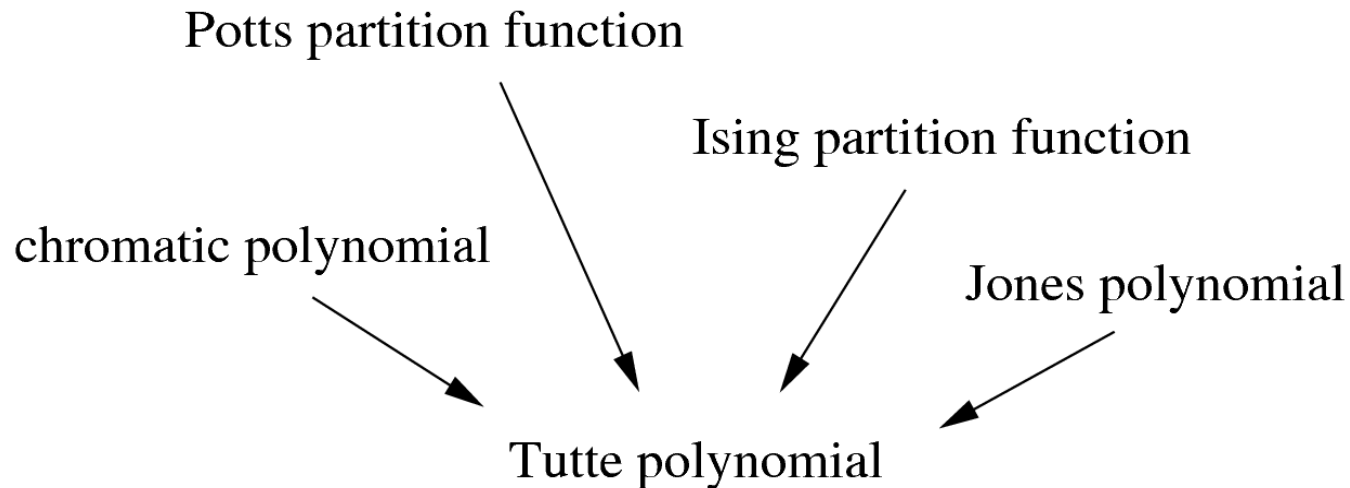
unitary time evolution of n particles for time t should be implementable by quantum circuit of $\text{poly}(n, t)$ gates


does **not** cover: partition functions, ground states,



Why should we care?

- reducibility



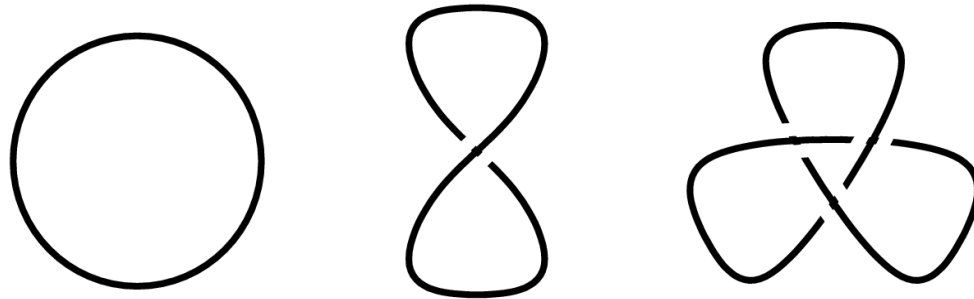
- cryptography
- unforeseen applications (e.g. )
- test the Church-Turing thesis

Overview

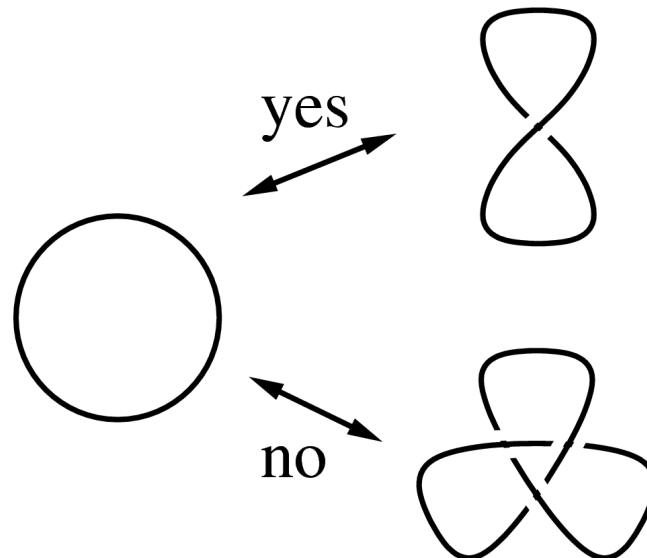
- our Church-Turing heuristic yields quantum algorithms to approximate:
 - knot invariants
 - 3-manifold invariants
- these represent exponential speedups over classical computation
- some of these algorithms can be run on modest hardware

