The Era of
Algorithmic Experiments

Dorit Aharonov,
Hebrew University

Based on

1. Aharonov Ben-Or Eban (2008) [ITCS 2010]
   Aharonov Ben-Or Eban Mahadev [submitted, 2017]
   Aharonov, Vazirani [Computability: MIT anthology, 2013
2. Arrad,Vinkler,Aharonov,Retzker [PRL 2014]
3. Atia, Aharonov [NatureComm.2017]

KITP October 2017

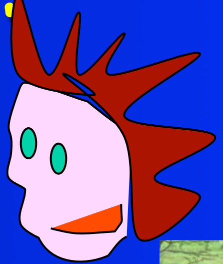
Some quantum revolutions…

90's: Quantum computation
Building quantum computers,
algorithms, cryptography

2000's:
Quantum Hamiltonian complexity
The computational lens on Q physics;
QMA hardness +
Complexity of tensor networks

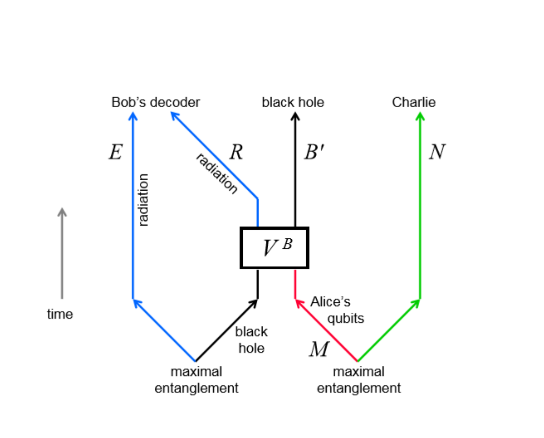
2010's:
Quantum algorithmic experiments
Introducing quantum algorithmic techniques into experiments

A Physical Experiment: "Predict & compare"



A physical theory: F=ma
parameter estimation, etc

Three examples of algorithmic experiments:



Ex1: Blackholes as mirrors
(An experiment that tests the hypothesis that Black holes reradiates Quantum information quickly)
Hayden Preskill [JHEP'07]

Ex2: Increasing sensing resolution using QECC
(From SQL to Heizenberg limit)
Arrad Vinkler Aharonov Retzker [PRL'14]
Kessler Lovchinsky Sushkov Lukin [PRL'14]
Dür Skotiniotis Frowis Kraus [PRL'14]
Ozeri [Preprint'13]
Zhou Zhang Preskill Jiang [preprint'17]

Ex3: Energy measurements which expo.violate $\Delta t \Delta E > 1$
(Shor/commuting/quadratic LH). Non blackbox!
Atia Aharonov [NatureComm'17] (Y.AharonovMassarPopescu'02)

Ex4:
Interactive experiments

[Aharonov,Ben-Or,Eban(2008) [ICS2010]
Yonatan Yaari [Thesis, 2008]
Fitzsimons Kashefi [2012]
Aharonov Vazirani [Computability, 2013]
Aharonov Ben-Or Eban Mahadev [submitted, 2017]

A Disturbing Conversation at Radcliffe Institute in 2004…

Oded Goldreich

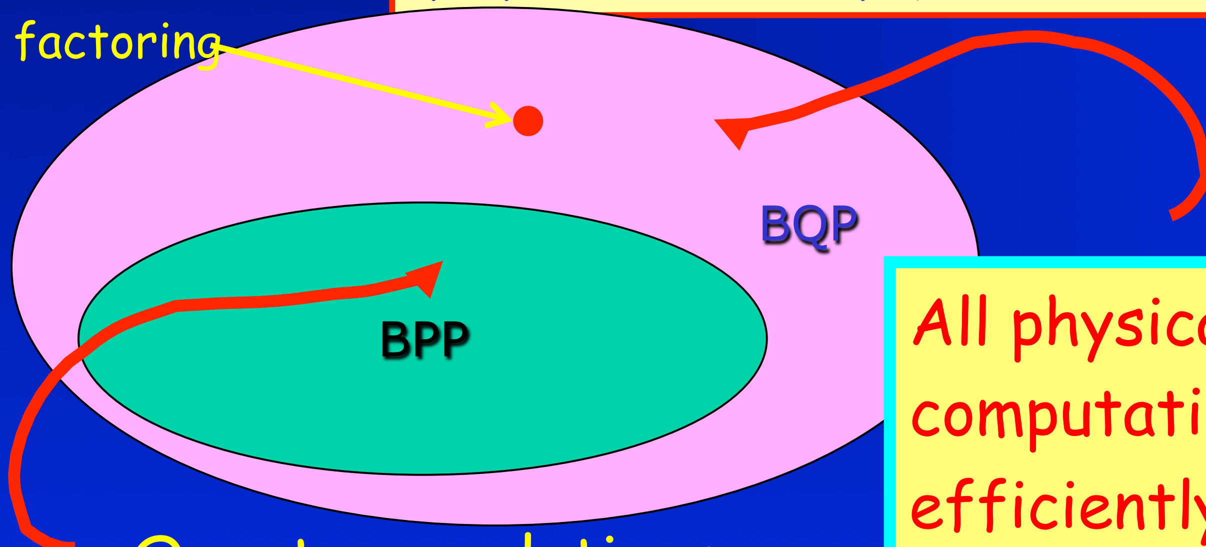
Madhu Sudan

"If Quantum Mechanics is indeed exponentially stronger, and computes things we cannot compute in BPP, show me evidence to this fact, from existing experimental results."

"Give a mathematical problem to challenge classical computers. which, (by our current experimental data) Can be solved only by quantum systems efficiently."

Complexity Jargon

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



high complexity regime of QM

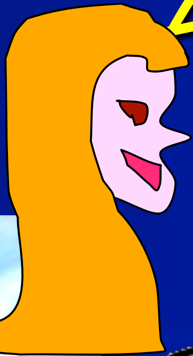
Quantum evolutions of low complexity (classically simulable)

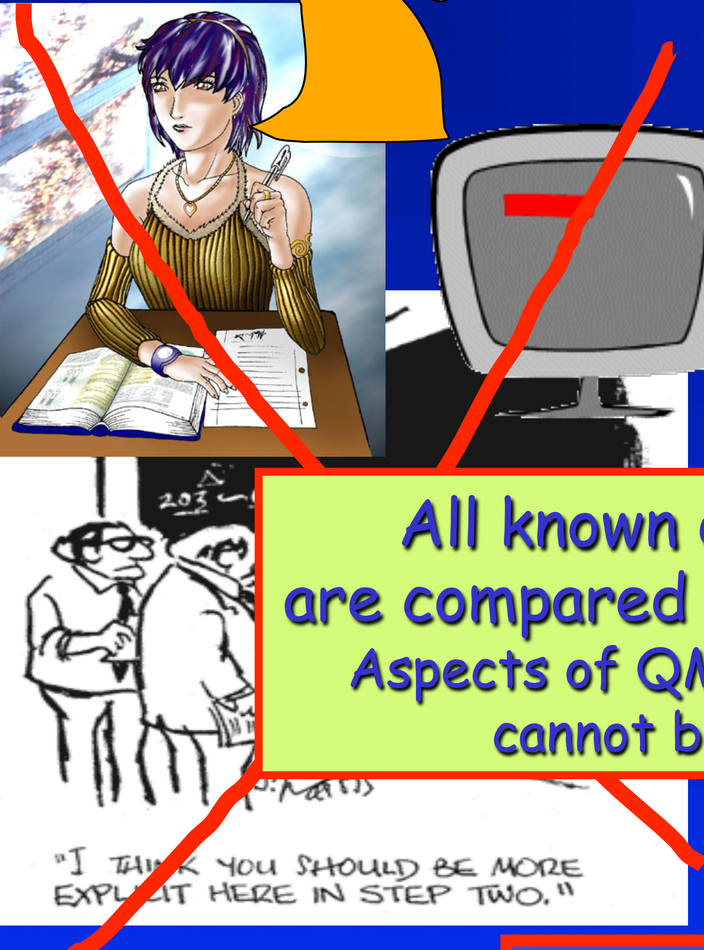
All physically realizable computational models can be efficiently simulated by a Turing machine" (Extended CTT)

