Quantum Computing with Noninteracting Bosons

Scott Aaronson (MIT)

Based on joint work with Alex Arkhipov

www.scottaaronson.com/papers/optics.pdf

This talk will involve two topics in which Mike Freedman played a pioneering role…

"Quantum computing beyond qubits":
TQFT, nonabelian anyons…
- Yields new links between complexity and physics
- Can provide new implementation proposals

Quantum computing and #P:
Quantum computers can additively estimate the Jones polynomial, which is **#P**-complete to compute exactly

The Extended Church-Turing Thesis (ECT)

Everything feasibly computable in the physical world is feasibly computable by a (probabilistic) Turing machine

But building a QC able to factor n>>15 is **damn** hard!
Can't CS "meet physics halfway" on this one?

I.e., show computational hardness in more easily-accessible quantum systems?

Also, factoring is an extremely "special" problem

Our Starting Point

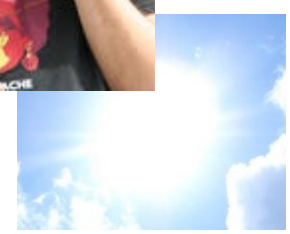
$$\text{Det}(A) = \sum_{\sigma \in S_n} (-1)^{\text{sgn}(\sigma)} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

All I can say is, the bosons got the harder job

FERMIONS

$$\text{Per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

e [Valiant]



BOSONS

This Talk: The Bosons Indeed Got The Harder Job

Valiant 2001, Terhal-DiVincenzo 2002, "folklore":
A QC built of noninteracting fermions can be efficiently simulated by a classical computer

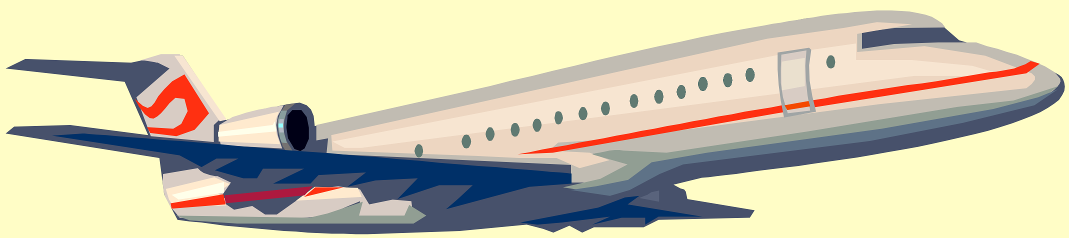
Our Result: By contrast, a QC built of noninteracting **bosons** can solve a sampling problem that's hard for classical computers, under plausible assumptions

The Sampling Problem: Output a matrix $A \sim N(0,1)_C^{n\times n}$ with probability weighted by $|\mathrm{Per}(A)|^2$

But wait!

If n-boson amplitudes correspond to n×n permanents, doesn't that mean "Nature is solving #P-complete

