(Bipartite) Gaussian BosonSampling

Daniel J. Brod (Universidade Federal Fluminense)

https://arxiv.org/abs/2110.06964

Joint work with: D. Grier, J. M. Arrazola, M. Alonso and N. Quesada

Rio - Warsaw
January 2022

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

- Cons:
  - High susceptibility to noise (no error correction);
  - No concrete practical applications (yet!);
  - Hard to check if the device is working (very intense debate!);
- Pros:
  - Simpler resource requirements;
  - New insights on quantum computing (and optics);
  - Pushes technological development;

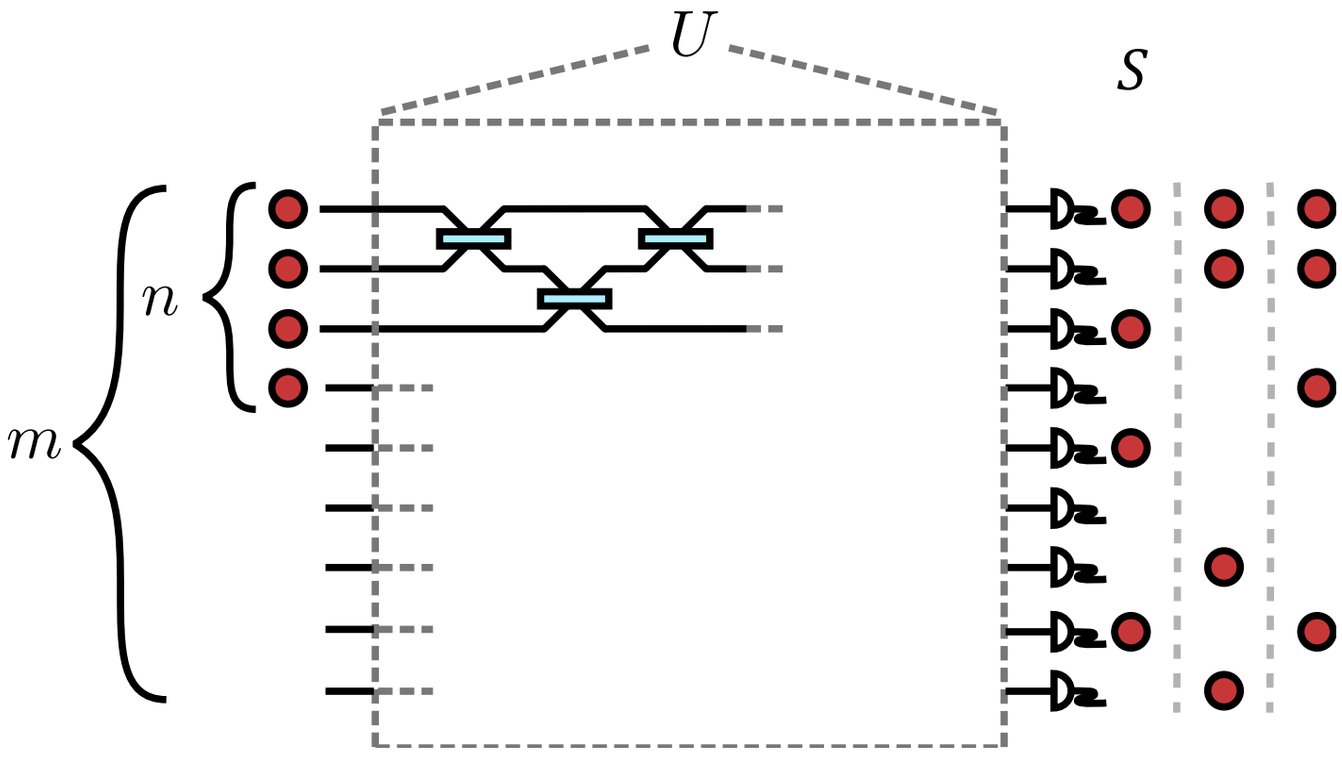
Summary

- BosonSampling 101
  - Outline of hardness proof
- Gaussian BosonSampling (GBS)
  - Experimental achievements
  - What's missing?
- New proposal: BipartiteGBS
  - Hardness proof
  - Additional result – dealing with collision outcomes
- Conclusions and outlook

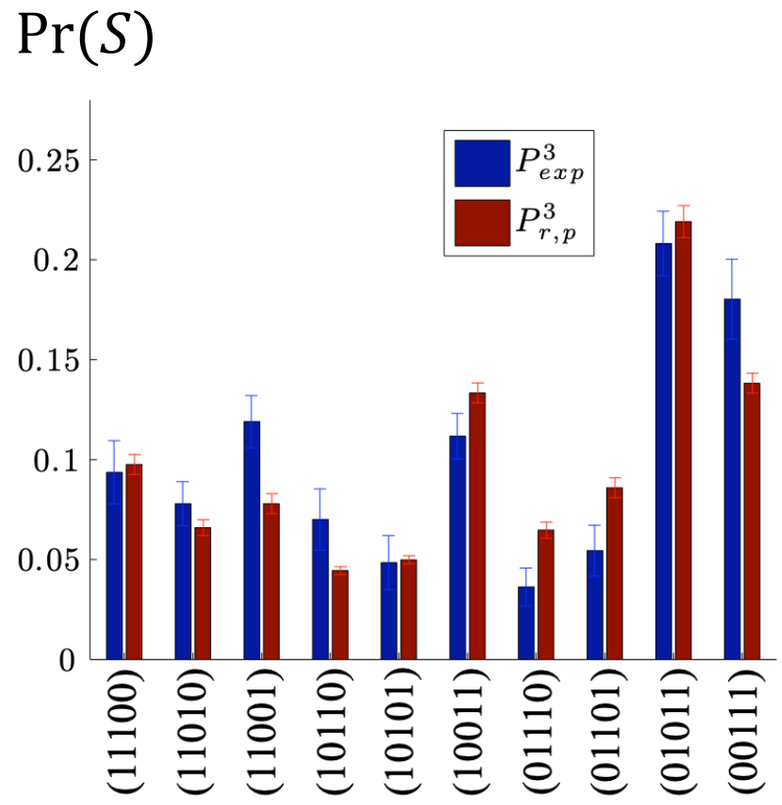
Summary

- BosonSampling 101
  - Outline of hardness proof
- Gaussian BosonSampling (GBS)
  - Experimental achievements
  - What's missing?
- New proposal: BipartiteGBS
  - Hardness proof
  - Additional result – dealing with collision outcomes
- Conclusions and outlook

BosonSampling 101



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



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

Distribution $\mathcal{D}_U$

BosonSampling 101

- **Computational task**: Sample from output distribution.
  - For a quantum device, this is “easy”;
  - There is evidence that it is very hard for classical computers!

