“The Computational Complexity of Linear Optics” by Scott Aaronson and Alex Arkhipov

arXiv:1011.3245

Maris Ozols

April 21, 2011

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

Which one do we believe in?

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

Which one do we believe in?

- Shor's algorithm
  $\Rightarrow$ You can't simulate a quantum computer
  unless you can factor efficiently!

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

Which one do we believe in?

- Shor's algorithm
  $\Rightarrow$ You can't simulate a quantum computer
  unless you can factor efficiently!
- This result
  $\Rightarrow$ You can't simulate a quantum computer
  unless...

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

Which one do we believe in?

- Shor's algorithm
  $\Rightarrow$ You can't simulate a quantum computer unless you can factor efficiently!
- This result
  $\Rightarrow$ You can't simulate a quantum computer unless... something bad happens...

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

Which one do we believe in?

- Shor's algorithm
  $\Rightarrow$ You can't simulate a quantum computer unless you can factor efficiently!
- This result
  $\Rightarrow$ You can't simulate a quantum computer unless. . . something bad happens. . .

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

Which one do we believe in?

- Shor's algorithm
  $\Rightarrow$ You can't simulate a quantum computer unless you can factor efficiently!
- This result
  $\Rightarrow$ You can't simulate a quantum computer unless. . . something bad happens. . .

The BIG dilemma...

The great dream

Quantum computers are more powerful than classical computers

The sad possibility

Church–Turing thesis: Everything that is efficiently computable by any physical device is efficiently computable by a Turing machine

Which one do we believe in?

- Shor's algorithm
  $\Rightarrow$ You can't simulate a quantum computer unless you can factor efficiently!
- This result
  $\Rightarrow$ You can't simulate a quantum computer unless...something bad happens...

Polynomial hierarchy collapses!

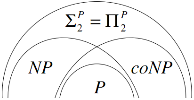
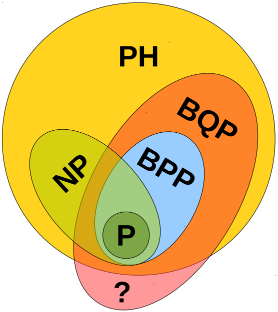


PHOTO: The scene of the devastation.

Complexity theory crash course



Complexity classes

- P – polynomial time
- NP – non-deterministic polynomial time
- PH – polynomial hierarchy (2nd order logic)
- BPP – bounded-error probabilistic polynomial time
- BQP – bounded-error quantum polynomial time

Computation with non-interacting bosons

Model of computation

- Parameters: n photons in $m = \mathrm{poly}(n)$ modes
- State space: $\mathrm{span}\{|s_1, \ldots, s_m\rangle : s_k \geq 0, \sum_{k=1}^m s_k = n\}$
- Initial state: $|1_n\rangle := |1, \ldots, 1, 0, \ldots, 0\rangle$
- Transformations: $\varphi_n(U)$ for any $U \in \mathrm{U}(m)$, where φ_n extends the action from 1 to n photons
- Measurement: the number of photons in each mode

The BosonSampling problem

Given a description of $U \in \mathrm{U}(m)$, produce samples from the probability distribution

$$\Pr[S] := |\langle S|\varphi_n(U)|1_n\rangle|^2$$

Transition matrix

Definition

If $|S\rangle = |s_1, \ldots, s_m\rangle$ and $|T\rangle = |t_1, \ldots, t_m\rangle$ then φ_n is defined as

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1! \cdots s_m! t_1! \cdots t_m!}}$$

where $A_{S,T}$ is the $n \times n$ matrix obtained by taking s_i copies of the ith row and t_j copies of jth column of A

Transition matrix

Definition

If $|S\rangle = |s_1, \ldots, s_m\rangle$ and $|T\rangle = |t_1, \ldots, t_m\rangle$ then φ_n is defined as

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1! \cdots s_m! t_1! \cdots t_m!}}$$

where $A_{S,T}$ is the $n \times n$ matrix obtained by taking s_i copies of the ith row and t_j copies of jth column of A