Knot Equivalence

- A knot is an embedding of the circle into \mathbb{R}^3

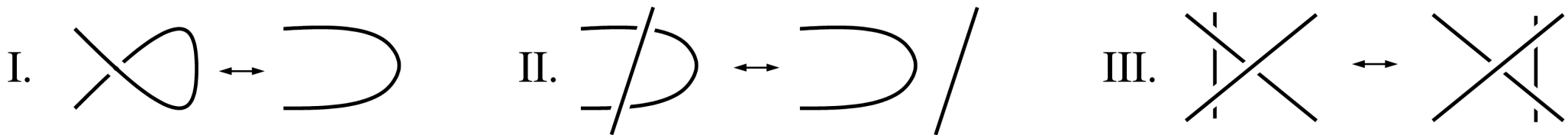


- Are two knots equivalent?



Reidemeister Moves



- Two knots are equivalent if and only if one can be reached from the other by a sequence of Reidemeister moves





- This gives us a more combinatorial way to think about knot theory.

- no polynomial time algorithm for knot equivalence is known
- partial solution:

knot invariant

if  is equivalent to  then

$$f(\text{)} = f(\text{)}$$

- Jones polynomial
 - distinguishes many knots
 - exact value is hard to compute

Jones Polynomial from TQFT

- **1985** Jones discovers Jones polynomial
- **1989** Witten discovers that Jones polynomial arises as amplitude in Chern-Simons TQFT

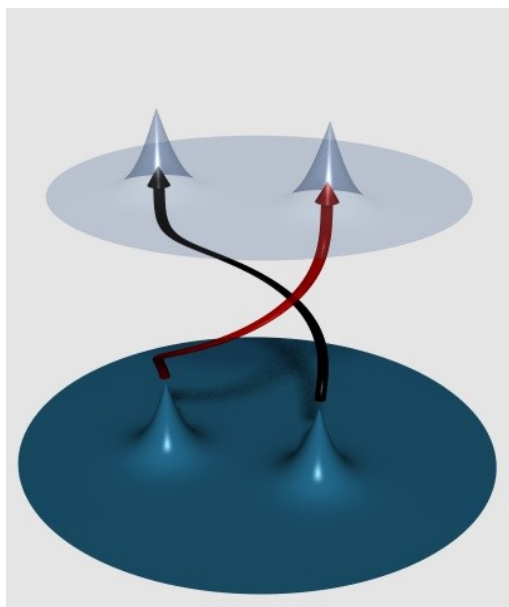


Every physical system can be efficiently simulated by a standard quantum computer.

- **2000** Freedman, Kitaev, Larsen, Wang: quantum algorithm for Jones polynomial

Anyons

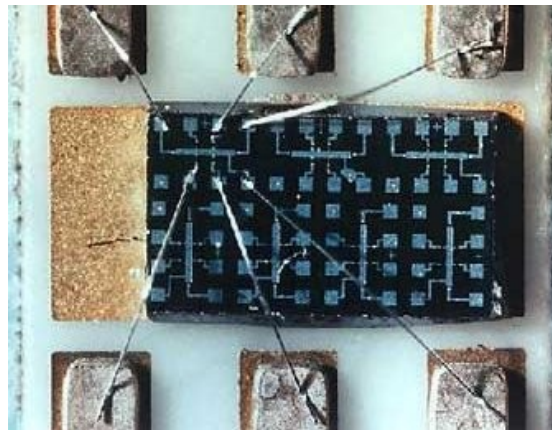
- quasiparticles confined to two dimensions
- world lines are braids

