Title: BosonSampling with a linear number of modes

Speakers:

Collection: Foundations of Quantum Computational Advantage

Date: April 30, 2024 - 1:00 PM

URL: https://pirsa.org/24050014

Abstract: BosonSampling is one of the leading candidate models for a demonstration of quantum computational advantage. However, there are still important gaps between our best theoretical results and what can be implemented realistically in the laboratory. One of the largest gaps concerns the scaling between the number of modes (m) and number of photons (n) in the experiment. The original proposal by Aaronson and Arkhipov, as well as all subsequent improvements, required m to scale as n^2, whereas most state-of-the-art typically operate in a regime where m is linear in n. In this talk, I will describe how our recent work bridges this gap by providing evidence that BosonSampling remains hard even for m as low as 2n. I will review the template for proofs of computational advantage used in BosonSampling and other proposals, and discuss how we solved the new challenges that appear in this regime.

BosonSampling with a linear number of modes

Daniel J. Brod (Universidade Federal Fluminense)

https://arxiv.org/abs/2312.00286

Joint work with: A. Bouland, I. Datta, B. Fefferman, D. Grier, F. Hernandez and M. Oszmaniec

Foundations of quantum computational advantage
April 2024

Quantum computational advantage

- Building a universal quantum computer is really hard![citation needed]
- Demonstration of "raw computational power" in the near future?
- Several proposals:
  - BosonSampling (standard, scattershot, Gaussian);
  - Random circuit sampling;
  - Alternatives (circuits of commuting gates, magic-state fermionsampling, and a host of others);

Quantum computational advantage

- Building a universal quantum computer is really hard! [citation needed]
- Demonstration of “raw computational power” in the near future?
- Several proposals:
  - BosonSampling (standard, scattershot, Gaussian);
  - Random circuit sampling;
  - Alternatives (circuits of commuting gates, magic-state fermionsampling, and a host of others);

Quantum computational advantage

- Building a universal quantum computer is really hard![citation needed]
- Demonstration of "raw computational power" in the near future?
- Several proposals:
  - BosonSampling (standard, scattershot, Gaussian);

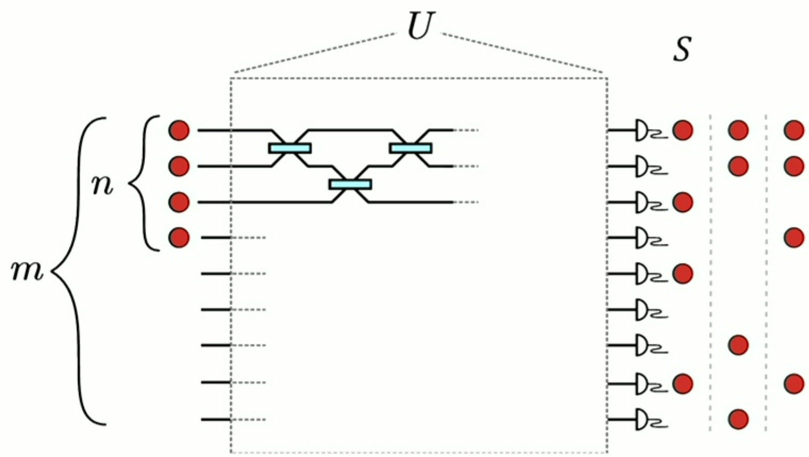
This work:

- Theoretical advances in BosonSampling.
- Improved scaling: BosonSampling works if modes grow only linearly with number of photons.
- Comparable evidence to previous results (quadratic scaling).

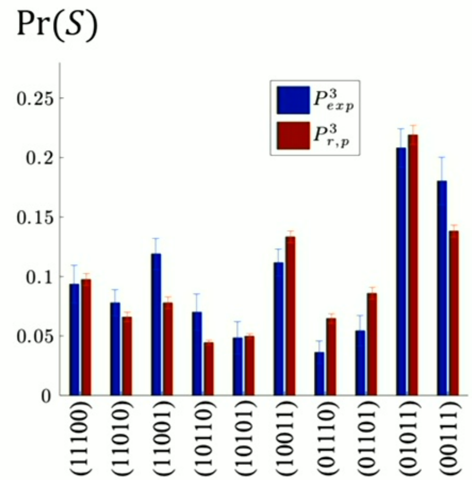
Summary

- BosonSampling 101
- Outline of original hardness proof
- BosonSampling when $m = O(n)$
- Summary and outlook