Example

$$\varphi_2 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{array}{c} |10\rangle \\ |01\rangle \end{array} \mapsto \begin{pmatrix} a^2 & \sqrt{2}ab & b^2 \\ \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ c^2 & \sqrt{2}cd & d^2 \end{pmatrix} \begin{array}{c} |20\rangle \\ |11\rangle \\ |02\rangle \end{array}$$

Transition matrix

Definition

If $|S\rangle = |s_1, \ldots, s_m\rangle$ and $|T\rangle = |t_1, \ldots, t_m\rangle$ then φ_n is defined as

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1! \cdots s_m! t_1! \cdots t_m!}}$$

where $A_{S,T}$ is the $n \times n$ matrix obtained by taking s_i copies of the ith row and t_j copies of jth column of A

Example

$$\varphi_2 : \begin{array}{cc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \begin{array}{c} |10\rangle \\ |01\rangle \end{array} \end{array} \mapsto \begin{array}{cc} \begin{pmatrix} a^2 & \sqrt{2}ab & b^2 \\ \sqrt{2}ac & ad + bc & \sqrt{2}bd \\ c^2 & \sqrt{2}cd & d^2 \end{pmatrix} & \begin{array}{c} |20\rangle \\ |11\rangle \\ |02\rangle \end{array} \end{array}$$

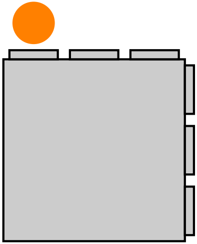
Properties

- φ_n is a homomorphism: $\varphi_n(A \cdot B) = \varphi_n(A) \cdot \varphi_n(B)$
- if U is unitary then so is $\varphi_n(U)$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

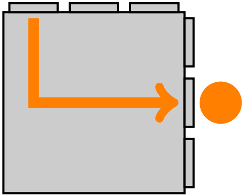
The magic box



Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1! \cdots s_m! t_1! \cdots t_m!}}$$

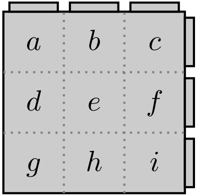
The magic box



Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m! t_1! \cdots t_m!}}$$

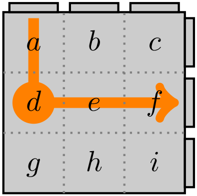
The magic box



Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

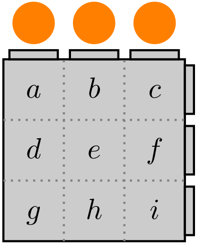
The magic box



Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m! t_1!\cdots t_m!}}$$

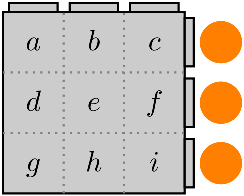
The magic box



Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\operatorname{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

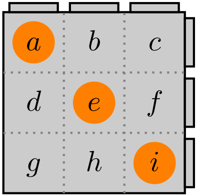
The magic box



Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box

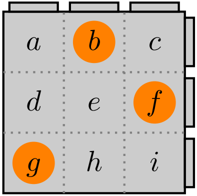


aei

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box

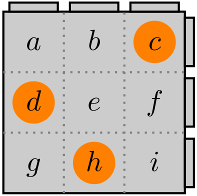


$$aei + gbf$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box

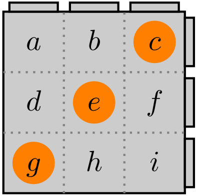


$$aei + gbf + dhc$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box

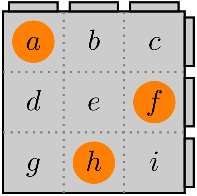


$$aei + gbf + dhc + gec$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box

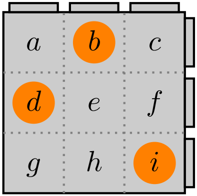


$$aei + gbf + dhc + gec + ahf$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box

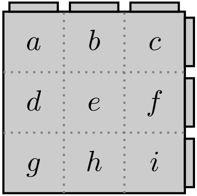


$$aei + gbf + dhc + gec + ahf + dbi$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m! t_1! \cdots t_m!}}$$

