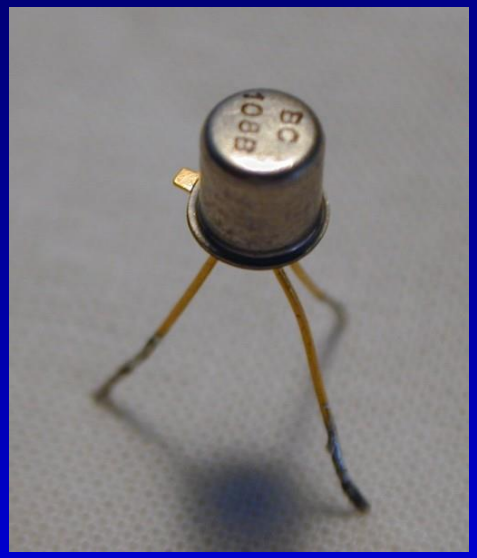
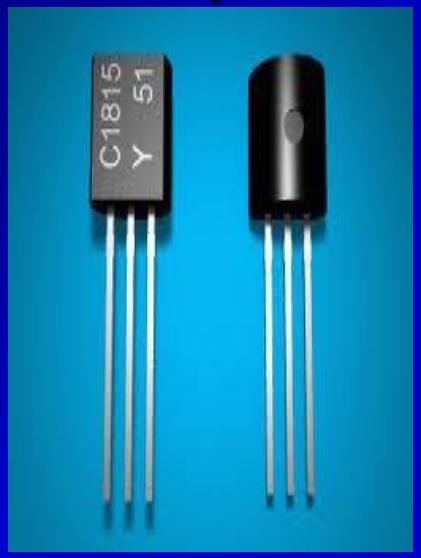
# Quantum Computing:

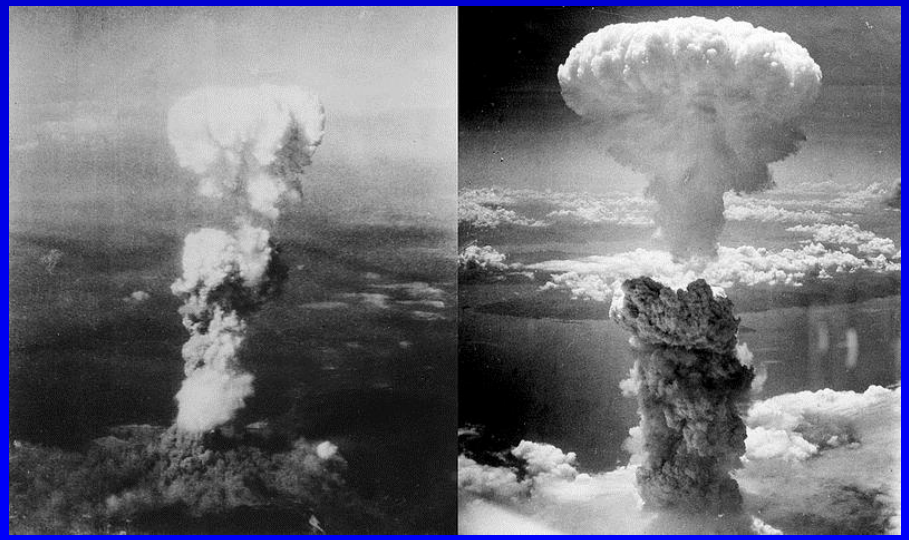
## The 2nd quantum revolution from a Computer Scientists view

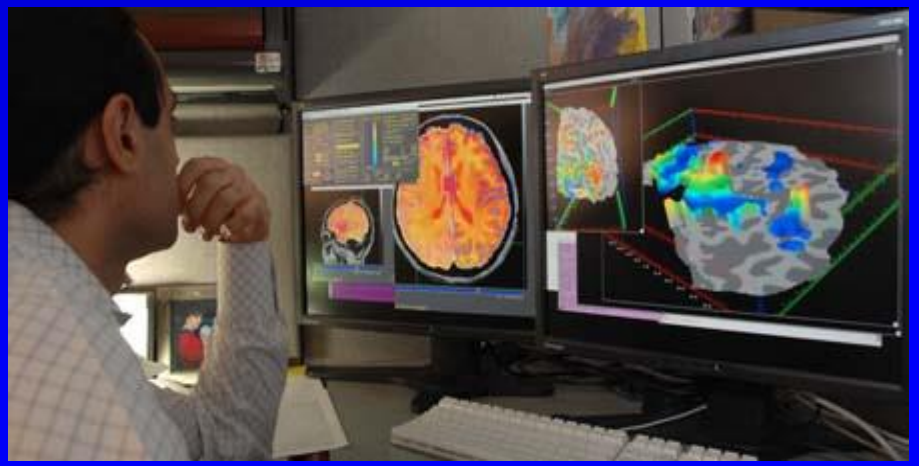

Dorit Aharonov,
The Hebrew University

# The 1st Quantum Revolution (Early 19th century)





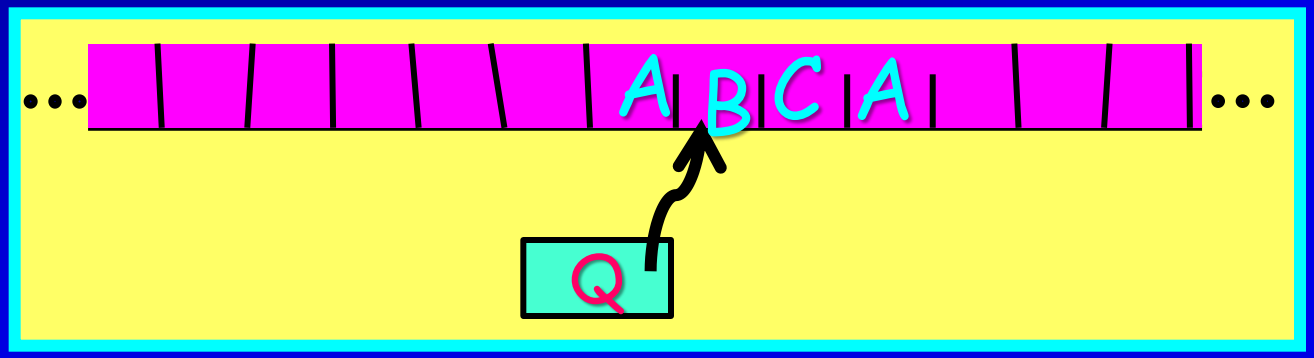
# What is a computation?

Input
0111001

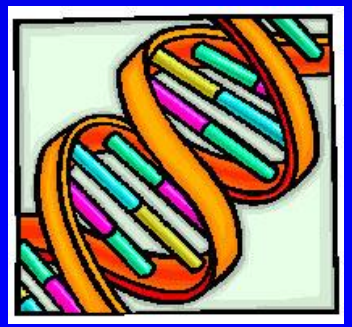
→ Computation (Algorithm) →

Output
011000

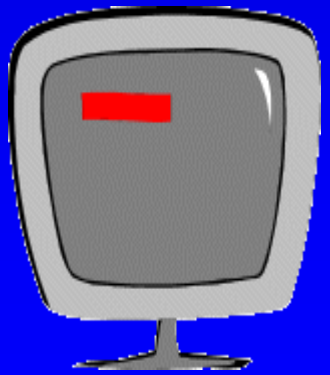
Universal computation model:



