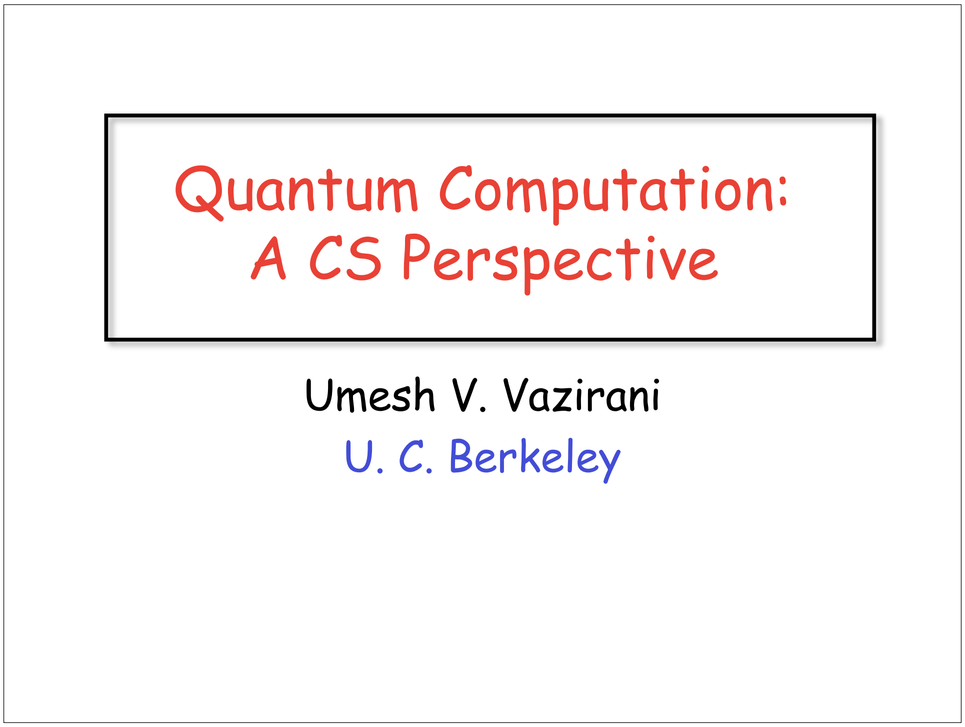
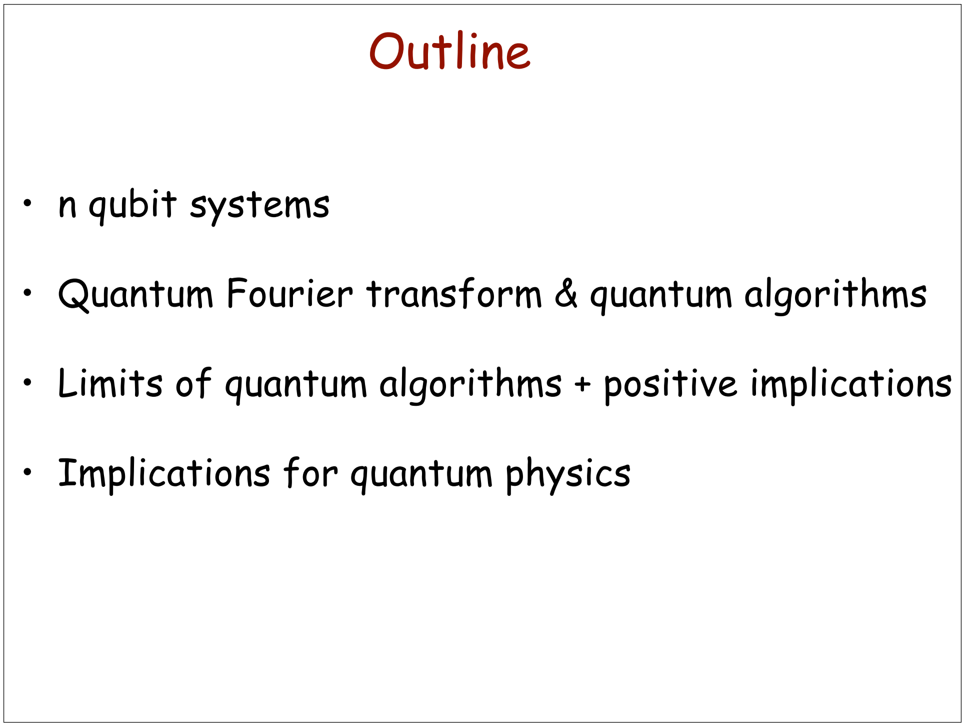