The magic box



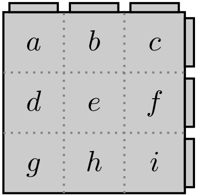
$$aei + gbf + dhc + gec + ahf + dbi$$

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

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box



$$aei + gbf + dhc + gec + ahf + dbi$$

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

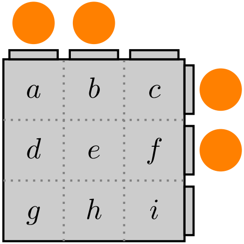
Definition

$$\mathrm{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m! t_1!\cdots t_m!}}$$

The magic box



$$aei + gbf + dhc + gec + ahf + dbi$$

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

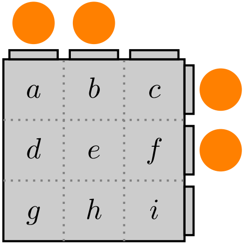
Definition

$$\mathrm{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box



$$\mathrm{perm}\begin{pmatrix} a & b \\ d & e \end{pmatrix}$$

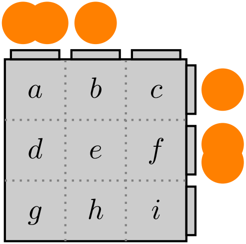
Definition

$$\mathrm{perm}(A) = \sum_{\sigma\in S_n}\prod_{i=1}^{n} A_{i,\sigma(i)}$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box



$$\mathrm{perm}\begin{pmatrix} a & b \\ d & e \end{pmatrix}$$

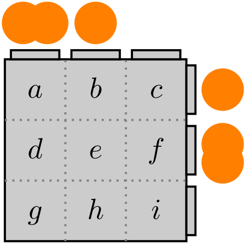
Definition

$$\mathrm{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\mathrm{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box



$$\mathrm{perm}\begin{pmatrix} a & a & b \\ d & d & e \\ d & d & e \end{pmatrix}$$

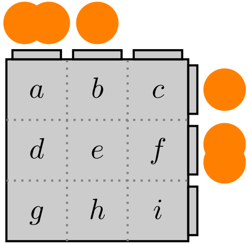
Definition

$$\mathrm{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A_{i,\sigma(i)}$$

Permanent

$$\langle S|\varphi_n(A)|T\rangle = \frac{\text{perm}(A_{S,T})}{\sqrt{s_1!\cdots s_m!t_1!\cdots t_m!}}$$

The magic box



$$\text{perm}\begin{pmatrix} a & a & b \\ d & d & e \\ d & d & e \end{pmatrix}$$

Definition

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

Theorem (Valiant '79)

Computing $\text{perm}(A)$ is #P-hard

Main results

Theorem (exact case)

The exact BosonSampling problem is not efficiently solvable by a classical computer, unless polynomial hierarchy collapses

Main results

Theorem (exact case)

The exact BosonSampling problem is not efficiently solvable by a classical computer, unless polynomial hierarchy collapses

Theorem (approximate case)

If the following two conjectures are true:

1. the permanent of a random Gaussian matrix is #P-hard to approximate and
2. it is not too concentrated around 0

then it is not possible to approximately solve the BosonSampling problem, unless polynomial hierarchy collapses

Experimental feasibility

Linear optics

- prepare photons using single photon sources
- use beam splitters and phase shifters to implement U
- use photodetectors to perform the readout
- the order of parameters: $n = 10$, $m = 20$

Experimental feasibility

Linear optics

- prepare photons using single photon sources
- use beam splitters and phase shifters to implement U
- use photodetectors to perform the readout
- the order of parameters: $n = 10$, $m = 20$

Good

- easier to build than a full-scale QC (no interaction between pairs of photons needed)
- photons are never used as qubits (no need to store them)

Experimental feasibility

Linear optics

- prepare photons using single photon sources
- use beam splitters and phase shifters to implement U
- use photodetectors to perform the readout
- the order of parameters: $n = 10$, $m = 20$

Good

- easier to build than a full-scale QC (no interaction between pairs of photons needed)
- photons are never used as qubits (no need to store them)

Problems

- need good photon sources and detectors
- all n photons must arrive at the destination at the same time

Thank you!