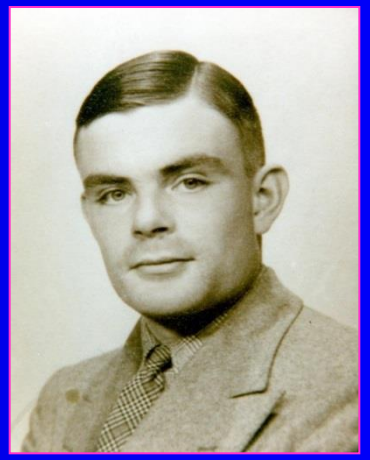

Turing machine, 1936



≈

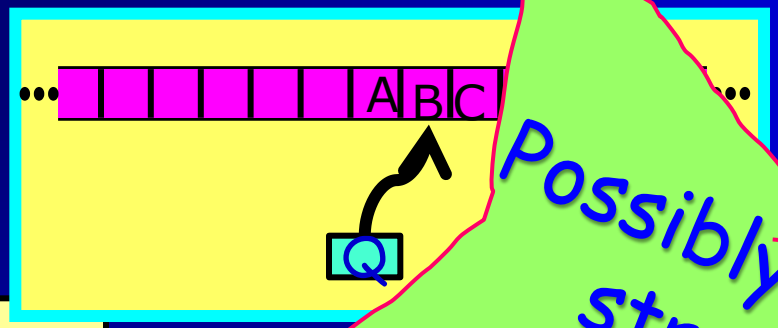


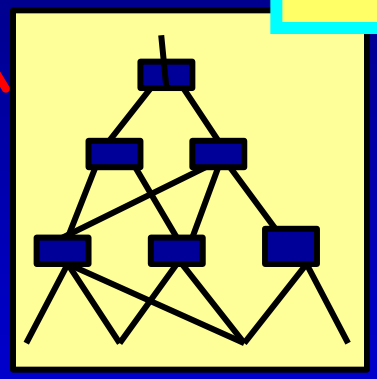
≈



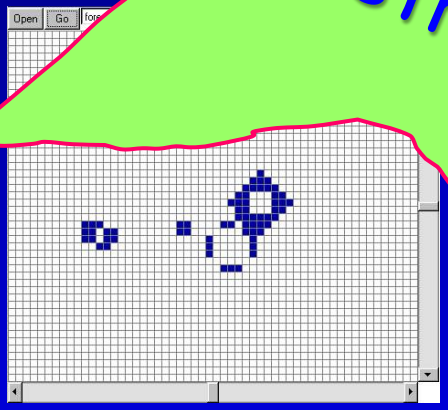
Alan Turing
1912-1954

# The Extended Church Turing Thesis

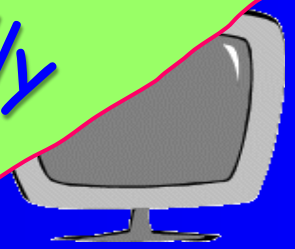


≈



Possibly exponentially stronger model



Extended Church Turing Thesis: "All phy[illegible] reasonable (classical) computational models can be si[illegible]lated with polynomial overhead by a Turing machine"

Quantum computation - only model that credibly challenges the Extended Church Turing Thesis.

# One Quantum Bit (a qubit)

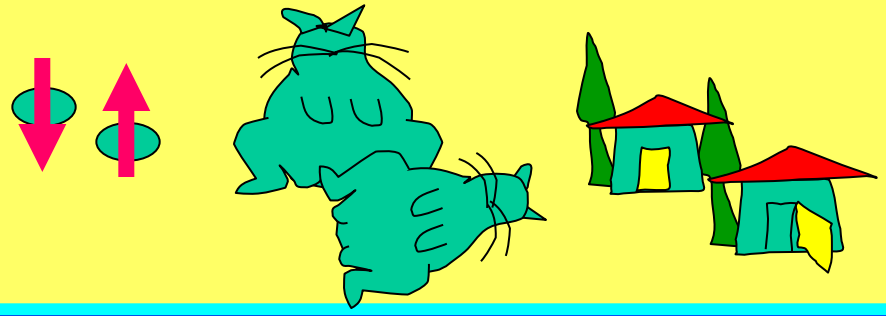
When we say a qubit we mean $C^2$

The state of one qubit is a unit vector:

$$a|0\rangle + b|1\rangle \in C^2$$

Superposition principle

A quantum system can be in a Superposition of its possible "classical" states 0,1



Measurement principle

A measurement is a probabilistic process:

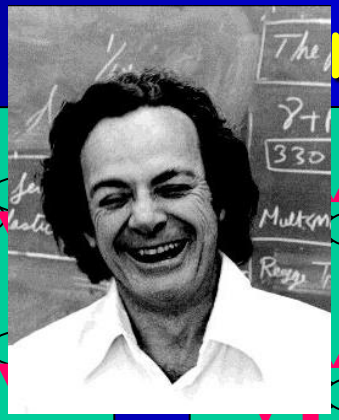
1. Classical outcome
2. The state is projected onto one basis state (collapse)

$$a|0\rangle + b|1\rangle$$

$$|0\rangle \quad |a|^2 \quad |b|^2 \quad |1\rangle$$

# n Quantum Bits (Qubits)

one two three





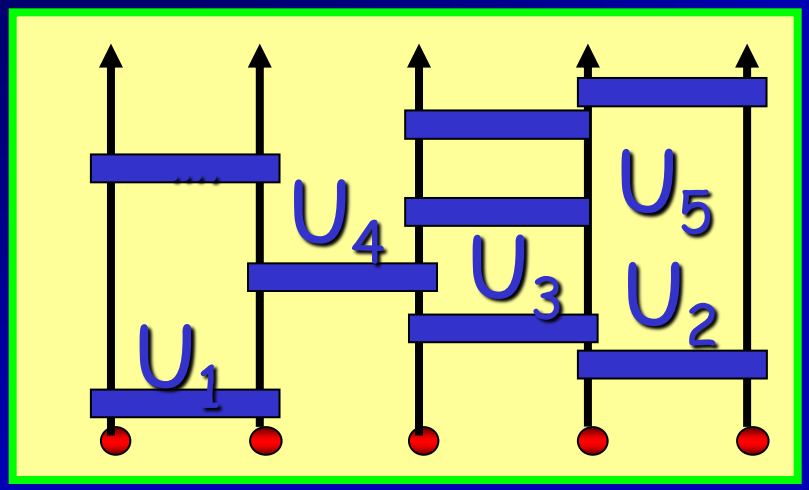
**Manin** [80], **Benoiff** [81], **Feynman** [82]:
**Exponential dimension → Quantum computer?**

$$|\psi\rangle = \sum_{i_j \in \{0,1\}} a_i \, | i_1, i_2, \ldots, i_n \rangle$$

The state of n classical bit – described by n bits…
The state of n Quantum bits – by $2^n$ coefficients!

Linear(n) Exponential($2^n$)

# Quantum Computation




Input: $|\psi(0)\rangle = |0,1,1,\ldots,1,0\rangle$

Dynamics: $i\hbar \frac{d\psi}{dt} = H\psi$

$|\psi(t)\rangle = U\,|\psi(0)\rangle \quad U\,U^{T} = I$

Measurement → output

## NOT

$|0\rangle \rightarrow |1\rangle \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$|1\rangle \rightarrow |0\rangle$

## CNOT

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

## Hadamard

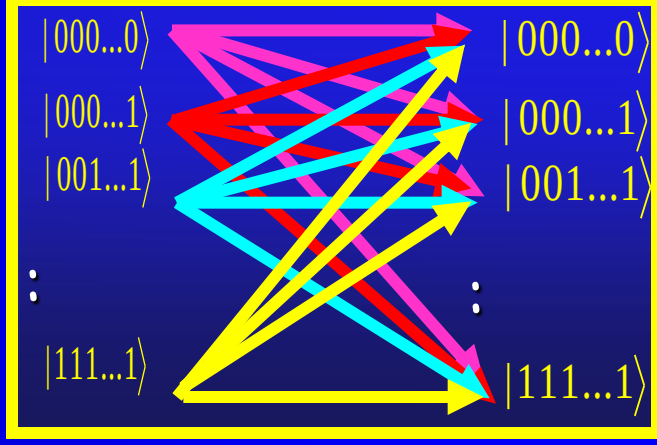
$|0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$

$|1\rangle \rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Hadamard + classical gates
are quantum universal
Complexity measure: number of gates.

# Interference




Hadamard

$$|0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

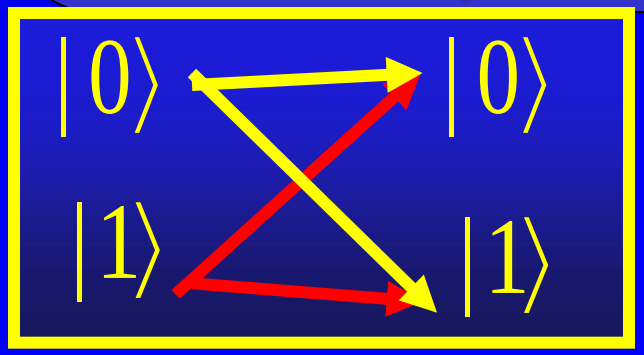
$$|1\rangle \rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

*Ex:*

$$\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H}$$

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

Destructive and Constructive Interference




Weights on arrows can be negative!

# Exponential algorithmic speedups

Break RSA!

