The Complexity of Bipartite Gaussian Boson Sampling

Daniel Grier
University of Waterloo

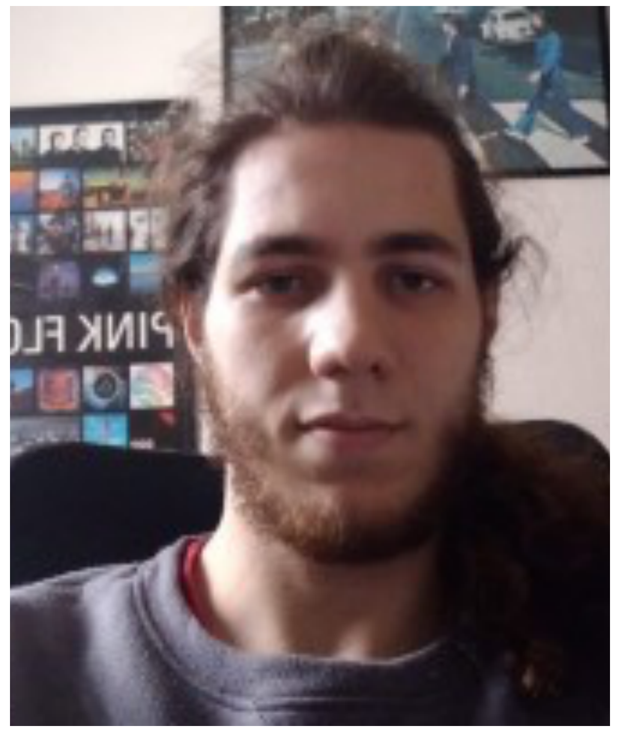
Daniel Brod

Fluminense Federal University

Juan Miguel Arrazola

Xanadu Quantum Technologies

Marcos Benicio de Andrade Alonso



Fluminense Federal University

Nicolás Quesada

Polytechnique Montréal

Quantum computational advantage with linear optics

Is it hard to classically sample from the distributions produced by weak photonic quantum computers?

Strong candidates:

(Fock) BosonSampling [Aaronson, Arkhipov STOC 11]

Fermion Sampling with magic input states [Oszmaniec et al. QIP 22]

Gaussian Boson Sampling [Lund et al. PRL 14, Hamilton et al. PRL 17]

Scattershot BosonSampling

Problems:

1) Disconnected landscape of conjectures
2) Extra conjectures needed to accommodate experimental costs

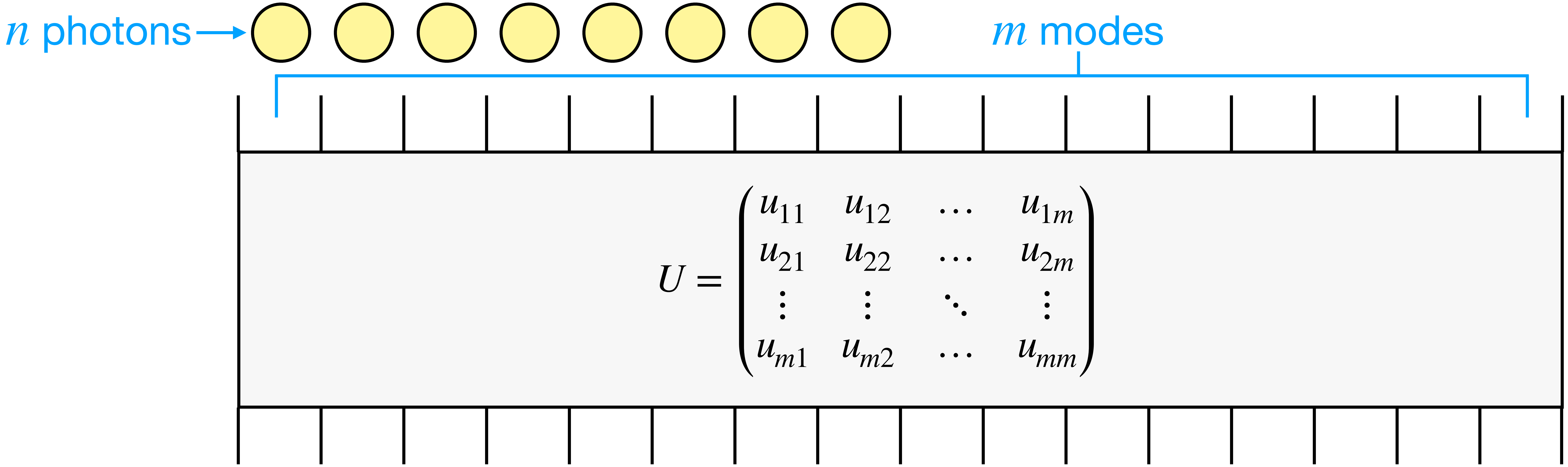
BipartiteGBS - quantum advantage with fewer assumptions

Bipartite Gaussian Boson Sampling (BipartiteGBS):
Method for programming a Gaussian Boson Sampling device

- Connects Gaussian Boson Sampling with (Fock) BosonSampling
- Removes a conjecture that is required for BosonSampling:
  Theorem: Hardness when modes are quadratic in the number of photons
- Versatile tool for building future hardness arguments:
  Theorem: Hardness with constantly-many collisions

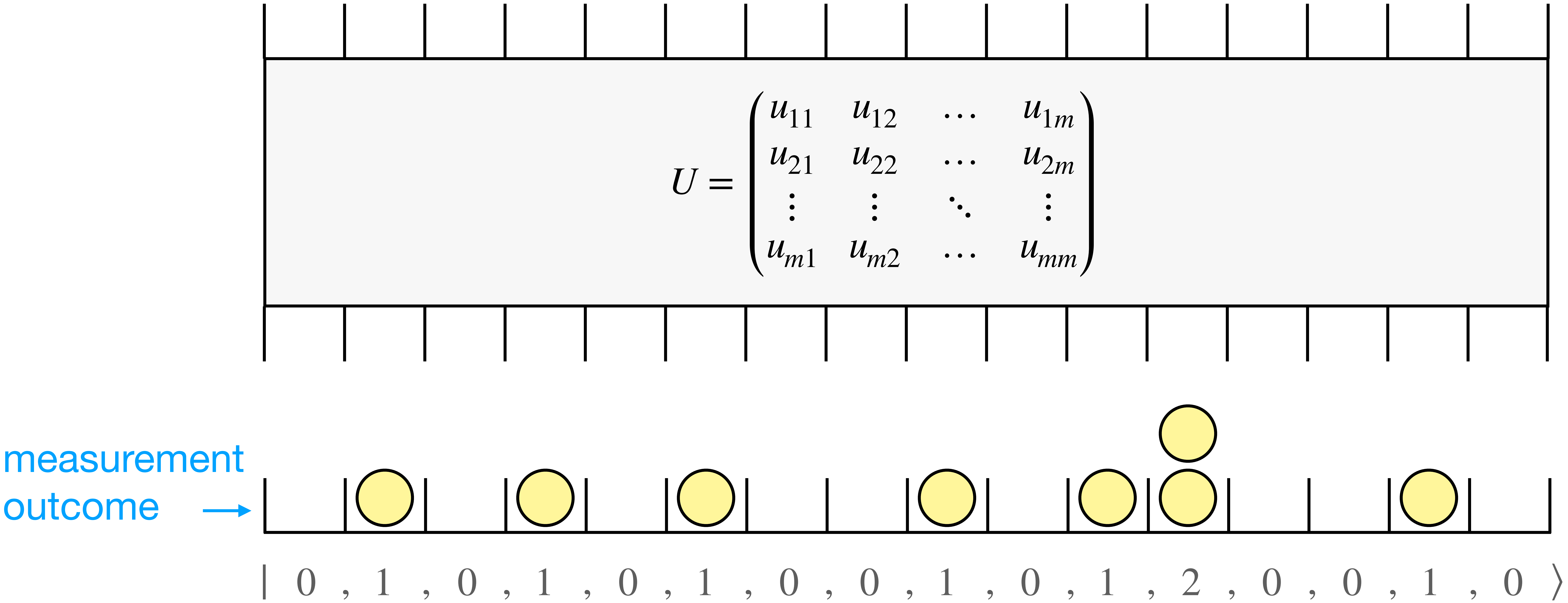
BosonSampling revisited

Theorem [AA]: It is hard* to classically sample from the output of a BosonSampling experiment (even approximately).