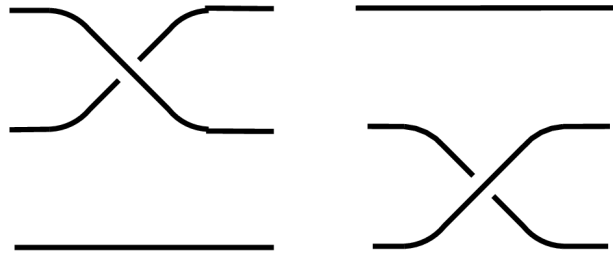


- Adiabatically drag them around
- the corresponding Berry's phases are a representation of the braid group

Nonabelian Anyons

- The n -quasiparticle eigenspace is d -fold degenerate.
- The Berry's “phase” is a d -dimensional unitary representation of the braid group.
- There is indirect evidence that anyons occur in fractional quantum hall systems.





composing braids

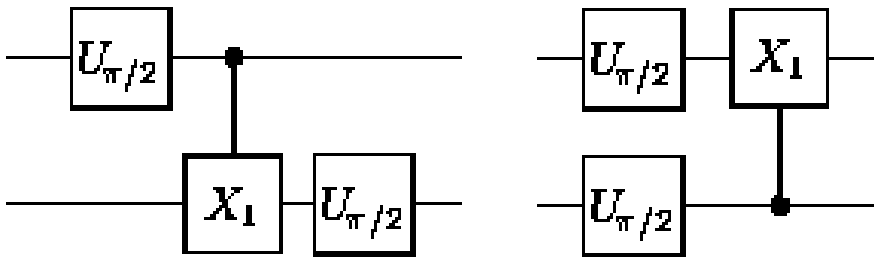


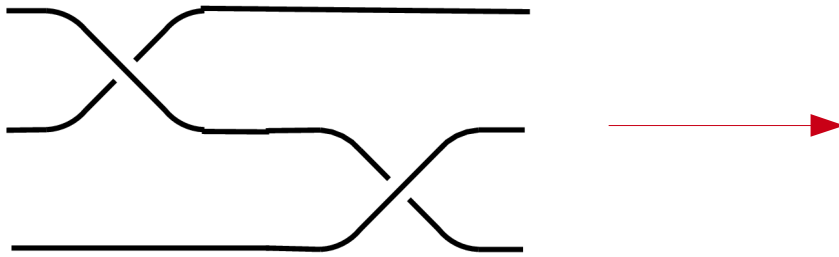
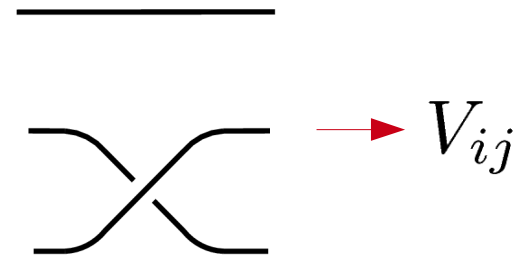
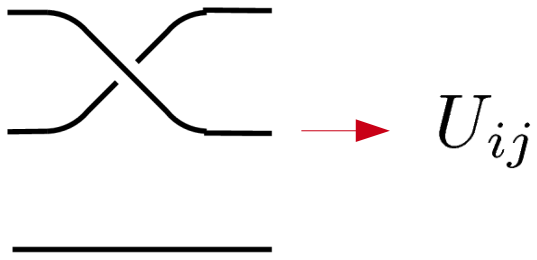
multiplying matrices