Shor

Factoring ['94]

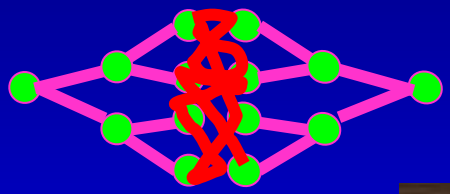
N=PQ

N

P Q

UNITGROUP

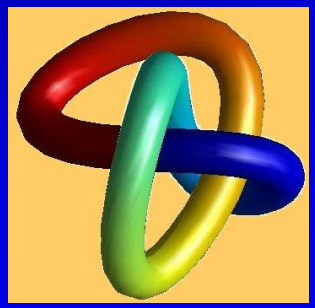
EHKS'14



Graph reachability [CCDFGS'02]

$x^2 - dy^2 = 1$

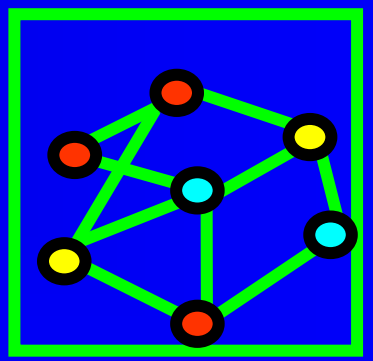
Pell's equation [Hallgren'02]



Approximate Jones Polynomial [AJL'05]

$$\begin{pmatrix} a & b & c \\ d & e & f \\ h & i & j \end{pmatrix}$$

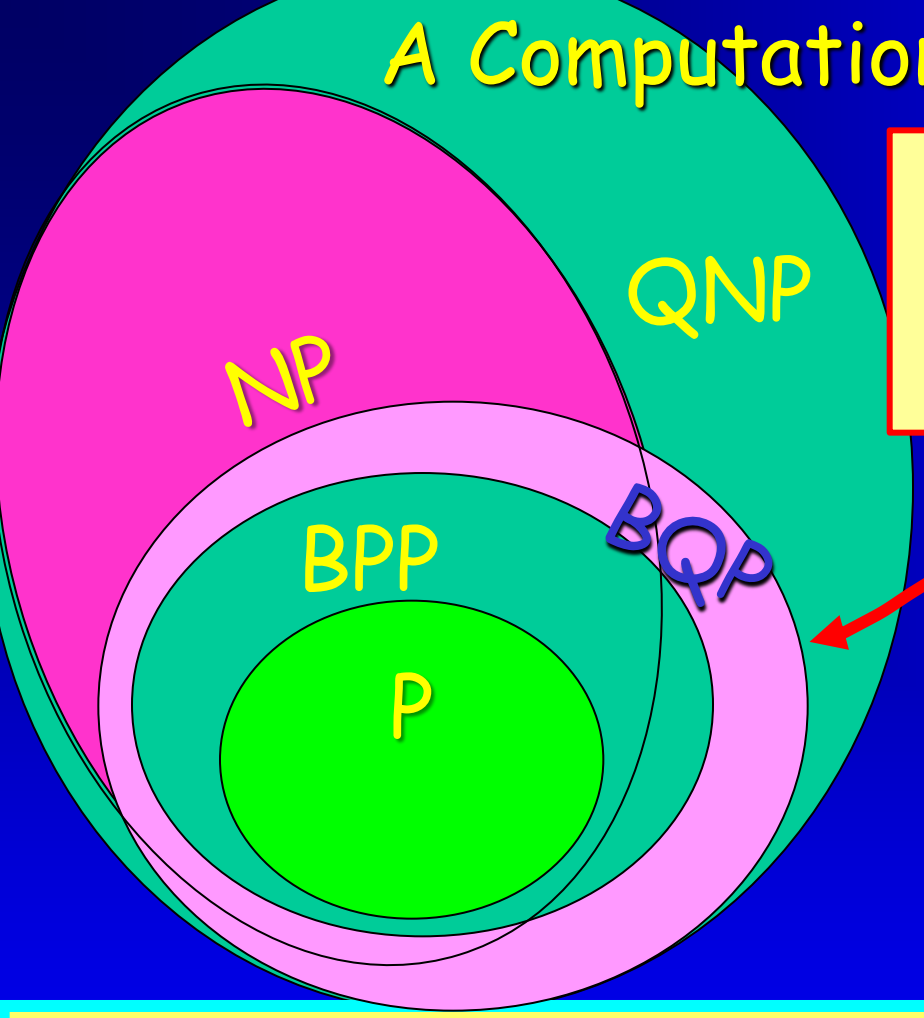
Linear Equations [HHL'08 ....]



Simulating Quantum systems [L'96, JLP'11]

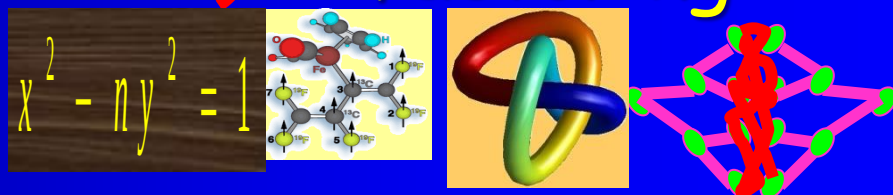
Quantum computation seems to provide <u>exponential</u> algorithmic speed-ups !

# A Computational complexity map




**BQP**: Class of problems solvable in polynomial time by **quantum** computers
**BPP**: Class of problems solvable in polynomial time by **classical** computers

factoring




All physically realizable computational models can be simulated in poly time by a Turing machine" (Extended CTT)

Widely believed:
**QC violates ECTT**
BQP is strictly larger than BPP,
Quantum Systems can in principle physically implement BQP

# Entanglement

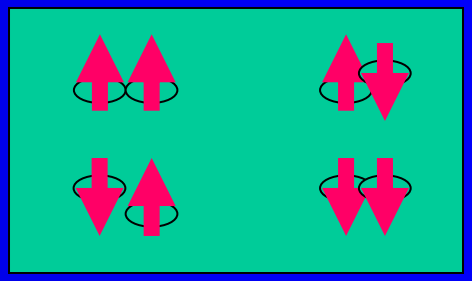
$$|\psi\rangle = \sum_{i_j \in \{0,1\}} a_i \, |i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle \equiv \sum_{i_j \in \{0,1\}} a_i \, |i_1, i_2, \ldots, i_n\rangle$$

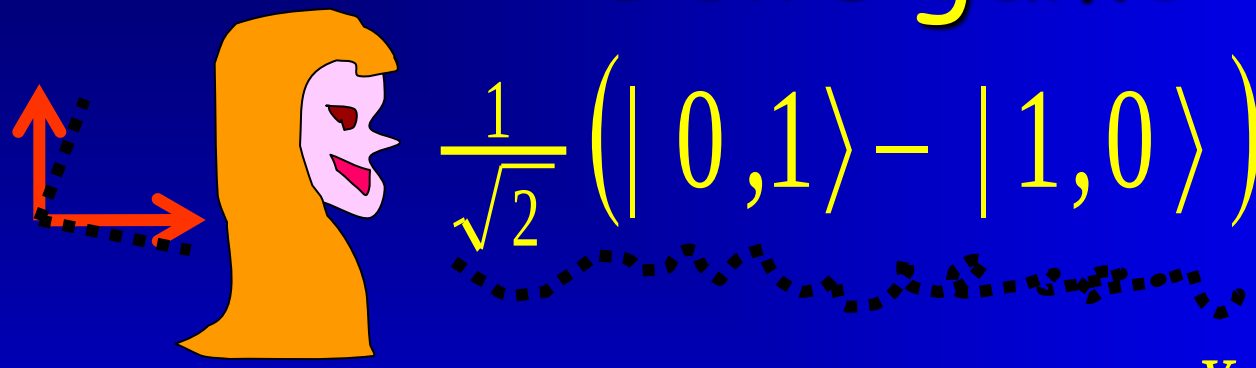
$$\overbrace{C^2 \otimes C^2 \otimes \ldots \otimes C^2}^{n} \qquad \sum_i |a_i|^2 = 1$$

n quantum bits – require $2^n$ complex numbers.

Multiparticle Entanglement

# Type 1: Bell's game






$X_A \in \{0,1\}$ $X_B \in \{0,1\}$

$a$ b

They win if:

$$X_A, X_B \in \{(0,0), (0,1), (1,0)\} : a = b$$
$$X_A, X_B \in \{(1,1)\} : a \neq b$$

$a_0 + b_0 = 1$

$a_0 + b_1 = 1$

$a_1 + b_0 = 1$

$a_1 + b_1 = 0$

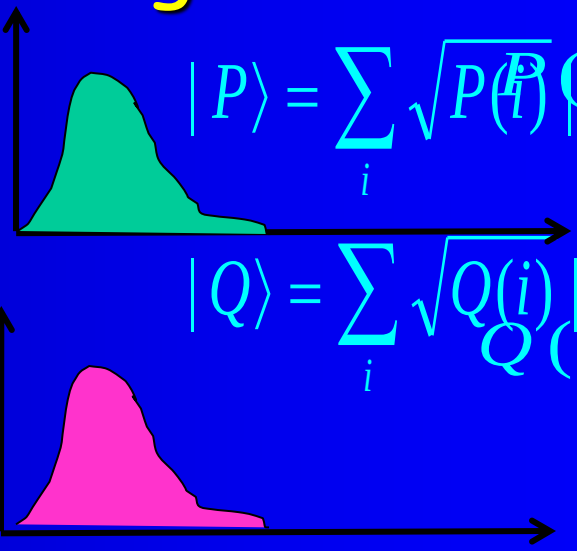
!0.85 < Pr(success) with EPR

$\Pr(\text{Win}) = 0.75$

# Type II: Two Registers entanglement

Two distributions over n bit strings.
Are they equal or their supports do not intersect?
need exp(n) many samples.