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

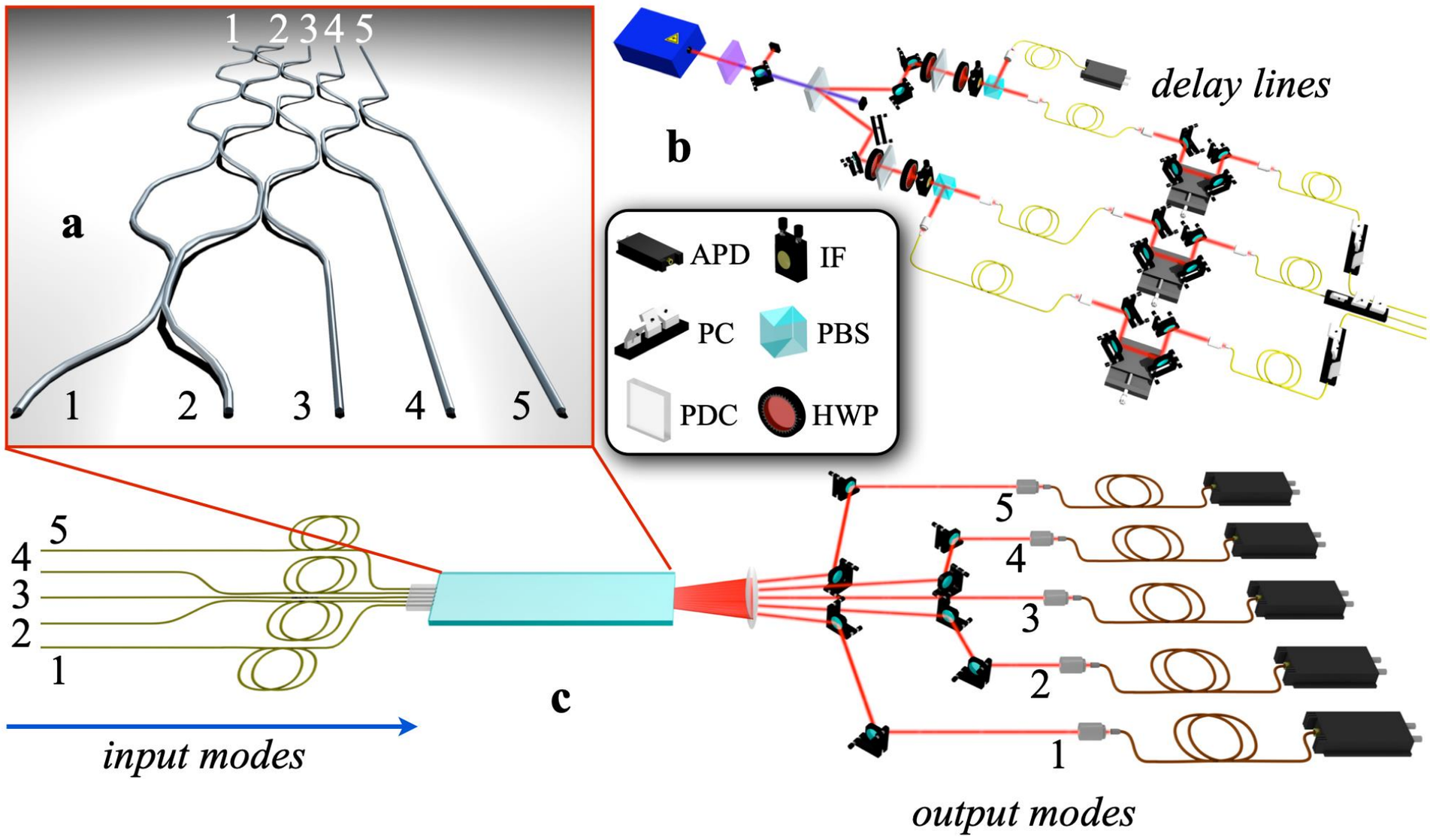
- Even approximate simulation is hard!

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

- Permanent for n-photon transition: time $\mathrm{O}(n2^n)$
  - Milestone: 50 – 200 photons?

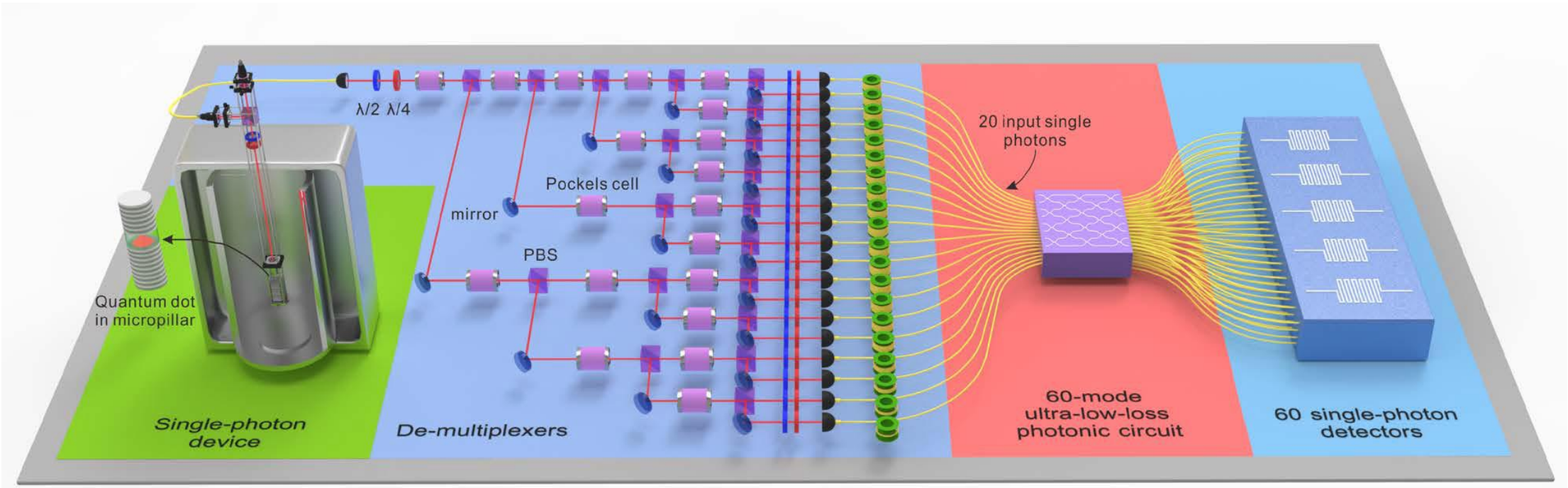
[Aaronson e Arkhipov, Theo. Comput. **9,** 143 (2013)]

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).]

Experimental advances



- 20 photons in 60 modes;
- Largest (?) experiment within original BS proposal;
  - Uses quantum dot sources.
  - GBS experiments to appear later on!

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

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);
  - Same for our proposal and BS – stronger than GBS.