BosonSampling 101



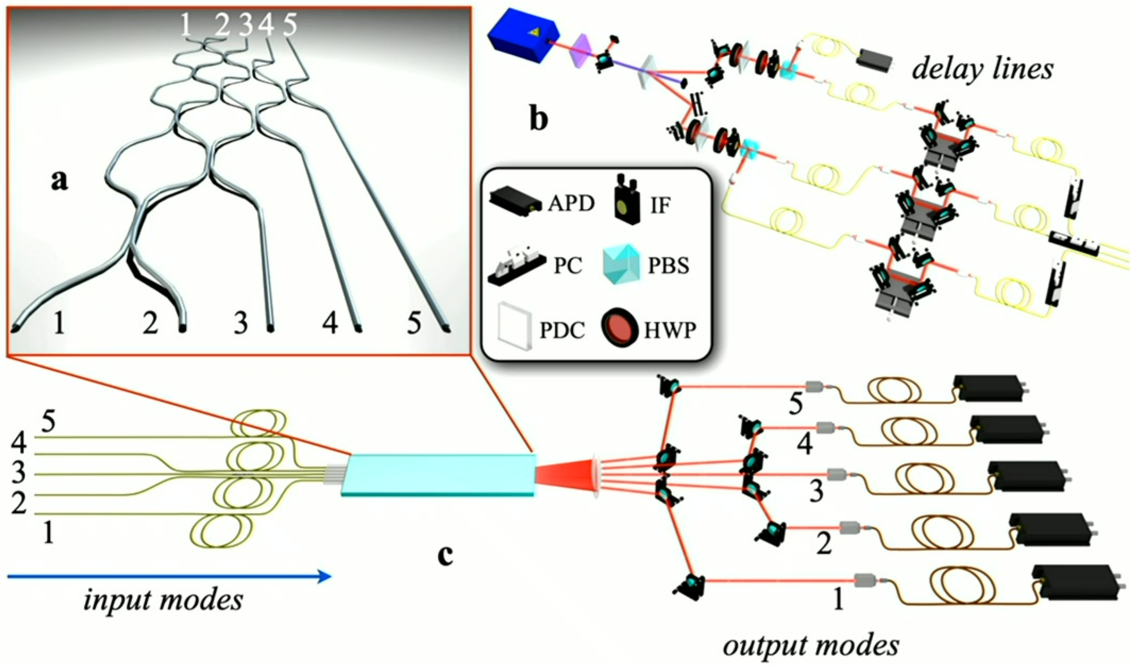
$a_i \rightarrow \sum_j U_{ij} a_j$



$S = (s_1, s_2, \dots s_m)$

Distribution $\mathcal{D}_U$

First experiments (12/2012)



[Broome *et al*, Science **339**, 794 (2013). Spring *et al*, Science **339**, 798 (2013). Tillman *et al*, Nat. Phot. **7**, 540 (2013). Crespi *et al*, Nat. Phot. **7**, 545 (2013).]

BosonSampling 101

- **Computational task**: Sample from output distribution $\mathcal{D}_U$.
  - For a quantum device, this is "easy";
  - There is evidence that it is very hard for classical computers!

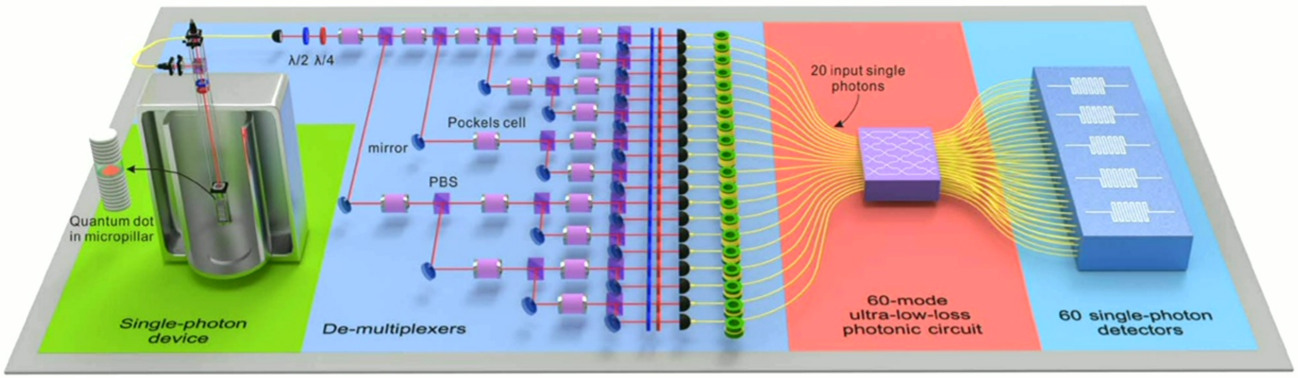
$$\mathcal{D}_U : \Pr(T \to S) \propto |Per(U_{ST})|^2$$

  - Permanent for n-photon transition: time $O(n2^n)$
  - Even approximate simulation is hard!

$$\widetilde{\mathcal{D}}_U : \|\widetilde{\mathcal{D}}_U - \mathcal{D}_U\|_1 < \epsilon$$

[Aaronson e Arkhipov, Theo. Comput. **9,** 143 (2013)]