$$\langle P \mid Q \rangle = 1 \quad \text{or} \quad 0 \; ?$$




$$\frac{1}{\sqrt{2}}|0\rangle\otimes|P\rangle + \frac{1}{\sqrt{2}}|1\rangle\otimes|Q\rangle \xrightarrow{H}$$

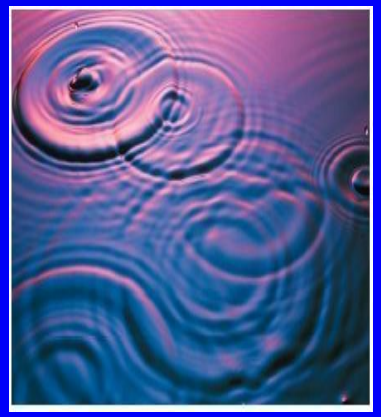
$$\frac{1}{2}|0\rangle\otimes|P\rangle + \frac{1}{2}|1\rangle\otimes|P\rangle + \frac{1}{2}|0\rangle\otimes|Q\rangle - \frac{1}{2}|1\rangle\otimes|Q\rangle$$

$$|0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

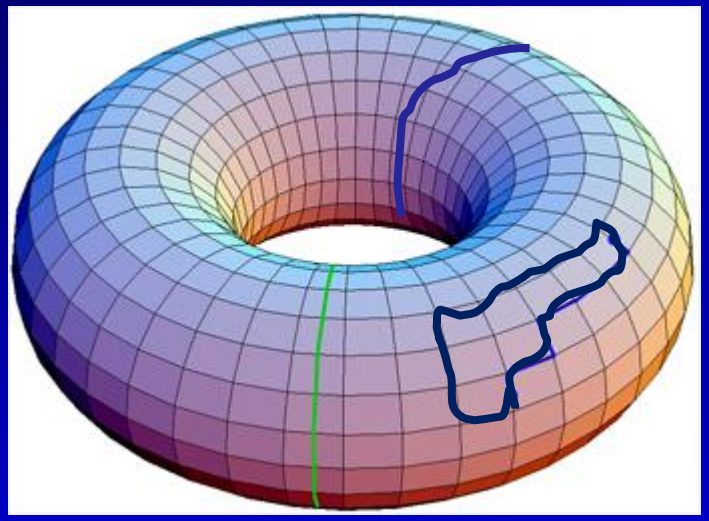
$$|1\rangle \rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

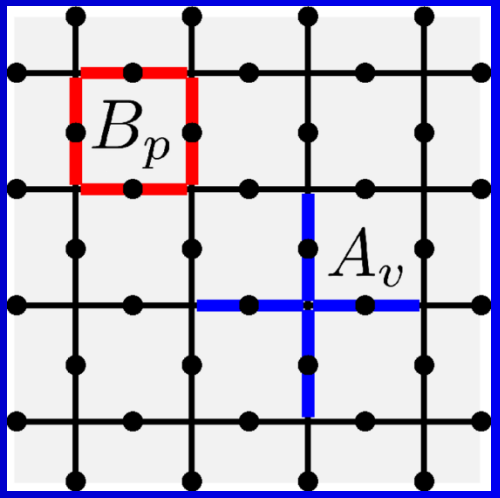
$$\text{Prob}(0) = \frac{1+\langle P|Q\rangle}{2}$$

Can estimate <P|Q> efficiently
(by measuring the left qubit)



# Type III: Quantum error correcting codes






$$H = -\sum_P B_P - \sum_V A_V$$

A=ZZZZ
B=XXXX

# The 2nd quantum revolution: Concepts from CS


Complexity

Universality

Hardness

Reductions

Approximation

Robustness

Error correction

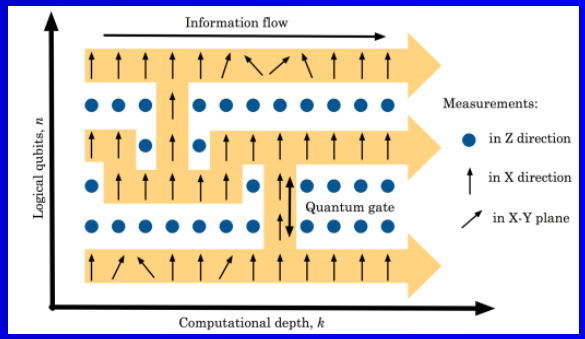
Interaction

Computational lens on Physics

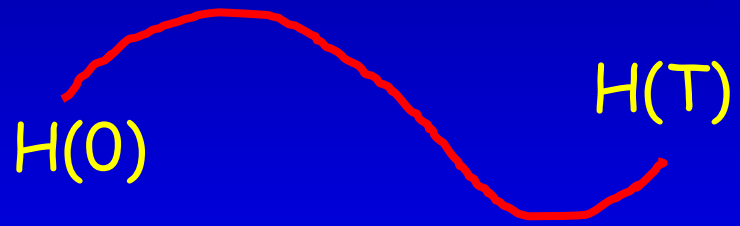
# Complexity, Universality

# Universal quantum models

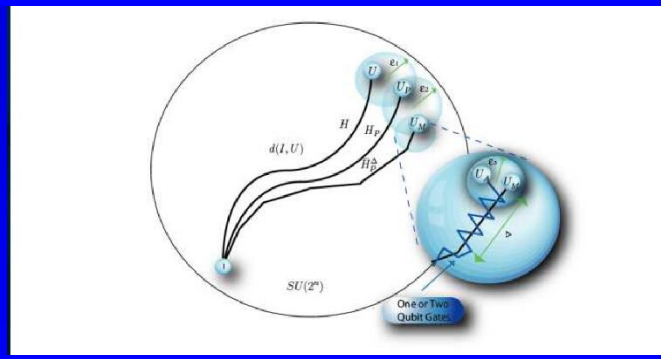
TQFT:
KitaevFreedmanWang'02,
KitaevLarsenWang'02

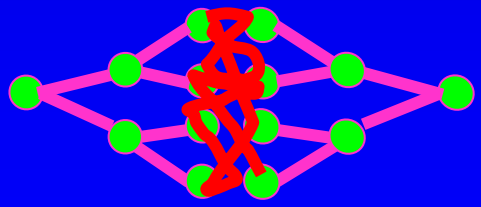



Measurement based quantum computation:
RaussendorfBrowneBriegel'03




Adiabatic:
FarhiGoldstoneGutmann'00
AharonovKempeLandauLloydRegevVanDam'04



Quantum Walks: Childs'08

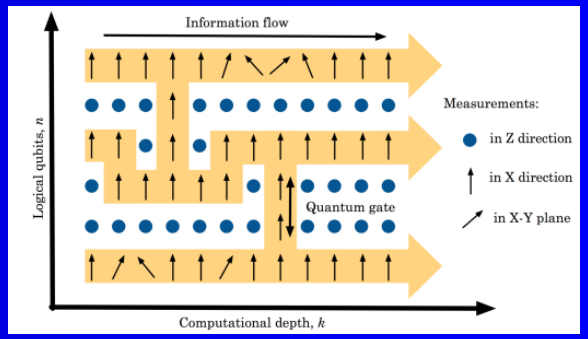
Riemannian Geometry:
NielsenDowlingGuDoherty'06