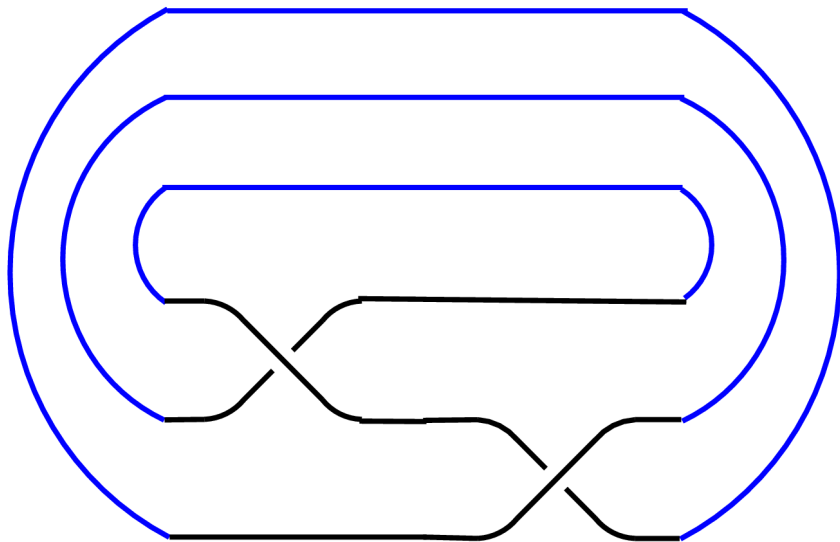
concatenating circuits

$$\begin{bmatrix} e & d & 0 \\ d & c & 0 \\ 0 & 0 & a \end{bmatrix} \quad \begin{bmatrix} e & 0 & d \\ 0 & a & 0 \\ d & 0 & c \end{bmatrix}$$





$$\sum_j U_{ij} V_{jk} = (UV)_{ik}$$



$$\sum_{i,j} U_{ij} V_{ji} = \text{Tr}[UV]$$

= Jones polynomial

One Clean Qubit



- Initial state: one qubit pure, the rest maximally mixed
- Idealized model of high entropy quantum computer such as NMR [Knill & Laflamme, 1998]
- Canonical problem: estimating the trace of a quantum circuit

One Clean Qubit

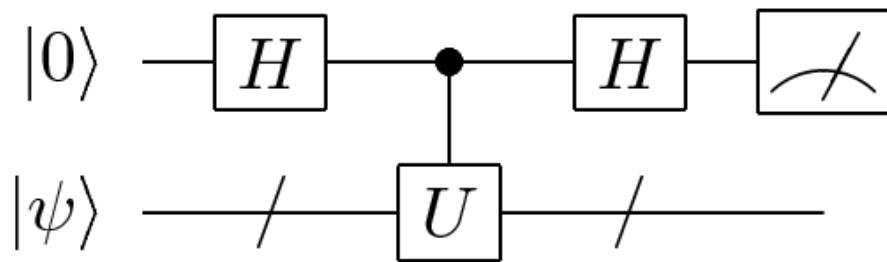
- initial density matrix: $\rho = |0\rangle\langle 0| \otimes \frac{\mathbb{1}}{2^n}$
- entropy n out of $n+1$ maximum
- apply quantum circuit $\rho \rightarrow U\rho U^\dagger$
- with entropy $n+1$ nothing would ever happen!

$$\rho = \frac{\mathbb{1}}{2^{n+1}}$$

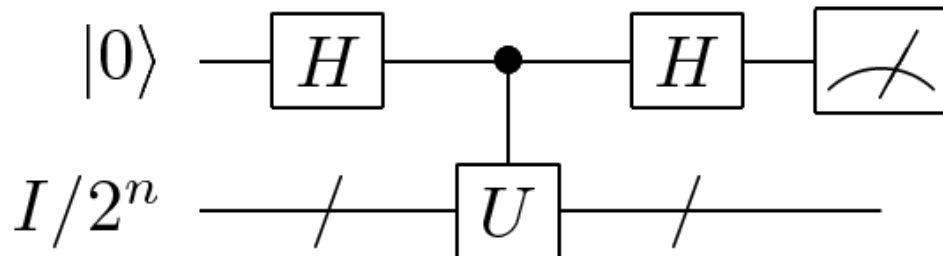
- apparently yields exponential speedups over classical computation

Trace Estimation

- One clean qubit computers can efficiently estimate the normalized trace of a quantum circuit to polynomial accuracy



$$p_0 = \frac{1}{2} + \frac{\text{Re}(\langle\psi|U|\psi\rangle)}{2}$$



$$p_0 = \frac{1}{2} + \frac{\text{Re}(\text{Tr}U)}{2^{n+1}}$$

- Estimating the Jones polynomial is a “complete” problem for one clean qubit computers
 - one clean qubit computer can efficiently solve this problem
 - by solving this problem we can simulate a one clean qubit computer