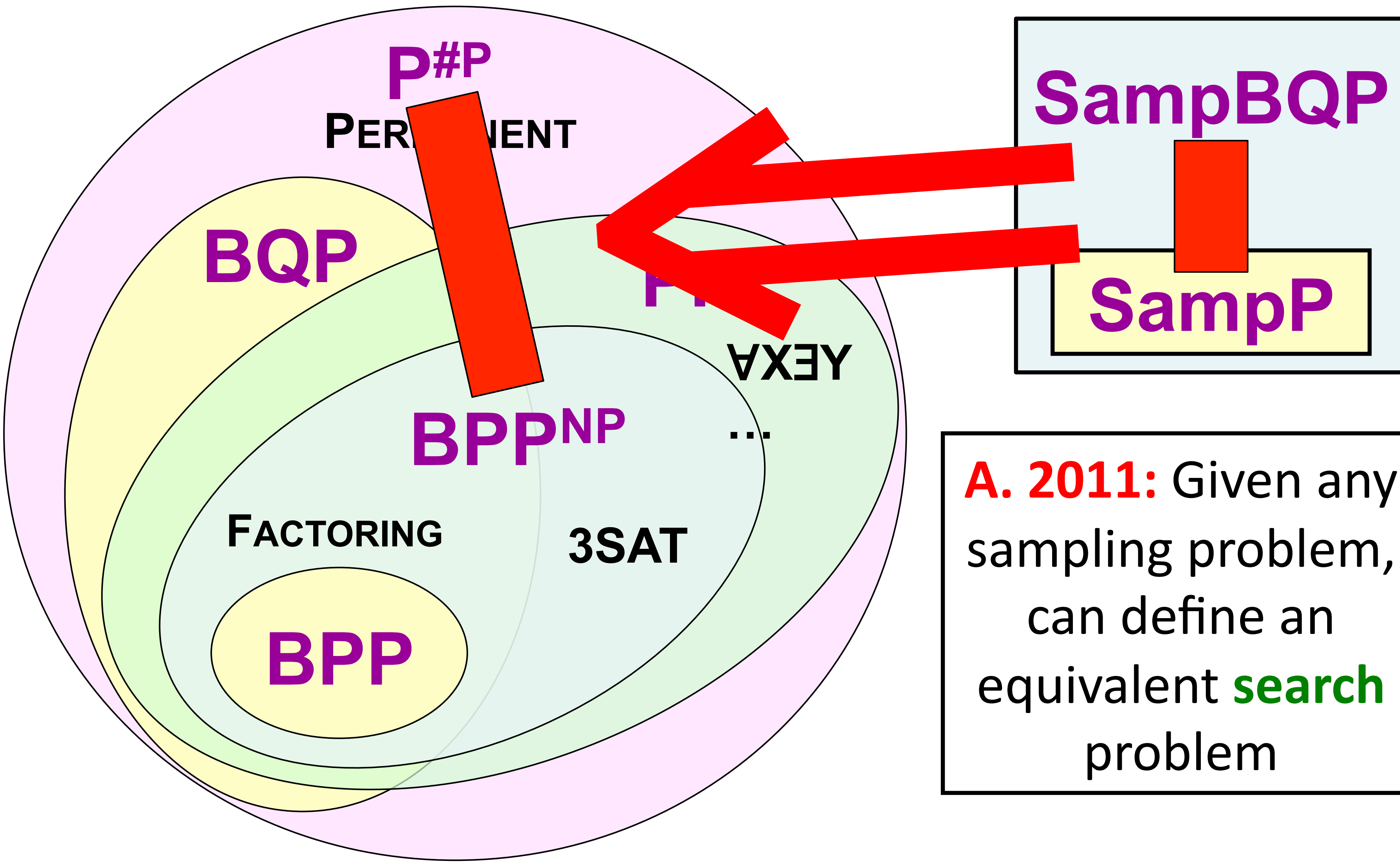
New result (from my flight here): Poly-time randomized algorithm to estimate the probability of **any** final state of a "boson computer," to within ±1/poly(n) additive error



Yes, but only up to additive error $\pm \frac{\|A\|^n}{\mathrm{poly}(n)}$

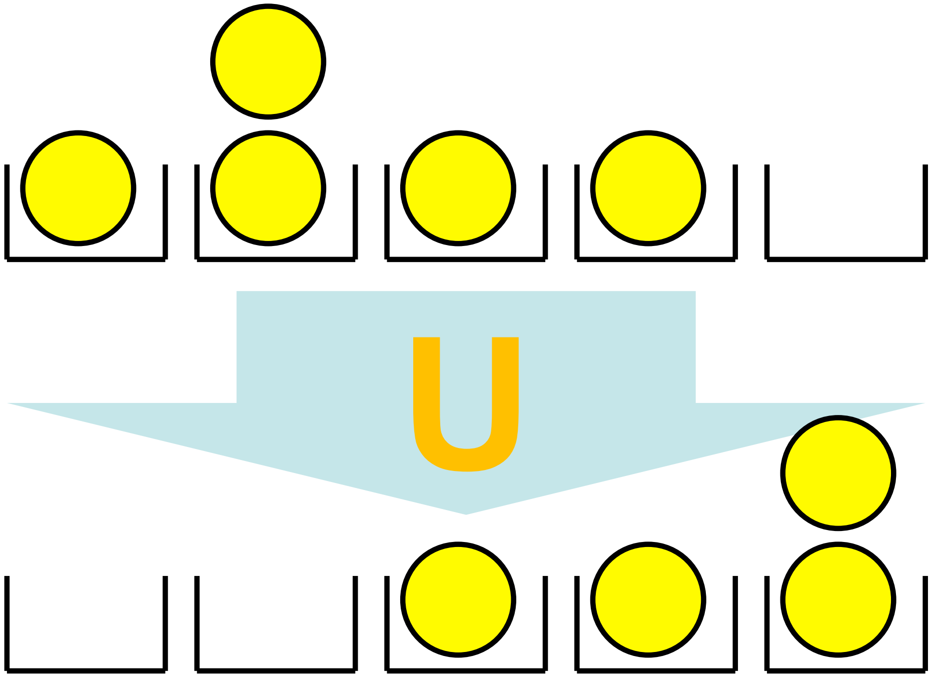
And Gurvits gave a poly-time classical randomized algorithm that estimates $|\mathrm{Per}(A)|^2$ just as well!