# Reduction

# Universal quantum models = efficient reductions

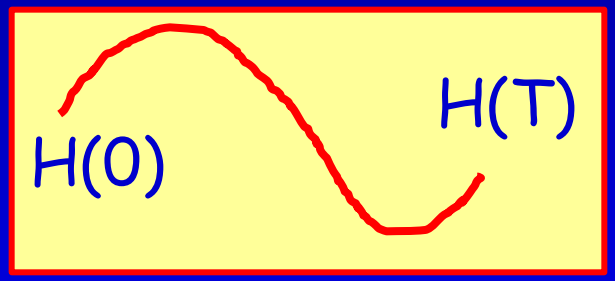
TQFT

BQP

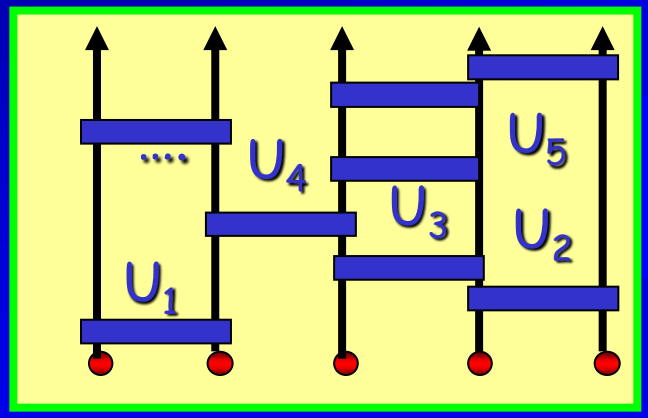


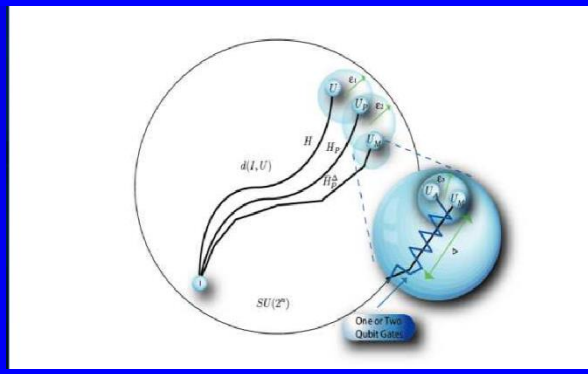

The quantum circuit model

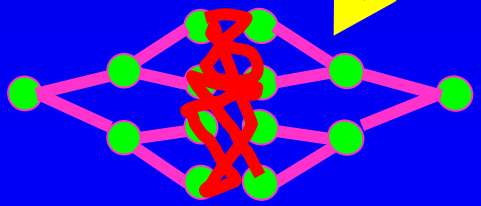
Measurement based quantum computation




Adiabatic



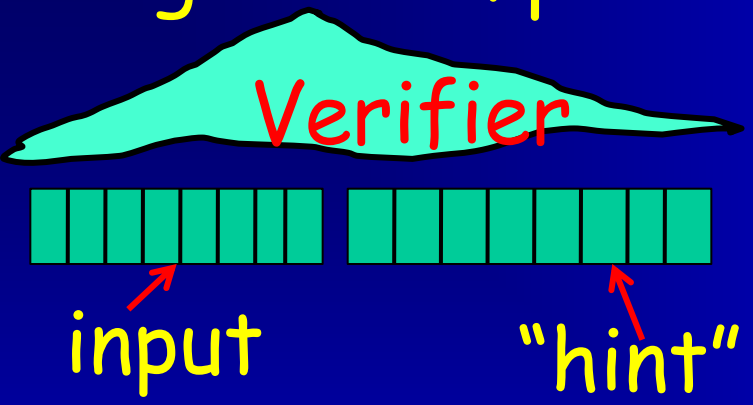



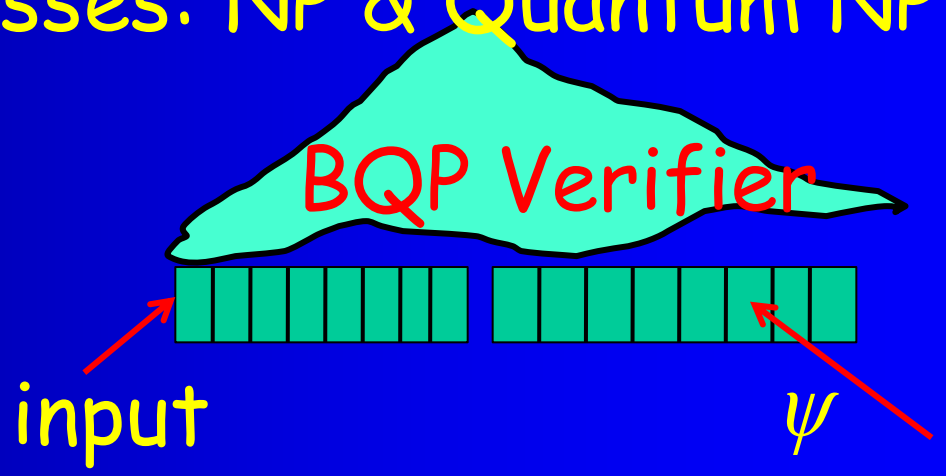



Quantum Walks

Riemannian Geometry

# Higher Complexity classes: NP & Quantum NP




## 3-SAT

$$(x_1 \cup \bar{x}_3 \cup x_7) \cap (\bar{x}_4 \cup x_3 \cup \bar{x}_{12})$$

Is the input formula satisfiable?

Given:
Local Hamiltonian H on n qubits ,
a,b s.t. b-a>1/poly(n)
Objective:
Is min. eigenvalue of H <a or >b

$$H = \sum_{j=1}^{m} H_j$$

## Cook-Levin'71:

3-sat is NP complete:
Any problem in NP can be reduced to it.

Quantum Cook-Levin [Kitaev'98]

# Quantum Hamiltonian complexity

Classical CSPs

CSP is a special case!

Local Hamiltonians

Multiparticle Entanglement

Major CS problem:
Constraint Satisfaction Problem (CSP)

$$(x_1 \cup \overline{x_3} \cup x_7) \cap (x_4 \cup \overline{x_3} \cup x_{12}) \cap \ldots$$

Major CMP problem:
The Local Hamiltonian Problem:

$$H = \sum_{j=1}^{m} H_j$$

Given: CSP formula
Objectives: Min. # of Violations
Optimal assignment
Approximations

Given: Local Hamiltonian
Objective: Ground energy

A roadmap for Hamiltonians

# Reductions for Quantum simulations?

Simulating Physics with computers
[Feynman'1982]

Simulating with noisy systems
[CiracZoller'12]

# Robustness

# Robustness in quantum computation

Controlled robustness:

Quantum Error correcting codes [Shor'95,Steane'95]

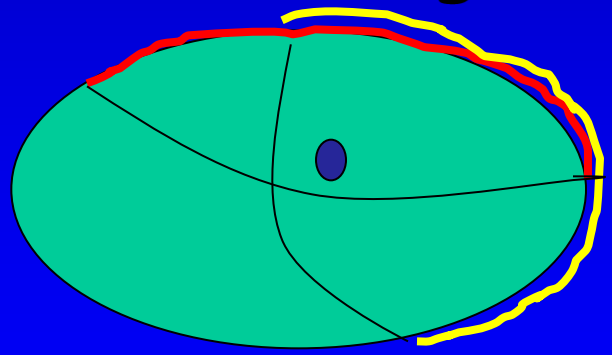
Fault tolerant quantum computation

[AharonovBenOr'96,Kitaev'96,KnillLafflammeZurek'96]

Is the noise local?

Quantum Error correction for sensing

Quantum gravity & AdS/CFT



CFT as a Quantum code subspace

[AlmheiriDongHarlow'14]

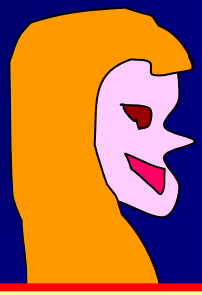

Quantum simulations of noisy systems

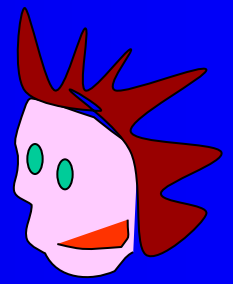
Understanding the complexity of rubust systems

# Interaction

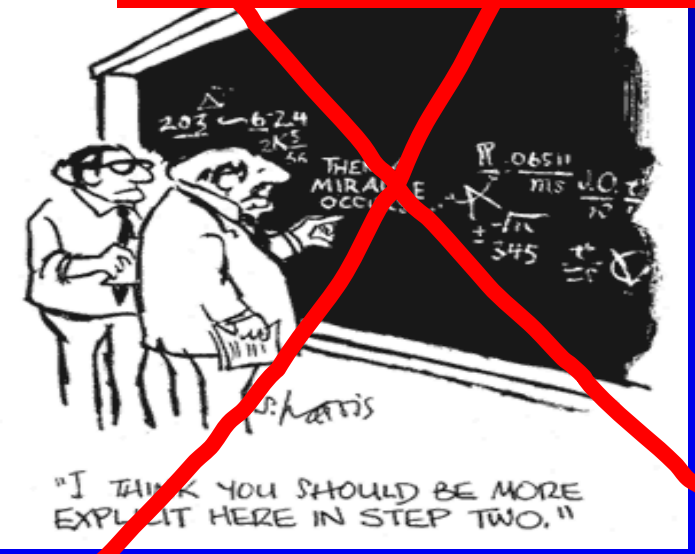
Inspired by GoldwasserMicaliRakoff'85
Motivated by conversations with Oded Goldreich and Madhu Sudan

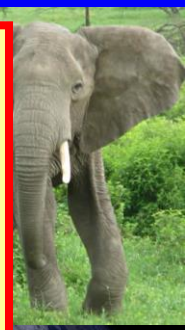
# A Physical Experiment
## Predict & compare paradigm