Quantum Computation: A CS Perspective

Umesh V. Vazirani

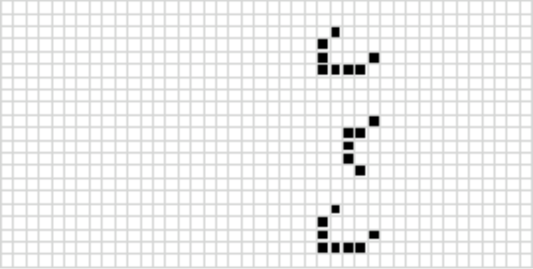
U. C. Berkeley



Outline

- n qubit systems
- Quantum Fourier transform & quantum algorithms
- Limits of quantum algorithms + positive implications
- Implications for quantum physics

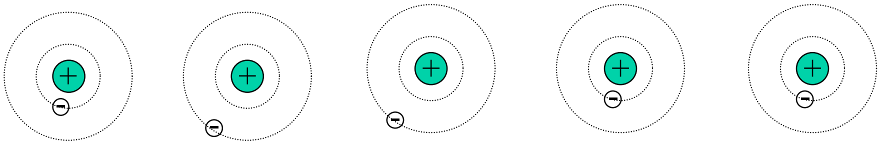
Importance: Quantum computers violate
Extended Church-Turing Thesis.



≡

Either Extended Church-Turing thesis is false
OR
Quantum Physics is false
OR
Our picture of computational complexity theory is false

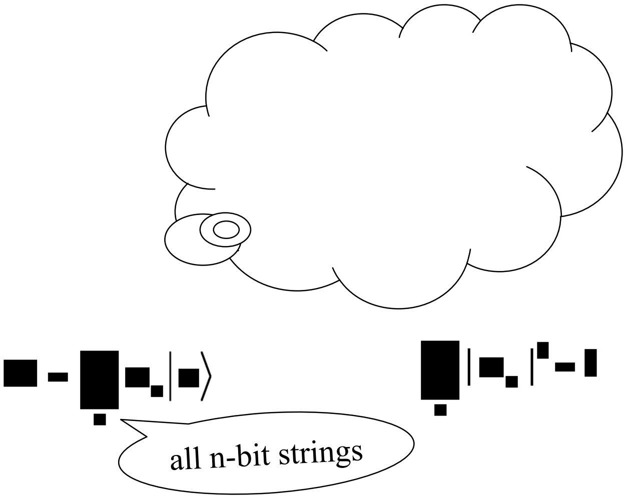
n Qubits



Exponentially Large Hilbert Space

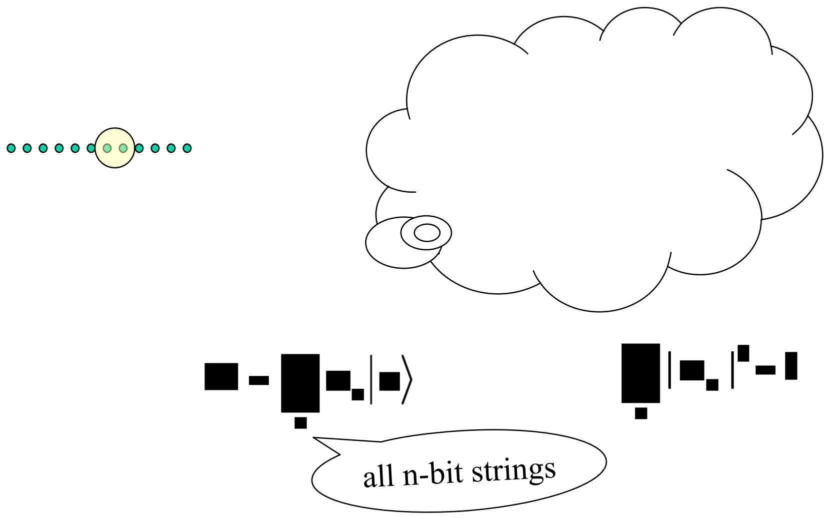
Exponentially Large Hilbert Space

Storing the state



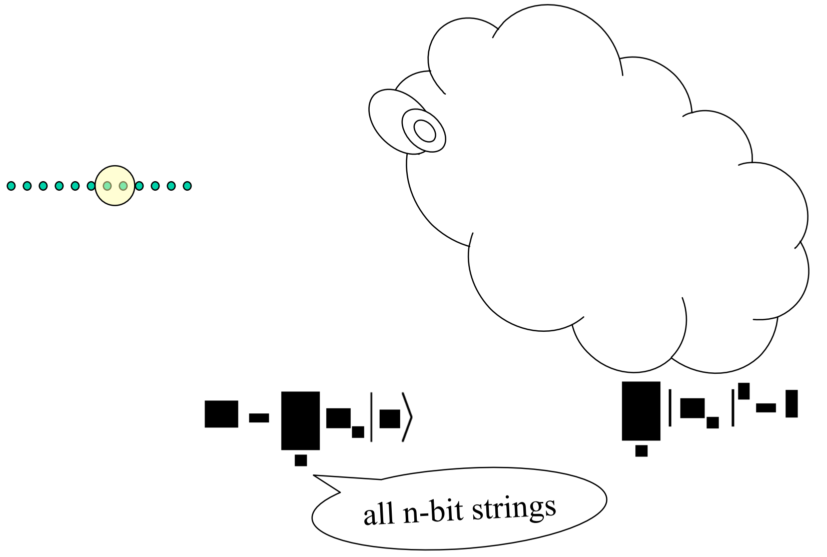
Quantum entanglement: 2^n versus 2n parameters