[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 $\widetilde{D}_U$:

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

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

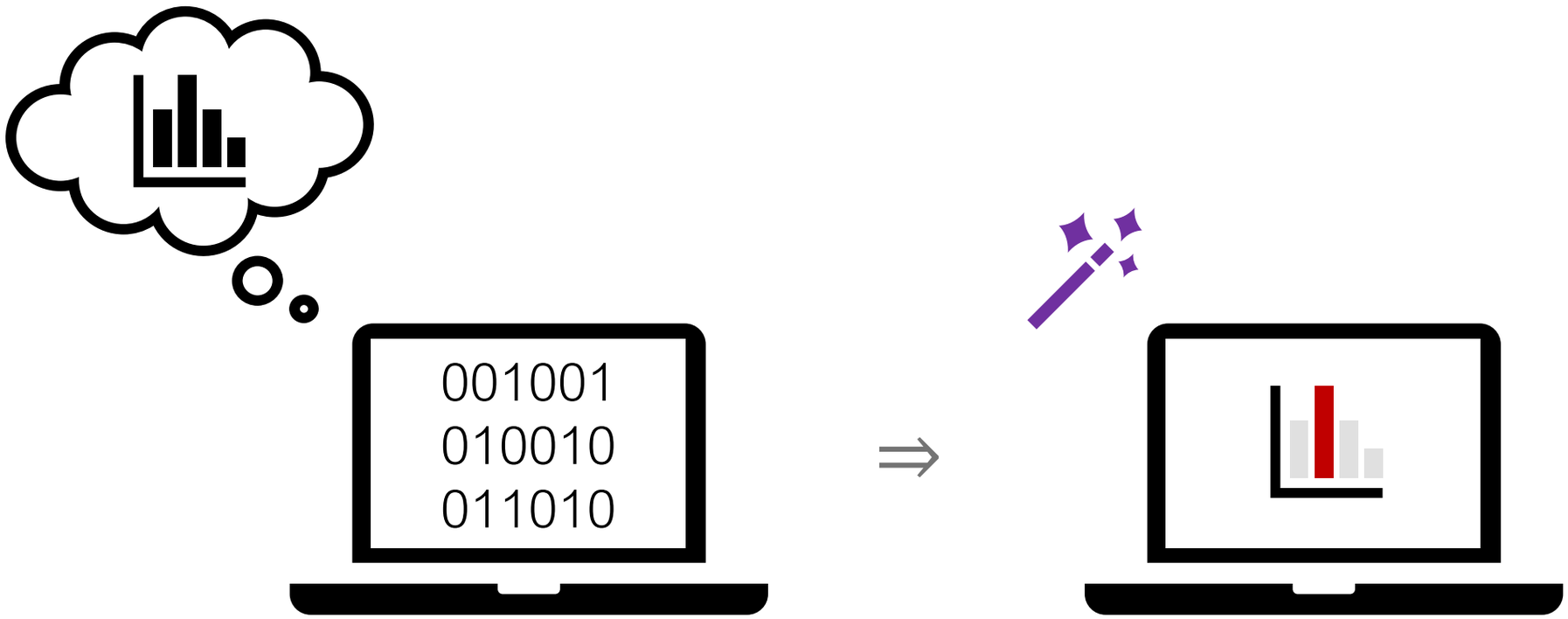
BosonSampling 101 – Main proof outline

- **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., U Haar-random → permutation invariance of outcomes.
- 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 ($\mathrm{BPP}^{\mathrm{NP}}$) can efficiently estimate $\mathbf{Pr}(S)$ to error $\epsilon/|\mathcal{H}_S|$



[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:

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

$$U = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix} \quad \Rightarrow \quad U_{ST} = \begin{pmatrix} d & e \\ g & h \end{pmatrix}$$

$T = (1,1,0), \quad S = (0,1,1)$

[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:

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

- **Conclusion:** Moderately superpowerful classical machine (BPP^{NP}) can compute $|\mathrm{Per}(U_{ST})|^2$ **to error**

$$\frac{\epsilon}{|\mathcal{H}_S|} s_1! \dots s_m!$$

[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 (every s_i is 0 or 1) dominate;
  - If $m = O(n^{5.1})^*$, submatrices look independently Gaussian;

↳ Important: two independent 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!)
- **Conjecture 1** (anti-concentration):
  Permanents of Gaussian matrices do not concentrate too much around 0;

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

BosonSampling 101 – Main proof outline

- **Step 3**: Enter the conjectures (where the magic happens!)
- **Conjecture 2** (Permanent-of-Gaussians):
  Permanents of Gaussian matrices are typically super extra hard problems (#P-hard).

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

BosonSampling 101 – Main proof outline

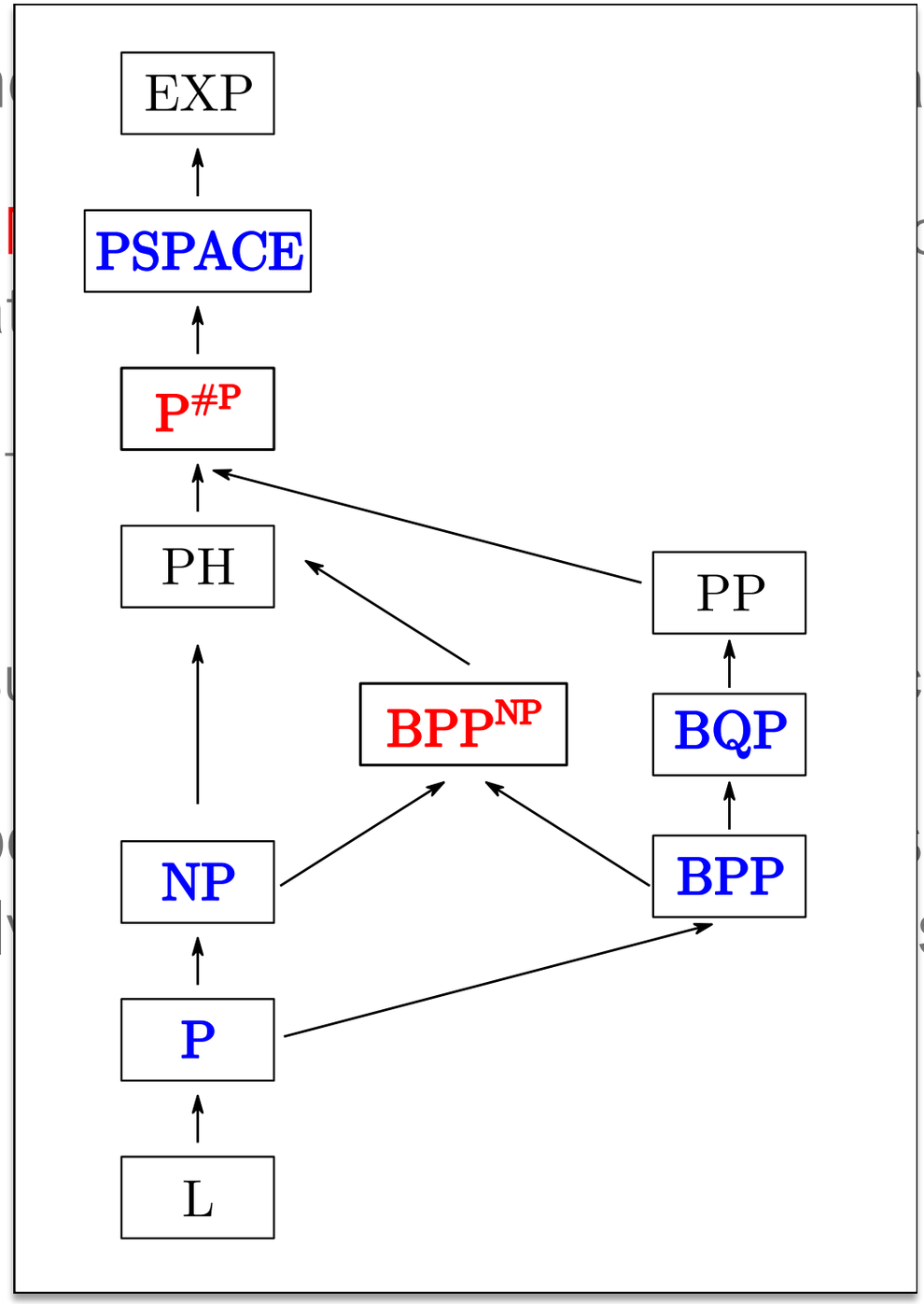
- Step 3: Enter the conjectures (where the magic happens!)
  - Steps 1 + 2 ⇒ Moderately superpowerful classical machines (BPP^{NP}) can approximate Gaussian permanents;
  - Conjectures 1 + 2 ⇒ Gaussian permanents are super extra hard (#P) to compute;
  - Collision-free subspace is large enough to match the two, and thus:
- **Conclusion:** Moderately superpowerful classical machines (BPP^{NP}) can solve super extra hard problems (#P-hard).