[Shor, Jordan. Quant. Inf. Comp. (8):8/9, 681 (2008)]

- one clean qubit computers can also efficiently estimate HOMFLY polynomials

[Jordan, Wocjan. Quant. Inf. Comp. (9):3/4, 264 (2009)]

Essence of Proof

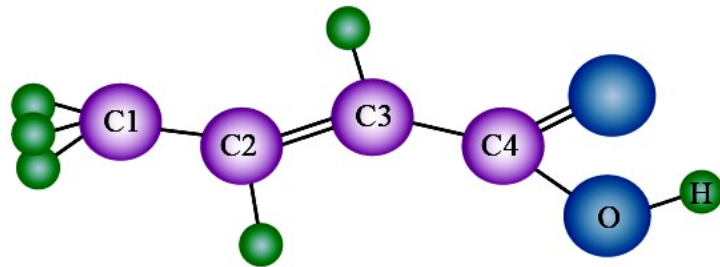
- correspondence between braids and circuits



- goes both ways:
 - braids \rightarrow circuits (yields algorithm)
 - circuits \rightarrow braids (proves hardness)

Experiments!

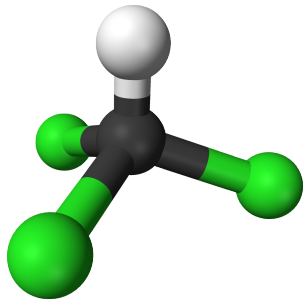
- four qubits, four strands



trans-crotonic acid

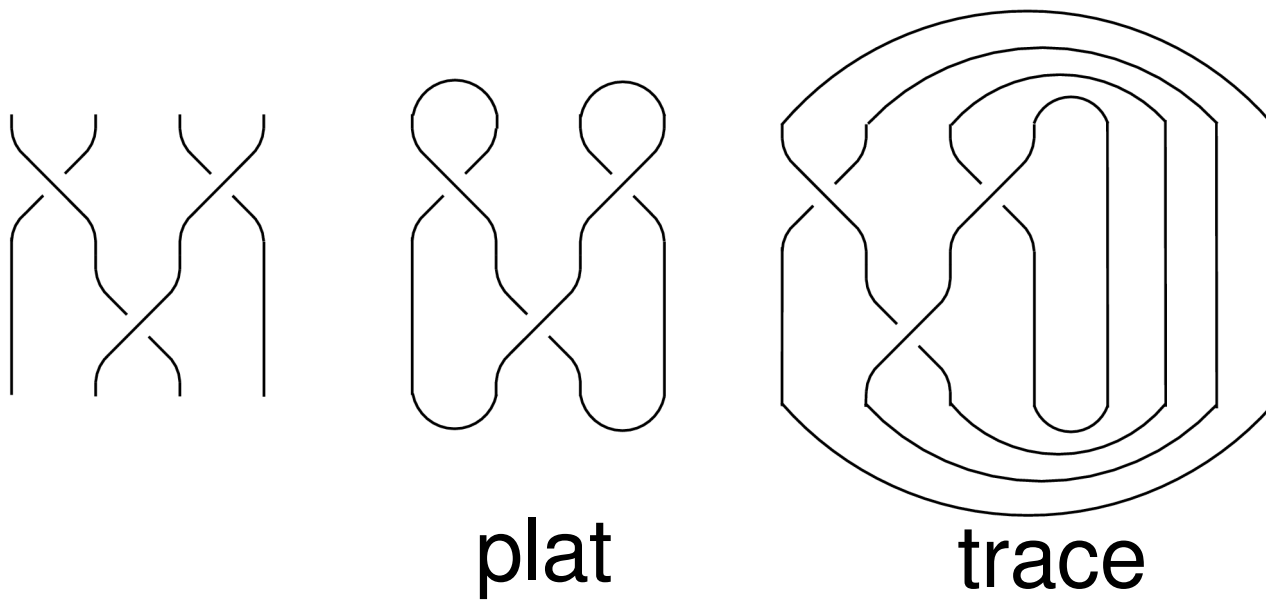
[Passante et al. PRL 103, 250501 (2009)]

- two qubits, three strands



chloroform

[Marx et al. arXiv:0909.1080 (2009)]



