Peaked Boson Sampling: towards efficiently verifiable and NISQ-able quantum advantage

Michelle Ding

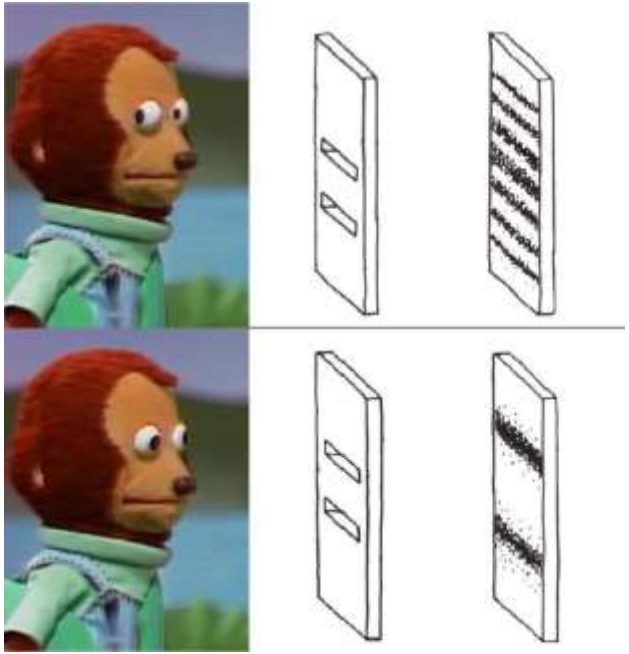
April 28th, 2025

Overview

- Introduction
- Related Work
- Our Work
  - Analytical Results
  - Experimental Results
- Remarks and Future Work

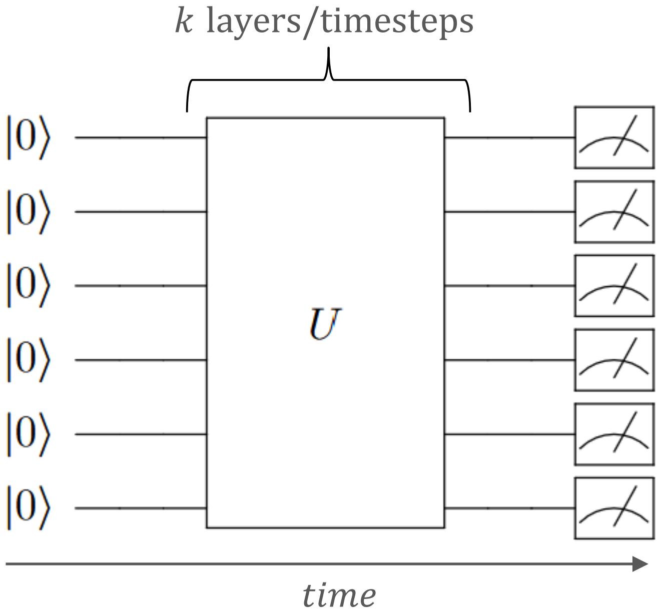
Introduction

- Quantum computing = solving hard problems based on quantum mechanics
  - decision problems
  - promise problems
  - sampling problems
    - RCS, BosonSampling