  ⇒ Unlikely, and so evidence that original assumption is false.

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

BosonSampling 101 – Main proof outline

- Step 3: Enter th … gic happens!)
  - Steps 1 + 2 ⇒ … cal machines (BPP^{NP}) can approximat…
  - Conjectures 1 … super extra hard (#P) to compute;
  - Collision-free su… h the two, and thus:
- **Conclusion:** Mo… sical machines (BPP^{NP}) can sol… s (#P-hard)



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

BosonSampling 101 – Main proof outline

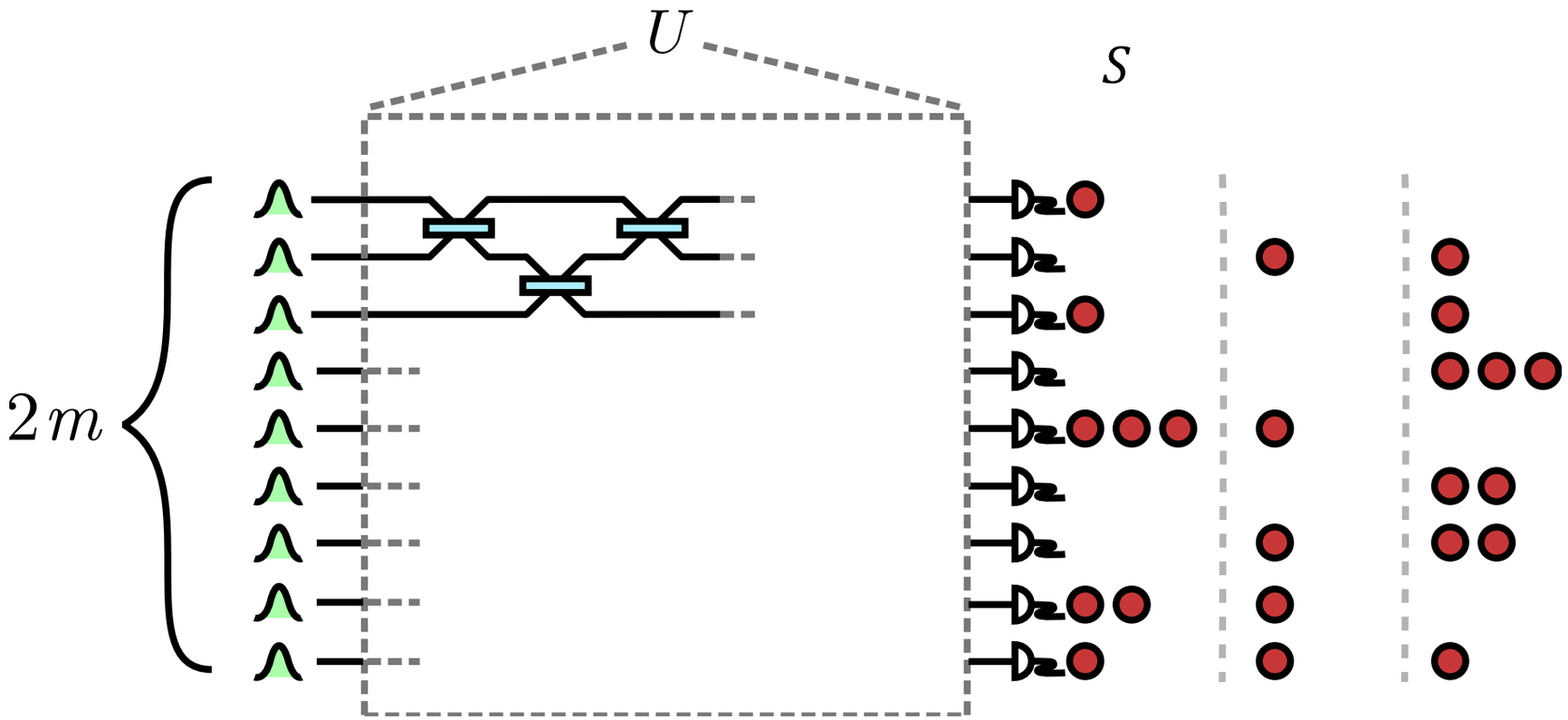
- To summarize:
  - Step 1: From distributions to probabilities; → We don't touch this!
    - Generic complexity argument;
  - Step 2: From probabilities to hard functions; → Main new idea lives here.
  - Step 3: Conjectures involving hard functions → Where most of the hard work went.
    - + standard complexity-theoretic arguments
      = Proof of hardness!

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

Summary

- BosonSampling 101
  - Outline of hardness proof
- Gaussian BosonSampling (GBS)
  - Experimental achievements
  - What's missing?
- New proposal: BipartiteGBS
  - Hardness proof
  - Additional result – dealing with collision outcomes
- Conclusions and outlook