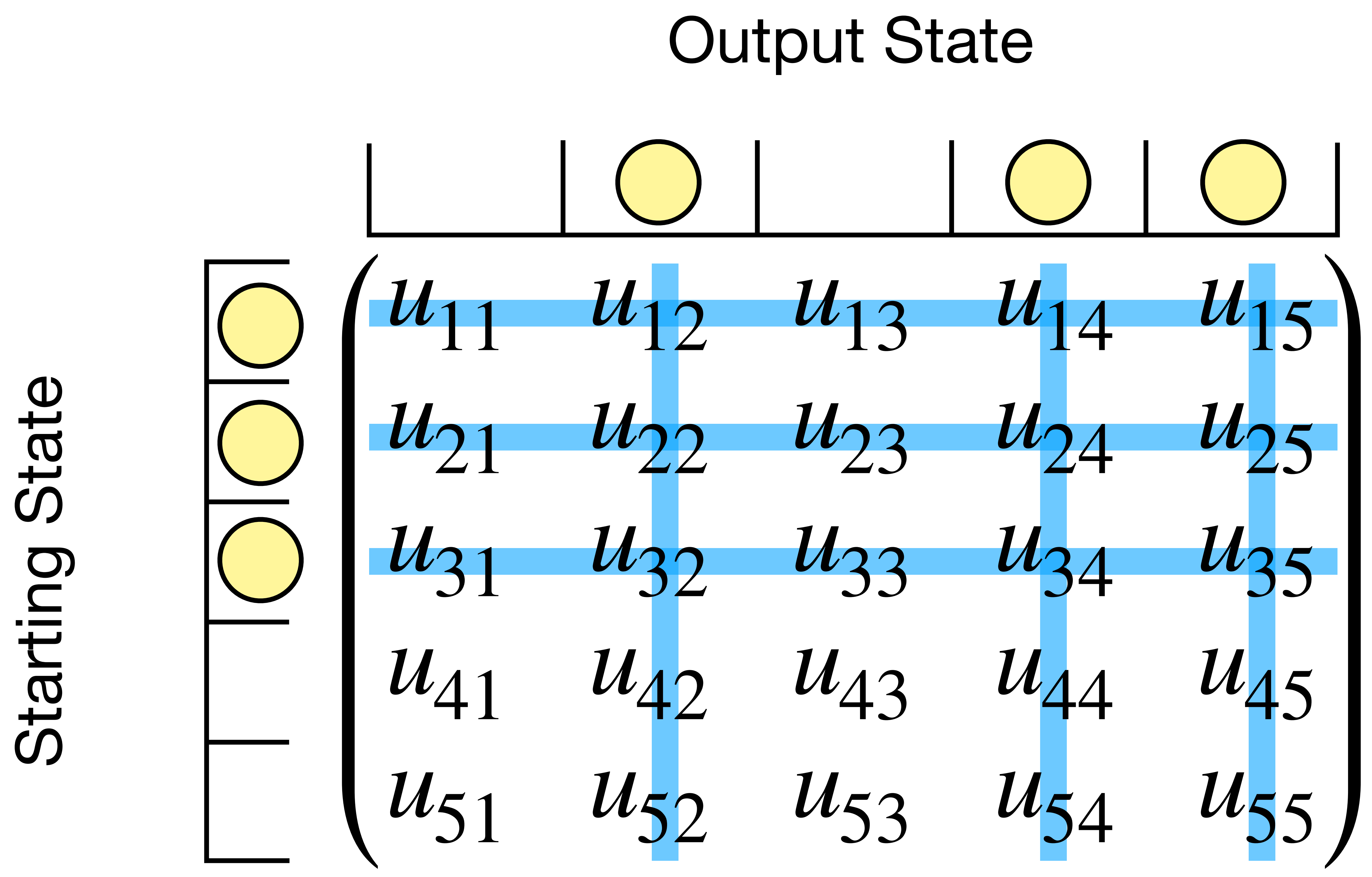


BosonSampling revisited

Theorem [AA]: It is hard* to classically sample from the output of a BosonSampling experiment (even approximately).