The standard circuit model

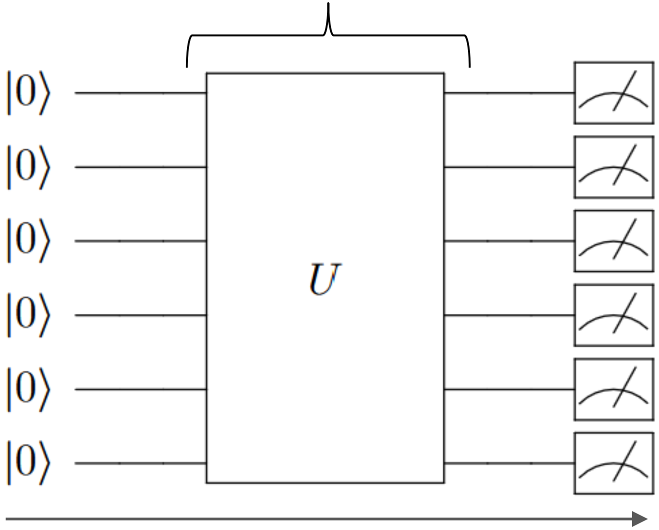
- qubits, gates, and measurement



The standard circuit model

- qubits, gates, and measurement

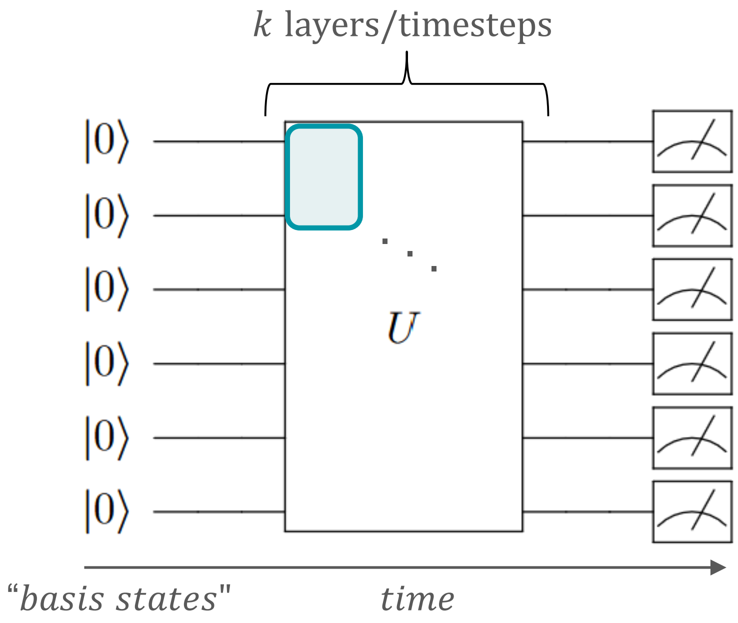
k layers/timesteps



“*basis states*" *time*

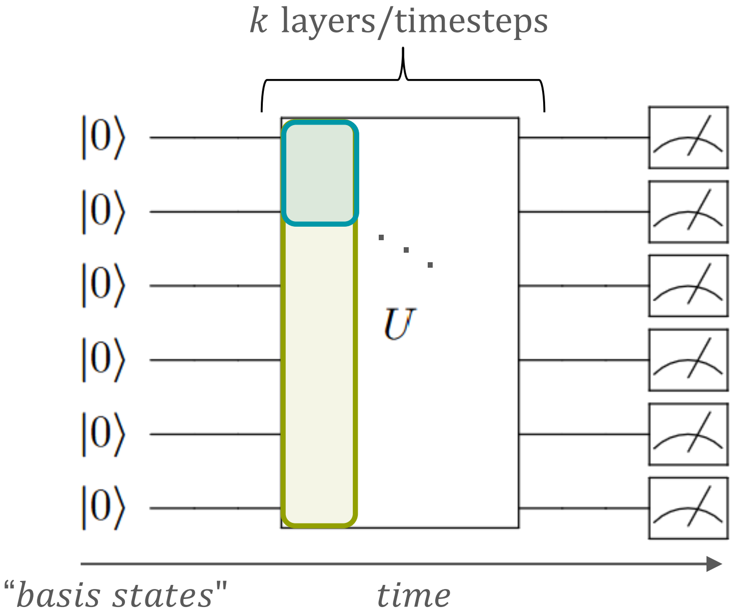
The standard circuit model

- qubits, gates, and measurement



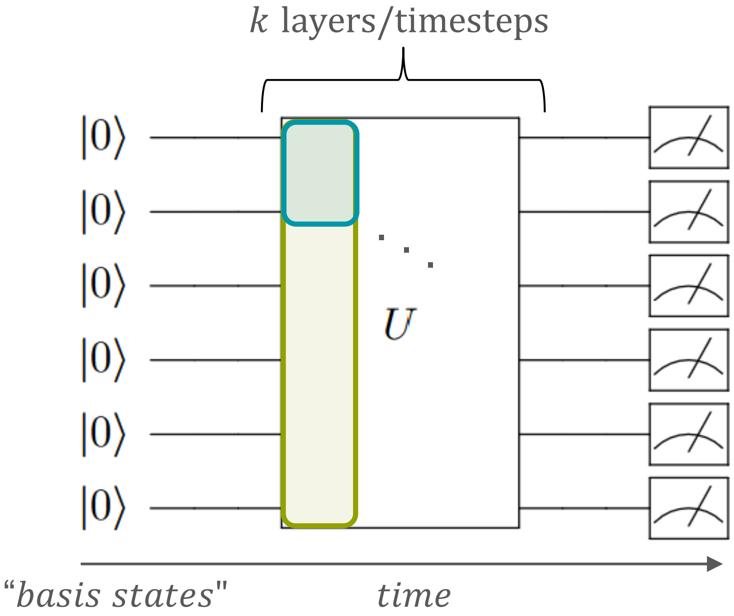
The standard circuit model

- qubits, gates, and measurement



The standard circuit model

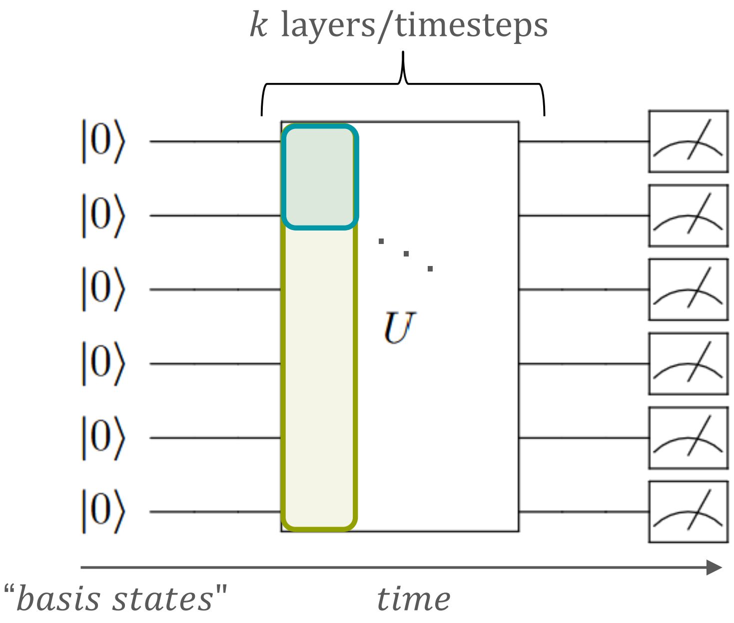
- qubits, gates, and measurement



entanglement, superposition, interference phenomena

The standard circuit model

- qubits, gates, and measurement

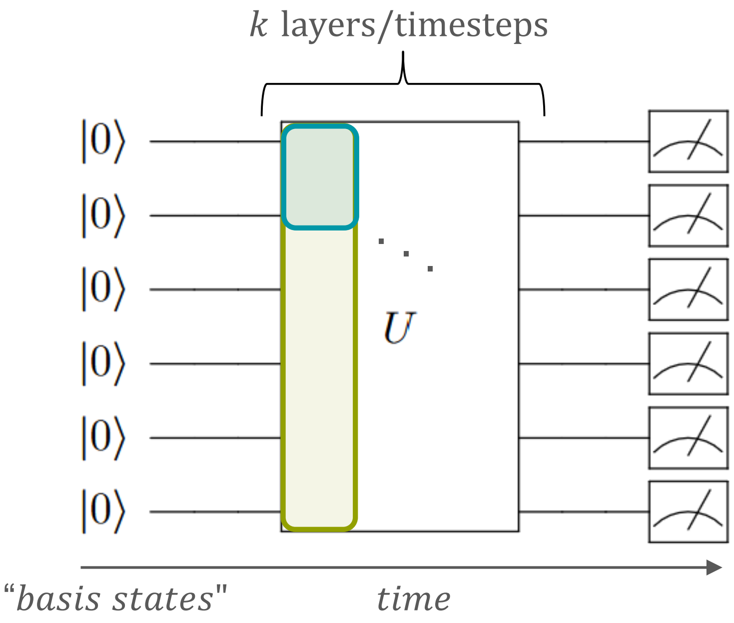


entanglement, superposition, interference phenomena

n *qubits* $\rightarrow 2^n$ *basis states*

The standard circuit model

- qubits, gates, and measurement



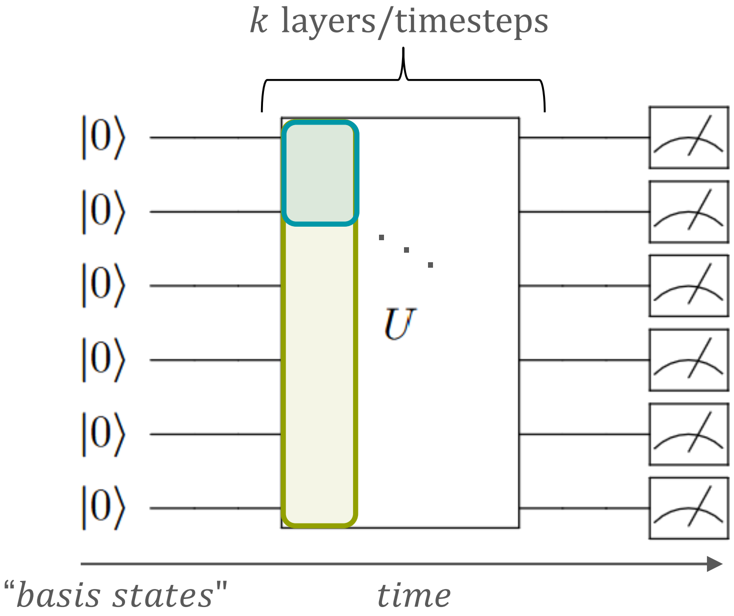
entanglement, superposition, interference phenomena

n *qubits* $\rightarrow 2^n$ *basis states*

$$\frac{|000000\rangle + |000001\rangle + \ldots + |111111\rangle}{2^n} \xrightarrow{M} |000001\rangle$$