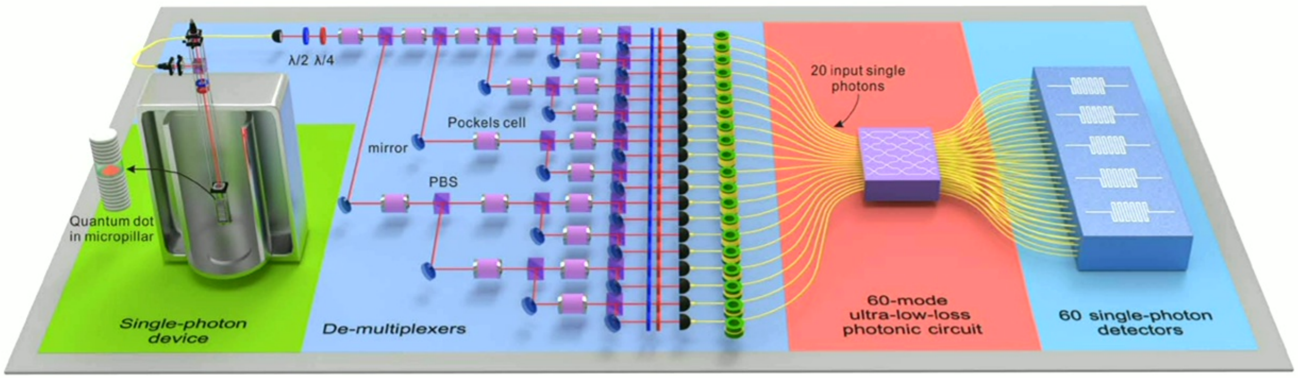
Experimental advances



- 20 photons in 60 modes;
- Largest (?) experiment within original BS proposal;
  - Uses quantum dot sources.

[Wang *et al,* PRL **123**, 250503 (2019)]

Experimental advances



- 20 photons in 60 modes;
- Largest (?) experiment within original BS proposal;
  - Uses quantum dot sources.
- Larger experiments with variants (GBS).

[Wang *et al,* PRL **123**, 250503 (2019)]

Experimental advances

- Larger experiments with variants of BosonSampling;

	n photons	m modes
USTC '20	45	100
USTC '21	113	144
Xanadu '22	125	216
USTC '23	255	144

- Important caveat:
  - Theoretical result needs $m = O(n^2)$; experiments far* from it.

BosonSampling 101 – Main proof outline

- Step 1: From distributions to probabilities;
  - Very generic step – used in most proposals.
- Step 2: From probabilities to hard functions (permanents);
  - Specific to each proposal (BosonSampling, GBS, RCS, etc).
- Step 3: Enter the conjectures (i.e., where the magic happens);
  - Also specific to each proposal.

[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

- Step 1: From distributions to probabilities;
- Assumption: efficient classical algorithm C to sample from $\widetilde{\mathcal{D}}_U$:

$$\|\widetilde{\mathcal{D}}_U - \mathcal{D}_U\|_1 < \epsilon$$

Input: U ⟶

[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

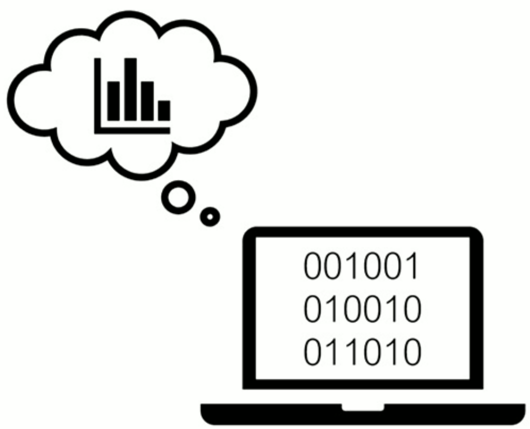
- Step 1: From distributions to probabilities;
- Suppose: Given outcome S, there is a class of states ($\mathcal{H}_S$) that "look the same" as S.
  - e.g., If U is Haar-random

    $\Rightarrow \mathcal{H}_S$: all outcomes related to S by permutation of modes.
- Use Stockmeyer's algorithm;

[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

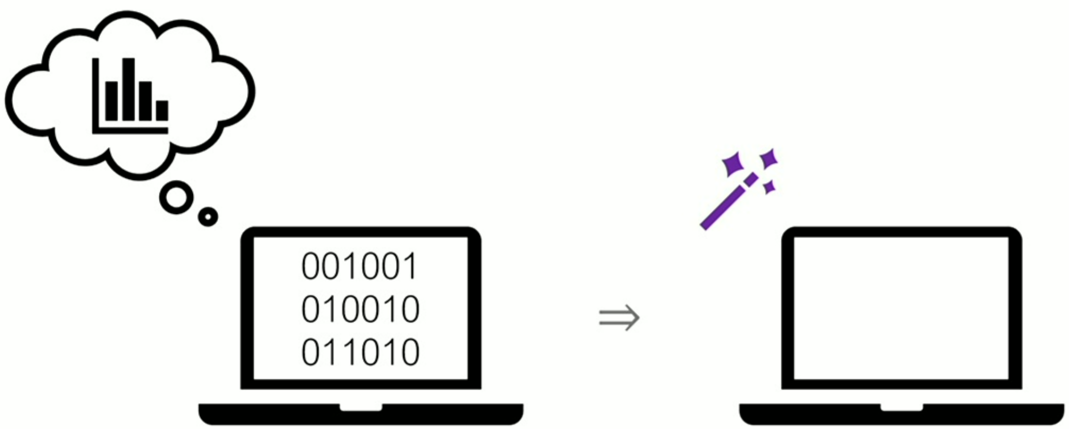
- Step 1: From distributions to probabilities;
- Conclusion: Moderately superpowerful classical machine (BPP^{NP}) can efficiently estimate $\mathbf{Pr}(S)$ to error $\frac{\epsilon}{|\mathcal{H}_S|}$