Evolving the state



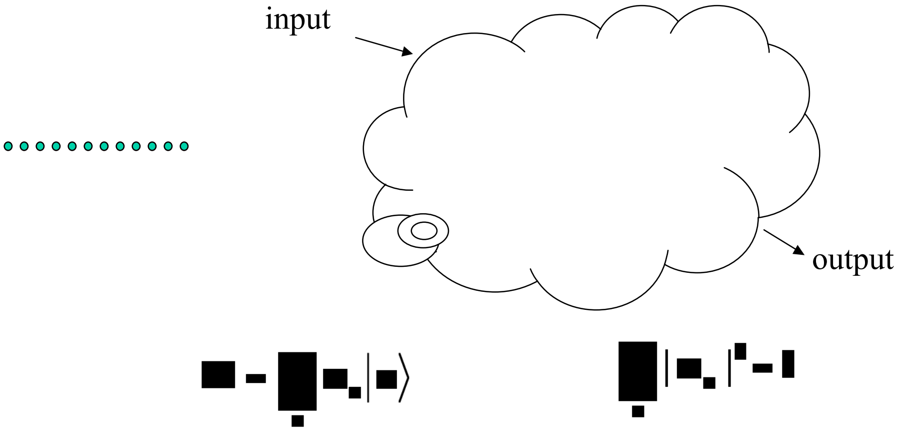
all n-bit strings

Evolving the state



all n-bit strings

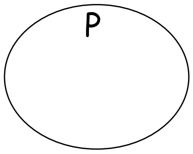
Limited Access - Measurement



- Measurement: See $|x\rangle$ with probability $|\alpha_x|^2$

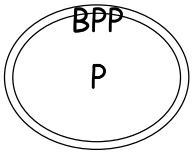
[Feynman '82]

Computational Complexity Classes



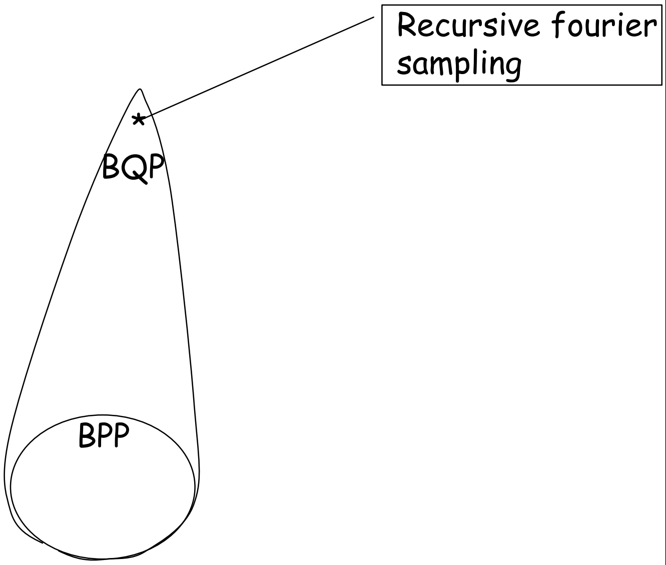
P - polynomial time. E.g. integer mult, solving linear equations

Complexity Classes



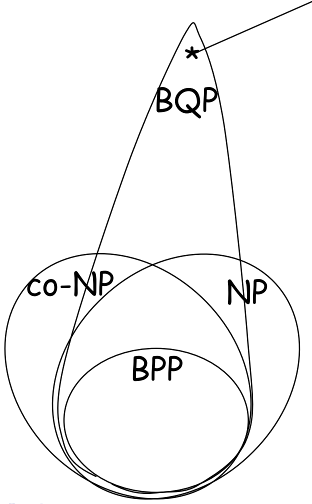
P - polynomial time
BPP – probabilistic polynomial time. Eg square roots mod p

Complexity Classes



[Bernstein,V 93] Quantum computers provably violate the Extended Church-Turing thesis in black box model.