The standard circuit model

- qubits, gates, and measurement



entanglement, superposition, interference phenomena

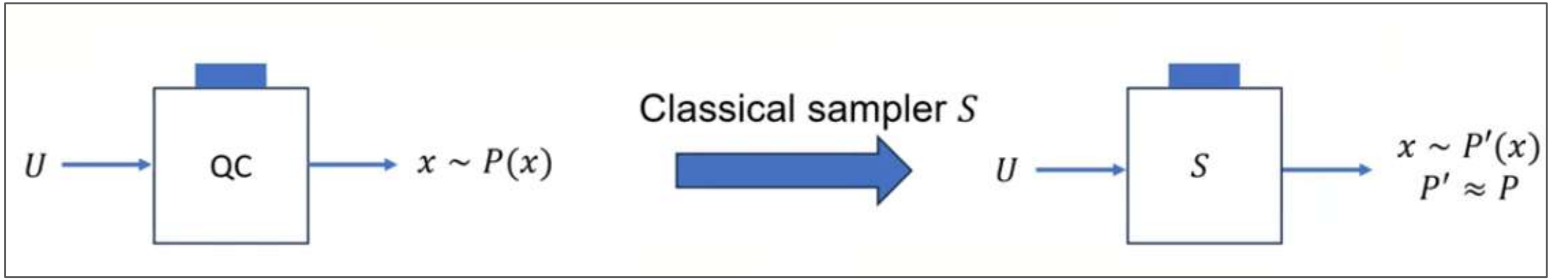
n *qubits* $\rightarrow 2^n$ *basis states*

(random)

$$\frac{|000000\rangle + |000001\rangle + \ldots + |111111\rangle}{2^n} \xrightarrow{M} |000001\rangle$$

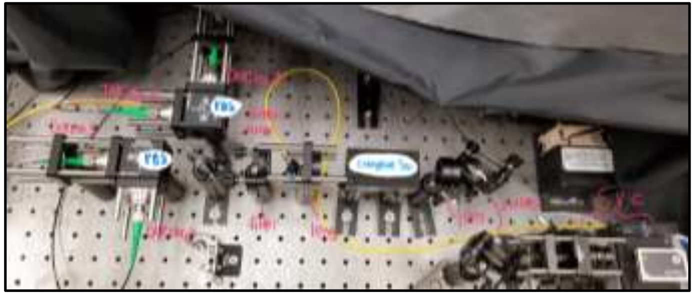
Sampling

- Input: A classical description of an n-qubit quantum circuit U
  and probability distribution $P(x) = |\langle x|U|0^n\rangle|^2$,
  classically sample from $P' \approx P$

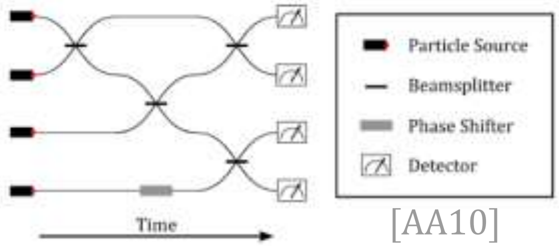


[BGL23b]

Boson Sampling



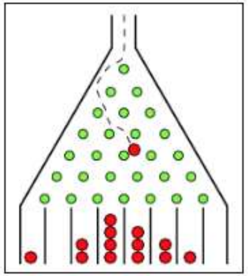
Ex. of a linear optical setup



[AA10]

Ex. of a beamsplitter network

Galton board showing the indistinguishability of bosons

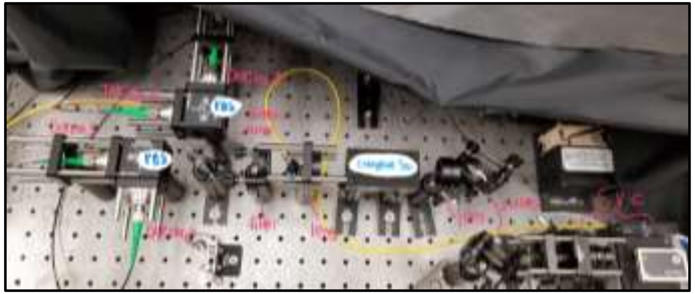


[AA10]

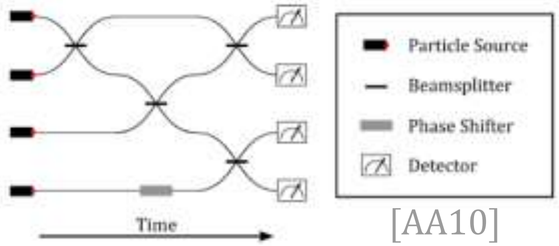
$$\Pr_{D_U}[S] = |\langle 1_n|\varphi(U)|S\rangle|^2 = \frac{|\mathrm{Per}(U_{S,S})|^2}{s_1!\, s_2! \cdots s_m!}$$

BosonSampling complexity as a function of the permanent

Boson Sampling



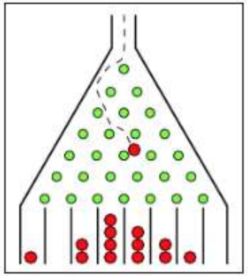
Ex. of a linear optical setup



[AA10]

Ex. of a beamsplitter network

Galton board showing the indistinguishability of bosons

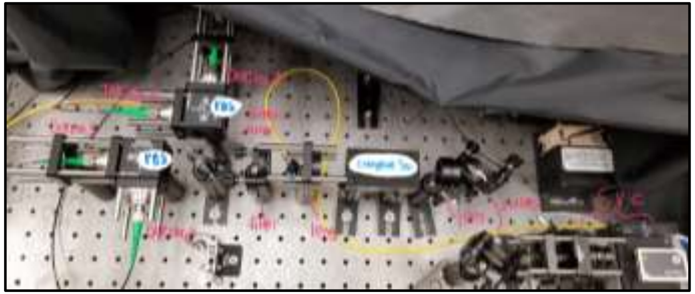


[AA10]

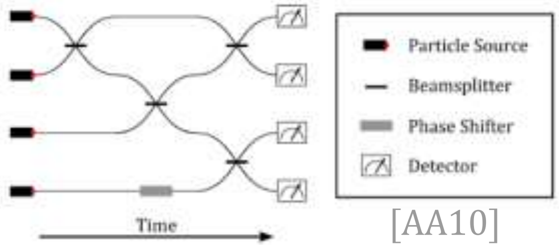
$$\Pr_{D_U}[S] = |\langle 1_n|\varphi(U)|S\rangle|^2 = \frac{|\mathrm{Per}(U_{S,S})|^2}{s_1!\, s_2! \cdots s_m!}$$