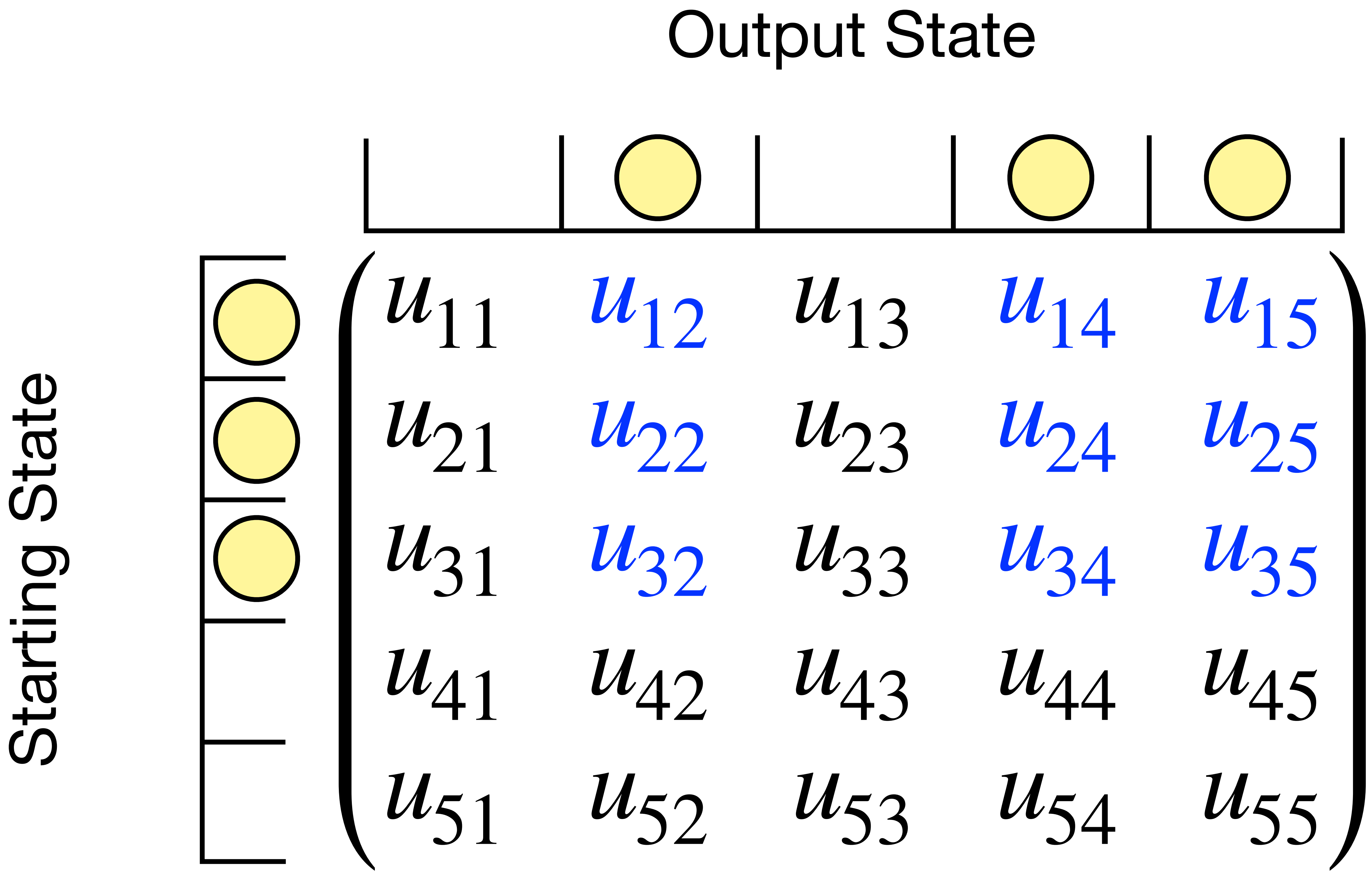


BosonSampling probabilities given by permanent



Pr[]

BosonSampling probabilities given by permanent



$$\begin{pmatrix} u_{11} & u_{12} & u_{13} & u_{14} & u_{15} \\ u_{21} & u_{22} & u_{23} & u_{24} & u_{25} \\ u_{31} & u_{32} & u_{33} & u_{34} & u_{35} \\ u_{41} & u_{42} & u_{43} & u_{44} & u_{45} \\ u_{51} & u_{52} & u_{53} & u_{54} & u_{55} \end{pmatrix}$$

Pr[] $= \text{Per} \circ \begin{pmatrix} u_{12} & u_{14} & u_{15} \\ u_{22} & u_{24} & u_{25} \\ u_{32} & u_{34} & u_{35} \end{pmatrix}$

Quantum computational advantage from linear optics

Theorem [AA]: There is no classical polynomial-time algorithm to approximately sample from the output distribution of a BosonSampling experiment.

Modulo four conjectures:

1) Non-collapse of the polynomial hierarchy
2) Gaussian permanent estimation is #P-hard
3) Anti-concentration of Gaussian permanents
4) The $n \times n$ submatrices of an $n^2 \times n^2$ unitary matrix look Gaussian

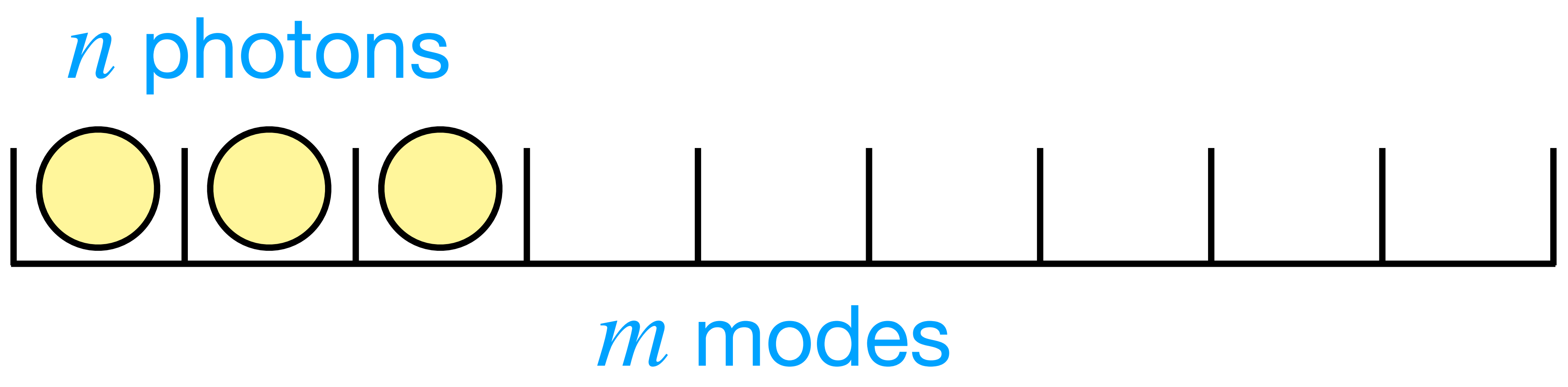
Quantum computational advantage from linear optics

Theorem [AA]: There is no classical polynomial-time algorithm to approximately sample from the output distribution of a BosonSampling experiment.

Modulo four conjectures:

1) Non-collapse of the polynomial hierarchy
2) Gaussian permanent estimation is #P-hard
3) Anti-concentration of Gaussian permanents
4) The $n \times n$ submatrices of an $n^2 \times n^2$ unitary matrix look Gaussian

Physical Interpretation:
Sufficient to have quadratically more modes than photons ($m \approx n^2$).



Quantum computational advantage from linear optics

Theorem [AA]: There is no classical polynomial-time algorithm to approximately sample from the output distribution of a BosonSampling experiment.

Modulo four conjectures:

1) Non-collapse of the polynomial hierarchy

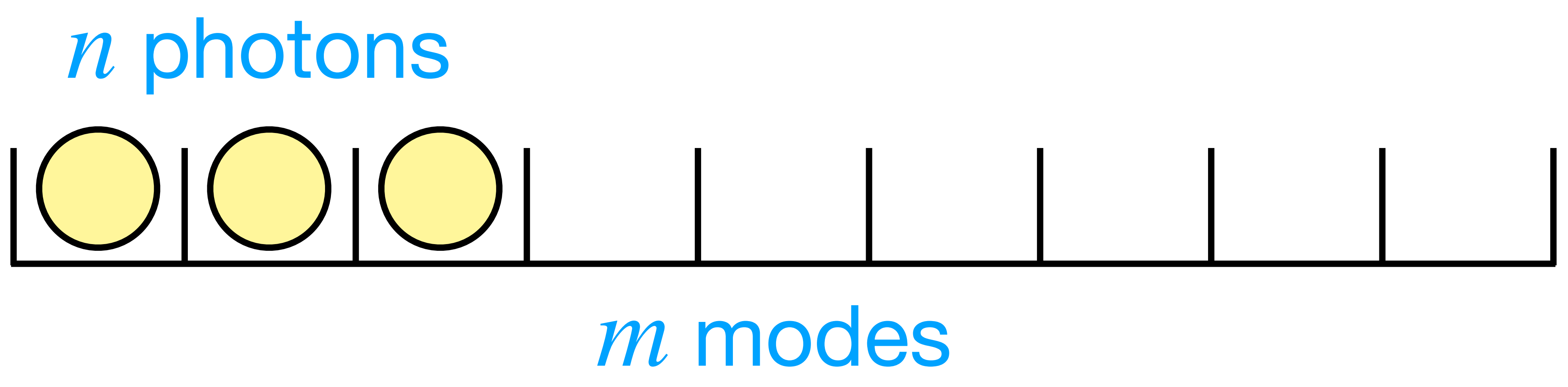
2) Gaussian permanent estimation is #P-hard

3) Anti-concentration of Gaussian permanents

4) ~~The $n \times n$ submatrices of an $n^2 \times n^2$ unitary matrix look Gaussian~~

Theorem [AA]: Can remove conjecture if $m \approx n^5$

Physical Interpretation:
Sufficient to have quadratically more modes than photons ($m \approx n^2$).