Complexity Classes

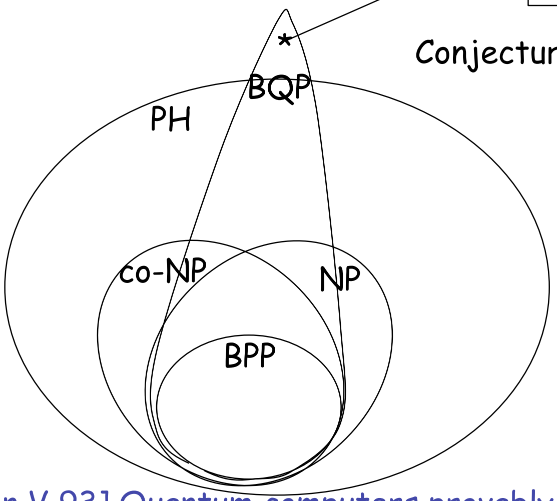


Recursive fourier sampling

Traveling salesman prob
Satisfiability

[Bernstein,V 93] Quantum computers provably violate the Extended Church-Turing thesis in black box model.

Complexity Classes

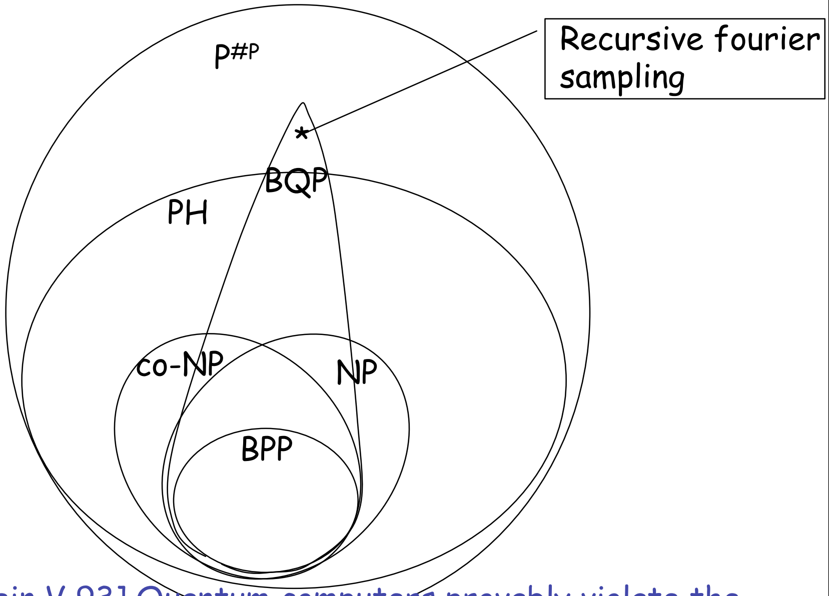


Recursive fourier sampling

Conjecture: RFS $\notin$ PH

[Bernstein,V 93] Quantum computers provably violate the Extended Church-Turing thesis in black box model.

Complexity Classes



[Bernstein,V 93] Quantum computers provably violate the Extended Church-Turing thesis in black box model.

Breaking Modern Cryptography

- [Shor 94] Factoring (RSA cryptosystem)
  Discrete Log (Diffie-Hellman key exchange)
- Elliptic curve cryptography
- [Hallgren 02] Pell's equation (Buchmann-Williams cryptosystem)
- [vanDam, Hallgren, Ip 03] Homomorphic encryption

The Key to Exponential Speedups

Fourier Transform

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ . \\ . \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & . & 1 \\ 1 & \omega & \omega^2 & . & \omega^{m-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & . & \omega^{(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{m-1} \end{pmatrix}$$

output

input

Classical: Naive O(m^2)

FFT O(m logm)

Quantum Fourier Transform

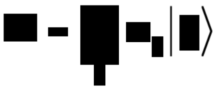
$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ . \\ . \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & . & 1 \\ 1 & \omega & \omega^2 & . & \omega^{m-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & . & \omega^{(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{m-1} \end{pmatrix}$$

Classical: Naive O(m^2)

FFT O(m logm)

Quantum:

Input: Quantum state of log m qubits



all log m bit strings

Quantum Fourier Transform

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ . \\ . \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & . & 1 \\ 1 & \omega & \omega^2 & . & \omega^{m-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & . & \omega^{(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{m-1} \end{pmatrix}$$

Classical: FFT O(m logm)

Quantum:

Input: Quantum state of log m qubits

Fourier transform: Quantum state after $O(\log^2 m)$ gates

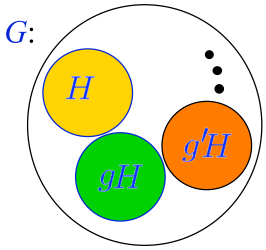
Limited Access:

Don’t get access to output vector. Not even one entry!

Measure: see index j with probability $|\beta_j|^2$

Hidden Subgroup Problem: Framework for exponential speedups by quantum algorithms.

Given $f: G \rightarrow S$, constant and distinct on cosets of subgroup H.
Find H.