BosonSampling complexity as a function of the permanent

Boson Sampling



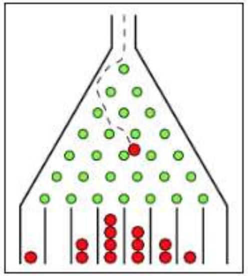
Ex. of a linear optical setup



[AA10]

Ex. of a beamsplitter network

Galton board showing the indistinguishability of bosons



[AA10]

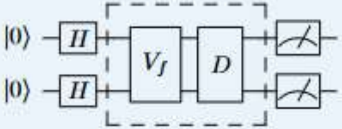
$$\Pr_{D_U}[S] = |\langle 1_n | \varphi(U) | S \rangle|^2 = \frac{|\mathrm{Per}(U_{S,S})|^2}{s_1!\, s_2! \cdots s_m!}$$

BosonSampling complexity as a function of the permanent

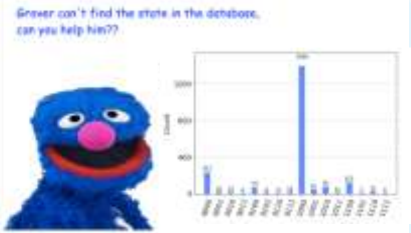
Examples of Peaked Circuits

Definition 1.5: Grover's Algorithm

Let $f : \{0,1\}^n \to \{0,1\}$ and <u>one marked item</u> x^* such that $f(x^*) = 1$.

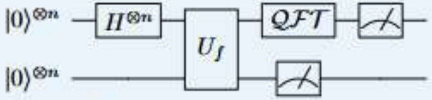


repeat $O(2^{n/2})$ times



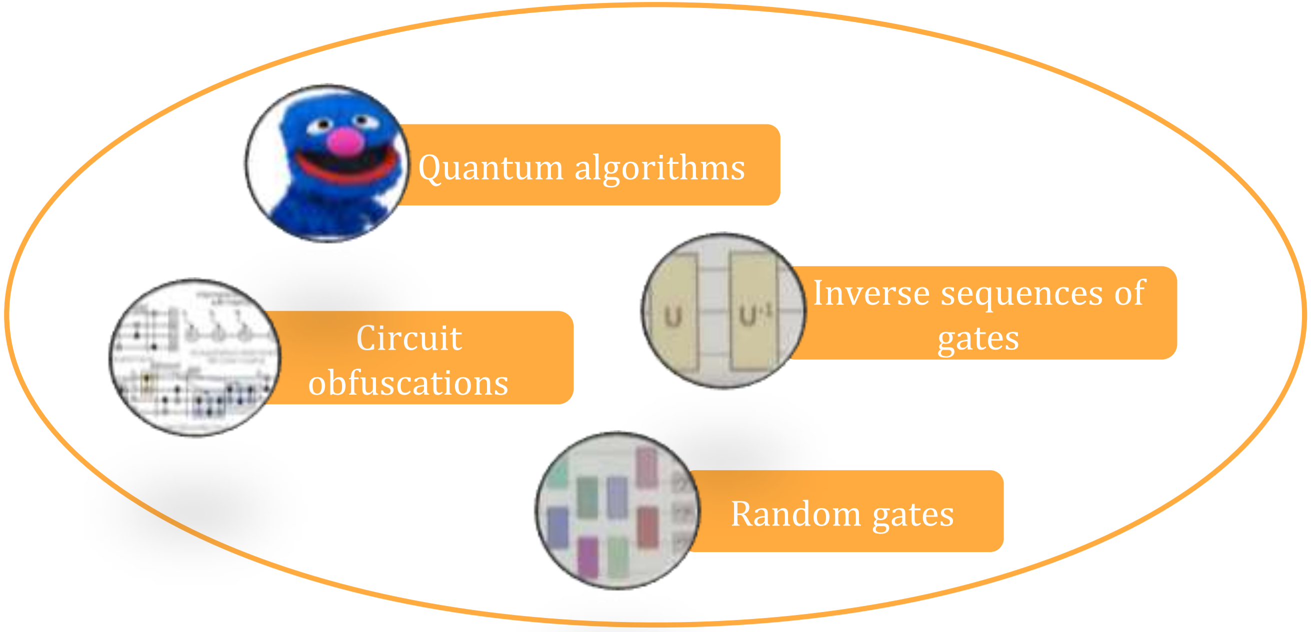
Definition 3.4: Shor's Factoring Algorithm

Let an integer $N = p \cdot q = 2^n$. Note p, q are primes and n is the number of bits used to represent N.
<u>Context:</u> Factoring is presumably hard, so used in modern cryptography systems ft. the RSA protocol
<u>Claim:</u> Consider a function $f(x) = a^x \pmod{N}$. Then computing the period of $f(x)$ allows us to factor N.



Denote U_f as the oracle computing $f(x)$: $U_f|x\rangle|0^{\otimes n}\rangle = |x\rangle|f(x)\rangle$.