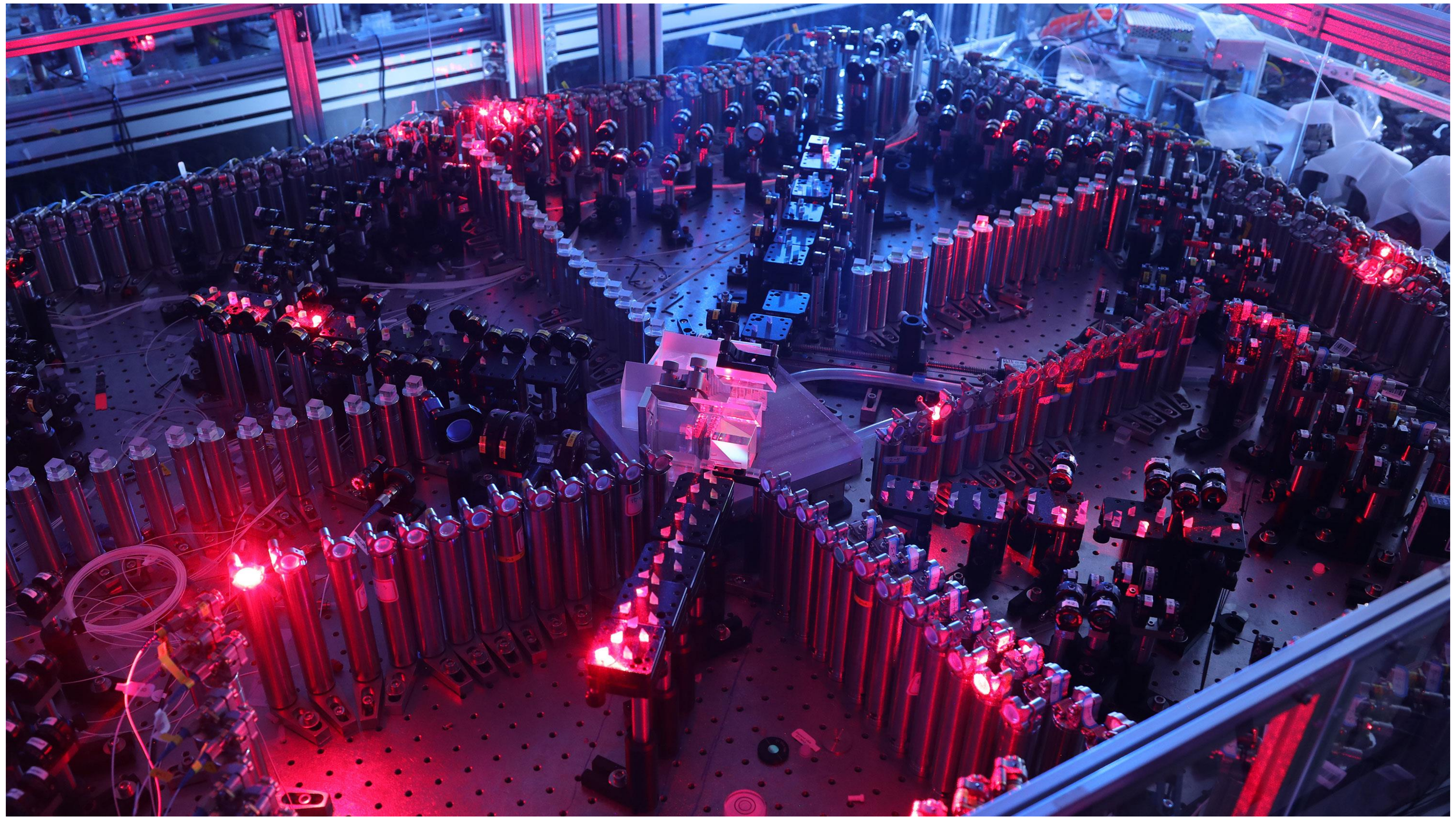


Experimental Gaussian Boson Sampling uses few modes

Gaussian Boson Sampling Experiments
Two recent experiments claiming quantum advantage [Science 20, PRL 21]

Experiment #1: 45 photons, 100 modes

Experiment #2: 113 photons, 144 modes



Credit: Quantum computational advantage using photons [Zhong, et al. Science 20]

Hardness of classical sampling with few modes

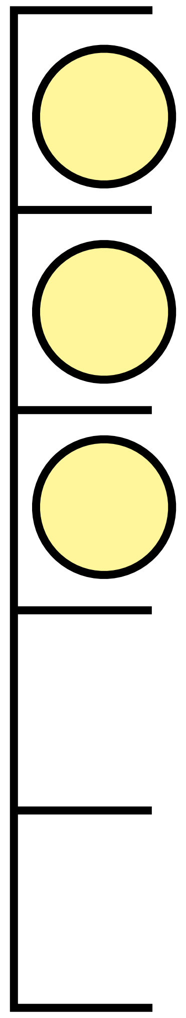
Theorem: There is no classical polynomial-time algorithm to approximately sample from the output distribution of a BipartiteGBS experiment whenever $m \approx \mathbb{E}[n]^2$.

→ Requires only three of the four BosonSampling conjectures

BosonSampling conjectures:

1) Non-collapse of the polynomial hierarchy
2) Gaussian permanent estimation is #P-hard
3) Anti-concentration of Gaussian permanents
4) ~~The $n \times n$ submatrices of an $n^2 \times n^2$ unitary matrix look Gaussian~~