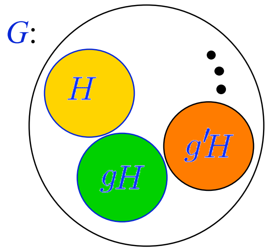


- Factoring $G = Z_M$
- Discrete Log $F = Z_{p-1} \times Z_{p-1}$

⋮

The Hidden Subgroup Problem (HSP)

Given $f : G \rightarrow S$, constant and distinct on cosets of subgroup H.
Find H.



- Use f to set up uniform superposition over random coset

|gH>

- Fourier transform and measure.
  - Yields random element of $H^{\perp}$.
    i.e. a constraint on H
  - Repeat until H is completely determined.

This procedure works for every finite abelian group G.

Non-abelian Hidden Subgroup Problem

- Important computational questions, such as graph isomorphism ($G = S_n$) and short lattice vectors ($G = D_n$) can be expressed in this framework.
- Efficient fourier sampling.
- Over last decade, sequence of results, culminating in [Hallgren, Moore, Roettler, Russell, Sen 06] providing credible evidence that quantum algorithms will not solve HSP for sufficiently non-abelian groups. Eg S_n, GL_n. in particular: graph isomorphism.
- Sufficiently non-abelian ~ exponential sized irreps + …

Negative results on non-abelian HSP

Explore other directions:

- [CSV] Use fourier sampling in new ways
  hidden polynomial problem
- [AJL] Topological based algorithms
  Jones polynomial, Tutte polynomial
- Polynomial speedup
  [Am] Quantum walk based algorithms,
  [FGG] Quadratic speedup for games

Making lemonade…

Impact of Quantum computers on Cryptography

- Quantum algorithms break much of modern cryptography
- So why isn't there greater impact on the practice of cryptography?

  - No one believes a quantum computer will be built
  - No good alternative

- Quantum cryptography

  - unconditional security
  - But: no-go theorems… bit commitment, protocols …
  - Need special equipment

Quantum Immune cryptography

- Create a cryptosystem that can be implemented efficiently on current (classical) computers.
- Provide credible evidence that cryptosystem will not be broken by quantum computers.

One-way functions: basic building block

f: $y = f(x)$ is easy to compute
$x = f^{-1}(y)$ is hard to compute

e.g. Multiplication $N = pq$ is easy
Factoring recover p, q from N hard

Quantum Immune cryptography

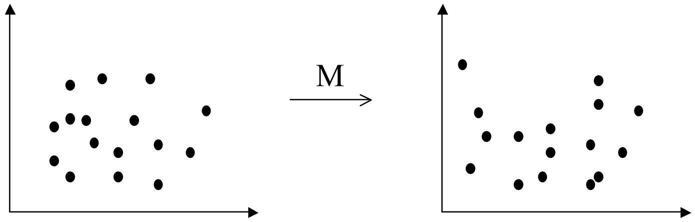
- Create a cryptosystem that can be implemented efficiently on current (classical) computers.
- Provide credible evidence that cryptosystem will not be broken by quantum computers.

Quantum Immune One-way functions: basic building block

f: $y = f(x)$ is easy to compute on a classical computer
$x = f^{-1}(y)$ is hard to compute on a quantum computer

One-way Function: Concrete Proposal

[Moore, Russell, V '07]



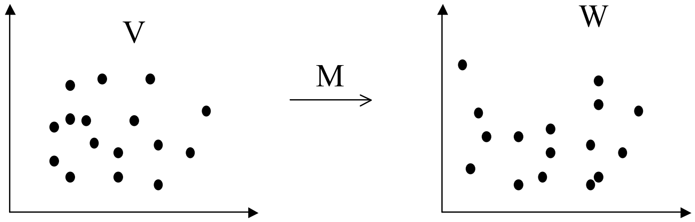
Cloud of Points:

Fix: m random vectors $v_1, \dots, v_m$ in F_p^n
Secret information: nxn matrix M
Output: $Mv_1, \dots, Mv_m$ in random order.

$$f_V(M) = W$$

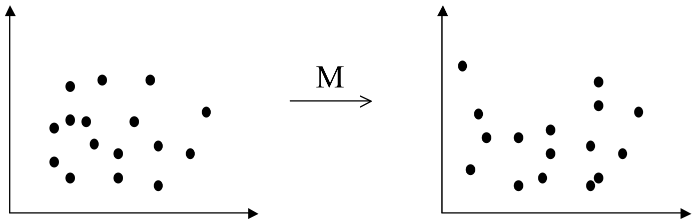
- n^2 bits mapped to nm bits.
- $m = n + O(\log^2 n)$ --- 1-1 function whp.

One-way Function: Concrete Proposal



- very efficiently computable – matrix multiplication.
- Reconstructing M as hard as graph isomorphism. [Petrank, Roth]
  Corresponds to permutation matrices M
- For V, M uniformly random, corresponding HSP over
  $GL_n \wr Z_2$ is hard in the sense of Hallgren, et. Al.