- **trace** closure: DQC1-complete

[Shor, Jordan. Quant. Inf. Comp. (8):8/9, 681 (2008)]

[Jordan, Wocjan. Quant. Inf. Comp. (9):3/4, 264 (2009)]

- **plat** closure: BQP-complete

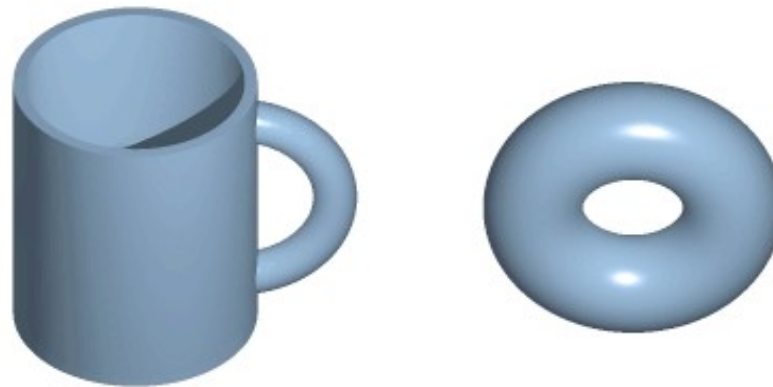
[Freedman, Kitaev, Wang. Comm. Math. Phys (227):681 (2002)]

[Freedman, Larsen, Wang, . Comm. Math. Phys (227):605 (2002)]

[Aharonov, Jones, Landau. STOC '06 pg. 427]

Quantum algorithms for Manifold Invariants

- n -manifold: topological space locally like \mathbb{R}^n
- Fundamental question: given two manifolds are they homeomorphic? (“the same”)