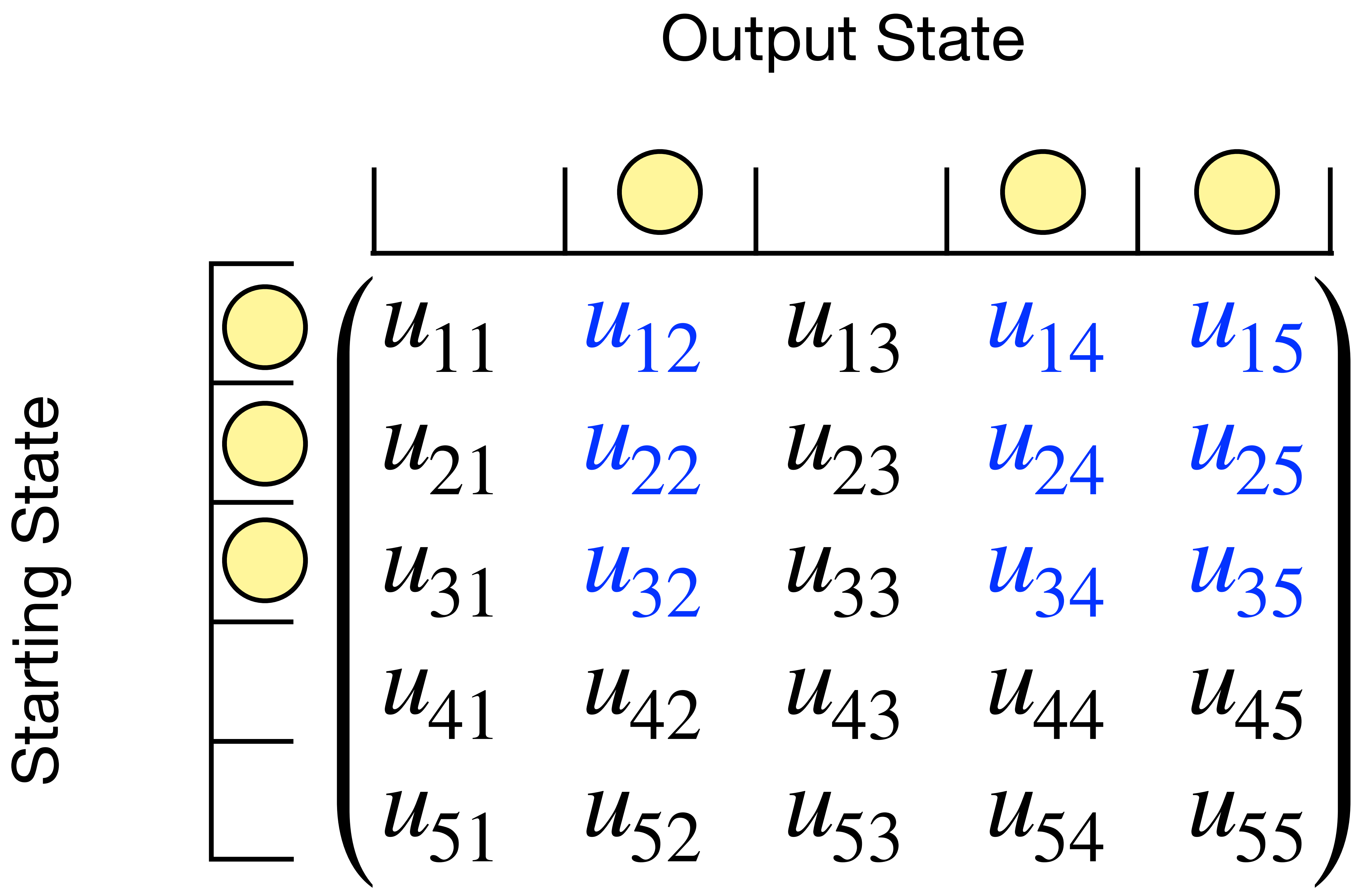
Submatrices of Haar random unitaries



$$\begin{pmatrix} u_{11} & \color{blue}{u_{12}} & u_{13} & \color{blue}{u_{14}} & \color{blue}{u_{15}} \\ u_{21} & \color{blue}{u_{22}} & u_{23} & \color{blue}{u_{24}} & \color{blue}{u_{25}} \\ u_{31} & \color{blue}{u_{32}} & u_{33} & \color{blue}{u_{34}} & \color{blue}{u_{35}} \\ u_{41} & u_{42} & u_{43} & u_{44} & u_{45} \\ u_{51} & u_{52} & u_{53} & u_{54} & u_{55} \end{pmatrix}$$

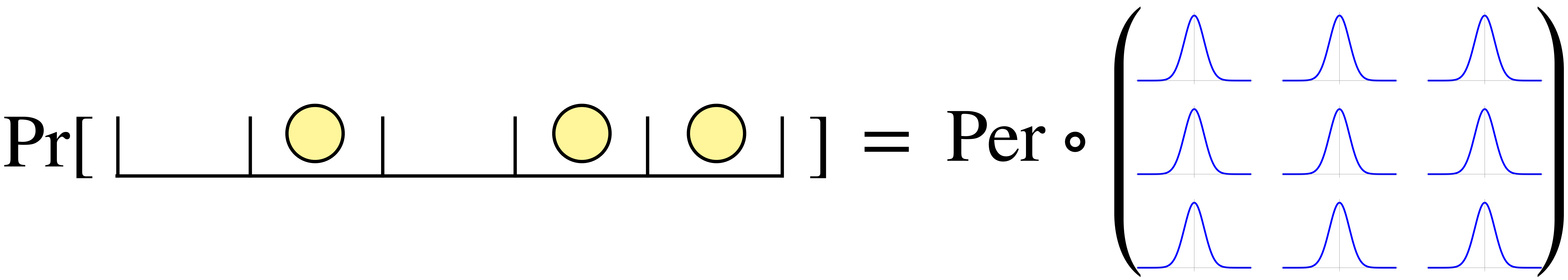
$\Pr[$  $] = \mathrm{Per} \circ \begin{pmatrix} u_{12} & u_{14} & u_{15} \\ u_{22} & u_{24} & u_{25} \\ u_{32} & u_{34} & u_{35} \end{pmatrix}$

Submatrices of Haar random unitaries



Problem: Only rigorous convergence bounds whenever $m = \omega(n^5)$.

Required Property: this submatrix approximates a matrix with i.i.d. complex Gaussian entries whenever the unitary is Haar random.



Prior work on submatrices of Haar random unitaries

Theorem [Jiang 2006]**:** The $n \times n$ submatrices of random $m \times m$ real orthogonal matrices converge (in total variation) to real Gaussian matrices whenever $m = \omega(n^2)$.

→ *Issues for BosonSampling:*

1) Real matrices rather than complex ones

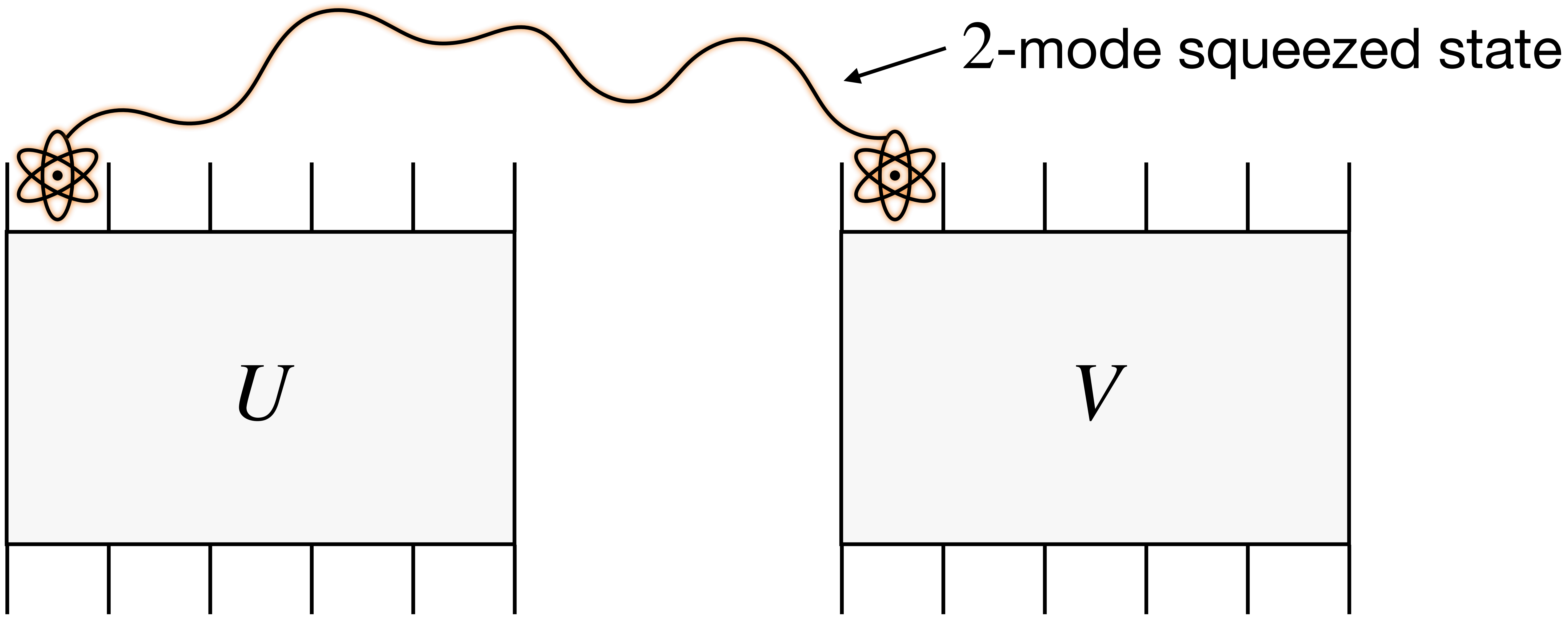
2) Does not bound the *rate* of this convergence