Cannot test the
"Quantum Universal" regime in
the usual "predict & compare" paradigm



A physical theory
Quantum Mechanics
F=ma

# Is Quantum Mechanics (QM) Falsifiable?


**Question 1**: Fundamental: Is QM Falsifiable?

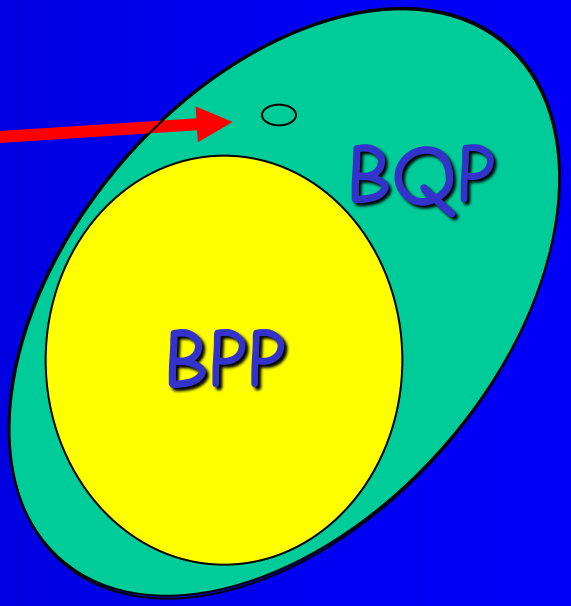
**Question 2**: Experimental: Can Experimentalists Test Their systems, claimed to be quantum computers?

**Question 3**: Cryptographic: How can we safely Delagate computations to an untrusted company claiming to have a Q comp.?

# Shor's Partial Answer [Vazirani'07]

Shor's algorithm : a recipe for an experiment to test QM outside of BPP
possible to check correctness efficiently

Factoring

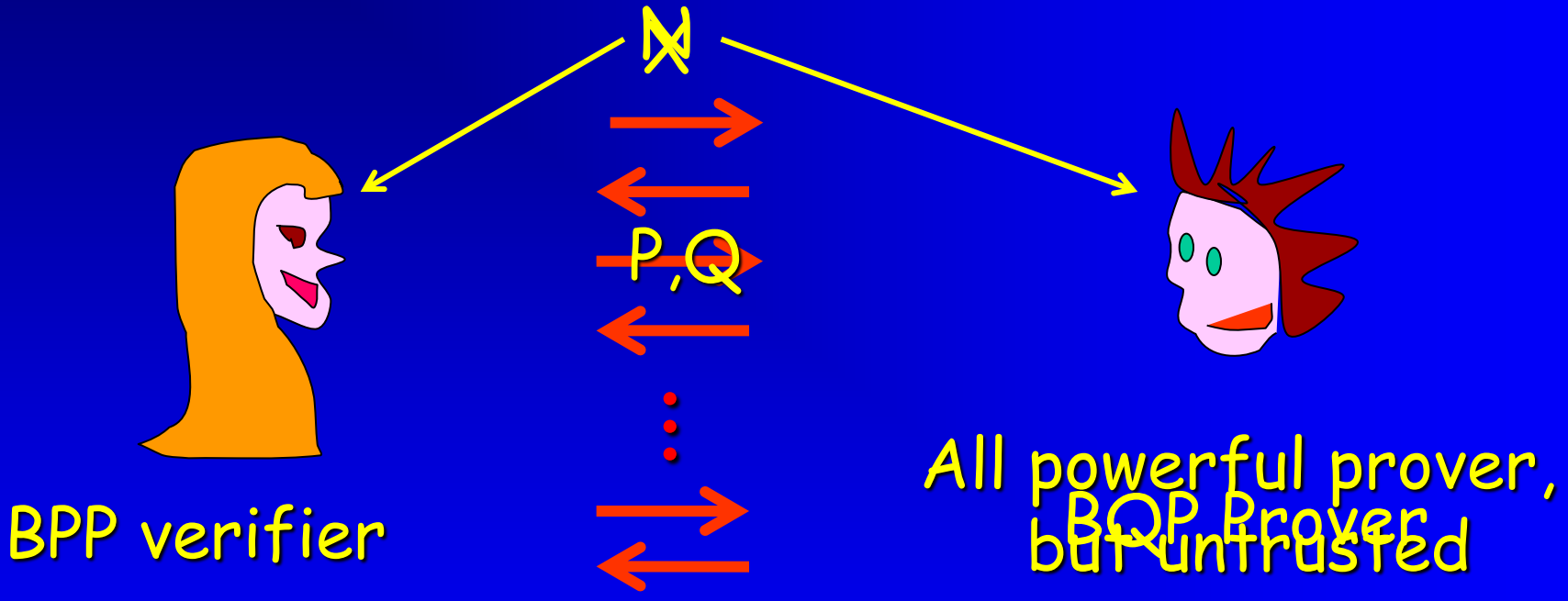



But Factoring does not suffice:

1. Factoring is probably not BQP universal .
2. What if I want to test a small system, with no ability to run Quantum error corrections?

Why did Shor's algorithm for factoring N=PQ succeed in getting arround the "usual type of experiments" pitfall?

# Interactive proofs [Goldwasser, Micali, Rackoff'85]



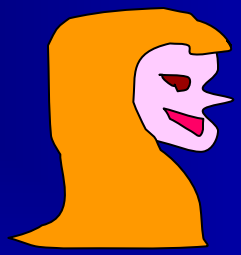

With interaction,
A computationally *weak* Verifier
Can get convinced of highly complex claims
Without knowing how to prove them!!!

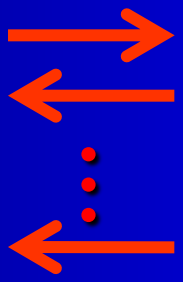
# The power of randomized interaction

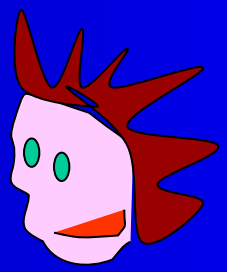
# Verifying quantum evolutions

[A'EbanBenOr'08, BroadbentKashefiFitzimons'09, Broadbent'15,A'BenOrMahadev'17]