One-way Function: Concrete Proposal



- $f_V(M)$ uniformly hard to invert:
  If any entry of M can be efficiently estimated better than random guessing, then M can be reconstructed in time $n^{O(\log n)}$.

Challenge

- Want a trapdoor function: easy to compute, hard to invert,
  but easy to invert with secret key
- f_V related to McEliece cryptosystem.
  - one-way function: noisy linear equations
    trapdoor: closely related to f_V
- [Regev 04] assume that the HSP over the dihedral group is hard for quantum algorithms. Then there is a lattice-based cryptosystem that is provably secure against quantum computers. Proof of security and improvement in efficiency makes use of quantum arguments.
- Challenge: design a practical cryptosystem with credible evidence of security against quantum attack.

Quantum Random Access Codes

[Ambainis, Nayak, Ta-Shma, V ‘02]

Disposable Quantum Phonebook:

d = 10^6 phone numbers

Wish to store them using n << d quantum bits:

Can look up any phone number of your choice

Measurement disturbs system, so must discard phonebook.

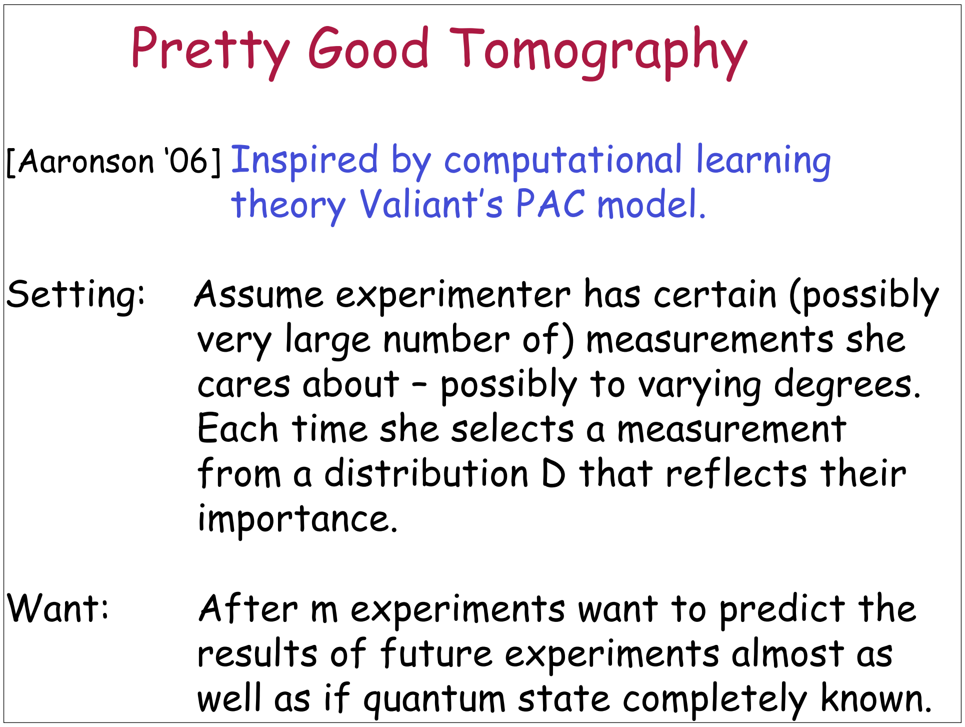
Theorem: d = O(n).

Quantum State Tomography PAC model

- Unknown n-qubit quantum state $|\blacksquare\rangle$
- Can repeatedly prepare $|\blacksquare\rangle$
- Wish to learn the state.

Problem: Exponential number of parameters to “know” the state.

What can one do?