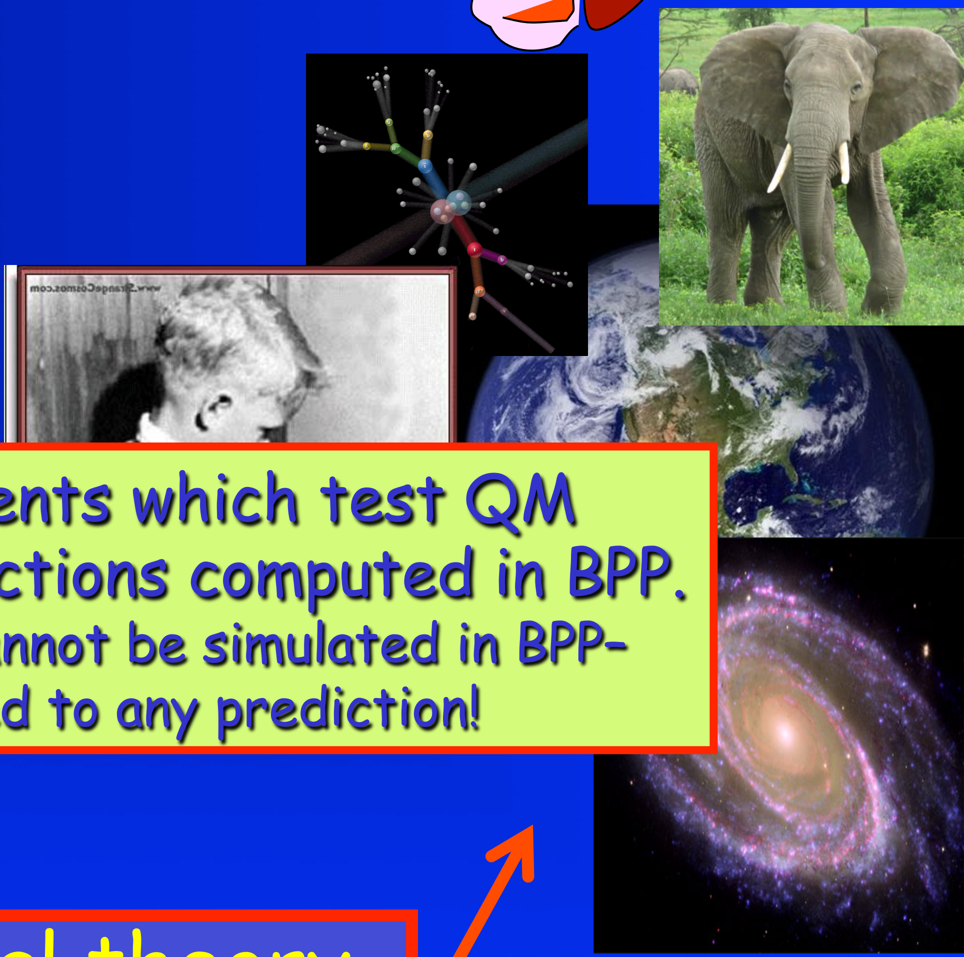
Widely believed:
QC violates ECTT
1. BQP is strictly larger than BPP,
2. Quantum Systems can in principle physically implement BQP

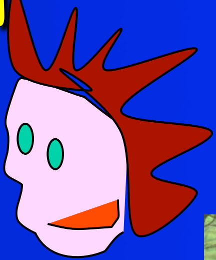
Evidence for quantum exponential advantage?

A Physical Experiment









All known experiments which test QM are compared to predictions computed in BPP.

Aspects of QM which cannot be simulated in BPP- cannot be compared to any prediction!

A physical theory

Quantum Mechanics

F=ma

Is Quantum Mechanics (QM) Falsifiable?

Because of the violation of the ECTT
we cannot test Quantum Mechanics
in the high complexity regime
(using the **usual** predict & compare paradigm).

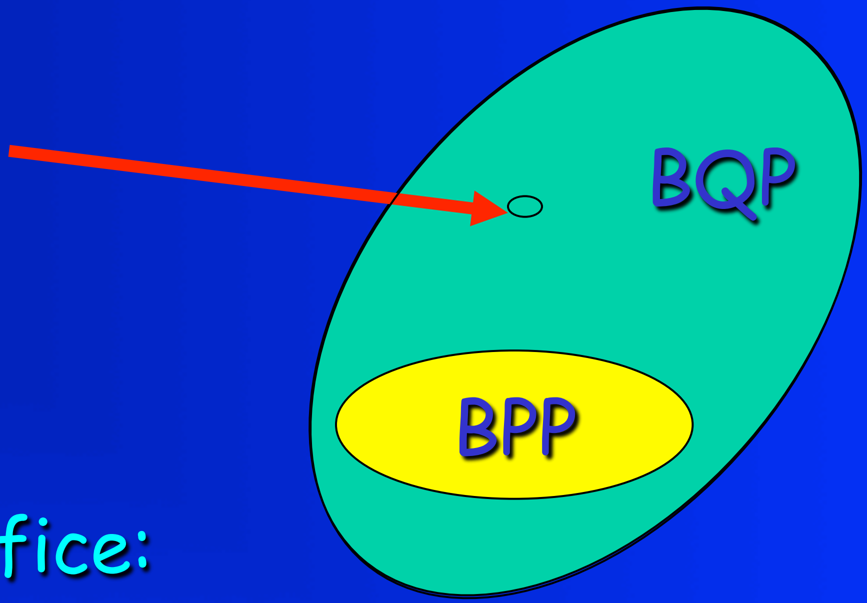
Question 1: Fundamental:
Is QM Falsifiable?

Question 2: Cryptographical:
Verify delegated Quantum Computations to untrusted parties? (gottesman'04)

Question 3: Experimental:
How to test our Quantum devices?

Shor's Algorithm as a Partial Answer [Vazirani' 07]

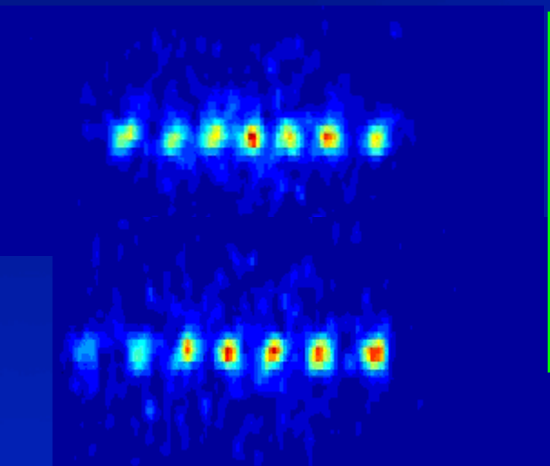
Factoring
Allows a test
in the high
complexity
regime!