[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

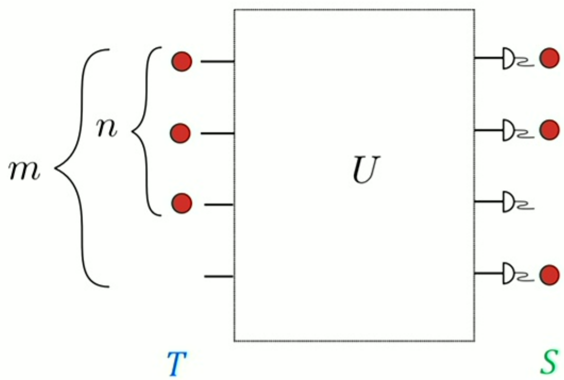
- Step 1: From distributions to probabilities;
- Conclusion: Moderately superpowerful classical machine (BPP^{NP}) can efficiently estimate $\mathbf{Pr}(S)$ to error $\frac{\epsilon}{|\mathcal{H}_S|}$



[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

- Step 2: From probabilities to hard functions;
- For BosonSampling, sort-of trivial:



$$\Pr(T \to S) = \frac{1}{s_1! \ldots s_m!} |Per(U_{ST})|^2$$

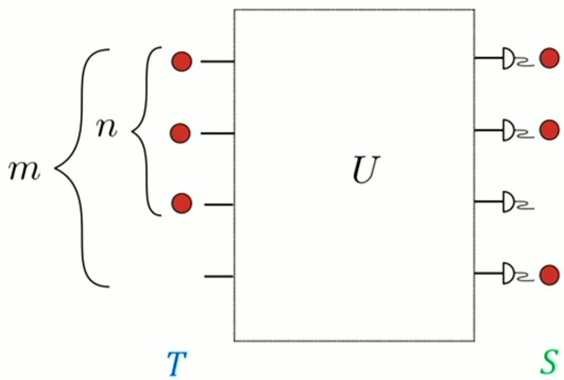
$$U = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}$$

$$T = (1,1,1,0)$$

$$a_i \to \sum_j U_{ij} a_j$$

BosonSampling 101 – Main proof outline

- Step 2: From probabilities to hard functions;
- For BosonSampling, sort-of trivial:



$$a_i \rightarrow \sum_j U_{ij} a_j$$

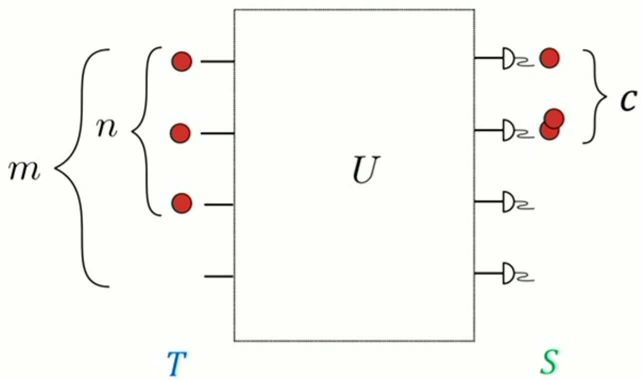
$$\Pr\left(T \rightarrow S\right) = \frac{1}{s_1! \ldots s_m!} \left|Per(U_{ST})\right|^2$$

$$U = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}$$

$$U_{ST} = \begin{pmatrix} a & b & c \\ e & f & g \\ m & n & o \end{pmatrix}$$

BosonSampling 101 – Main proof outline

- Step 2: From probabilities to hard functions;
- For BosonSampling, sort-of trivial:



$$\Pr\,(T \to S) = \frac{1}{s_1! \ldots s_m!} |Per(U_{ST})|^2$$

c: number of output detector "clicks"

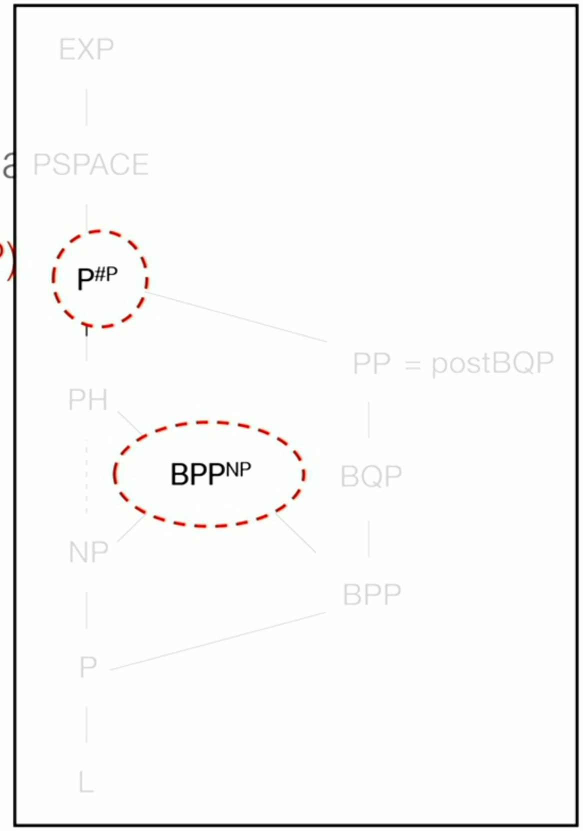
BosonSampling 101 – Main proof outline

- Interlude: So what?
- Why do I care? How hard is the Permanent anyway?
  - In the worst case: super extra hard! (#P)

[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

- Interlude: So what?
- Why do I care? How hard is the Perma
  - In the worst case: super extra hard! (#P)



[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

- Step 3: Enter the conjectures (where the magic happens!)
- Choices:
  - U is Haar-random, and
  - $m = O(n^2)$;
- Together, these imply:
  - No-collision states dominate ($s_i = 0, 1$);
  - Entries of submatrices look independent and Gaussian;

    └→ Two reasons to require $m = O(n^2)$;

[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

BosonSampling 101 – Main proof outline

- Step 3: Enter the conjectures (where the magic happens!)