Verifier: BPP
+ O(1) qubits





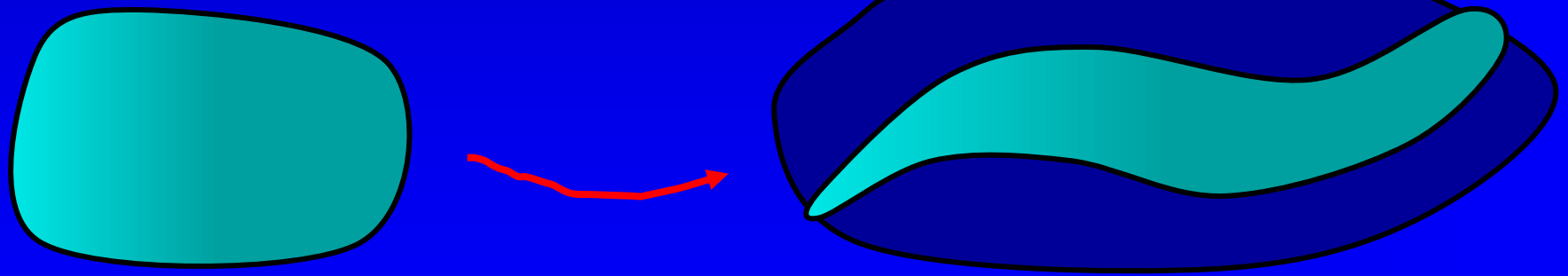


BQP Prover

**Theorem**: *A* BQP prover can prove *any* quantum circuit to a BPP+*O*(1) qubits verifier!

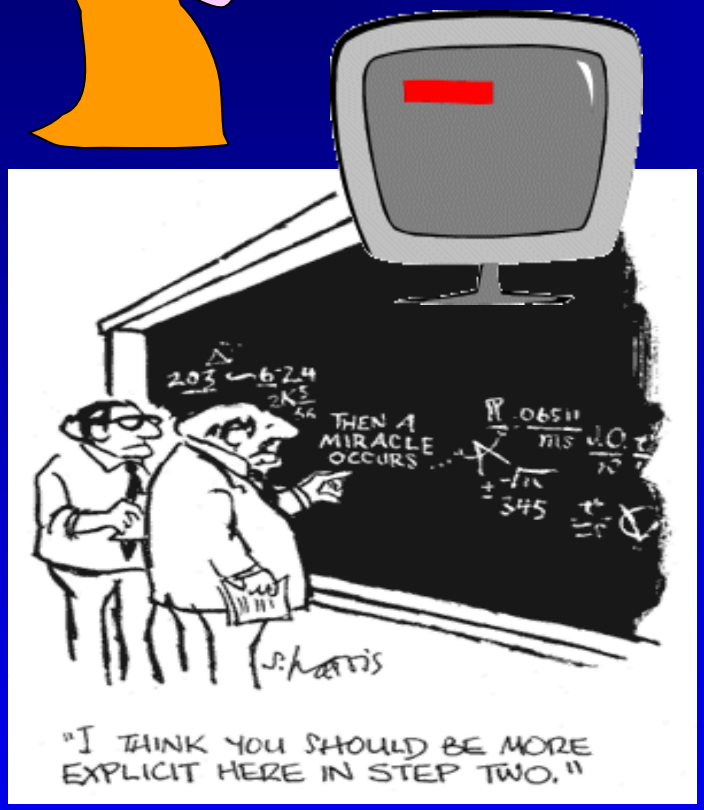
2 dim Hilbert space

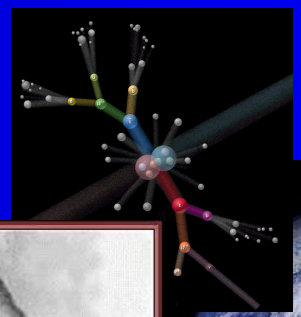
$2^{d+1}$ dim Hilbert space



Mahadev'18: verification by classical verifier

# Interactive Experiments With weak control



Could we more cleverly use interactions in experiments?
(e.g., to learn an unknown Hamiltonian)

# Main Challenges

## Quantum supremacy in NISQ devices

[BravyiGossetKoenig'18, Martinis group, BoulandFeffermanNirkheVazirani'18,IQC]

## Practical Quantum algorithms

HHL based linear algebra algorithms, Machine learning [KerenidisPrakash'17,Teng'18]

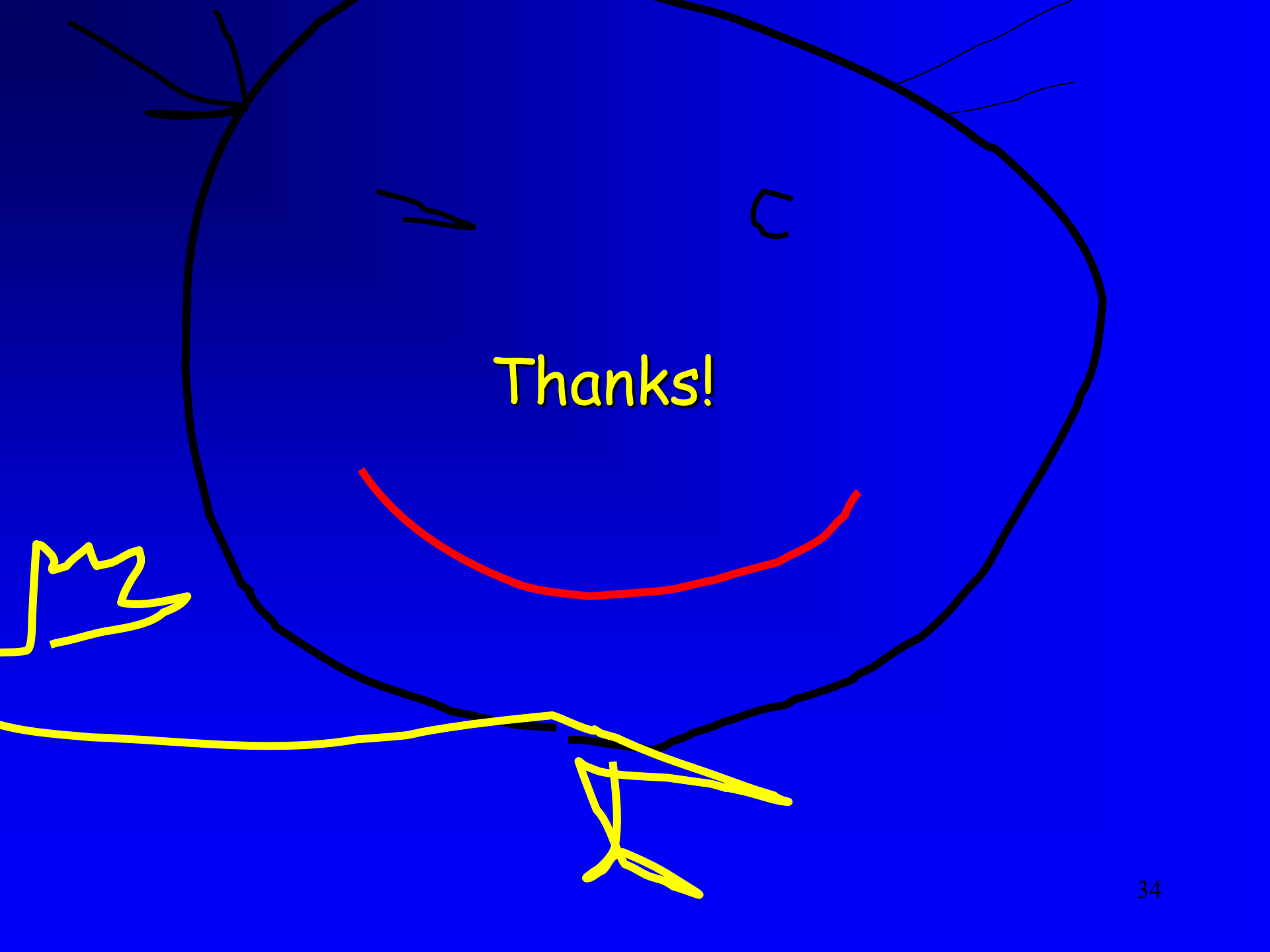
## Are noisy quantum devices useful?

Theory!

## Is the model of local noise correct?

How can we verify that!

## New Exponentially better Quantum algorithms!!


Thanks!

# Quantum Computation & Machine learning (CNT'D)

## Applied in:

K-means Clustering [LMR13]
Principal component analysis [LMR13]
Recommendation systems in poly(k)polylog(N) [KerenidisPrakash17]

## Many caveats

(see: "QML algorithms: Read the fine prints", Aaronson, Nature'15)

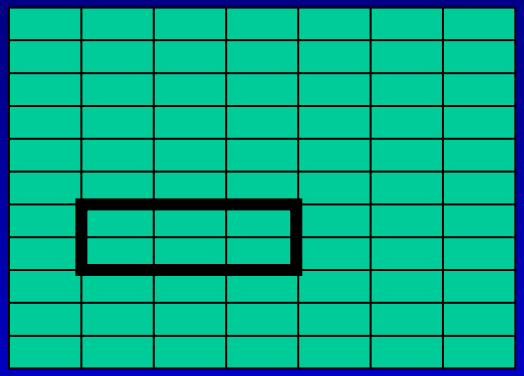
## Ewin Tang's breakthrough

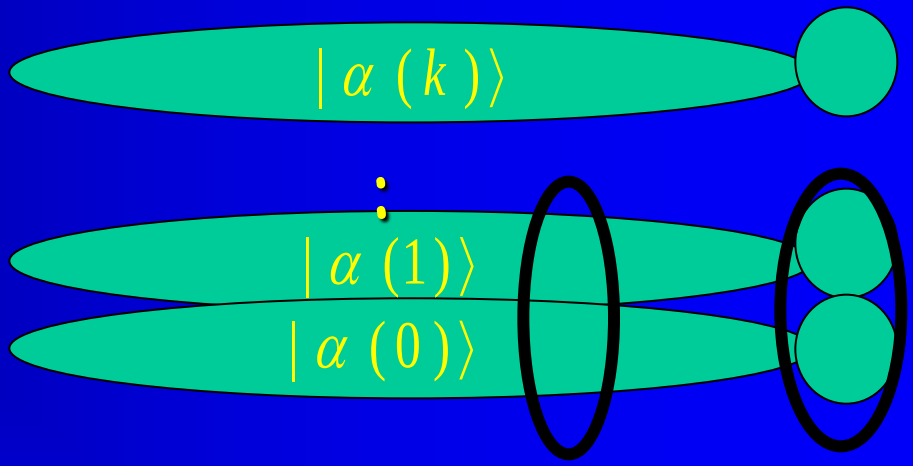
Quantum inspired classical poly(k)polylog(N) recommendation system [2018] (and follow up dequantizations)

Remains a big open question:
Find an Exponential quantum speed up for an interesting ML problem.