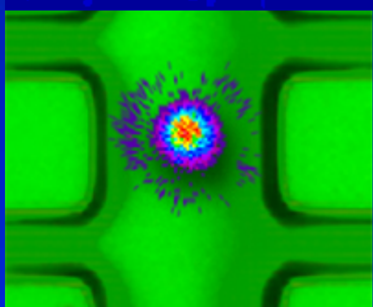


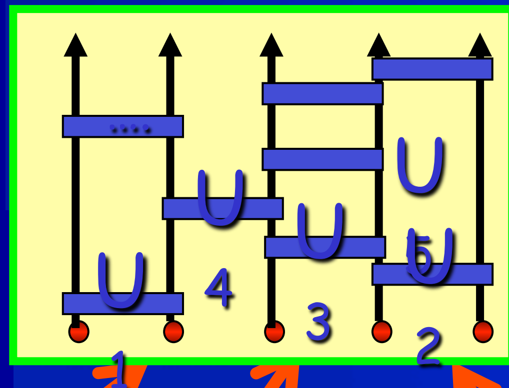
But Factoring does not suffice:

1. Factoring is probably not BQP complete .
2. What if we want to test small systems ~100 qubits?

We would like to verify
Any quantum computation

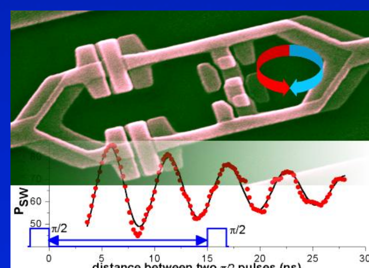


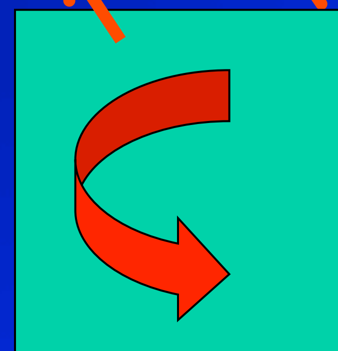


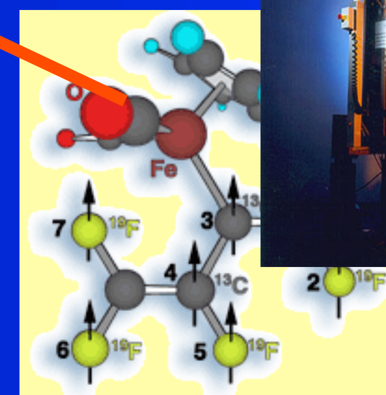


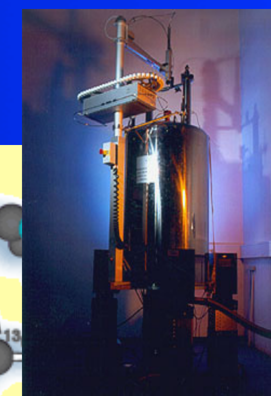
$$U_1,\cdots,U_L$$

$$|\alpha(L)\rangle = U_L\cdots U_1|0110...1\rangle$$







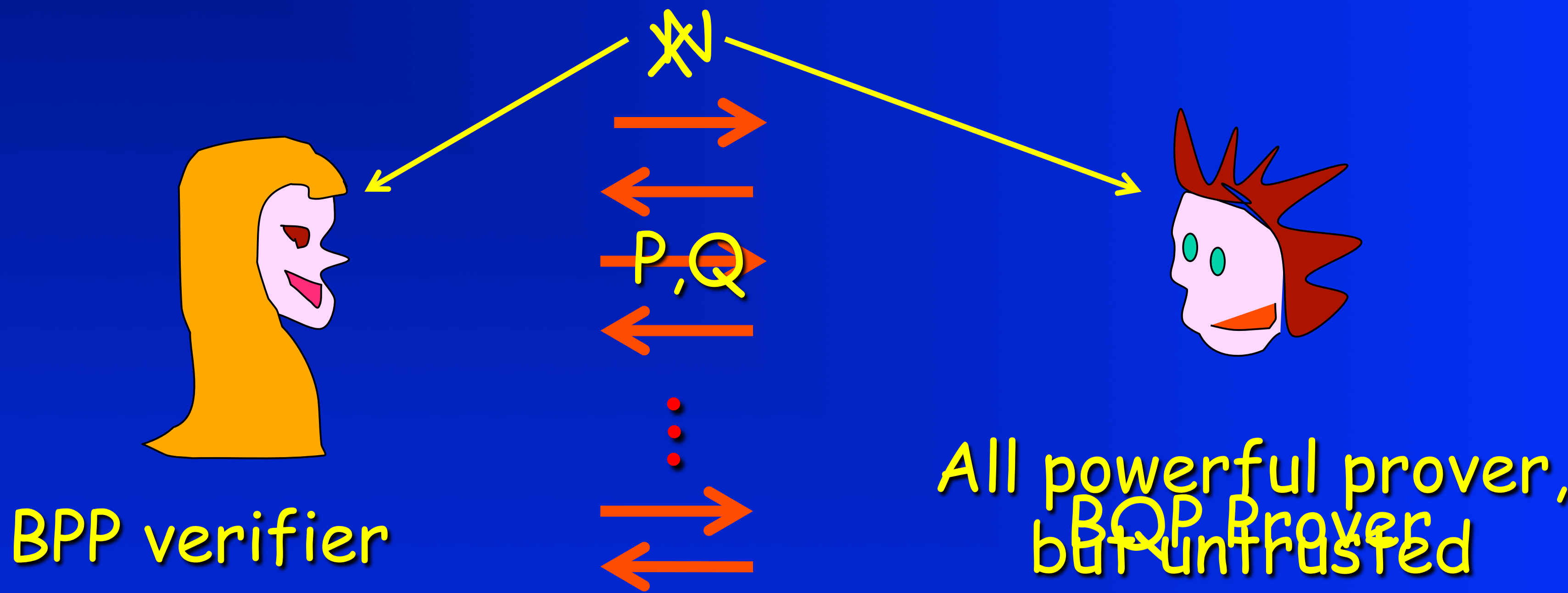


How would we know? We do not know the answer!

How did Shor's algorithm get around the pitfall?

Because it is an example of a new type of experiment

Interactive proofs [Goldwasser, Micali, Rackoff' 85]



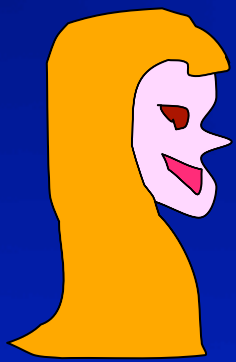
With interaction,
A computationally *weak* Verifier
Can get convinced of highly complex claims
Without knowing how to prove them!!!