Examples of Peaked Circuits



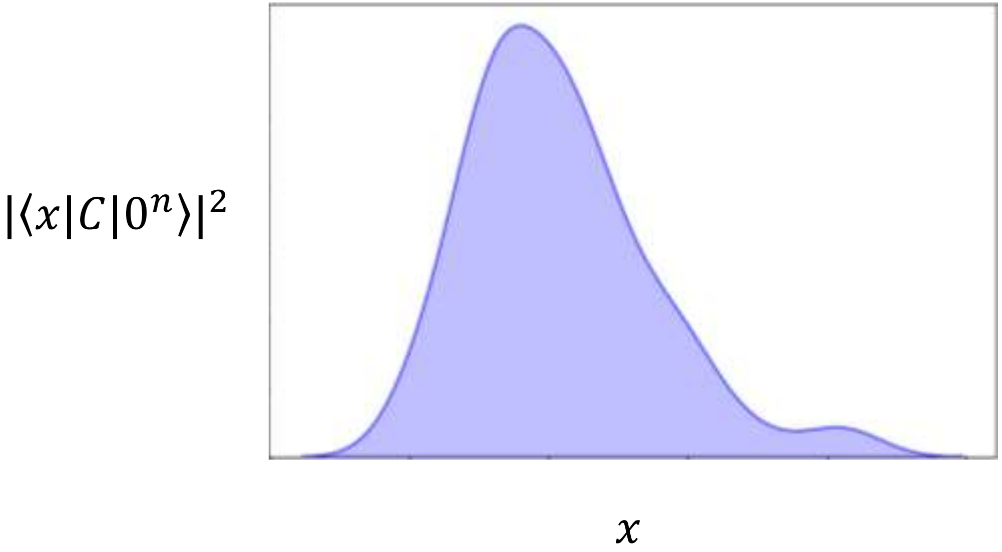
Peaked Interferometers

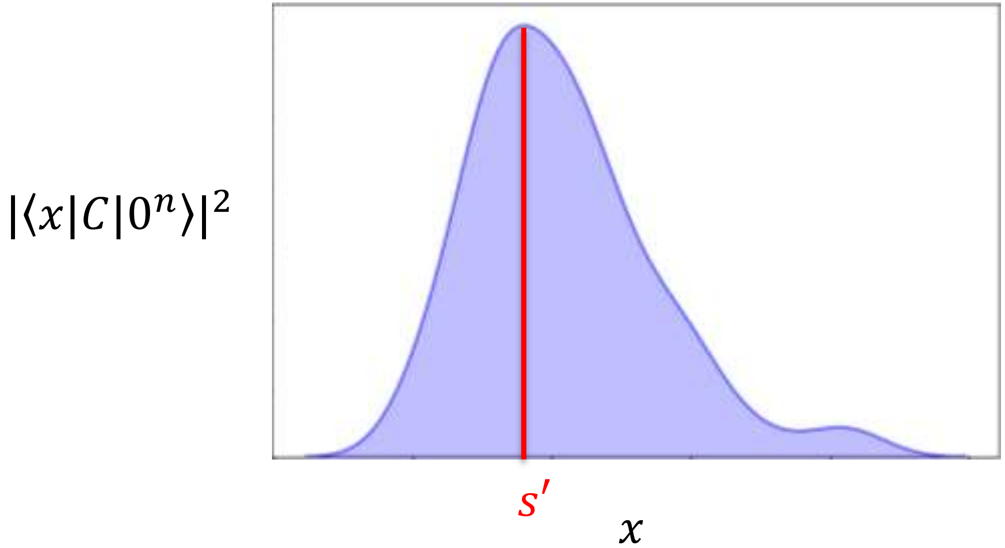
- We say an interferometer U is δ-peaked if:

$$\max_{s\epsilon\Phi_{m,n}} |\langle s|\varphi(U)|1_n\rangle|^2 \geq \delta$$

- Where $\Phi_{m,n}$ are basis vectors, $|1_n\rangle$ is the input Fock state and $\varphi(U)$ is the homomorphism described by [AA10].

- Let the max arg be s'. Giving s' to a classical verifier enables efficient verification.

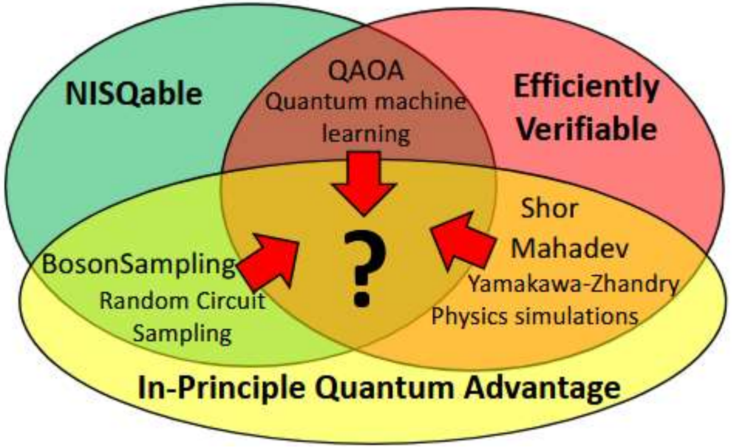

$|\langle x|C|0^n\rangle|^2$
x


$|\langle x|C|0^n\rangle|^2$
s'
x

Quantum Advantage

A convincing demonstration should ideally be:

1. (NISQable) It can be implemented **efficiently** with a feasible quantum experiment.
2. (IPQA) It is **provably** classically hard to solve.
3. (Eff. Verifiable) The solution can be **verified efficiently** on a classical device.

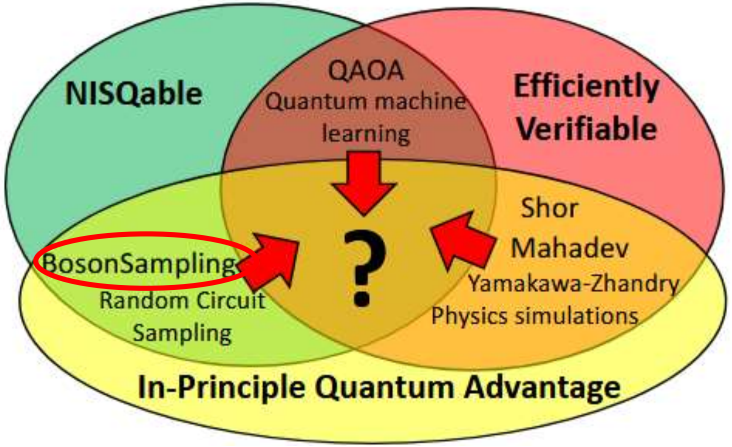


[AZ24]

Quantum Advantage

A convincing demonstration should ideally be:

1. (NISQable) It can be implemented **efficiently** with a feasible quantum experiment.
2. (IPQA) It is **provably** classically hard to solve.
3. (Eff. Verifiable) The solution can be **verified efficiently** on a classical device.

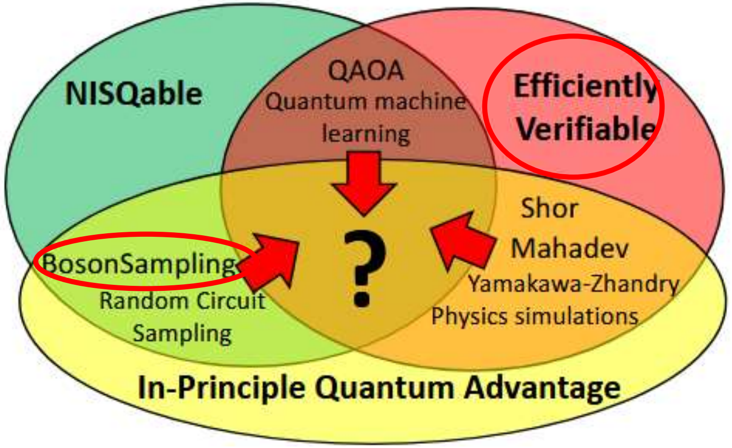


[AZ24]

Quantum Advantage

A convincing demonstration should ideally be:

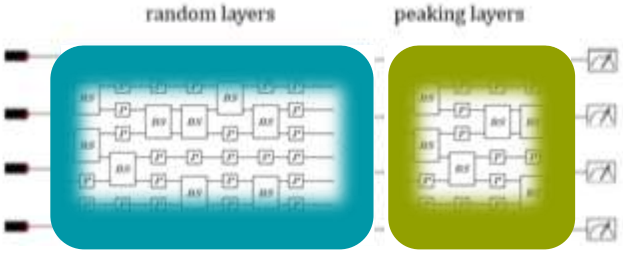
1. (NISQable) It can be implemented **efficiently** with a feasible quantum experiment.
2. (IPQA) It is **provably** classically hard to solve.
3. (Eff. Verifiable) The solution can be **verified efficiently** on a classical device.