> BPP^{NP} machines can solve #P-hard problems.

[Aaronson e Arkhipov, Theo. Comput. **9,** 13 (2013)]

Summary

- BosonSampling 101
- Outline of original hardness proof
- BosonSampling when $m = O(n)$
- Summary and outlook

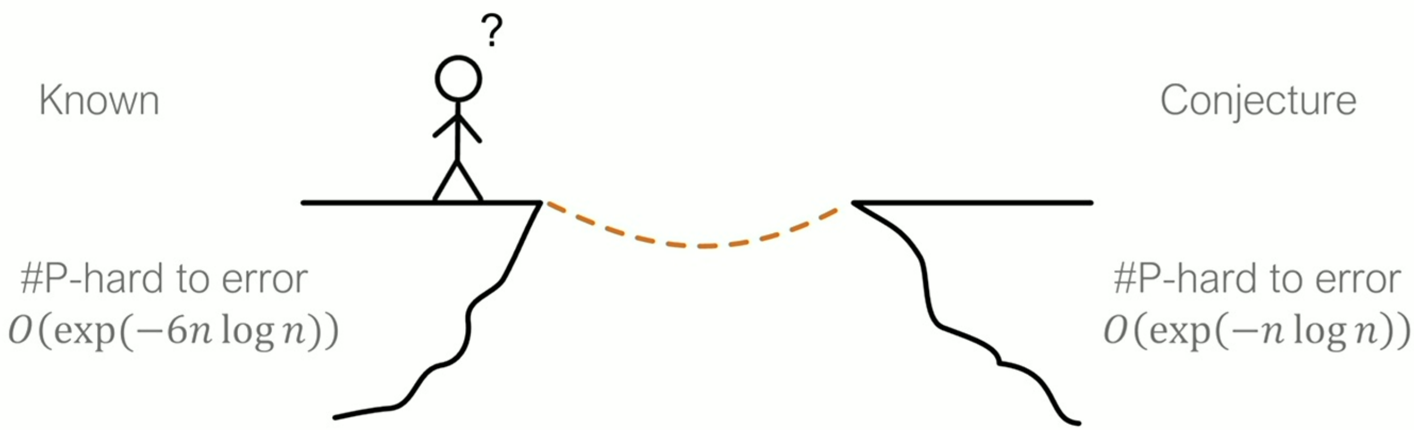
BosonSampling when $m = O(n)$

- What if we don't want $m = O(n^2)$?
- Easy! Just write a new conjecture!

Job done! Questions?

BosonSampling when $m = O(n)$

- Let's take a closer look at the original conjecture...
- Conjecture 1 (Permanent-of-Gaussians):
  Permanents of $n \times n$ matrices of i.i.d. Gaussian elements are #P-hard to compute (to high precision, most of the time).



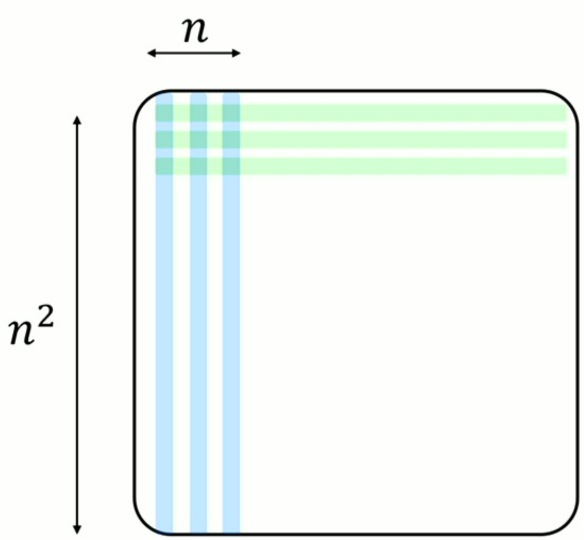
[Bouland, Fefferman, Landau, Liu, FOCS' 2021]

BosonSampling when $m = O(n)$

- New challenges:

  I. Submatrices do not have i.i.d. Gaussian entries;

  - Entries are very correlated!