The power of interaction

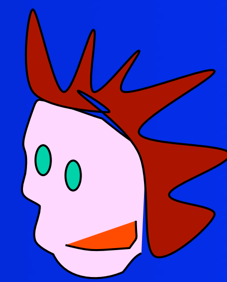
[Rabin]

Quantum prover Interactive Proofs (QPIP)

Aharonov Eban Ben-Or' 08' [ITCS2010]



Verifier: BPP + O(1) qubits



BQP Prover

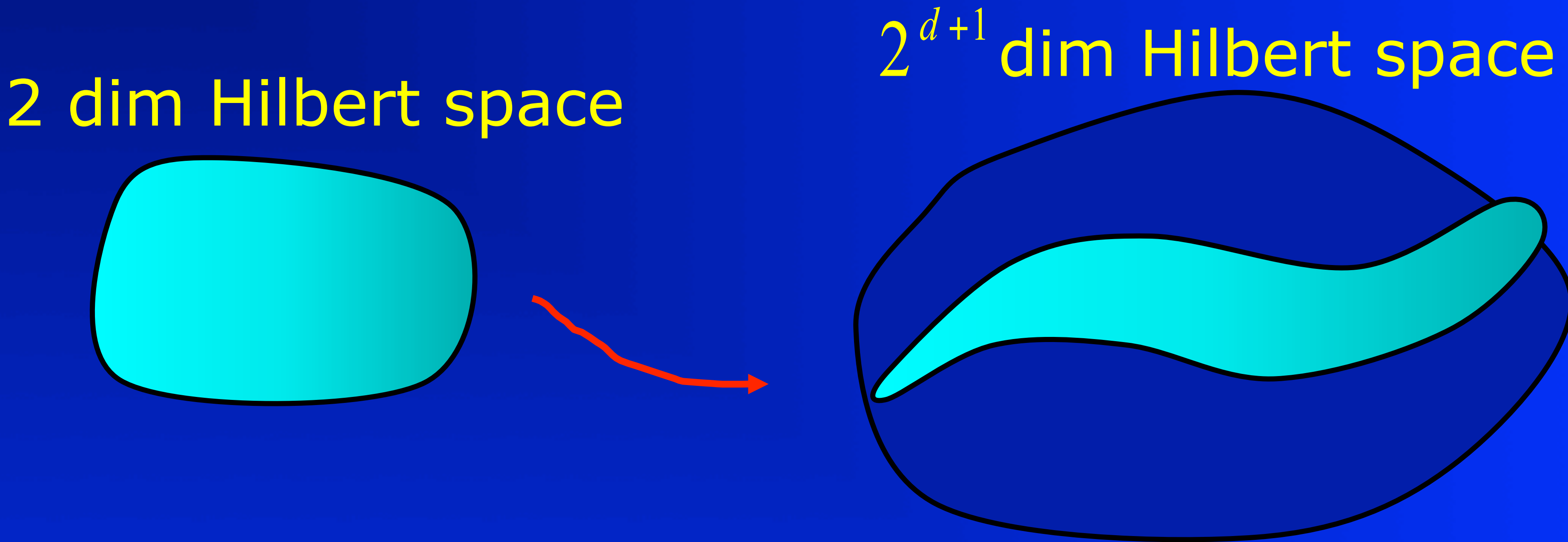
Theorem: A BQP prover can prove *any* quantum circuit to a BPP+O(1) qubits verifier!

Proof: Aharonov Ben-Or Eban Mahadev 2017 (submitted)

Also blind (interesting for cryptographic application, less for physical app.)

Broadbent Fitzsimons Kashefi [BFK2008] – Blind Q computation
Fitzsimons Kashefi [FK2012] – extended to verifiable blind Q computation

Basic idea: Random QECC



The prover doesn't know the random subspace, and so
If tampers with the state it will take it out of that SS.

The verifier doesn't know how to move the state inside
the SS but can test whether the state is there.

The prover will need to know how to compute in an unknown code…

A Scheme based on polynomials codes

[Ben-or,Crepeau,Gottesman,Hassidim,Smith'06]

Quantum Reed-Solomon ECCs [ABenOr'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∈{-1,+1}ⁿ** :

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

This can detect any error w.h.p (The sign key K protects against Pauli operators. The random Pauli translates a general operator to a random Pauli)

The prover applies gates on the bare state; the verifier corrects his own keys!

From Verifiable delegated computation to Ex4:
Interactive experiments

[Aharonov,Ben-Or,Eban(2008) [ICS2010]
Yonatan Yaari [Thesis, 2008]
Fitzsimons Kashefi [2012]
Aharonov Vazirani [Computability, 2013]
Aharonov Ben-Or Eban Mahadev [submitted, 2017]

Verify the correctness of a polytime quantum evolution of
a given encoded Hamiltonian

Hamiltonian is "malicious" – blackbox.
Seems to contradict Y.Aharonov,Massar Popescu'02

On a given input

Discussion & Open questions

Have seen different examples in which applying Q algorithms and protocols leads to interesting Q experiments

1.

Oded Goldreich *Madhu Sudan*

"Show me evidence for quantum supremacy"

Using quantum verification we could test Q supremacy (see next talk) using interactive experiments.

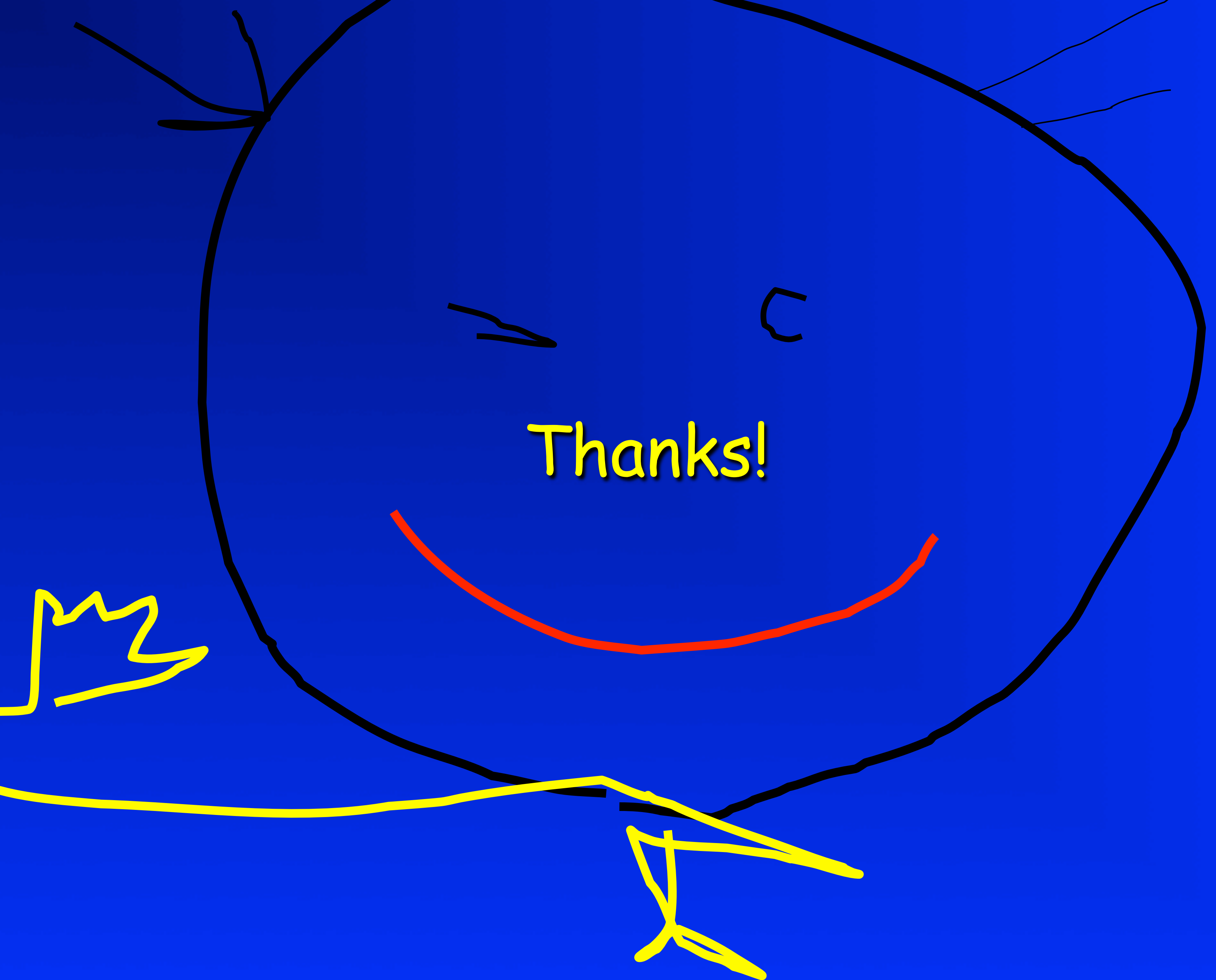
Shallow circuits: A possible application for ~50-100 qubits without EC