[AZ24]

Searching for Structure

- Generating peaked but hard-to-sample from linear optical distributions

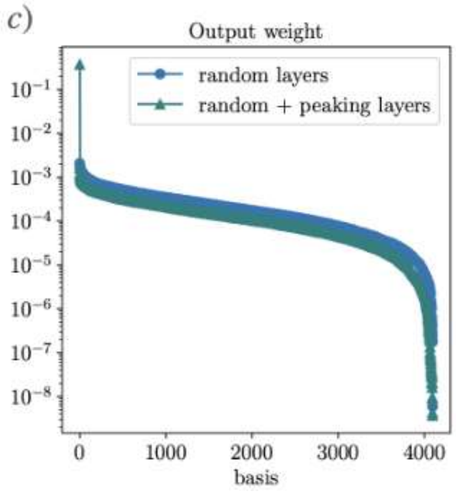


- Explicitly-peaked structures
- Postselected linear optical networks

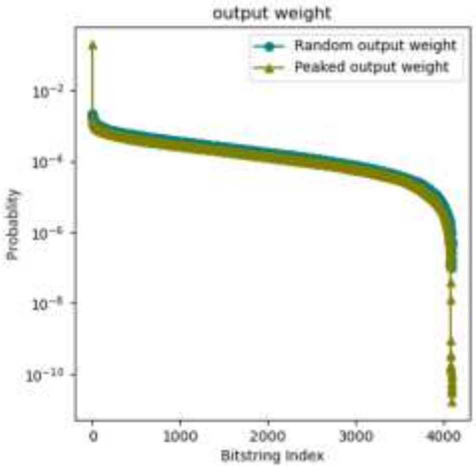
➢ We study this numerically

Related Work

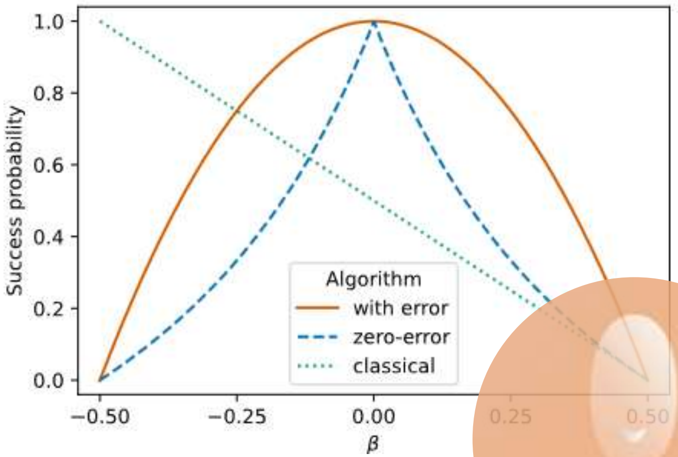
- Efficiently Verifiable Peaked Circuit Sampling [AZ24]
- Complement Sampling [BBW25]



[AZ24]



replication



[BBW25]

Analytical Results

- O(mn) peaking gates are sufficient to produce optimal peakedness.

Proof:

Theorem 45 (Parallelization of Linear-Optics Circuits) *Given any $m \times m$ unitary operation U, one can map the initial state $|1_n\rangle$ to $\varphi(U)|1_n\rangle$ using a linear-optical network of depth $O(n \log m)$, consisting of $O(mn)$ beamsplitters and phaseshifters.* [AA10]

- Upper bounded by a quadratic number of gates!

Analytical Results

- In comparison, the circuit model requires an exponential number of gates:

Theorem 1.3: Solovay-Kitaev

Most unitaries $U \in U(2^n)$ require an exponential number of gates from any gate set G to implement it within some tolerance ϵ. The maximal number of minimal gates, aka the circuit complexity upper bound is

$$C_\epsilon(U) \leq \frac{4^n}{\log |G|} \log\left(\frac{1}{\epsilon}\right)$$

Analytical Results

- Furthermore, we can optimize this to O(m) gates

Claim 2. *A network of $O(t)$ nonlocal peaking gates acting on mode 0 and mode $i \in [2, t]$ can transfer amplitude from the other $t-1$ modes to mode 0.*

- Simply tune the beamsplitter parameters to transfer amplitude.

$$B(\theta, \phi) = \begin{bmatrix} \cos(\theta) & -e^{-i\phi}\sin(\theta) \\ e^{i\phi}\sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$\Rightarrow B_{1,i} = \frac{|a_1|}{\sqrt{|a_1|^2 + |a_i|^2}} \begin{bmatrix} 1 & -\frac{a_2^*}{a_1^*} \\ -\frac{a_2}{a_1} & 1 \end{bmatrix}$$

Analytical Results

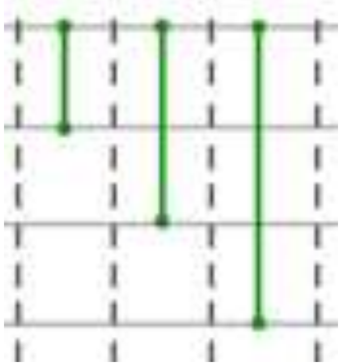
- Furthermore, we can optimize this to O(t) gates

Claim 2. *A network of $O(t)$ nonlocal peaking gates acting on mode 0 and mode $i \in [2, t]$ can transfer amplitude from the other $t-1$ modes to mode 0.*

- Simply tune the beamsplitter parameters to transfer amplitude.

$$B(\theta, \phi) = \begin{bmatrix} \cos(\theta) & -e^{-i\phi}\sin(\theta) \\ e^{i\phi}\sin(\theta) & \cos(\theta) \end{bmatrix}$$

$$\Rightarrow B_{1,i} = \frac{|a_1|}{\sqrt{|a_1|^2 + |a_i|^2}} \begin{bmatrix} 1 & -\frac{a_2^*}{a_1^*} \\ -\frac{a_2}{a_1} & 1 \end{bmatrix}$$



Analytical Results

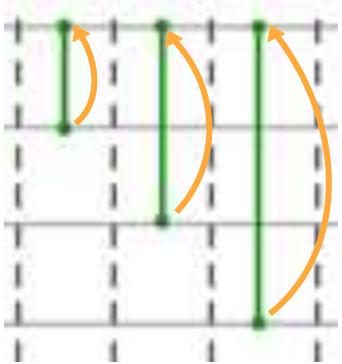
- Furthermore, we can optimize this to O(t) gates

Claim 2. *A network of $O(t)$ nonlocal peaking gates acting on mode 0 and mode $i \in [2, t]$ can transfer amplitude from the other $t-1$ modes to mode 0.*