Crucial step we take: switching attention to sampling problems



A. 2011: Given any sampling problem, can define an equivalent **search** problem

The Computational Model



Basis states: $|S\rangle = |s_1,\ldots,s_m\rangle$, s_i = # of bosons in i^{th} mode ($s_1+\ldots+s_m = n$)

Standard initial state: $|I\rangle = |1,\ldots,1,0,\ldots\ldots,0\rangle$

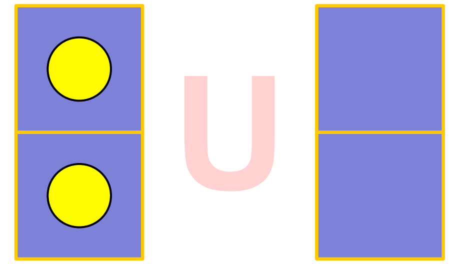
You get to apply any m×m mode-mixing unitary U

U induces a unitary φ(U) on the n-boson states, whose entries are permanents of submatrices of U:

$$\langle S|\varphi(\mathrm{U})|T\rangle = \frac{\mathrm{Per}(U_{S,T})}{\sqrt{s_1!\cdots s_m!\,t_1!\cdots t_m!}}$$

Example: The Hong-Ou-Mandel Dip

Suppose $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.



Then Pr[the two photons land in different modes] is

$$\left| \mathrm{Per}(U) \right|^2 = 0$$

Pr[they both land in the first mode] is

$$\left| \frac{1}{\sqrt{2!}} \mathrm{Per}\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right) \right|^2 = \frac{1}{2}$$

For Card-Carrying Physicists

Our model corresponds to **linear optics**, with single-photon Fock-state inputs and nonadaptive photon-number measurements

Physicists we consulted: "Sounds hard! But not as hard as building a universal QC"

Basi … n of the Hong-Ou-Mandel dip, where n = big as possible

Our main results strongly suggest that such a generalized

Remark: No point in scaling this experiment much beyond 20 or 30 photons, since then a classical computer can't even verify the answers!

Ex

- Reliable single-photon sources
- Reliable photodetector arrays
- Getting a large n-photon coincidence probability

OK, so why is it hard to sample the distribution over photon numbers classically?

Given **any** matrix $A \in C^{n \times n}$, we can construct an $m \times m$ unitary U (where $m \geq 2n$) as follows:

$$U = \begin{pmatrix} \varepsilon A & B \\ C & D \end{pmatrix}$$

Suppose we start with $|I\rangle = |1,\ldots,1,0,\ldots,0\rangle$ (one photon in each of the first n modes), apply U, and measure.

Then the probability of observing $|I\rangle$ again is

$$p := \left| \langle I | \varphi(U) | I \rangle \right|^2 = \varepsilon^{2n} \left| \mathrm{Per}(A) \right|^2$$

Claim 1: p is **#P**-complete to estimate (up to a constant factor)

Idea: Valiant proved that the PERMANENT is **#P**-complete.

Can use a classical reduction to go from a multiplicative approximation of |Per(A)|^2 to Per(A) itself.

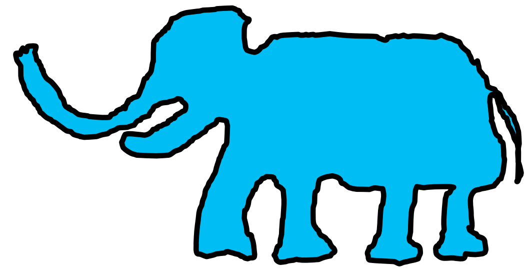
Claim 2: Suppose we had a fast classical algorithm for linear-optics sampling. Then we could estimate p in **BPP^{NP}**

Idea: Let M be our classical sampling algorithm, and let r be its randomness. Use approximate counting to estimate $\Pr_r\left[M(r)\,\text{outputs}\,|I\rangle\right]$

$$p := \left|\langle I|\varphi(U)|I\rangle\right|^2 = \varepsilon^{2n}\left|\mathrm{Per}(A)\right|^2$$

Conclusion: Suppose we had a fast classical algorithm for linear-optics sampling. Then **P$^{\#P}$**=**BPP^{NP}**.