Discussion & Open questions (Cont'd)

2. Could we test quantum Hamiltonians using Interactive experiments?

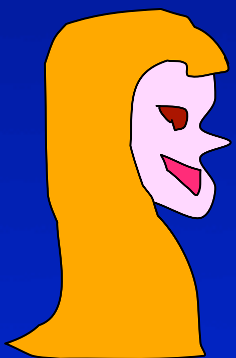
Current schemes assume almost full control of quantum device.
Can we test systems with much less control?
Eg, High Tc superconductivity
Reducing the resources but adding assumptions

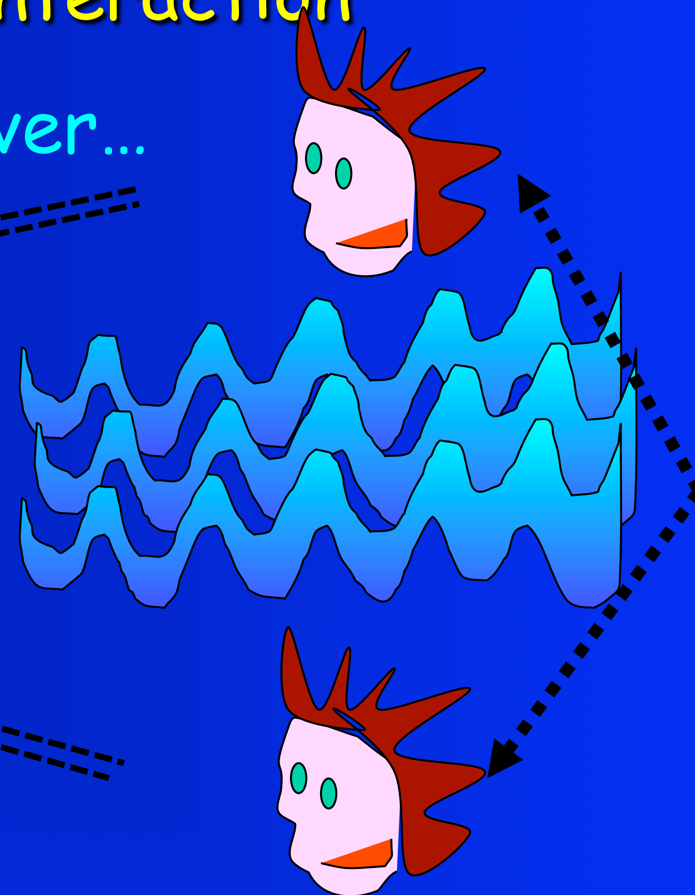
3. General theory of algorithmic measurements?


Thanks!

Reichardt, Unger, Vazirani: ’ 2012:
removing any *quantum* interaction

Perhaps impossible with one prover…





Possible
with two provers

Which are entangled

Direction I: A new theory of confirmation?

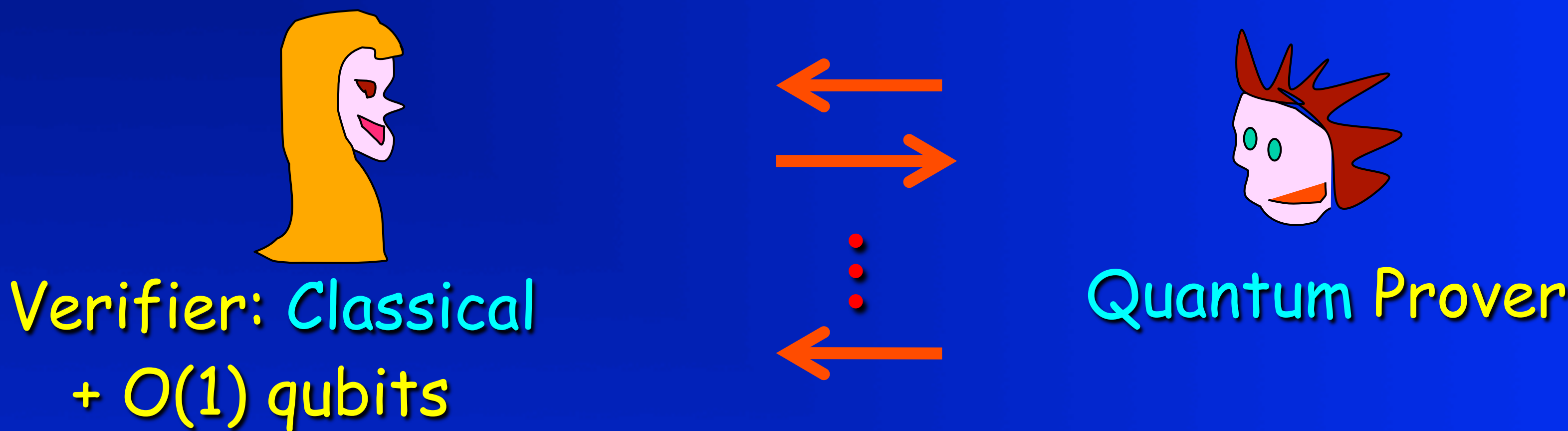
Interactive experiments as a new theory of confirmation [Yaari'12]

The verifier: has the power of the physics we trust.
The Prover: Things we do not yet understand or believe, and want to test:
Nature, a system claimed to be a quantum computer, etc.

It should suffice to have that power in an interactive proof to prove the theory's correctness to someone using only already proven theories

A new experimental paradigm – Verifying quantum systems **By Interactions**

[AharonovBen-OrEban' 08' 10, AharonovBen-OrEbanMahadev' 17]



Theorem: *any* quantum polytime evolution can be verified in the interactive experimental paradigm!