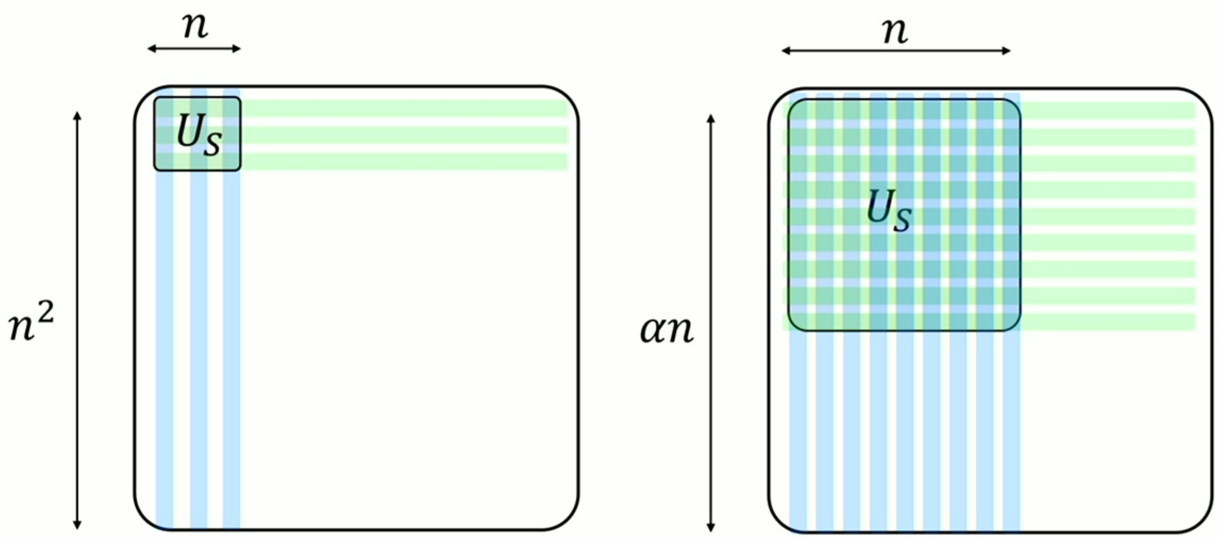


BosonSampling when $m = O(n)$

- New challenges:

  I. Submatrices do not have i.i.d. Gaussian entries;

  - Entries are very correlated!



BosonSampling when $m = O(n)$

- New challenges:

  I. Submatrices do not have i.i.d. Gaussian entries;

  - Entries are very correlated!

  II. Collisions are not unlikely;

  - Permanents have repeated rows;

BosonSampling when $m = O(n)$

- New challenges:

  I. Submatrices do not have i.i.d. Gaussian entries;

  - Entries are very correlated!

  II. Collisions are not unlikely;

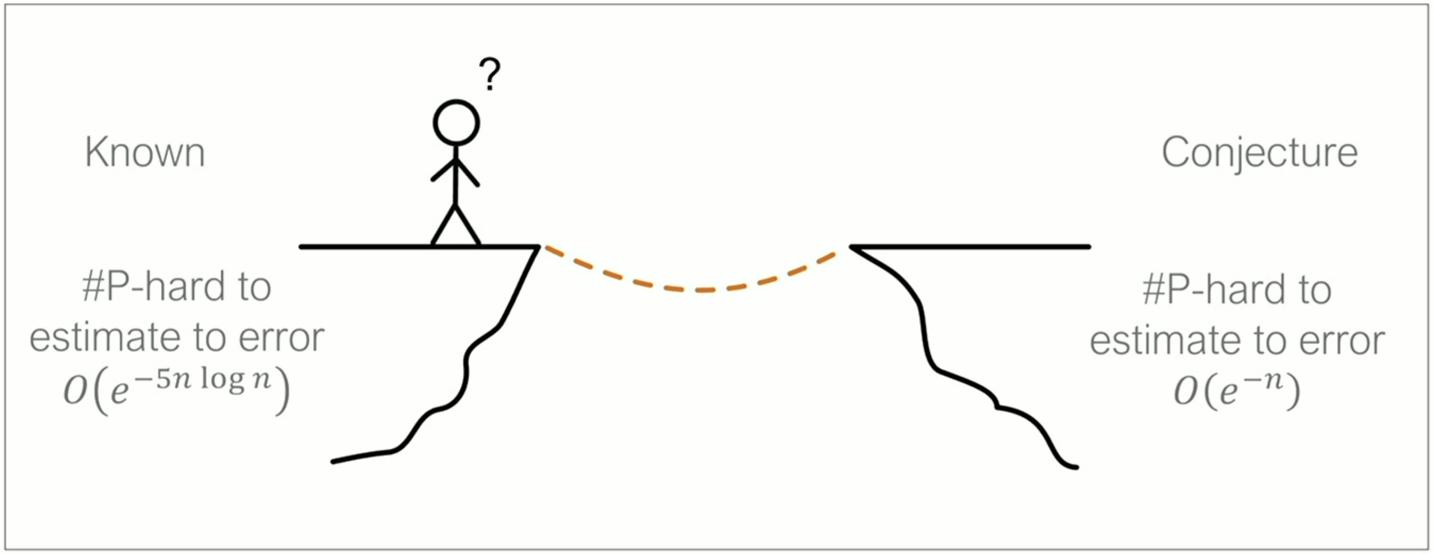
  - Permanents have repeated rows;

  III. Outcomes do not "look the same";

  - Exponentially many different outcome types.
  - (3, 1, 0, 0 ...) vs. (2, 2, 0, 0, ...) vs. (2, 1, 1, 0, ...)

Our contributions

- **Definition:** Sub-Unitary Permanent Estimation with Repetitions (SUPER)
  - Estimate $\mathrm{per}(U_S)$, with U_S drawn as a submatrix of a Haar-random matrix with (repeated) rows selected by outcome S.



Our contributions

- **Definition:** Sub-Unitary Permanent Estimation with Repetitions (SUPER)
  - Estimate $\mathrm{per}(U_S)$, with U_S drawn as a submatrix of a Haar-random matrix with (repeated) rows selected by outcome S.
- **Main result:** SUPER is #P-hard to aditive error $O\left(e^{-5n \log n}\right)$
- **Also important:**
  - Combinatorics to show that number of collisions is not overwhelming.
  - Modification of “computational advantage” template.