- Simply tune the beamsplitter parameters to transfer amplitude.

$$B(\theta, \phi) = \begin{bmatrix} \cos(\theta) & -e^{-i\phi}\sin(\theta) \\ e^{i\phi}\sin(\theta) & \cos(\theta) \end{bmatrix}$$

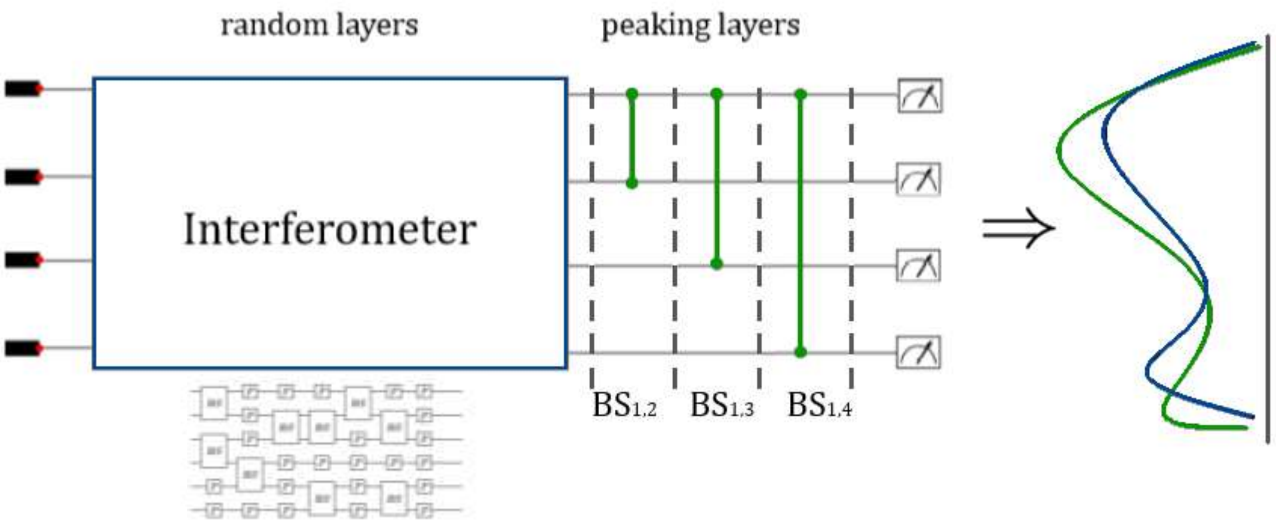
$$\Rightarrow B_{1,i} = \frac{|a_1|}{\sqrt{|a_1|^2 + |a_i|^2}} \begin{bmatrix} 1 & -\frac{a_2^*}{a_1^*} \\ -\frac{a_2}{a_1} & 1 \end{bmatrix}$$



Experimental Setup

- We use the optics construction from Claim 2. for SGD experiments.

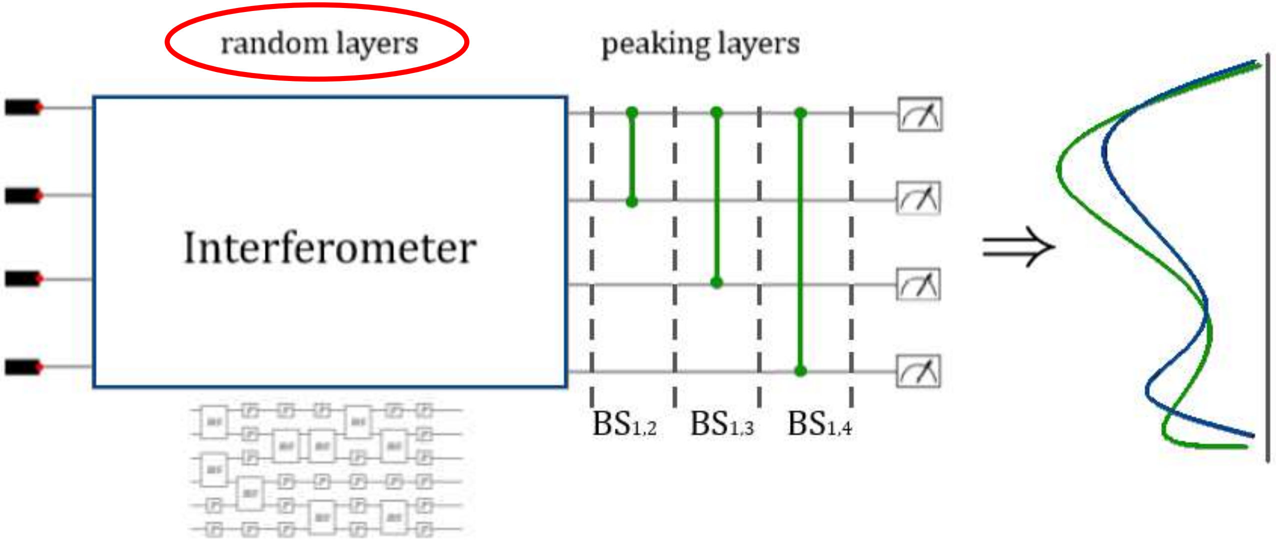
STRAWBERRY FIELDS



Experimental Setup

- We use the optics construction from Claim 2. for SGD experiments.