Gaussian BosonSampling



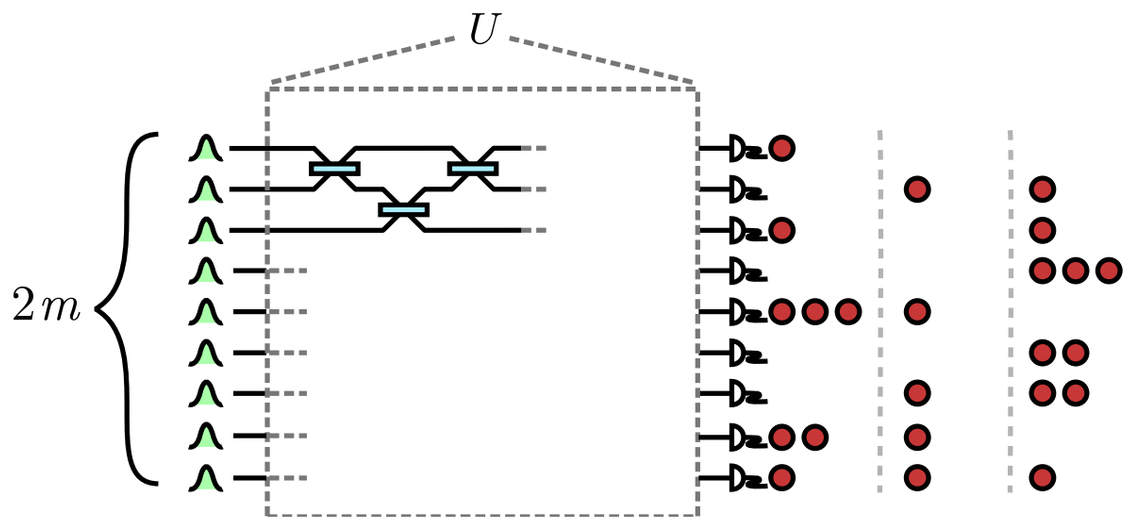
Squeezed states

Photon number varies!

Mean: $\langle n \rangle$

[Hamilton et al, PRL **119**, 170501 (2017).
Kruse et al, PRA **100**, 032326 (2019)]

Gaussian BosonSampling



- Probabilities now given by:

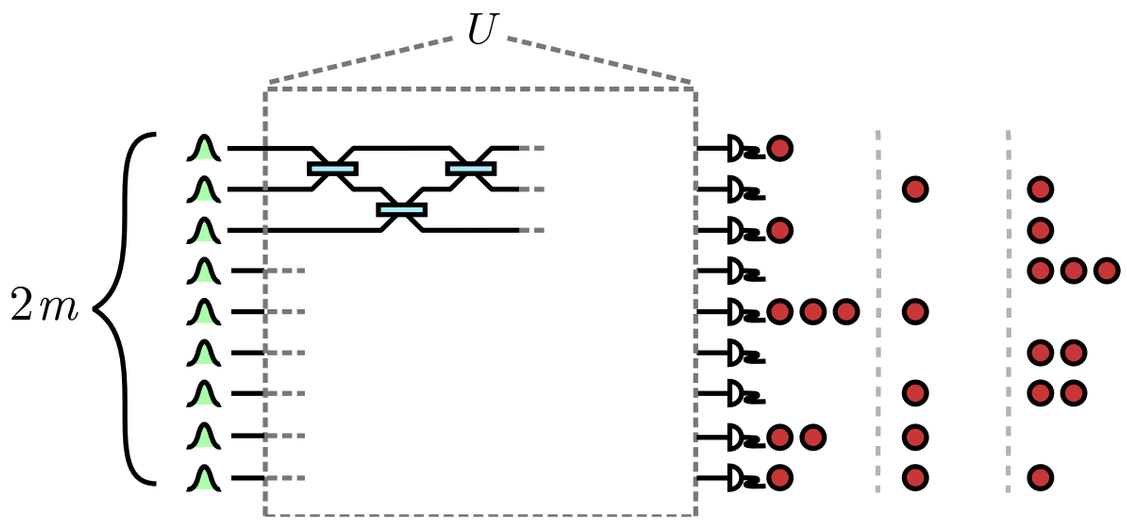
$$\Pr(S) = \frac{1}{\mathcal{Z}} \frac{|\mathrm{Haf}(A_s)|^2}{s_1!\, s_2! \ldots s_{2m}!} ,$$

where

$$\mathcal{Z} = \prod_{i=1}^{2m} \cosh(r_i)$$

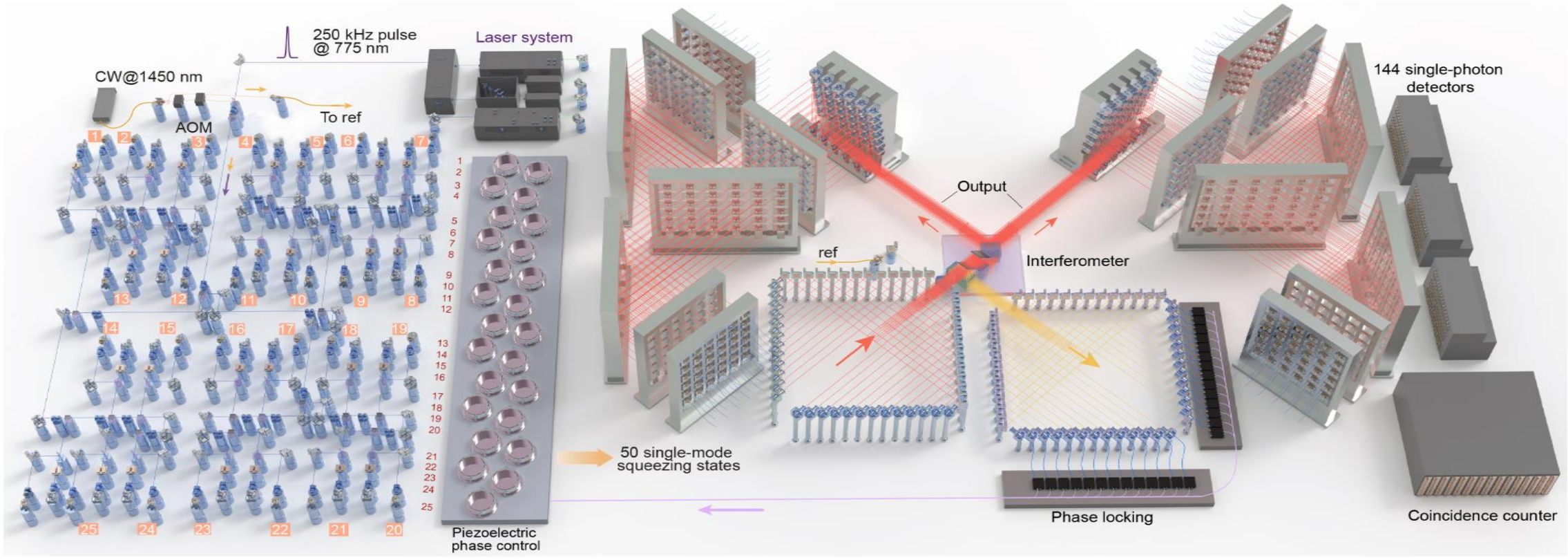
Squeezing in mode i

Gaussian BosonSampling



- Main differences to standard BosonSampling:
  - Easier to implement in the lab than Fock states; ☺