Theorem [AA]**:** Variation distance is $O(\delta)$ whenever $m \geq \frac{n^5}{\delta} \log^2 \frac{n}{\delta}$.

→ We do not try to improve this theorem directly!

Avoid conjecture by directly encoding Gaussian entries

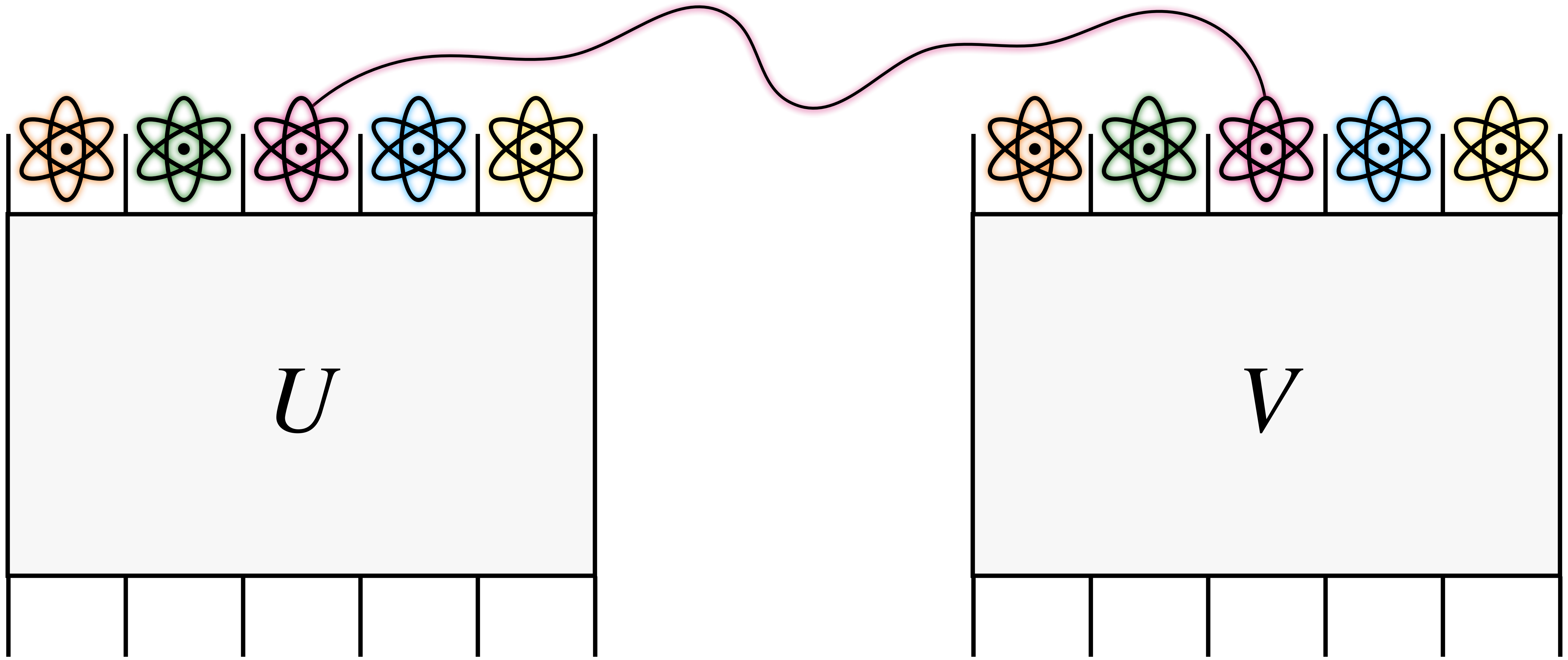
BipartiteGBS: There is a Gaussian Boson Sampling experiment such that the output probabilities are governed by the permanents of submatrices of *arbitrary* matrices.



Avoid conjecture by directly encoding Gaussian entries

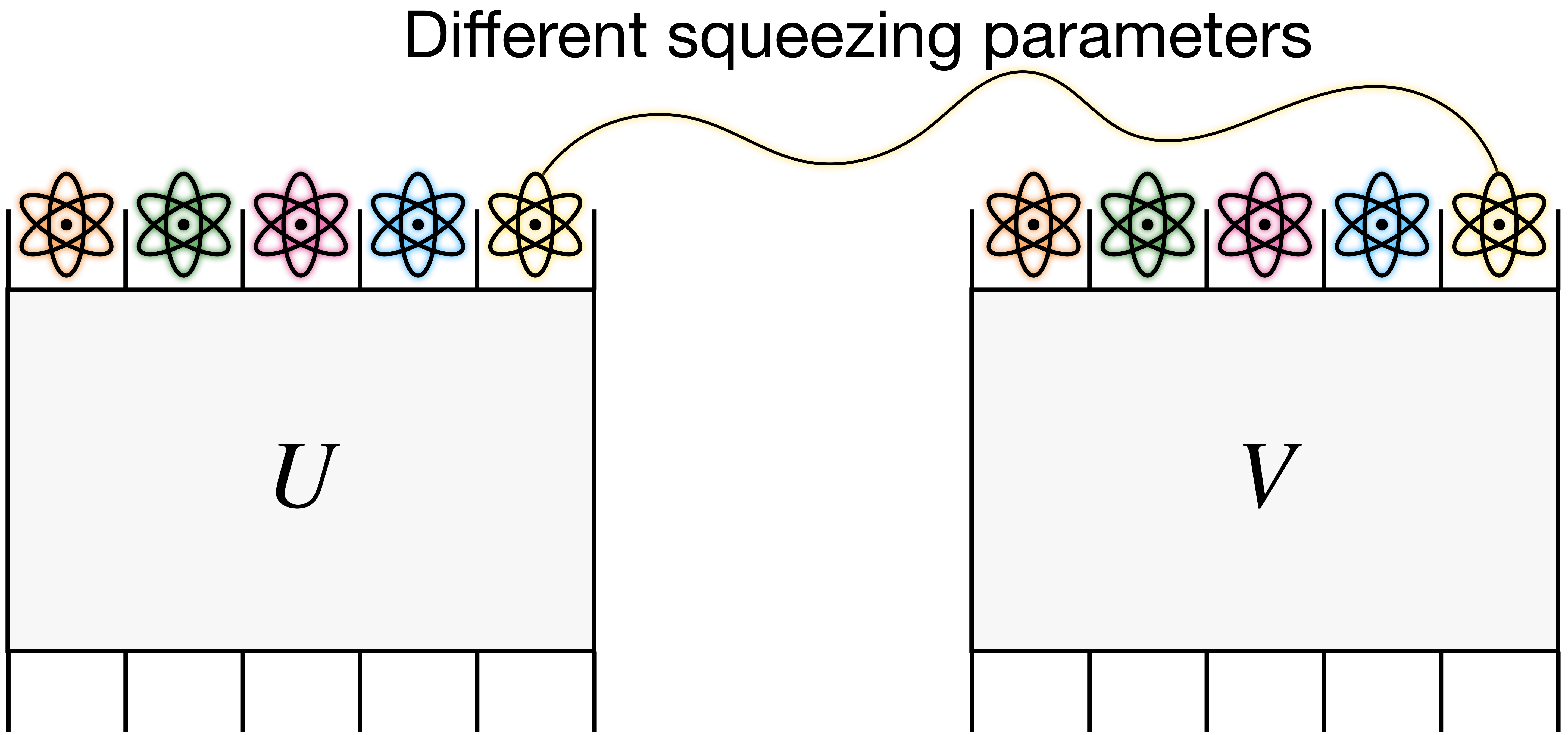
BipartiteGBS: There is a Gaussian Boson Sampling experiment such that the output probabilities are governed by the permanents of submatrices of *arbitrary* matrices.

