Computational Constraints on Scientific Theories:
Insights from Quantum Computation

Umesh Vazirani
U.C. Berkeley
Feynman ‘82: “It has not yet become obvious to me that there’s no real problem (with quantum mechanics).”

“Can I learn anything by asking this question about computers ...”
What have we learned?

Nature appears to expend extravagant resources in:

• Storing the state of a quantum system
• Evolving the state in time
Exponentially Large Hilbert Space
Exponentially Large Hilbert Space

Storing the state

\[ \Psi = \sum_{x} \alpha_x |x\rangle \]

\[ \sum_{x} |\alpha_x|^2 = 1 \]

all n-bit strings

Quantum entanglement
Evolving the state

\[ \Psi = \sum_x \alpha_x |x\rangle \]

\[ \sum_x |\alpha_x|^2 = 1 \]

all n-bit strings
Evolving the state

\[ \Psi = \sum_x \alpha_x |x\rangle \]

\[ \sum_x |\alpha_x|^2 = 1 \]

all n-bit strings
Limited Access - Measurement

\[ \Psi = \sum_{x} \alpha_{x} |x\rangle \]

\[ \sum_{x} |\alpha_{x}|^2 = 1 \]

- Measurement: See \(|x\rangle \) with probability \(|\alpha_{x}|^2\)
Impact on Computer Science

• Rethink the foundations of computational complexity theory

• Quantum computers break modern cryptography - factoring, discrete log, ...
Implications of exponential resources in physics?

• QED – light and electrons

• Structure of atoms, chemical properties

• Novel large scale quantum phenomena
  - Bose-Einstein condensates
  - Lasers
Exponential resources?

- QED - single particle
- Atoms/Molecules - single particle + mean field theories ...
- Bose-Einstein condensates - effectively two-state systems
- Bell states - 2 particle entanglement
• Topological quantum computing
• Fractional Hall effect
• Kitaev’s Honeycomb lattice:

Exact solution. Ground state highly entangled fermionic operators
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.
Statistical Properties:

*God does not play dice with the universe* --- 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.

• What about predictions using mean field approximations/perturbation theory?

• Can any theory that requires exponential resources possibly be refuted?
Computational Complexity Theory

One-way functions:

• $y = f(x)$ can be efficiently computed on input $x$.

• $f$ is hard to invert: given $y$, hard to recover $x = f^{-1}(y)$

E.g. Factoring $N = pq$

Shor’s quantum factoring algorithm.
NMR QC: 15=3x5

[Chuang, et al]

[Braunstein, Caves, Jozsa, Linden, Popescu, Schack]

State of quantum computer is separable mixed state.

Mixture: \( |\phi_1\rangle \otimes \ldots \otimes |\phi_n\rangle \) with probability \( p \)

After application of quantum gate mixture looks entangled, but can be written as equivalent separable mixed state.

Open: Can we perform non-trivial quantum computation in this model.
Infinite Precision?

\[ R_\theta = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \]

Error: \[ \theta \rightarrow \theta \pm \varepsilon \]

\[ \Psi = \sum_x \alpha_x |x\rangle \]

all n-bit strings

\[ U = R_\theta \otimes I \]
Quantum StateTomography
PAC model

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

Problem: Exponential number of parameters to "know" the state.

What can one do?
[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 $|\varphi\rangle$

Distribution $D$ on possible measurements.

Get to see $m$ samples

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

$O(n/\text{poly}(e))$ samples suffice.
Quantum Random Access Codes

[Ambainis, Nayak, Ta-Shma, Vazirani]

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).
**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?

\[
\begin{pmatrix}
M_1 & M_2 & M_3 & \cdots & M_m \\
|\phi_1\rangle & 0 & 1 & 1 & 1 \\
|\phi_2\rangle & 1 & 0 & 0 & 0 \\
|\phi_3\rangle & 0 & 1 & 0 & 1 \\
\vdots & & & & \\
|\phi_k\rangle & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]
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 $d = O(n)$.

\[
\begin{align*}
M_1 & \quad M_2 & \quad M_3 & \quad \cdots & \quad M_m \\
|\phi_1\rangle & \quad 0 & \quad 1 & \quad 1 & \quad 1 \\
|\phi_2\rangle & \quad 1 & \quad 0 & \quad 0 & \quad 0 \\
|\phi_3\rangle & \quad 0 & \quad 1 & \quad 0 & \quad 1 \\
\vdots & & & & & \\
|\phi_k\rangle & \quad 1 & \quad 1 & \quad 1 & \quad 1 
\end{align*}
\]
Classical Simulation of Quantum Systems

- Quantum entanglement necessary for quantum computation.
- Systems with low entanglement can be efficiently simulated.
- Succinct description

Vidal Polynomial time simulation of one dimensional spin chains with $O(\log n)$ entanglement length.

$$\rho_{AC} = \rho_A \otimes \rho_C$$

| A | 1 | B | 2 | C |

$$\rho_{ABC} = \rho_{AB1} \otimes \rho_{B2C}$$
Challenges

• Are there special classes of quantum states for which the learning algorithm is also efficient in time complexity.

• For special classes, can we actually learn the quantum state, not just a predictor for measurements.
Conclusions

• Exponential Hilbert space - challenge + opportunity.

• Quantum algorithms provide a falsifiable consequence of multi-particle quantum physics.

• Learning theory for quantum states and efficiently simulatable quantum systems.

• Efficient classical simulation of special quantum systems.