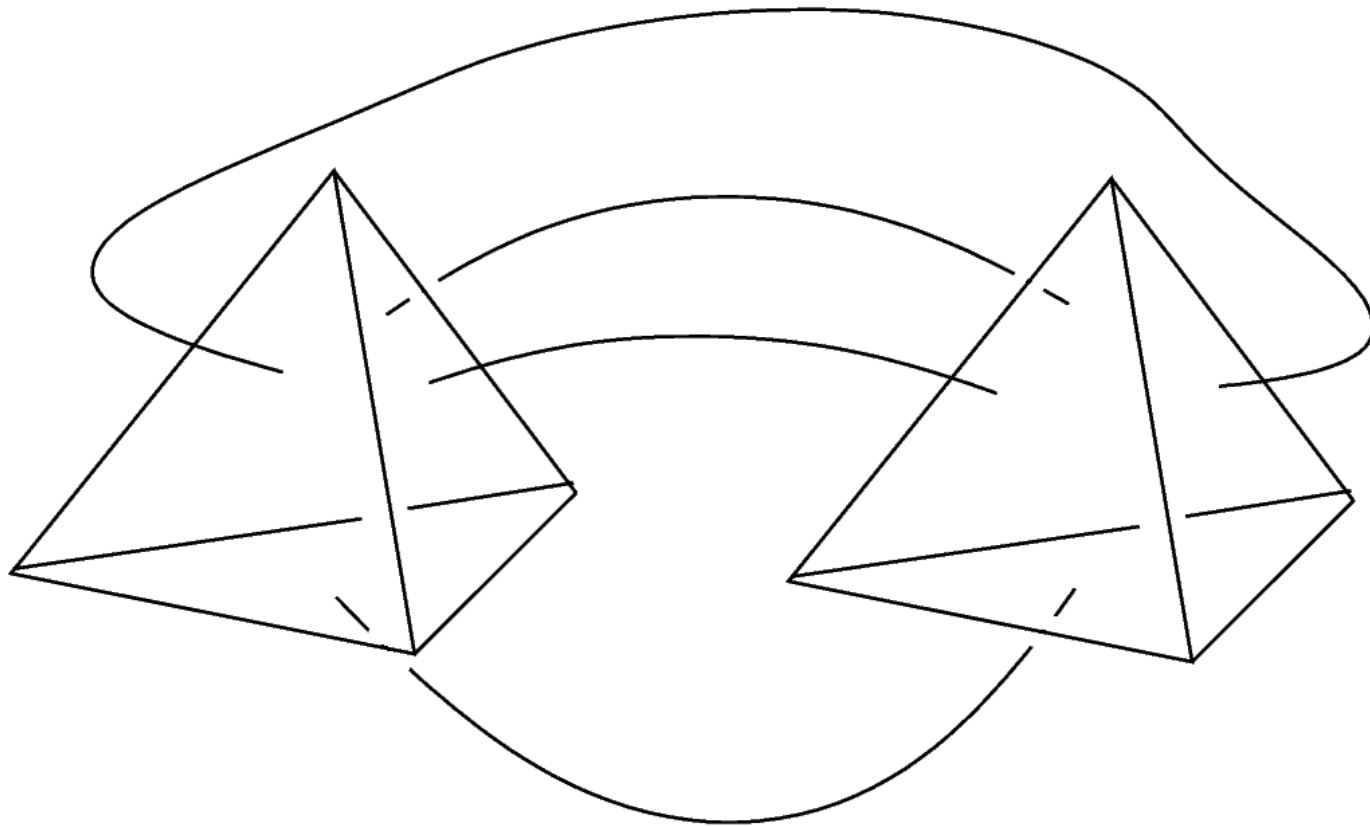


- partial solution:
manifold invariant – if manifolds A and B are homeomorphic then $f(A) = f(B)$