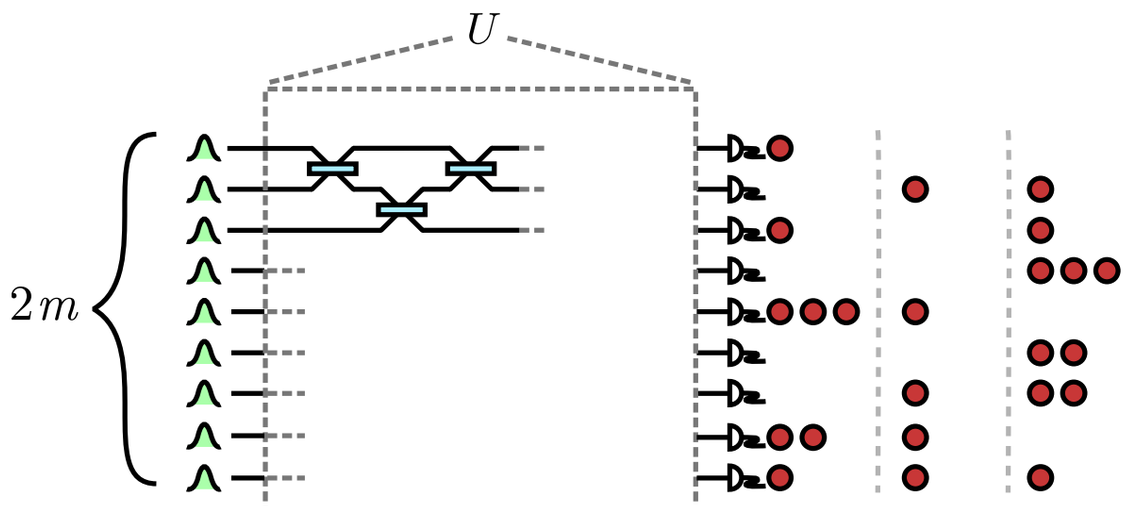
Gaussian BosonSampling



- Largest GBS experiment to date;
  - Up to 113 detected photons in 144 modes;
    - Compare to 20 photons in 60 modes in standard BS – but not too much.
  - Larger experiments are on the way!

[Zhong *et al,* PRL **127**, 180502 (2021)]

Gaussian BosonSampling



- Main differences to standard BosonSampling:
  - Easier to implement in the lab than Fock states; ☺
  - Variable photon number; ☹
  - Complexity argument not so tight / needs new conjectures; 😟

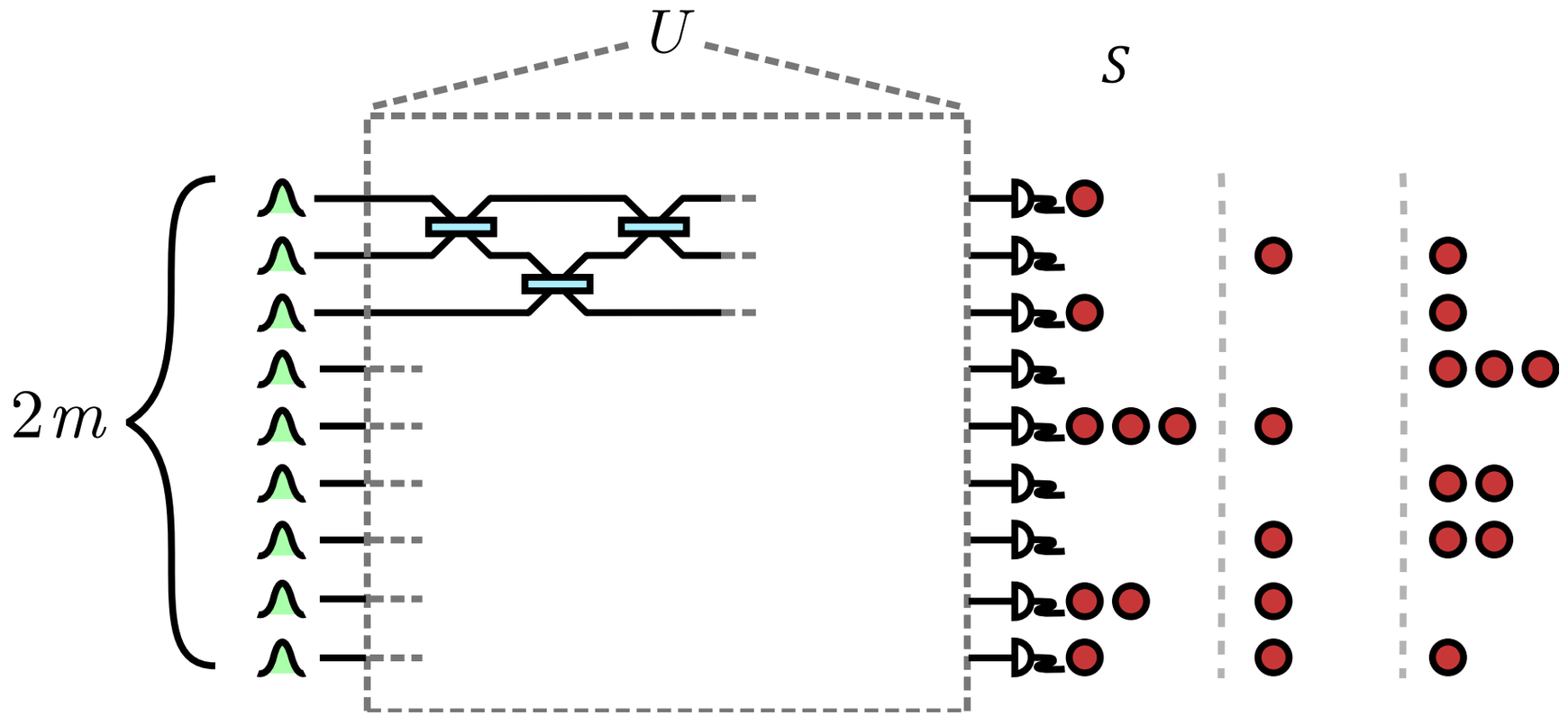
Gaussian BosonSampling

- What is (or was) missing?
- Original proposal was very light on complexity-theoretic details;
- A priori, GBS requires new conjectures (analogous to BS).
- So what?
  - Hafnian is a way less studied function;
  - For permanents, weaker versions of the conjectures hold;
  - “Conjectures are as good as the attacks they withstood”;
  - The fewer conjectures the better;

Summary

- BosonSampling 101
  - Outline of hardness proof
- Gaussian BosonSampling (GBS)
  - Experimental achievements
  - What's missing?
- New proposal: BipartiteGBS
  - Hardness proof
  - Additional result – dealing with collision outcomes
- Conclusions and outlook