Our contributions

- II. Permanents have repeated rows.
  - Grier *et al*. '22: worst-case permanent with repetitions as hard as worst-case permanent without repetitions.

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad \Rightarrow \quad A_S = \begin{pmatrix} a_1 & a_2 & 1 & 1 & 0 \\ a_1 & a_2 & 1 & 1 & 0 \\ a_1 & a_2 & 1 & 1 & 0 \\ a_3 & a_4 & 0 & 0 & 1 \\ a_3 & a_4 & 0 & 0 & 1 \end{pmatrix}$$

$$|\mathrm{Per}(A_S)|^2 = s_1! \ldots s_m! \, |\mathrm{Per} A|^2$$

[Grier, Brod, Arrazola, Alonso, Quesada, Quantum 6, 863 (2002)]

Our contributions

- II. Permanents have repeated rows.
  - Grier *et al*. '22: worst-case permanent with repetitions as hard as worst-case permanent without repetitions.

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad \Rightarrow \quad A_S = \begin{pmatrix} a_1 & a_2 & 1 & 1 & 0 \\ a_1 & a_2 & 1 & 1 & 0 \\ a_1 & a_2 & 1 & 1 & 0 \\ a_3 & a_4 & 0 & 0 & 1 \\ a_3 & a_4 & 0 & 0 & 1 \end{pmatrix}$$

$$|\mathrm{Per}(A_S)|^2 = s_1! \ldots s_m! \, |\mathrm{Per} A|^2$$

  - Worst-case hardness depends on number of detector clicks.

[Grier, Brod, Arrazola, Alonso, Quesada, Quantum 6, 863 (2002)]

Our contributions

- III. Exponentially many different outcome types.
  - If not enough detectors click, problem can actually be easy.
- Lemma: for $m = \alpha\, n$, at least $c = \frac{\alpha}{\alpha+2} n$ detectors click (w.h.p.)
- Corollary: most outcome probabilities can embed some #P-hard problem in the worst case.

Our contributions

- I. Entries are very correlated!
- Worst-to-average-case reduction (original AA paper):
  - To compute $\mathrm{per}(A)$, "smuggle" it into a random matrix:

$$X = (1 - t)R + t\,A$$

  - R Gaussian and t small $\Rightarrow$ X close enough to Gaussian.

Our contributions

- I. Entries are very correlated!
- Worst-to-average-case reduction (original AA paper):
  - To compute $\mathrm{per}(A)$, "smuggle" it into a random matrix:

$$X = (1-t)R + t\,A$$

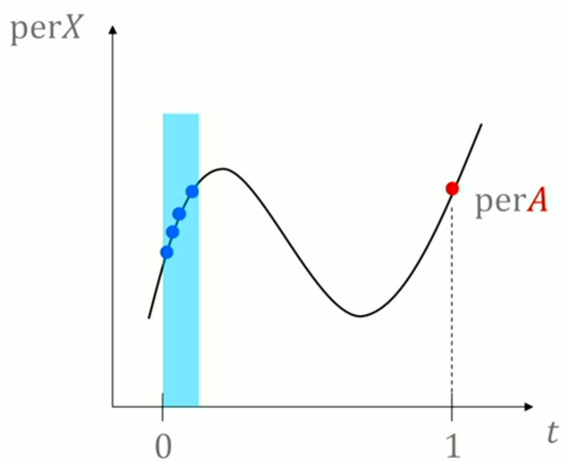
  - R Gaussian and t small $\Rightarrow$ X close enough to Gaussian.

$\Rightarrow$ computing $\mathrm{per}(X)$ for Gaussian X as hard* as computing $\mathrm{per}(A)$.

Our contributions

- I. Entries are very correlated!
- Worst-to-average-case reduction (original AA paper):
  - To compute $\mathrm{per}(A)$, "smuggle" it into a random matrix:

$$X = (1 - t)R + t\,A$$

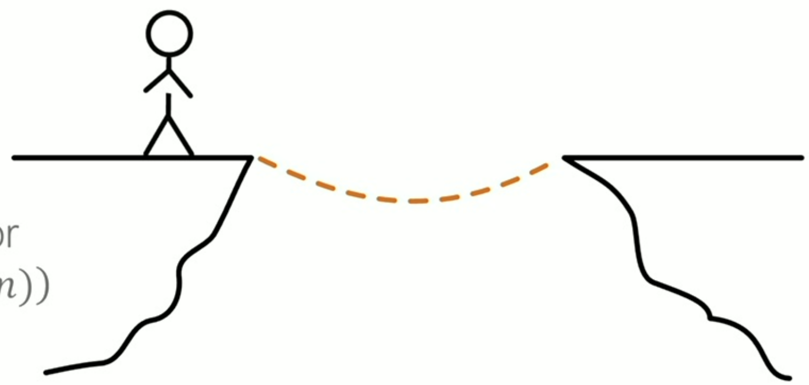


Our contributions

- I. Entries are very correlated!
- Worst-to-average-case reduction (original AA paper):
  - To compute $\mathrm{per}(A)$, "smuggle" it into a random matrix:

Known

Conjecture



#P-hard to error $O(\exp(-6n\log n))$

#P-hard to error $O(\exp(-n\log n))$

[Bouland, Fefferman, Landau, Liu, FOCS' 2021]

Our contributions

- I. Entries are very correlated!
- Worst-to-average-case reduction (original AA paper):
  - To compute $\mathrm{per}(A)$, "smuggle" it into a random matrix:

$$X = (1-t)R + t\,A$$

$\Rightarrow$ computing $\mathrm{per}(X)$ for Gaussian X as hard* as computing $\mathrm{per}(A)$.