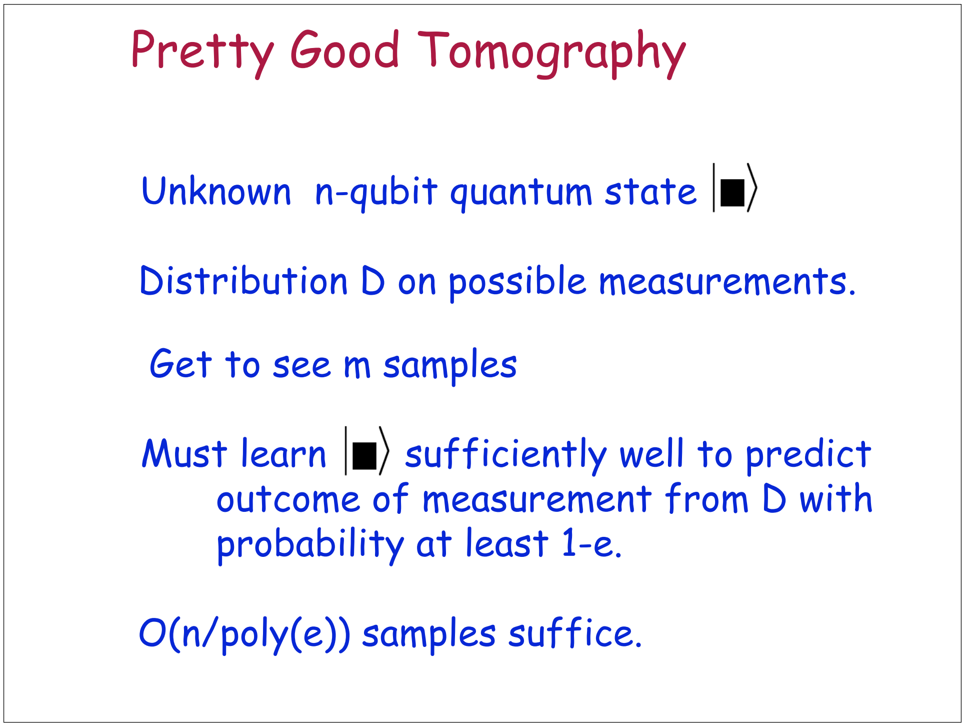


Pretty Good Tomography

[Aaronson '06] Inspired by computational learning theory Valiant's PAC model.

Setting: Assume experimenter has certain (possibly very large number of) measurements she cares about – possibly to varying degrees. Each time she selects a measurement from a distribution D that reflects their importance.

Want: After m experiments want to predict the results of future experiments almost as well as if quantum state completely known.



Pretty Good Tomography

Unknown n-qubit quantum state $|\blacksquare\rangle$

Distribution D on possible measurements.

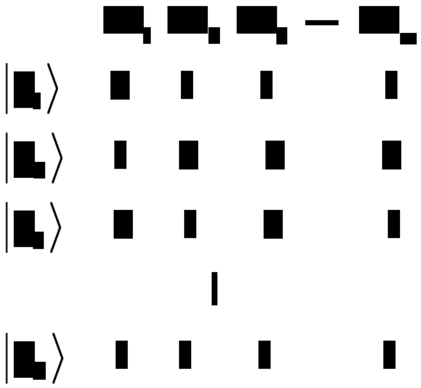
Get to see m samples

Must learn $|\blacksquare\rangle$ sufficiently well to predict outcome of measurement from D with probability at least 1-e.

O(n/poly(e)) samples suffice.

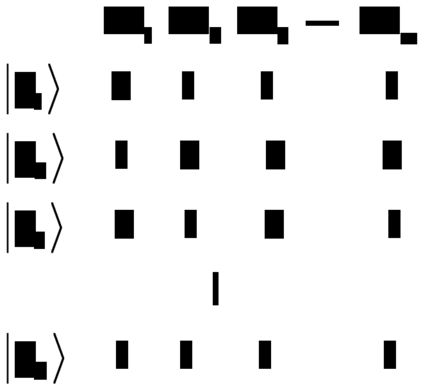
Key Ideas

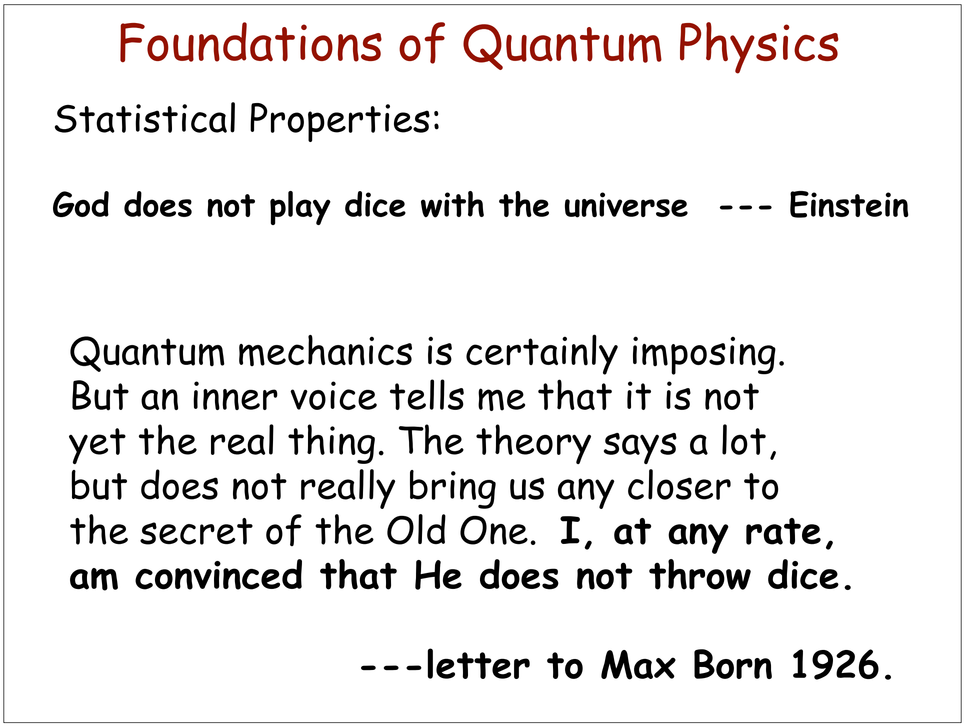
- Assume for simplicity 2 outcome measurements.
  - wish to know whether outcome 1 more likely.
- Fix any m measurements. Max number of distinct behaviors?