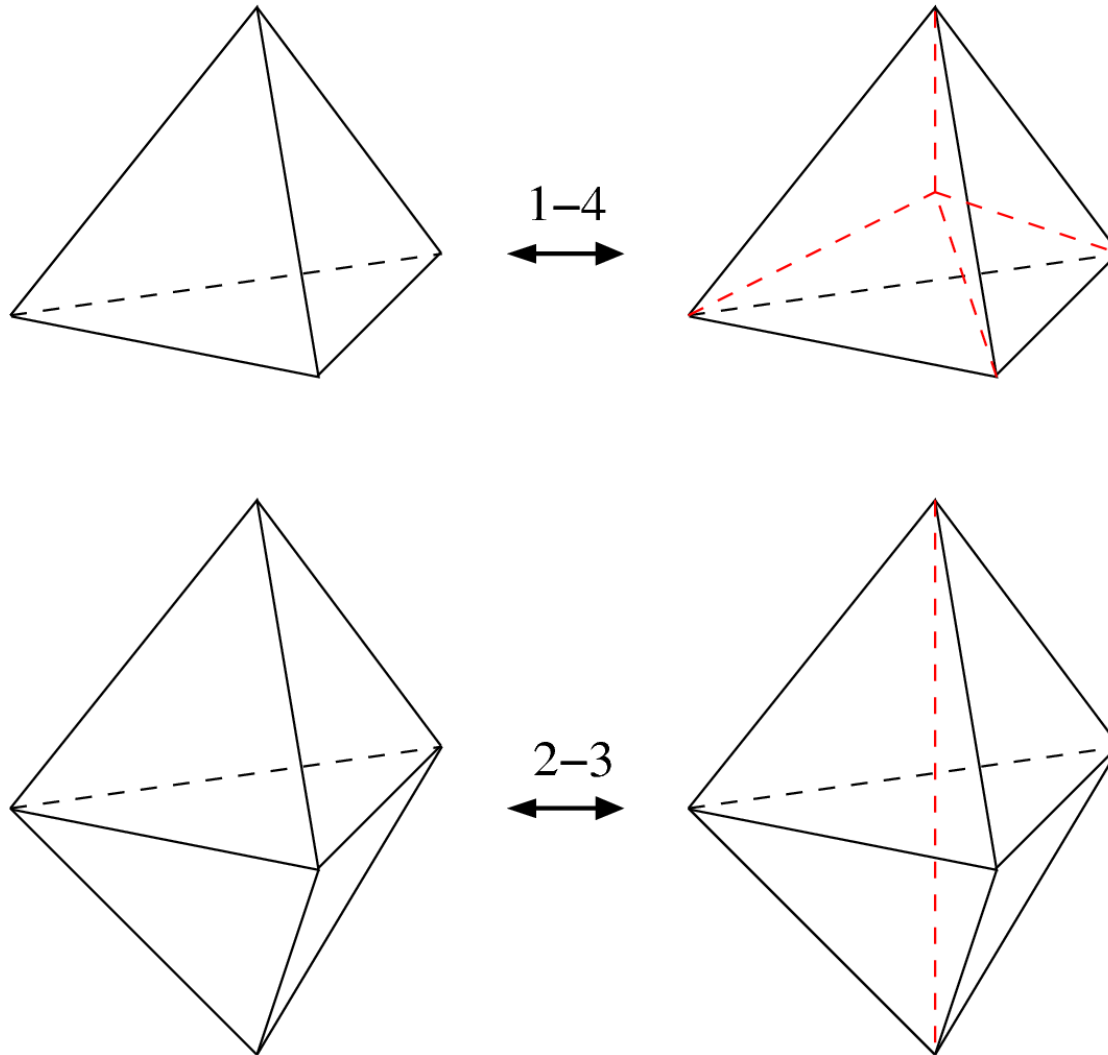
Higher Dimensions

| | | |
|-------------|------------------------------|-------------------------------|
| | equivalence | invariants |
| knots | computable, not efficient | Jones, HOMFLY |
| 2-manifolds | easy | Euler characteristic |
| 3-manifolds | computable, not efficient | Turaev-Viro, Ponzano-Regge |
| 4-manifolds | uncomputable | Donaldson |

- How do we describe a 3-manifold to a computer?
- one way is to use a **triangulation**:
 - a set of tetrahedra
 - a gluing of the faces



- manifolds equivalent iff connected by a finite sequence of Pachner moves



- sequence could be long!

Turaev-Viro invariant arises in a “spin-foam” model of quantum gravity



Every physical system can be efficiently simulated by a standard quantum computer.

We should be able to implement this process with an efficient quantum circuit.

Quantum Algorithms

- Turaev-Viro invariant
 - efficiently computable on quantum computer
 - BQP-hard: simulating a quantum computer reduces to estimating Turaev-Viro invariant

[G. Alagic, S. Jordan, R. Koenig, B. Reichardt, to appear]

- Ponzano-Regge invariant
 - efficiently computable on permutational computer

[S. Jordan, arXiv:0906.2508 (QIC, to appear)]

TV invariant is BQP-hard

- what does that mean?
 - given any quantum circuit we can construct a corresponding 3-manifold such that its TV invariant is $\simeq 1$ if circuit outputs TRUE and is $\simeq 0$ if FALSE
 - the problem of approximating the TV invariant is at least as hard as integer factorization
 - quantum algorithm for approximating TV invariant is nontrivial and cannot be duplicated classically (unless BQP = P)

Permutational Quantum Computation

- 1) prepare state spin-1/2 particles with definite total angular momenta
- 2) permute them around
- 3) measure total angular momentum of various subsets

sounds weak...but it evaluates Ponzano-Regge!

Permutational Quantum Computation

- can also compute irreps of S_n
- analogous to anyonic quantum computation
 - shares some of the favorable fault tolerances
 - but doesn't require any exotic anyons!
- possibly weaker than standard Q.C. but unlikely to be classically simulatable

[S. Jordan, arXiv:0906.2508 (QIC, to appear)]

A Moral of Our Story

- simulating physical systems by quantum computer
 - leads to other quantum algorithms
 - is useful as an end in itself
 - addresses a fundamental question: how computationally powerful is our universe

Summary

- from quantum simulation of TQFTs and spin foams we obtain quantum algorithms for
 - knot invariants (Jones, HOMFLY)
 - [Freedman, Larsen, Wang, Comm. Math. Phys (227):605 (2002)]
 - [Shor, Jordan. Quant. Inf. Comp. (8):8/9, 681 (2008)]
 - [Jordan, Wocjan. Quant. Inf. Comp. (9):3/4, 264 (2009)]
 - 3-manifold invariants(Turaev-Viro, Ponzano-Regge)
 - [Jordan, arXiv:0906.2508 (Quant. Inf. Comp., to appear)]
 - [Alagic, Jordan, Koenig, Reichardt, to appear]
 - many of these run on modest hardware

Outlook

- many quantum systems remain to be simulated
 - QFT (Current work with Preskill, Lee, and Shaw)
 - 3+1 dimensional spin foam models
 - three-manifold invariants with one clean qubit?