Different squeezing parameters



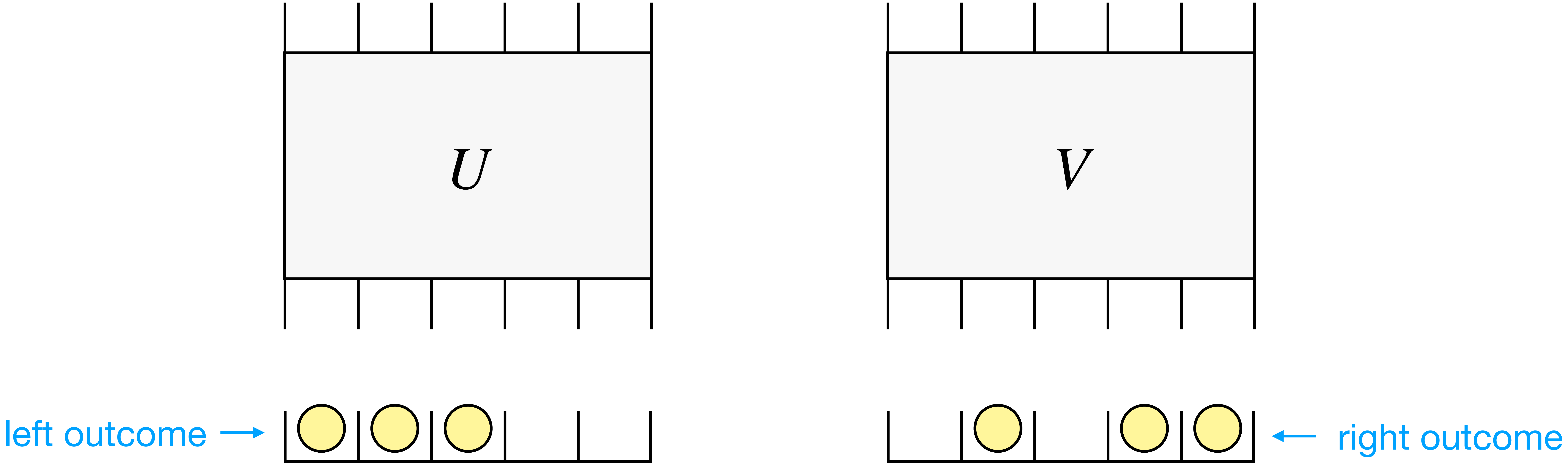
Avoid conjecture by directly encoding Gaussian entries

BipartiteGBS: There is a Gaussian Boson Sampling experiment such that the output probabilities are governed by the permanents of submatrices of *arbitrary* matrices.



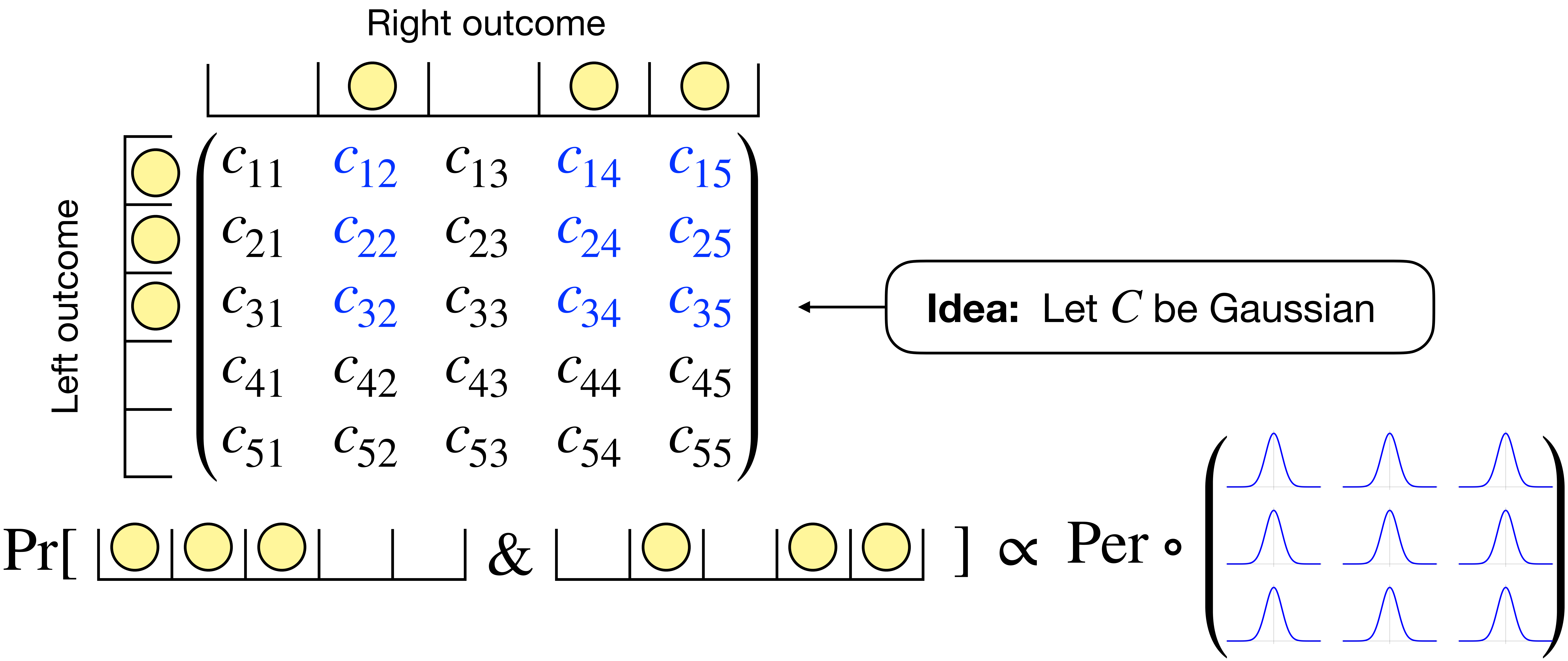
Avoid conjecture by directly encoding Gaussian entries

BipartiteGBS: There is a Gaussian Boson Sampling experiment such that the output probabilities are governed by the permanents of submatrices of *arbitrary* matrices.