Key Ideas

- CLT: number of behaviors is either 2^m or m^d
- Number of samples to reconstruct = O(d)
- (n,d) random access code implies d = O(n).





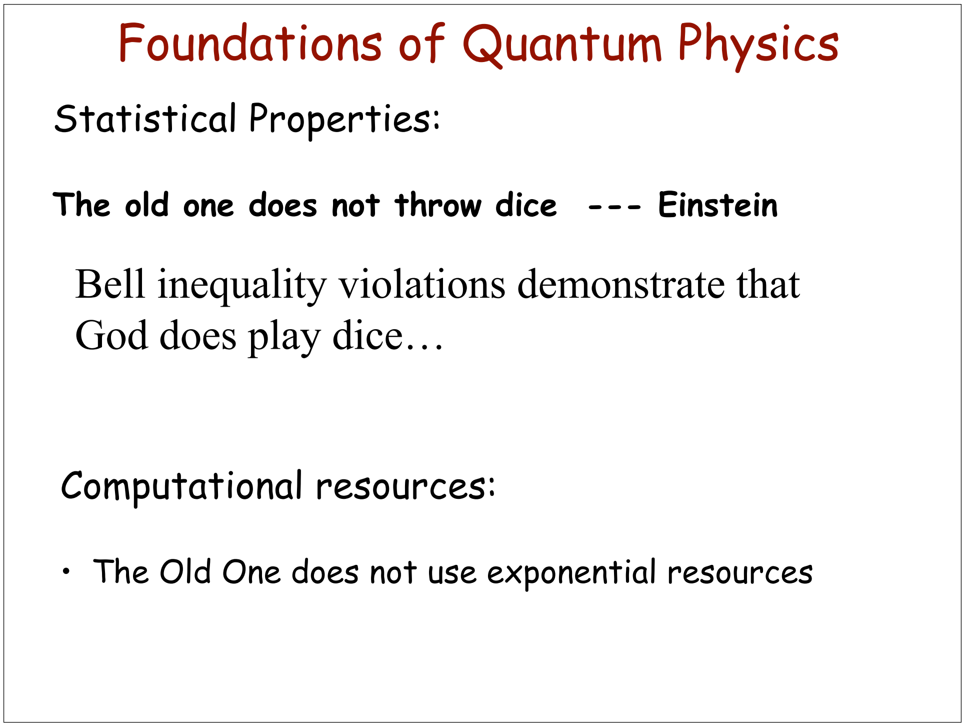
Foundations of Quantum Physics

Statistical Properties:

God does not play dice with the universe --- Einstein

Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. The theory says a lot, but does not really bring us any closer to the secret of the Old One. **I, at any rate, am convinced that He does not throw dice.**

---letter to Max Born 1926.



Foundations of Quantum Physics

Statistical Properties:

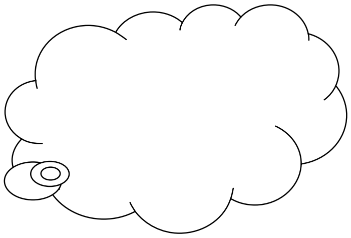
The old one does not throw dice --- Einstein

Bell inequality violations demonstrate that God does play dice…

Computational resources:

- The Old One does not use exponential resources

- Occam’s razor



- Falsifiability

The criterion of *the scientific status of a theory is its **falsifiability**, or refutability, or testability.*

Some theories are more testable, more exposed to refutation, than others; they take, as it were, greater risks.

--Karl Popper

Is Quantum Physics Falsifiable?

- Single particle quantum physics has been verified to exquisite accuracy.
- Multi-particle quantum systems – exponentially hard to compute what the theory predicts.
- Can any theory that requires exponential resources possibly be refuted?

Is Quantum Physics Falsifiable?

- Computer Science Answer: Yes.
- Pick primes p, q and multiply to get N
- Run quantum computer and check if it correctly outputs p and q.
- One-way function – we compute the easy direction!

Conclusions

- Quantum algorithms: tension between exponentially large Hilbert space and small amount of information accessible by measurement.
- Quantum fourier sampling + HSP
- Non-abelian HSP hard for sufficiently non-abelian groups
- Positive consequences of negative results:
  Quantum immune cryptography
  Pretty Good Tomography
- Quantum algorithms provide a falsifiable consequence of multi-particle quantum physics.