# Quantum Cook Levin

Theorem: Approx groundvalue of a local Hamiltonian is QNP complete [Kitaev98 (based on Feynman82)]




$$(x_1 \cup \bar{x}_3 \cup \bar{x}_7) \cap (x_4 \cup \bar{x}_3 \cup x_{12}) \cap \ldots$$

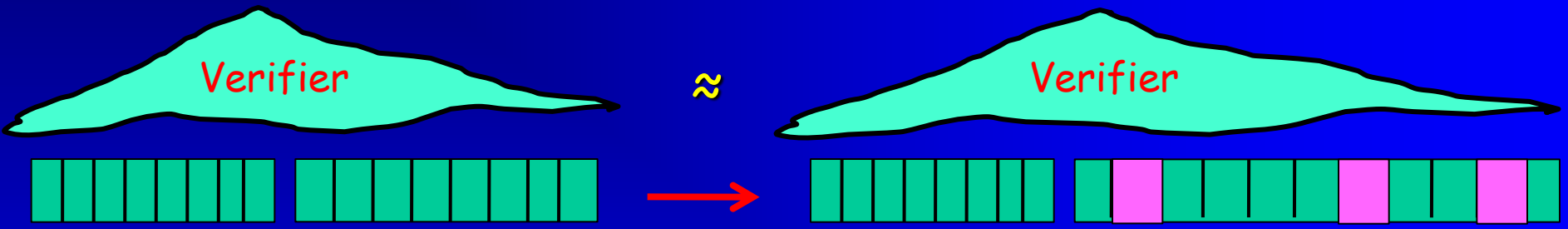
Computation is local

$$\frac{1}{\sqrt{2}}|0\rangle \otimes |P\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |Q\rangle$$

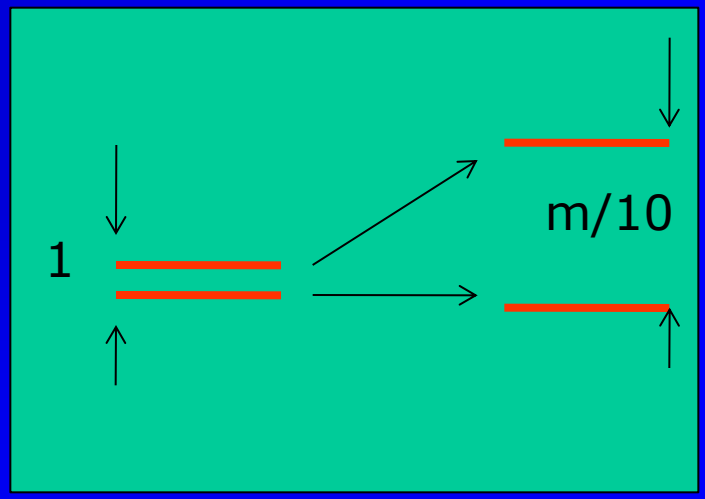
$$|history\rangle = \frac{1}{\sqrt{L+1}} \sum_{k=0}^{L} |\alpha(k)\rangle |k\rangle \quad \rightarrow \quad H = \sum_{j=1}^{m} \Pi_j$$

# The (classical) PCP theorem [AS'92,ALMSS'02]

PCP theorem (query version): Proofs have a slightly longer format in which the verifier can read only O(1) random bits!



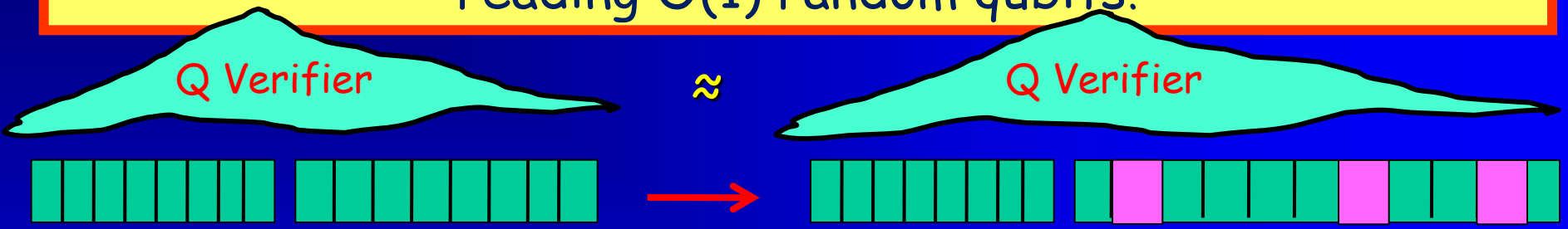

PCP thm, Gap amplification version:
There exists an efficient transformation f: CSP → CSP' s.t.
X is satisfiable → so is f(X)
X is unsatisfiable → UNSAT(f(x))>10%.



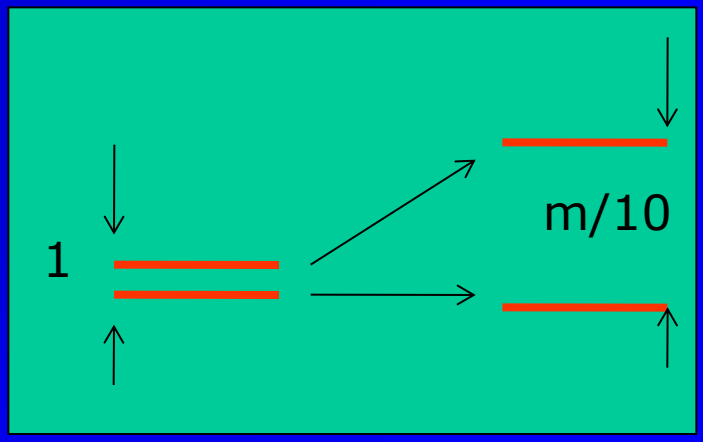

Implications: hardness of approximation.
In physical language → Exist systems which need to solve NP to relax to their Gibbs state at room temperature!

# The qPCP conjecture [AALV'10]

qPCP conjecture, query version: QMA is equivalent to the class of languages in which the witness is checked by reading O(1) random qubits!




qPCP, Gap amplification version:
There exists a (quantum) efficient transformation f: H → H' s.t.
H has 0 groundvalue → so does H'
gv(H)>b → gv(H')>m/10.



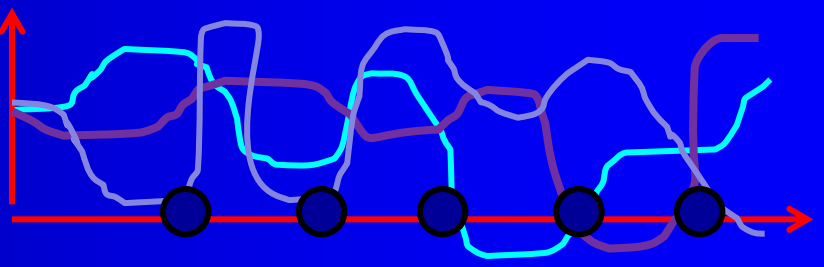

qPCP: O(1)-Approximation of average Energy is QMA hard

In physics language → Exist systems which need to solve QMA to relax to their Gibbs state at room temperature!

Compare to quantum fault tolerance :long range quantum entanglement

# A scheme based on random quantum polynomial codes [Ben-Or,Crepeau,Gottesman,Hassidim,Smith'06]

## Quantum Reed-Solomon ECCs [A'BenOr'96]



$$|s_a\rangle = \frac{1}{\sqrt{q^m}} \sum_{\substack{g:\deg(g)\le d \\ g(0)=a}} |g(\alpha_1), g(\alpha_2)\ldots, g(\alpha_m)\rangle$$

Shifted by a random Pauli key Q on m qudits, and a random sign key $k\in\{-1,+1\}^n$ :

$$|s_a\rangle_{Q,k} = Q \circ \Big( \sum_{\substack{g:\deg(g)\le d \\ g(0)=a}} |k_1 g(\alpha_1), k_2 g(\alpha_2)\ldots, k_n g(\alpha_m)\rangle$$

The prover can apply gates without knowing the code!!!
He applies gates on the bare state; the verifier corrects his own keys

This can detect any error, not necessarily local, w.h.p.

(The sign key K protects against Paulis. The random Pauli translates general operators to random Paulis)

# Verifying quantum evolutions

Open: Can this be done with one classical verifier?

Possible with two entangled provers
[ReichardtUngerVazirani'12]

Can interactive experiments be used elsewhere?

Testing unitarity of blackhole evolution [Hayden & Preskill'07]

# Quantum Computation & Machine learning (CNT'D)

## Applied in:

K-means Clustering [LMR13]
Principal component analysis [LMR13]
Recommendation systems in poly(k)polylog(N) [KerenidisPrakash17]

## Many caveats

(see: "QML algorithms: Read the fine prints", Aaronson, Nature'15)

## Ewin Tang's breakthrough

Quantum inspired classical poly(k)polylog(N) recommendation system [2018] (and follow up dequantizations)

Remains a big open question:
Find an Exponential quantum speed up for an interesting ML problem.