(Using random quantum error correcting codes)

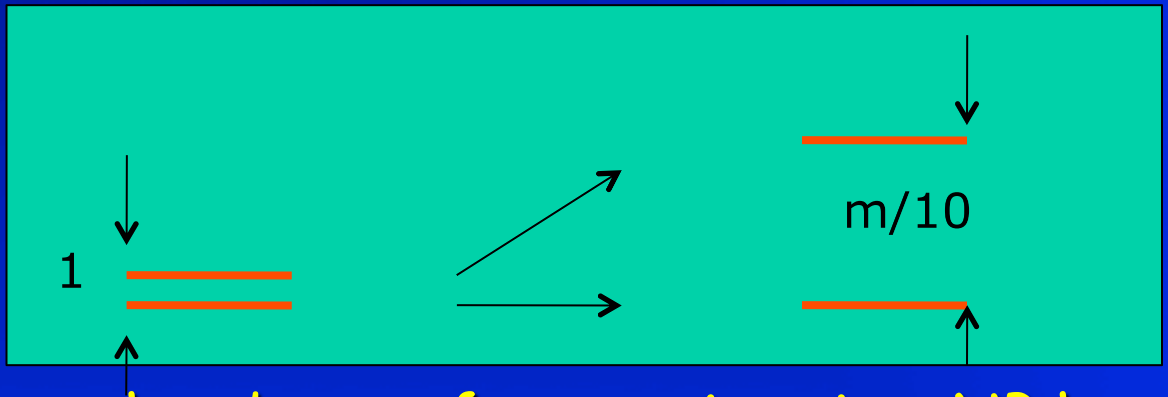
A long line of works followed [BKF'09, KF'12, RUV12, BGS'13, Vidick et al 2016, 2017…]

Major open questions related to cryptography & complexity, and experimental implications, studied in our lab

A probe to understanding and testing QM where it was never tested before

The PCP theorem

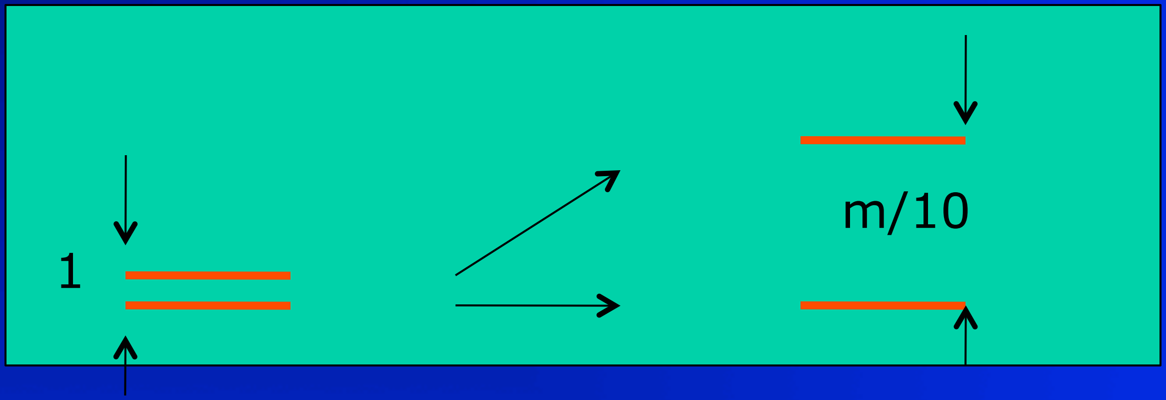
PCP theorem: All NP Languages can be checked by reading only O(1) bits from the proof!
(long history… Beautiful recent proof by Dinur'06)



Implications: hardness of approximation. NP hard to check whether 100% of constraints are satisfiable, or less than 90%. i.e., to estimate number of unsatisfied constraints up to 10%.

PCP theorem→ systems which need to solve NP to relax to their Gibbs state at room temperature!

Quantum PCP: A gap amplification map on Hamiltonians



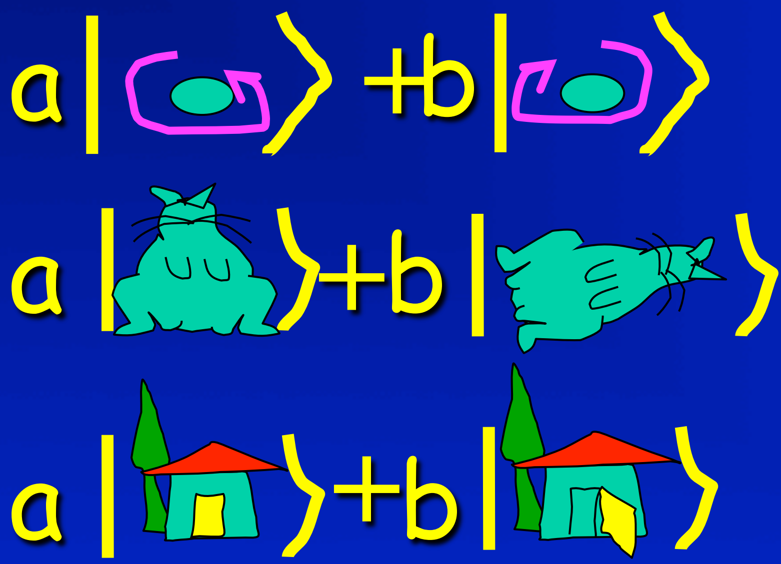
Implications: quantum hardness of approximation: Quantum NP hard to estimate ground energy of local Hamiltonian up to 10%!

Quantum PCP theorem→ quantum systems which, in order to Relax to their Gibbs state at room temperature, need to solve a Quantum NP Complete problem

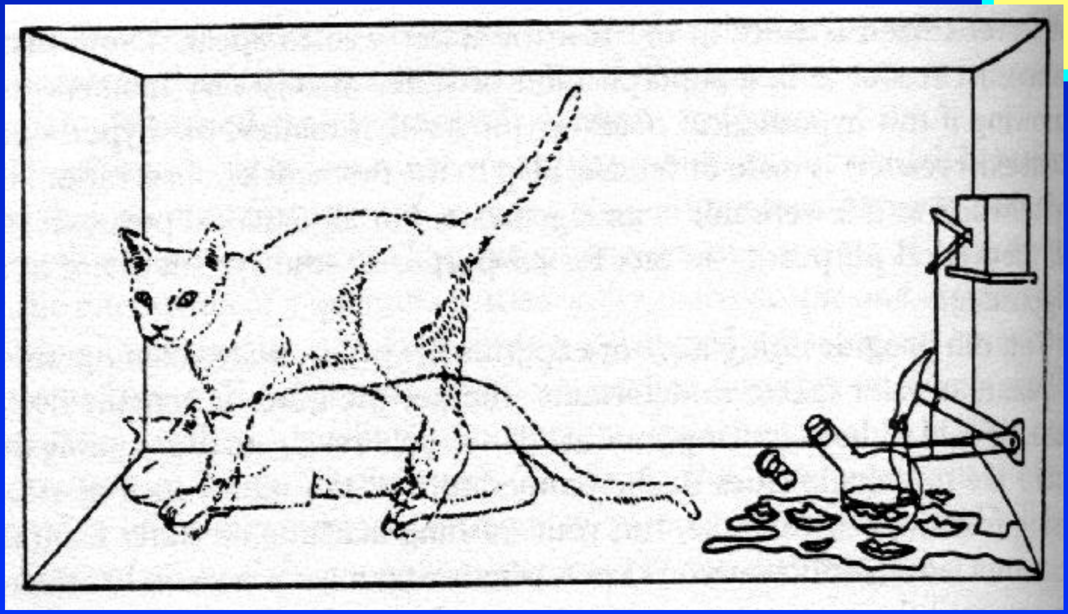
Could it be? Related to no cloning, fault tolerance…

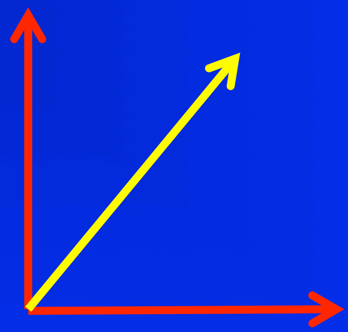
Partial results: [A'AradLandauVazirani'09]

The Superposition Principle



A quantum particle can be in a **Superposition** of all its possible **"classical" states**



