RMT and boson computers

[Aaronson-Arkhipov 2011]

John Napp

May 11, 2016

Introduction

- Simple type of quantum computer proposed in 2011 by Aaronson and Arkhipov based on the statistics of noninteracting bosons
- The computer A outputs a sample from a probability distribution $\mathcal{D}_A$
- They prove that if there exists a classical algorithm that can efficiently output a sample from a distribution close to $\mathcal{D}_A$, then $\mathrm{P}^{\#\mathrm{P}} = \mathrm{BPP}^{\mathrm{NP}}$: a drastic consequence for complexity theory!
- Among the strongest evidence to date that quantum computers have capabilities beyond classical computers.
- Proof relies on random matrix techniques, and requires two unproven RMT conjectures

Complexity Preliminaries

- **Definition ($\#$P)**

  A function $f : \{0,1\}^* \to \mathbb{N}$ is in $\#$P if there exists a polynomial $p : \mathbb{N} \to \mathbb{N}$ and a polynomial-time TM M such that for every $x \in \{0,1\}^*$:

  $$f(x) = \left|\left\{ y \in \{0,1\}^{p(|x|)} : M(x,y) = 1 \right\}\right|$$

- **Theorem (Valiant)**

  The following problem is $\#\mathrm{P}$-complete: given a matrix $X \in \{0,1\}^{n\times n}$, compute $\mathrm{Per}(X)$.

- **Theorem (Aaronson-Arkhipov)**

  The following problem is $\#\mathrm{P}$-hard, for any $g \in [1, poly(n)]$: given a matrix $X \in \mathbb{R}^{n\times n}$, approximate $\mathrm{Per}(X)^2$ to within a multiplicative factor of g.

Complexity Preliminaries (2)

- BPP: class of languages efficiently decided with high probability by a probabilistic TM
- $\mathsf{BPP}^{\mathsf{NP}}$ machine: a BPP machine that can also solve NP-complete problems in a single step
- $\mathsf{P}^{\#\mathsf{P}}$ machine: a P machine that can compute $\#$P-complete functions in a single step
- Stockmeyer: a $\mathsf{BPP}^{\mathsf{NP}}$ machine can efficiently estimate the acceptance probability of a BPP machine
- Widely believed that $\mathsf{BPP}^{\mathsf{NP}} \subsetneq \mathsf{P}^{\#\mathsf{P}}$ (can only prove $\mathsf{BPP}^{\mathsf{NP}} \subseteq \mathsf{P}^{\#\mathsf{P}}$)

Preview: Gaussian Permanent Estimation problems

- $|\text{GPE}|^2_{\pm}$: Given as input a matrix $X \sim \mathcal{N}(0,1)^{n\times n}_{\mathbb{C}}$ of iid Gaussians, together with error bounds $\varepsilon, \delta > 0$, estimate $|\text{Per}(X)|^2$ to within additive error $\pm\varepsilon \cdot n!$, with probability at least $1-\delta$ over X, in *poly*$(n, 1/\varepsilon, 1/\delta)$ time.

- $\text{GPE}_{\times}$: Given as input a matrix $X \sim \mathcal{N}(0,1)^{n\times n}_{\mathbb{C}}$ of iid Gaussians, together with error bounds $\varepsilon, \delta > 0$, estimate $\text{Per}(X)$ to within $\pm\varepsilon \cdot |\text{Per}(X)|$, with probability at least $1-\delta$ over X, in *poly*$(n, 1/\varepsilon, 1/\delta)$ time.

Preview: RMT conjectures

- Permanent-of-Gaussians Conjecture (PGC): $\mathrm{GPE}_\times$ is $\#$P-hard.

- Permanent Anti-Concentration Conjecture (PACC): There exists a polynomial p such that for all n and $\delta > 0$,

$$\Pr_{X \sim \mathcal{N}(0,1)_{\mathbb{C}}^{n \times n}} \left[|\mathrm{Per}(X)| < \frac{\sqrt{n!}}{p(n, 1/\delta)} \right] < \delta$$

- Theorem: if PACC is true, then $\mathrm{GPE}_\times$ and $|\mathrm{GPE}|_\pm^2$ are equivalent