BipartiteGBS

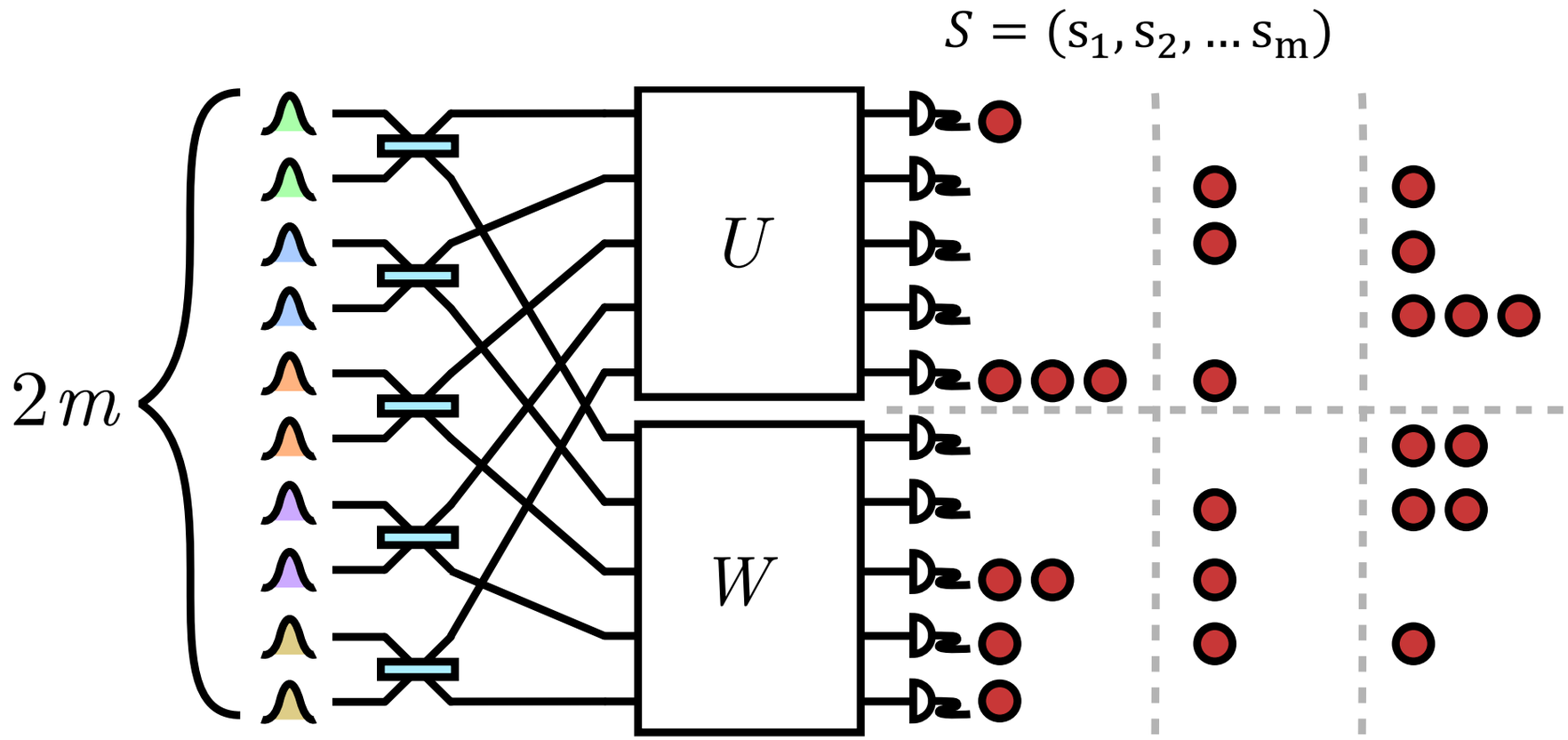


Squeezed states

Photon number varies!

Mean: $\langle n \rangle$

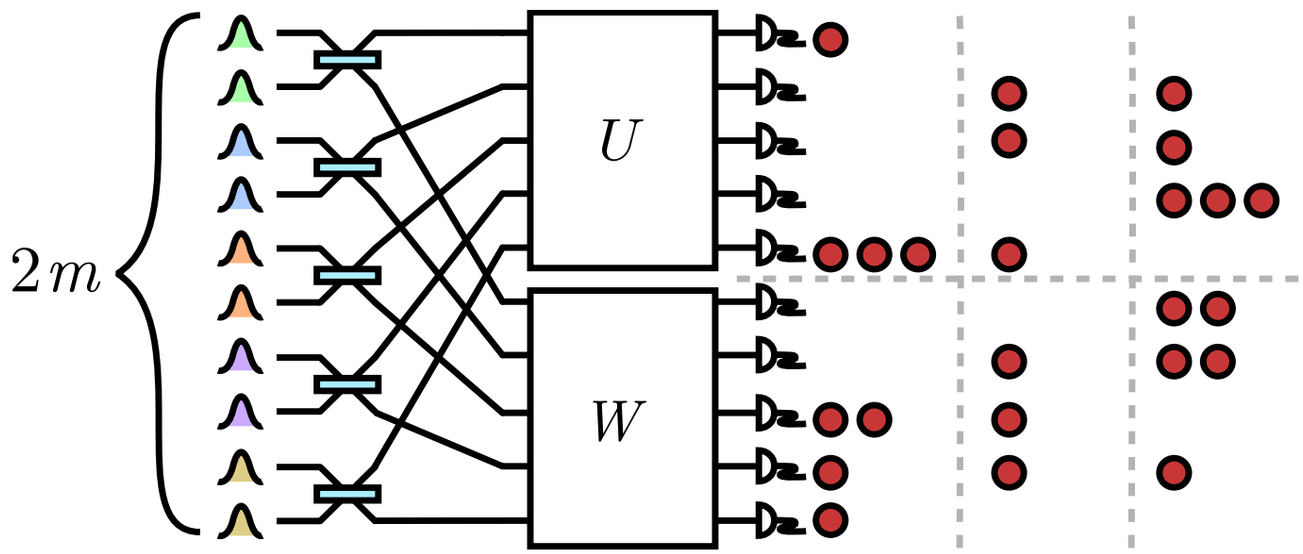
BipartiteGBS



Squeezed states
(with variable parameters)

*is a particular case of GBS and generalizes scattershot BS.

BipartiteGBS



- Probabilities can be written as:

$$\Pr(S) = \frac{1}{\mathcal{Z}} \frac{|\mathrm{Haf}(A_s)|^2}{s_1!\, s_2! \ldots s_{2m}!} \Rightarrow \Pr(S;T) = \frac{1}{\mathcal{Z}} \frac{|\mathrm{Per}(C_{ST})|^2}{s_1! \ldots s_m!\, t_1! \ldots t_m!}$$

where

$$C = U.\,\mathrm{diag}(\tanh r_i).\,W^T$$

BipartiteGBS

$$C = U.\mathrm{diag}(\tanh r_i).V^T$$

- Singular value decomposition of arbitrary complex matrix.
- We can implement random Gaussian matrices **directly**.
  - This removes **one** barrier to the $m \ll n^2$ regime.
- Other matrix ensembles:
  - Better/simpler hardness proofs?
  - Applications?