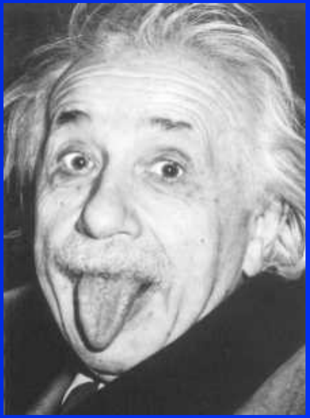


$$a\,|0\rangle + b\,|1\rangle$$

Limited access to the state..
The quantum measurement

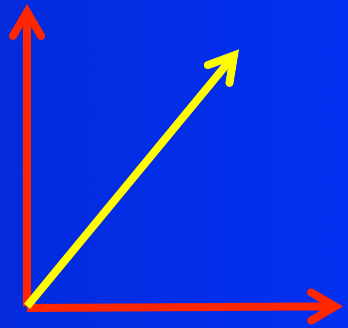
$$a\,|0\rangle + b\,|1\rangle$$

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



When a quantum particle is measured
the answer is Probabilistic

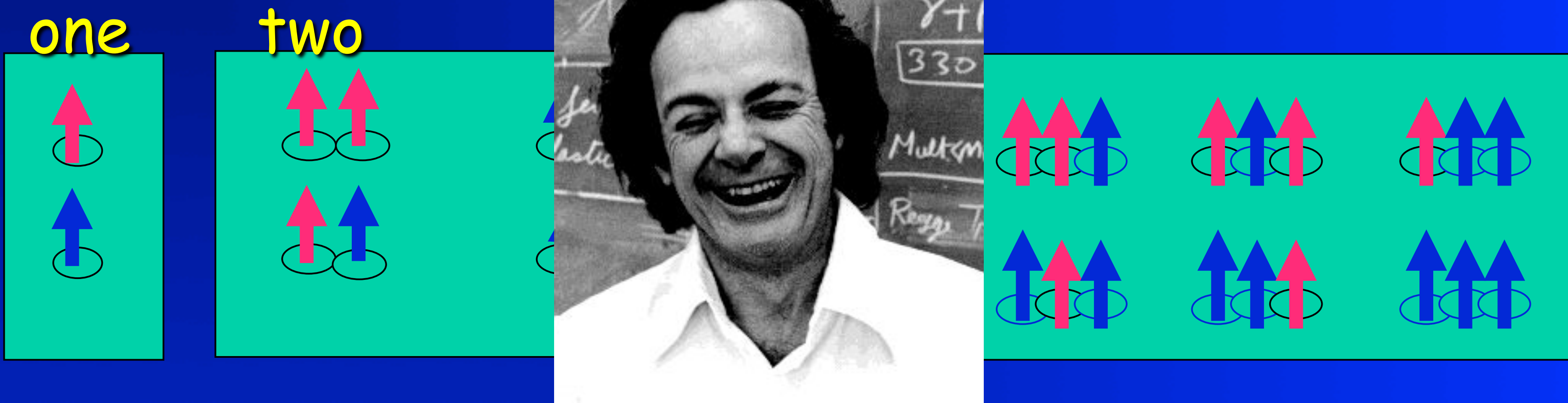
The Superposition collapses
to one of its possible classical states



Those (weird!) aspects have been
tested in thousands of experiments

2.
The high complexity regime of Quantum Mechanics (QM)

The extrava … exity of QM



The state of n quantum bits is a superposition of all 2^n possible configurations, each with its own weight!

Feynman [82]

(And independently, Manin '80, Bennoif' 81):

Quantum systems seem Exponentially hard to simulate…

n classical particles - described by 6n numbers

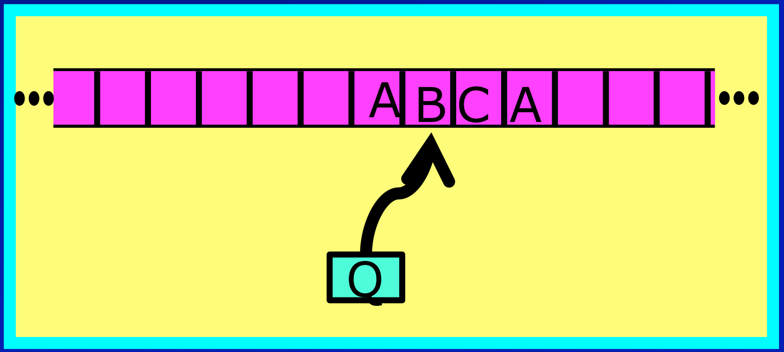
n Quantum particles - by 2^n.

(though don't forget our limited access to it!)

Linear(n) Exponential(2^n)

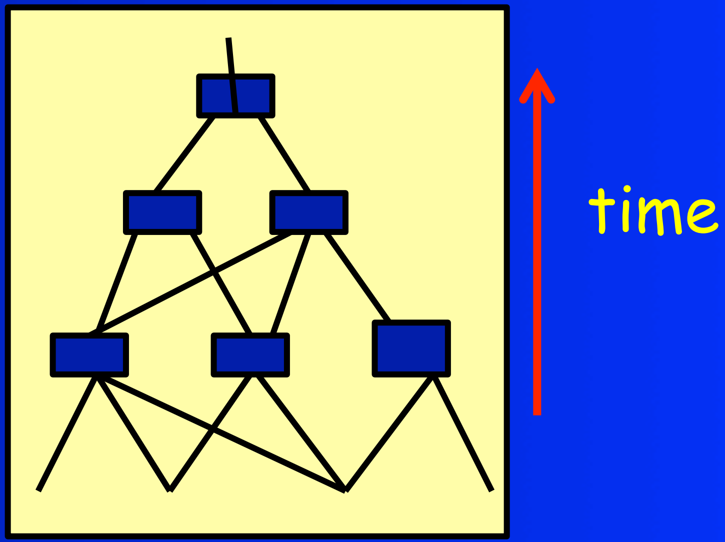
Classical and Quantum Computation

Turing Machine



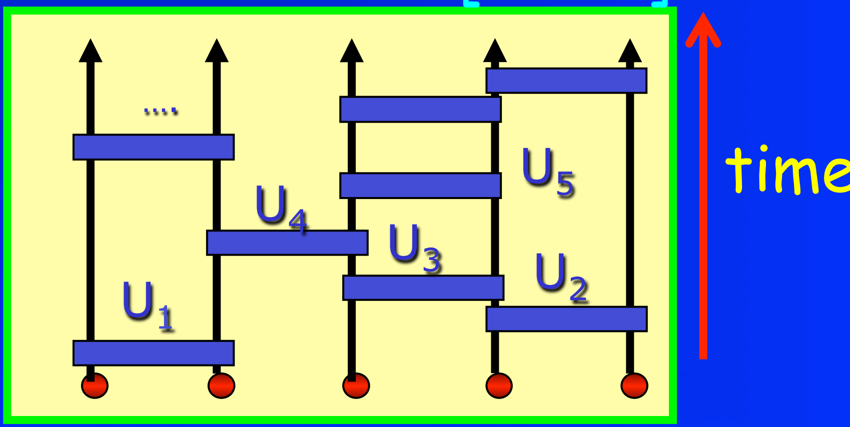
≈

Circuits C_n



Quantum Turing Machine…
[Deutch'85]

Quantum circuits [Yao'89]



- **Input:** $|\alpha(0)\rangle = |0,1,1,\ldots,1,0\rangle$
- **Gates** $|\alpha(L)\rangle = U_L \cdots U_1 |\alpha(0)\rangle$
- **Measure**

Running time: number of gates L.