BosonSampling

- n photons sent through linear optical network. Can end up in m possible photodetectors, for $m \geq n$.
- Description of network encoded by $m \times n$ column-orthonormal complex matrix $A \in \mathcal{U}_{m,n}$
- Output of computer: measurement of how many photons end up in each photodetector.
  - $S \in \Phi_{m,n}$, where $\Phi_{m,n}$ is the set of tuples $(s_1, \ldots, s_m)$ s.t. $s_i \geq 0$ and $\sum s_i = n$
- By quantum mechanics, output distribution of computer is

$$\Pr_{\mathcal{D}_A}[S] = \frac{|\mathrm{Per}(A_S)|^2}{s_1! \cdots s_m!}$$

where A_S is $n \times n$ matrix constructed by keeping s_i copies of row i of A

Exact BosonSampling $\implies \mathsf{P}^{\#\mathsf{P}} = \mathsf{BPP}^{\mathsf{NP}}$

- Assume $\exists$ a classical algorithm $\mathcal{O}(A, r)$ for $A \in \mathcal{U}_{m,n}$ and r a string s.t. the distribution of $\mathcal{O}$ over r is $\mathcal{D}_A$.
- Then with $\mathsf{BPP}^{\mathsf{NP}}$ machine, we can compute the squared permanent of an arbitrary real matrix X: a $\#$P-hard problem!
  - Embed scaled X as a submatrix of $A \in \mathcal{U}_{m,n}$ (can prove this is possible)
  - Now a certain output probability is proportional to the squared permanent of X (exponentially small due to scaling during the embedding)
  - Use Stockmeyer result to compute this probability with a $\mathsf{BPP}^{\mathsf{NP}}$ machine
- $\mathsf{P}^{\#\mathsf{P}} = \mathsf{BPP}^{\mathsf{NP}}$

The problem with the above result

- The classical algorithm $\mathcal{O}$ used above was assumed to sample exactly from $\mathcal{D}_A$.
- Not physically reasonable - due to noise, even a boson computer can't sample exactly from $\mathcal{D}_A$!
- To be reasonable, let $\mathcal{O}$ sample from some distribution $\mathcal{D}'_A$ s.t. $\|\mathcal{D}'_A - \mathcal{D}_A\| < \varepsilon$ in variation distance.
- But this ruins the above result! If $\mathcal{O}$ were adversarial and knew where we embedded X in A, it could concentrate its error on the probability corresponding to the permanent of X, and so a $\mathsf{BPP}^{\mathsf{NP}}$ machine would no longer be able to use $\mathcal{O}$ to estimate the squared permanent.
- Solution: "smuggle" X into A with the help of RMT, so $\mathcal{O}$ has no way of detecting where the embedded X is in A.

Haar-Unitary Hiding Theorem

- $\mathcal{H}_{m,n}$: Haar measure over $m \times n$ column-orthonormal matrices
- $\mathcal{S}_{m,n}$: Distribution obtained by drawing $U \sim \mathcal{H}_{m,m}$, and outputting $\sqrt{m} U_{n,n}$
- $\mathcal{G}^{n \times n}$: Distribution of complex $n \times n$ matrices with iid standard complex Gaussian entries

Theorem

Let $m \geq \frac{n^5}{\delta} \log^2 \frac{n}{\delta}$, for any $\delta > 0$. Then $\|\mathcal{S}_{m,n} - \mathcal{G}^{n \times n}\| = O(\delta)$.

- $m^{1/6} \times m^{1/6}$ truncations of $m \times m$ unitaries look like iid Gaussians

Hiding Lemma

Lemma

Let $m \geq \frac{n^5}{\delta} \log^2 \frac{n}{\delta}$ for some $\delta > 0$. Then there exists a $\mathsf{BPP}^{\mathsf{NP}}$ *algorithm $\mathcal{A}$ that takes as input a matrix $X \sim \mathcal{G}^{n \times n}$, that "succeeds" with probability* $1 - O(\delta)$ *over X, and that, conditioned on succeeding, samples a matrix $A \in \mathcal{U}_{m,n}$ from a probability distribution $\mathcal{D}_X$, such that the following properties hold:*

i) *$X/\sqrt{m}$ occurs as a uniformly-random $n \times n$ submatrix of $A \sim \mathcal{D}_X$, for every X such that* $\Pr[\mathcal{A}(X)$ *succeeds*$] > 0$.

ii) *The distribution over $A \in \mathbb{C}^{m \times n}$ induced by drawing $X \sim \mathcal{G}^{n \times n}$, running $\mathcal{A}(X)$, and conditioning on $\mathcal{A}(X)$ succeeding is simply $\mathcal{H}_{m,n}$.*