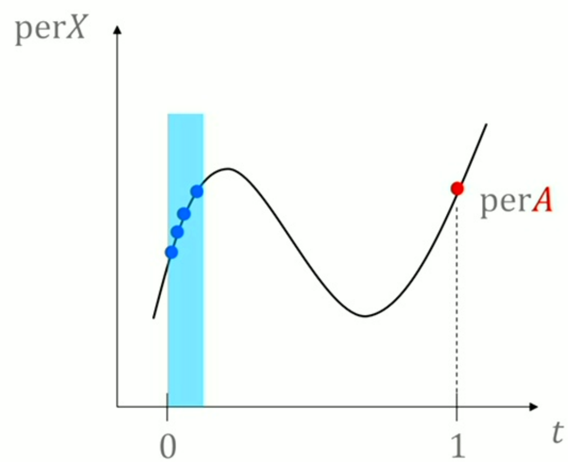
- Original proof breaks down if entries are correlated.

* Need to keep track of error blow-up!

Our contributions

- I. Entries are very correlated!
- Worst-to-average-case reduction (original AA paper):
  - To compute $\mathrm{per}(A)$, "smuggle" it into a random matrix:

$$X = (1-t)R + t\,A$$

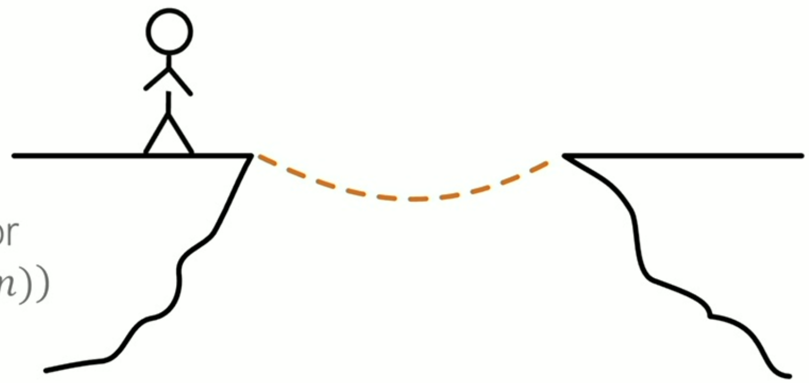


Our contributions

- I. Entries are very correlated!
- Worst-to-average-case reduction (original AA paper):
  - To compute $\mathrm{per}(A)$, "smuggle" it into a random matrix:

Known

Conjecture



#P-hard to error $O(\exp(-6n \log n))$

#P-hard to error $O(\exp(-n \log n))$

[Bouland, Fefferman, Landau, Liu, FOCS' 2021]

Our contributions

- I. Entries are very correlated!
  - Lemma: Let R be a random $n \times n$ matrix sampled as a submatrix of an $m \times m$ Haar-random matrix. Define the random matrix

    $$X \approx R + t\,A$$

    for some "worst-case" matrix A, and $t = O\left(\frac{1}{n^2}\right)$.

    Then X is approximately taken from the same ensemble as R.

Our contributions

- I. Entries are very correlated!
  - Lemma: Let R be a random $n \times n$ matrix sampled as a submatrix of an $m \times m$ Haar-random matrix. Define the random matrix

    $$X \approx R + t\,A$$

    for some "worst-case" matrix A, and $t = O\left(\frac{1}{n^2}\right)$.

    Then X is approximately taken from the same ensemble as R.
  - Add some (better) polynomial interpolation.

Main result: SUPER is #P-hard to additive precision $O\left(e^{-5n \log n}\right)$.

Our results

- Proposed new computational problem SUPER.
  - Arises as probabilities of BosonSampling when $m = O(n)$.
- Proof that SUPER is hard to additive error $\mathrm{O}\left(e^{-5n \log n}\right)$.
  - Conjectured robustness to error $\mathrm{O}(e^{-n})$.
- Gap between conjecture and what we can prove:
  - similar to standard BosonSampling proposal (where $m = O(n^2)$);
  - remains open, as for every quantum advantage proposal.

Our results

- Proposed new computational problem SUPER.
  - Arises as probabilities of BosonSampling when $m = O(n)$.
- Proof that SUPER is hard to additive error $O\left(e^{-5n \log n}\right)$.
  - Conjectured robustness to error $O(e^{-n})$.
- Gap between conjecture and what we can prove:
  - similar to standard BosonSampling proposal (where $m = O(n^2)$);
  - remains open, as for every quantum advantage proposal.
- $m = 2n$ is much more experimentally friendly!

Open questions

- Similar statement for Gaussian BosonSampling?
  - We're on it!
- Can a classical algorithm leverage the collisions to speed-up the classical simulation?
  - Would our conjecture be less likely to hold that the one by AA?
  - How relevant would it be for current finite-sized experiments?

Questions?