Quantum Algorithms


Deutsch ['92]


Deutsch
Josza ['92]


Bernstein
Vazirani['93]

Simon
['94]

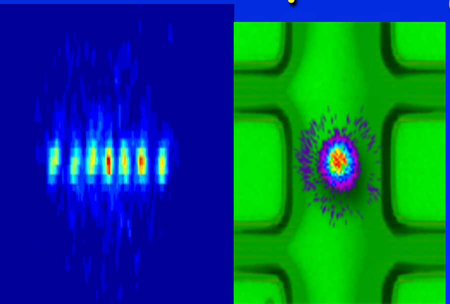

Shor[' 94]

Break
RSA!

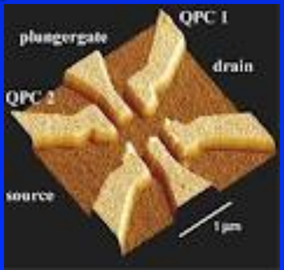
Polynomial time Quantum algorithm for factoring

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

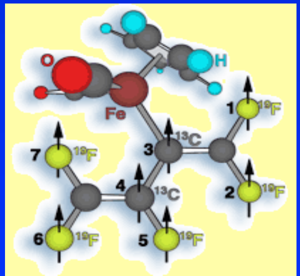
Ion traps



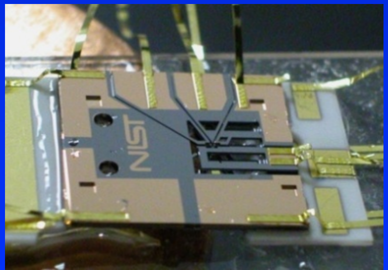
Quantum dots



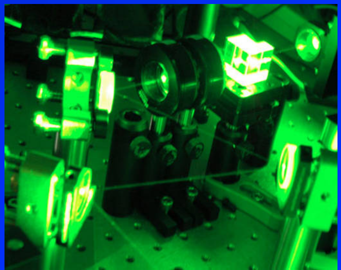
NMR



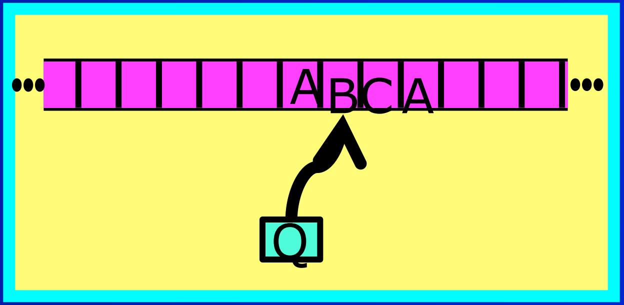
Josephson
Junctions



Optics

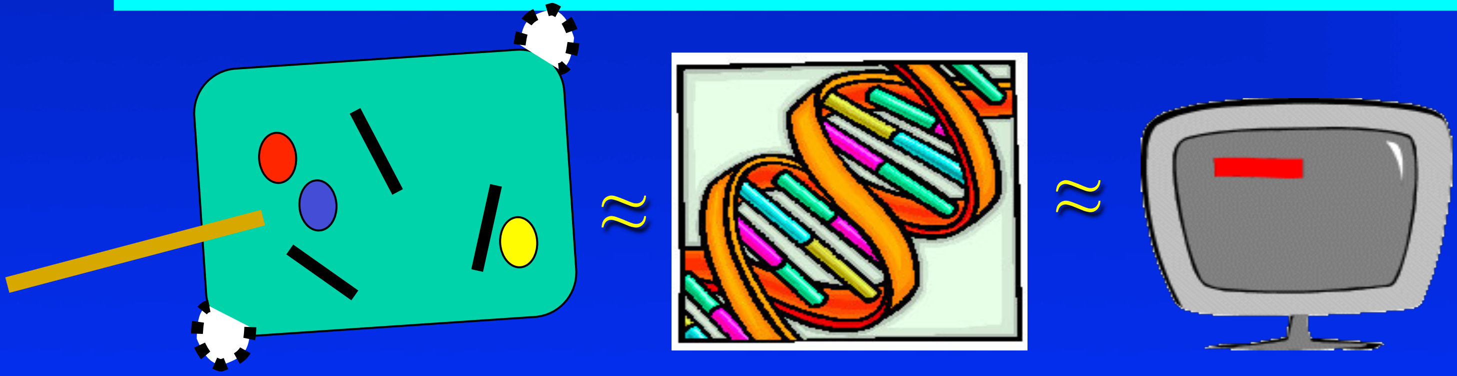


The Church-Turing thesis (CTT) & physical reality



"everything algorithmically computable is computable by a Turing machine"

" All physically realizable computational models can be simulated by a Turing machine"

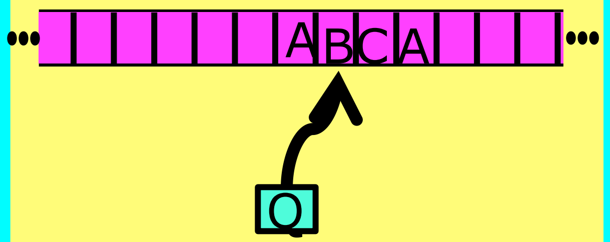


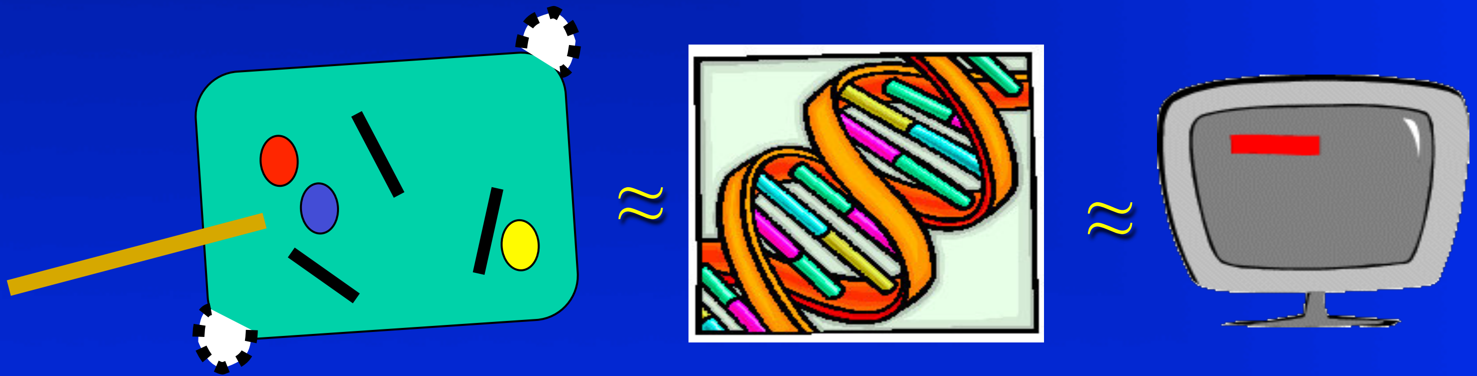
Holds for quantum computers as well

The **Extended** Church-Turing thesis (ECTT)

Corner stone of modern theoretical computer science

" All physically realizable computational models can be efficiently simulated by a Turing machine"





But: Quantum systems seem to require exponential overhead to simulate. Quantum computers are thus the only model that credibly challenges the ECTT.