Hiding Lemma - proof strategy

- Sample $X \sim \mathcal{G}^{n \times n}$
- Using rejection sampling and the previous theorem, with high probability turn X into a sample from $\mathcal{S}_{m,n}$
- Define $\mathcal{D}_X$ as sampling from $\mathcal{H}_{m,n}$, conditioned on X appearing as a submatrix (up to scaling).
- Complexity theory: $\mathsf{BPP}^{\mathsf{NP}}$ machine can produce sample from $\mathcal{D}_X$
- By symmetry, distribution of outputs is $\mathcal{H}_{m,n}$

Approximate BosonSampling

- Assuming $\exists$ approximate classical sampler $\mathcal{O}$, want to prove $|\text{GPE}|^2_{\pm} \in \text{BPP}^{\text{NP}}$
- Generate sample $X \sim \mathcal{G}^{n \times n}$
- With high probability, use the Hiding Lemma to smuggle X into a matrix $A \in \mathcal{U}_{m,n}$
- With X smuggled into A, we can compute the squared permanent of X with BPP^{NP} machine as before, up to $\pm$ error
- Since $A \sim \mathcal{H}_{m,n}$ and $X \sim \mathcal{S}_{m,n}$, adversarial $\mathcal{O}$ can't corrupt: no way of knowing where the smuggled X is!
- Assuming RMT conjectures, $|\text{GPE}|^2_{\pm}$ is $\#$P-hard problem, hence $\text{P}^{\#\text{P}} = \text{BPP}^{\text{NP}}$ as desired.

Permanent of Gaussians Conjecture

PGC: $\mathrm{GPE}_\times$ is $\#$P-hard.

- Plausible for complexity-theoretic reasons
- Analogous result is true for finite fields. Just need to generalize to $\mathbb{C}$

Permanent Anti-Concentration Conjecture

PACC: There exists a polynomial p such that for all n and $\delta > 0$,

$$\Pr_{X \sim \mathcal{N}(0,1)_{\mathbb{C}}^{n \times n}} \left[|\mathrm{Per}(X)| < \frac{\sqrt{n!}}{p(n, 1/\delta)} \right] < \delta$$

- Standard deviation of $\mathrm{Per}(X)$ is $\sqrt{n!}$.
- PACC: probability mass of $\mathrm{Per}(X)$ does not concentrate at very small values relative to σ

Some PACC Evidence

- Tao-Vu (2009): For all $\varepsilon > 0$ and sufficiently large *n*,

$$\Pr_{X \in \{-1,1\}^{n \times n}} \left[|\mathrm{Per}(X)| < \frac{\sqrt{n!}}{n^{\varepsilon n}} \right] < \frac{1}{n^{0.1}}$$

- Aaronson-Arkhipov (Weak PACC): For all $\alpha < 1$,

$$\Pr_{X \sim \mathcal{G}^{n \times n}} \left[|\mathrm{Per}(X)|^2 \geq \alpha \cdot n! \right] > \frac{(1-\alpha)^2}{n+1}.$$

- Conjecture is proven for determinant instead of permanent
- Supported by numerics

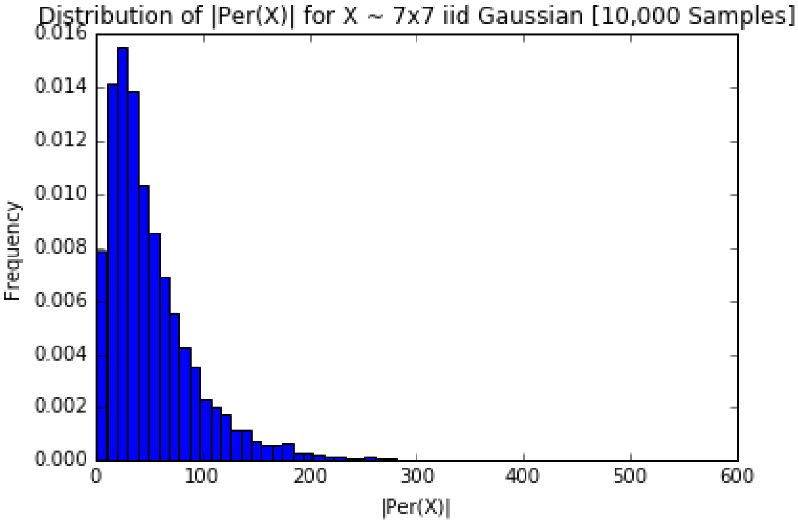

Figure 1: Distribution of $|\mathrm{Per}(X)|$ for $X \sim \mathcal{G}^{7\times 7}$. 10,000 samples were taken. Note that $\sqrt{7!} \approx 71$.