BipartiteGBS

- Sounds like free lunch! What's the catch?
- If C is random, so are the squeezing parameters – so what?
- Problem 1: Are the squeezing parameters likely (over choice of C) to require extreme resources?
- Solution: RMT literature has bounds on largest singular value;

BipartiteGBS

- Sounds like free lunch! What's the catch?
- If C is random, so are the squeezing parameters – so what?
- Problem 2:

$$\langle n \rangle = \frac{1}{2}\sum \frac{(\tanh r_i)^2}{1-(\tanh r_i)^2}$$

Lemma 4. *For any $\delta > 0$, we have*

$$\Pr\left[\left|\langle n\rangle - \frac{m}{\alpha^2}\right| \geq \frac{512m}{\alpha^4} + \frac{1}{\alpha^2}\sqrt{\frac{2}{\delta}}\right] \leq \delta$$

$$\Pr\left[\left|n - \frac{m}{\alpha^2}\right| \geq \frac{2\sqrt{m}}{\alpha\sqrt{\delta}} + \frac{3}{\alpha\delta^{3/4}} + \frac{84\sqrt{m}}{\alpha^2\sqrt{\delta}} + \frac{512m}{\alpha^4}\right] \leq \delta$$

whenever $\alpha \geq 6$, and $m \geq \ln(1/\delta)$. The first probability is over the choice of Gaussian matrix C, whereas the second probability is over both the choice of C and over the photon number distribution.

BipartiteGBS

- Sounds like free lunch! What's the catch?
- If C is random, so are the squeezing parameters – so what?
- Problem 3:

$$\mathcal{Z} = \prod_{i=1}^{2m} \cosh(r_i)$$

Lemma 5. *For any* $\delta > 0$

$$\Pr\left[\mathcal{Z} \geq \frac{2}{\delta} e^{m/\alpha^2} e^{272m/\alpha^4}\right] \leq \delta, \tag{18}$$

whenever $\alpha \geq 6$, *and* $m \geq \ln(1/\delta)$.

Recall that $\alpha = \Theta(m^{1/4})$ in the dilute limit, and so Lemma 5 implies that $\mathcal{Z}$ behaves asymptotically as e^{m/α^2}.

BipartiteGBS – Main proof outline

- Step 1: From distributions to probabilities; ✓
- Step 2: From probabilities to hard functions;
  - Permanents, as in BS (instead of Hafnians, as in GBS);
  - Arbitrary transition matrices (instead of unitary, as in BS);
    - No need for $m = O(n^{5.1})$ to get Gaussian matrices;
- Step 3: Conjectures involving hard functions
  - Permanents of Gaussian matrices:
    - Same two conjectures as standard BS! ✓
    - Still uses no-collision subspace → This obstacle to improving m vs n regime remains.

Additional result: dealing with collisions

- Recall:

$$\Pr(S;T) = \frac{1}{\mathcal{Z}} \frac{|Per(C_{ST})|^2}{s_1! \dots s_m!\, t_1! \dots t_m!}$$

- Collisions ⇒ Permanents with repeated rows/columns;
  - Too many collisions ⇒ easy to simulate classically;
- What about a few collisions?
- Method: intervention only on **step 2**;

Ability to compute $|\mathrm{per}(.)|^2$ for Gaussian matrix with repetitions (to error ϵ) ⇒ Ability to compute $|\mathrm{per}(.)|^2$ for (smaller) Gaussian matrix with no repetitions (to error ε)

Inspired by: [Aaronson and Brod, PRA **93**, 012335 (2016)]

Additional result: dealing with collisions

- A: $c \times c$ Gaussian matrix;
- A_S: $(c+k) \times (c+k)$ matrix obtained by repeating k rows/columns of A (according to S).

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad \Rightarrow \quad A_S = \begin{pmatrix} a_1 & a_2 & y_1 & y_2 & y_3 \\ a_1 & a_2 & y_1 & y_2 & y_3 \\ a_1 & a_2 & y_1 & y_2 & y_3 \\ a_3 & a_4 & y_4 & y_5 & y_6 \\ a_3 & a_4 & y_4 & y_5 & y_6 \end{pmatrix}$$

$$S = (3,2)$$

*Every y_i needs to be a Gaussian random variable.

Additional result: dealing with collisions

- A: $c \times c$ Gaussian matrix;
- A_S: $(c+k) \times (c+k)$ matrix obtained by repeating k rows/columns of A (according to S).

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad \Rightarrow \quad A_S[z] = \begin{pmatrix} a_1 & a_2 & y_1 & y_2 & z.y_3 \\ a_1 & a_2 & y_1 & y_2 & z.y_3 \\ a_1 & a_2 & y_1 & y_2 & z.y_3 \\ a_3 & a_4 & z.y_4 & z.y_5 & y_6 \\ a_3 & a_4 & z.y_4 & z.y_5 & y_6 \end{pmatrix}$$

$$|\mathrm{Per}(A_S[z])|^2 = \alpha\,|\mathrm{Per}A|^2 + \gamma_1 z + \gamma_2\, z^2 + \cdots + \gamma_k z^k$$

Additional result: dealing with collisions

- A: $c \times c$ Gaussian matrix;
- A_S: $(c+k) \times (c+k)$ matrix obtained by repeating k rows/columns of A (according to S).

$$\phi(z) \coloneqq |\mathrm{Per}(A_S[z])|^2 = \alpha\, |\mathrm{Per}A|^2 + \gamma_1 z + \gamma_2\, z^2 + \cdots + \gamma_k z^k$$

- By assumption, we <u>can</u> estimate $\phi(z)$ for $z \approx 1$.
- We <u>want</u> $\phi(0)$.
- **Solution**: Compute $\phi(z)$ for $k+1$ values of $z \approx 1$ and use least squares method.

Additional result

- Working out all the details:

Theorem 14. *Given access to an oracle for* $|\mathrm{RGPE}|_{\pm}^{2}$ *with error* $\varepsilon(c+k)!\prod s_i!t_j!$*, it is possible to use* $O(k)$ *calls to the oracle to solve* $|\mathrm{GPE}|_{\pm}^{2}$ *with additive error* $\epsilon c!$*, for*

$$\epsilon := O\left(\frac{(c+k)^{2k}k^{2k}}{\delta^{3k+1/2}2^{k}}\varepsilon\right) \tag{50}$$

Whenever $k = O(1)$*, we have* $\epsilon = \mathsf{poly}(c, \varepsilon, \delta)$.

- This scales **quite poorly** with number of collisions k. ☹
- Only implies hardness for $k = 0(1)$.
  - Still, the method has some promising features.

Summary

- BosonSampling 101
  - Outline of hardness proof
- Gaussian BosonSampling (GBS)
  - Experimental achievements
  - What's missing?
- New proposal: BipartiteGBS
  - Hardness proof
  - Additional result – dealing with collision outcomes
- Conclusions and outlook

Conclusions

- New proposal: BipartiteGBS;
- Improves on standard BS by allowing for arbitrary matrices;
  - Provably removes need for $m = O(n^{5.1})$, suggests $m = O(n^2)$ can be improved.
  - Caveat: Few people took the $m = O(n^{5.1})$ scaling too seriously.
- Improves on standard GBS by not needing new conjectures;
  - Unifies the complexities of GBS and BS;
  - Caveat: something similar could be said of scattershot BosonSampling;
- Makes everything robust to $O(1)$ collisions;

Outlook

- New proposal: BipartiteGBS;
- Leverage the fact that we can implement an arbitrary matrix?
  - For applications (encode some interesting problem);
  - To prove something in the $m = O(n)$ regime?
  - Different matrix ensembles (Bernoulli, etc) where conjectures are easier to prove?
- Improvement on robustness to collisions?