Avoid conjecture by directly encoding Gaussian entries

BipartiteGBS: There is a Gaussian Boson Sampling experiment such that the output probabilities are governed by the permanents of submatrices of *arbitrary* matrices.

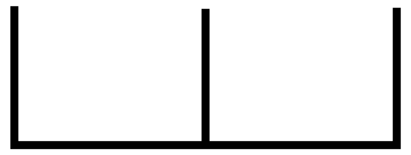
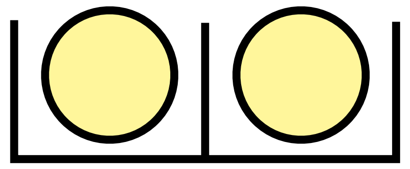
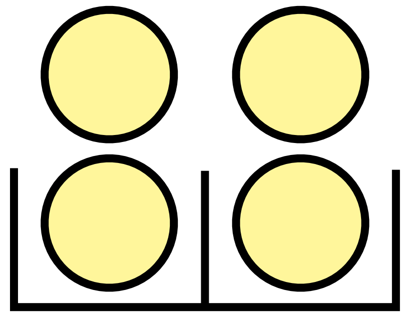


BipartiteGBS - input states and output probabilities

Input states:

$$S_2(r)\,|\,0{,}0\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}(\tanh r)^n\,|\,n,n\rangle$$

Expected photon number
$\langle n\rangle = \sinh^2(r)$

$S_2(1)\,|\,0{,}0\rangle =$ .65  + .49  + .38  + $\cdots$

Output probabilities:

Left modes: $S = |\,s_1, \ldots, s_m\rangle$

Right modes: $T = |\,t_1, \ldots, t_m\rangle$

Singular value decomposition of arbitrary matrix with singular values in $[0,1)$.

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

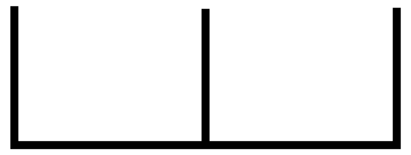
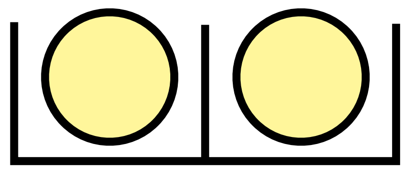
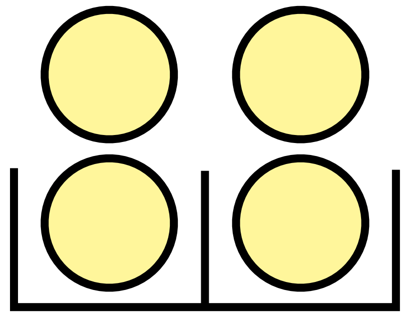
$$\Pr[S\;\&\;T] = \frac{1}{\mathcal{Z}}\frac{|\,\mathrm{Per}(C_{S,T})\,|^2}{\prod_{i=1}^{m} s_i!t_i!}$$

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

BipartiteGBS - input states and output probabilities

Input states: $S_2(r)\,|0,0\rangle = \dfrac{1}{\cosh r}\sum_{n=0}^{\infty}(\tanh r)^n\,|n,n\rangle$

Expected photon number
$\langle n\rangle = \sinh^2(r)$

$S_2(1)\,|0,0\rangle = $ .65  + .49  + .38  + $\cdots$

Output probabilities:

Left modes: $S = |s_1,\ldots,s_m\rangle$

Right modes: $T = |t_1,\ldots,t_m\rangle$

$$\Pr[S\ \&\ T] = \frac{1}{\mathcal{Z}}\frac{|\mathrm{Per}(C_{S,T})|^2}{\prod_{i=1}^{m} s_i!\,t_i!}$$

Scattershot BosonSampling:
$V = I$ and r_i's constant

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

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

Proof outline for main theorem

1) Suppose there is a classical algorithm that samples from the output distribution of a BipartiteGBS experiment

$$\|\mathcal{D}_C - \mathcal{D}'_C\| \leq \beta$$

Gaussian Permanent Estimation: Given $n \times n$ matrix X with i.i.d. standard complex Gaussian entries, estimate $|\text{Per}\, X|^2$ to $(\epsilon n!)$-additive accuracy with probability $1 - \delta$.

→ *Conjecture* [AA]: Gaussian Permanent Estimation is #P-hard.

2) Hide the $n \times n$ Gaussian matrix X in an $m \times m$ Gaussian matrix C

3) BipartiteGBS with matrix C has output with probability proportional to $|\text{Per}\, X|^2$

4) Estimate this probability using Stockmeyer counting on $\mathcal{D}'_C$ to compute $|\text{Per}\, X|^2$

5) By conjecture, algorithm for $|\text{Per}\, \text{X}|^2$ implies collapse of polynomial hierarchy

Is the Stockmeyer counting argument good enough?

Gaussian Permanent Estimation: Estimate $|\mathrm{Per}\,X|^2$ to $(\epsilon n!)$-additive accuracy

Lemma: There is a $\mathsf{BPP}^{\mathsf{NP}}$ algorithm that estimates $|\mathrm{Per}\,X|^2$ to additive error

$$\epsilon\left(\mathcal{Z} m^{(3/2)n}\binom{m}{n}^{-2}\right)$$

- Accuracy of this estimate depends on $\mathcal{Z} = \prod_{i=1}^{m}\cosh^2(r_i)$
- $\mathcal{Z}$ depends on the singular values of matrix with i.i.d. Gaussian entries

Have we just traded one problem in random matrix theory with another?

Is the Stockmeyer counting argument good enough?

Gaussian Permanent Estimation: Estimate $|\mathrm{Per}\, X|^2$ to $(\epsilon n!)$-additive accuracy

Lemma: There is a $\mathsf{BPP}^{\mathsf{NP}}$ algorithm that estimates $|\mathrm{Per}\, X|^2$ to additive error

$$\epsilon\left(\mathscr{Z} m^{(3/2)n} \binom{m}{n}^{-2}\right)$$

- Accuracy of this estimate depends on $\mathscr{Z} = \prod_{i=1}^{m} \cosh^2(r_i)$
- $\mathscr{Z}$ depends on the singular values of matrix with i.i.d. Gaussian entries

Theorem: $\Pr[\mathscr{Z} \leq \frac{1}{\delta} e^{\sqrt{m}}] \leq \delta$ whenever $m = \Theta(n^2)$.

- *Proof tool:* for Gaussian C, we have $\mathscr{Z}^{-1} = \det(I - CC^\dagger)$.

Summary and future directions

Theorem: Hard to approximately sample from the output distribution of a GBS experiment in the no-collision regime ($m \approx n^2$) under BosonSampling conjectures.

Can we get hardness in the high-collision regime ($m = o(n^2)$)?

→ Probabilities given by permanents of Gaussian matrices with repeated rows/columns

Repeated Gaussian Permanent Estimation: Given $c \times c$ Gaussian matrix X and collision patterns $S = (s_1, \ldots, s_c)$, $T = (t_1, \ldots, t_c)$ with $s_1 + \ldots + s_c = t_1 + \ldots + t_c = n$, estimate $|\mathrm{Per}\, X_{S,T}|^2$ to $(\epsilon n! s_1! \cdots s_c! t_1! \cdots t_c!)$-additive accuracy with probability $1 - \delta$.

→ *Speculative conjecture:* Repeated Gaussian Permanent Estimation is #P-hard