The Elephant in the Room



Our whole result hinged on the difficulty of estimating a **single, exponentially-small probability** p—but what about noise and error?

The "right" question: can a classical computer efficiently sample a distribution with **1/poly(n) variation distance** from the linear-optical distribution?

Our Main Result: Suppose it can. Then there's a **BPP^{NP}** algorithm to estimate $|Per(A)|^2$, with high probability over a Gaussian matrix $A \sim N(0,1)_{C}^{n \times n}$

Our Main Conjecture

Estimating $|\text{Per}(A)|^2$, for most Gaussian matrices A, is a **#P**-hard problem

If the conjecture holds, then even a **noisy** n-photon

Hong-

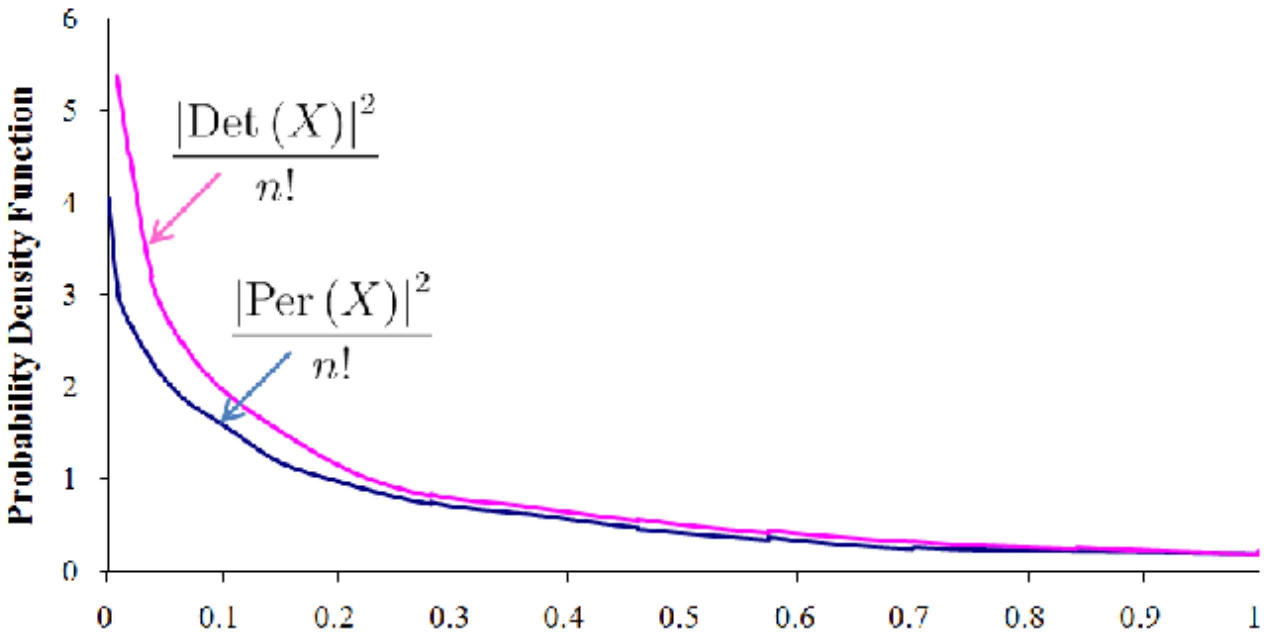
Extenc

Most c e for

this co

We car

“calcul



First step: Understand the **distribution** of $|\text{Per}(A)|^2$ for Gaussian A

Related Result: The KLM Theorem

Theorem (Knill, Laflamme, Milburn 2001): Linear optics with **adaptive measurements** can do universal QC

Yields an alternate proof of our first result (fast **exact** classical algorithm $\Rightarrow$ $P^{\#P} = BPP^{NP}$)

A., last month: KLM also yields an alternate proof of Valiant's Theorem, that the permanent is **#P**-complete!

To me, more "intuitive" than Valiant's original proof

Similarly, **Kuperberg 2009** used Freedman-Kitaev-Larsen-Wang to reprove the **#P**-hardness of the Jones polynomial

Open Problems

Prove our main conjecture ($1,000)!

Can our model solve classically-intractable **decision** problems?

Similar hardness results for other quantum systems (besides noninteracting bosons)?

> **Bremner, Jozsa, Shepherd 2010:** QC with commuting Hamiltonians can sample hard distributions

Fault-tolerance within the noninteracting-boson model?