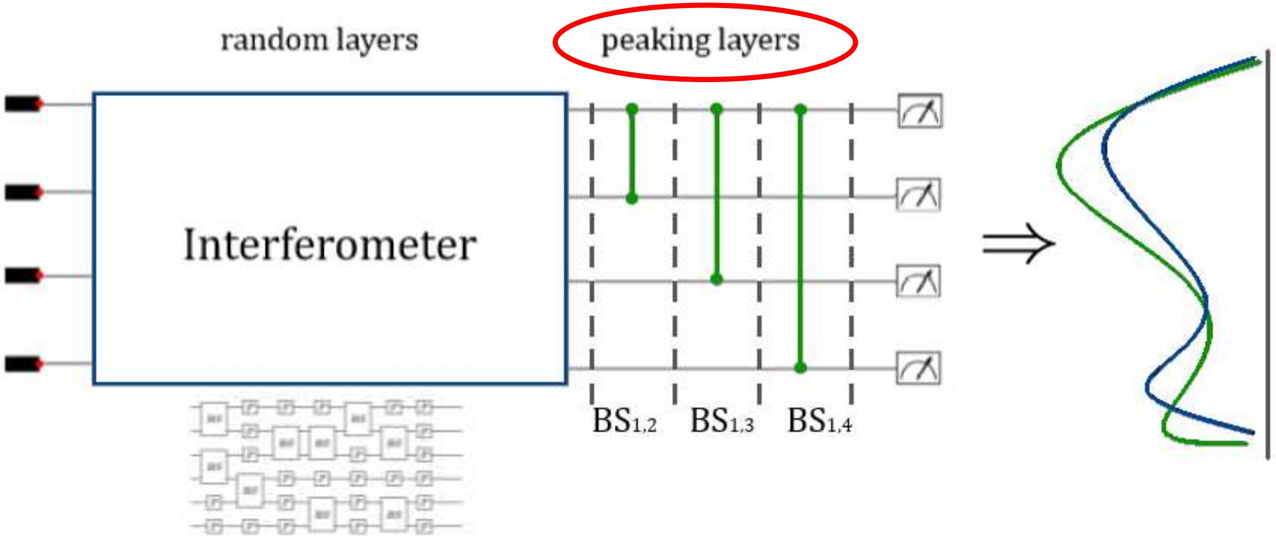
STRAWBERRY FIELDS



Experimental Setup

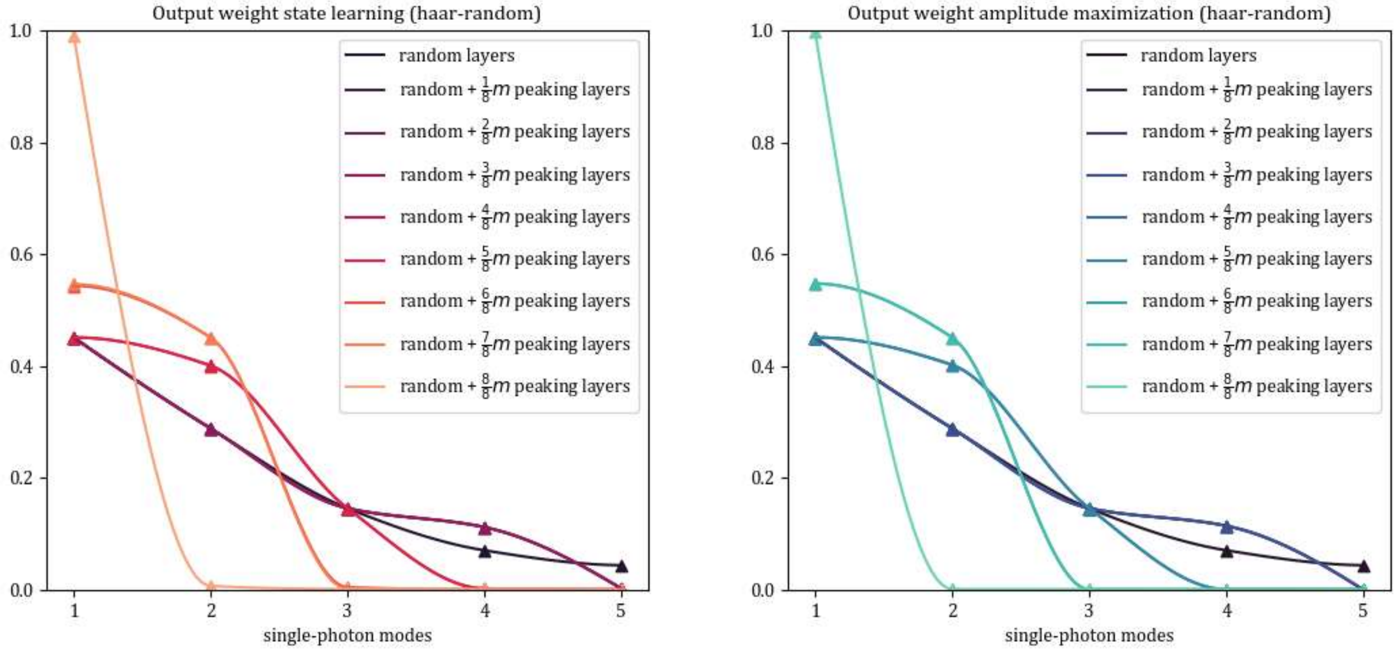
- We use the optics construction from Claim 2. for SGD experiments.

STRAWBERRY FIELDS



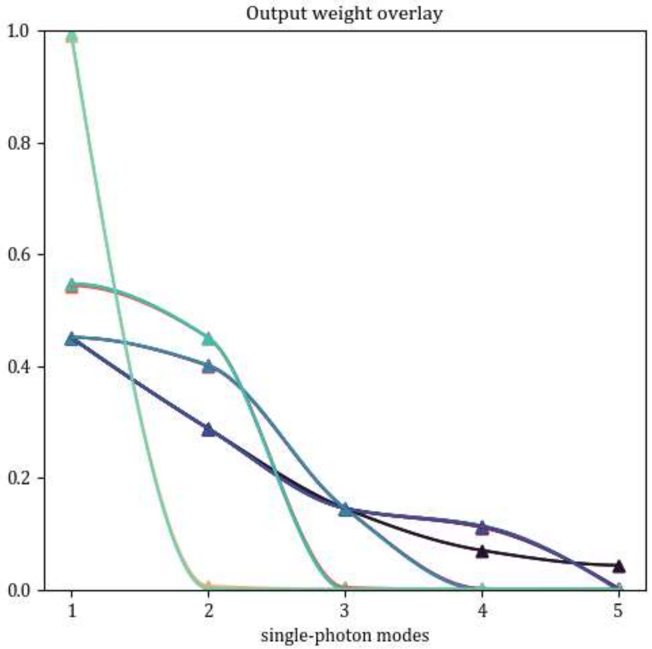
Explicitly-peaked structures

- Two different cost functions:



Explicitly-peaked structures

- Overlay of the two graphs



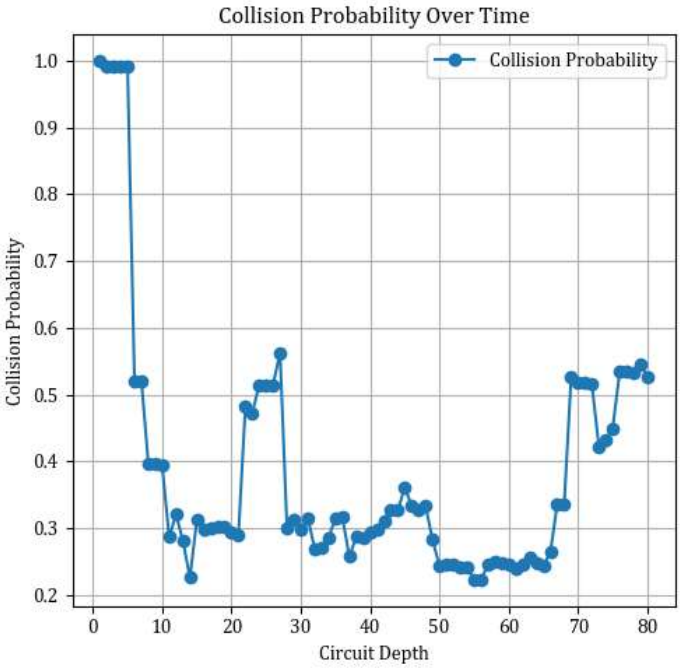
Postselection

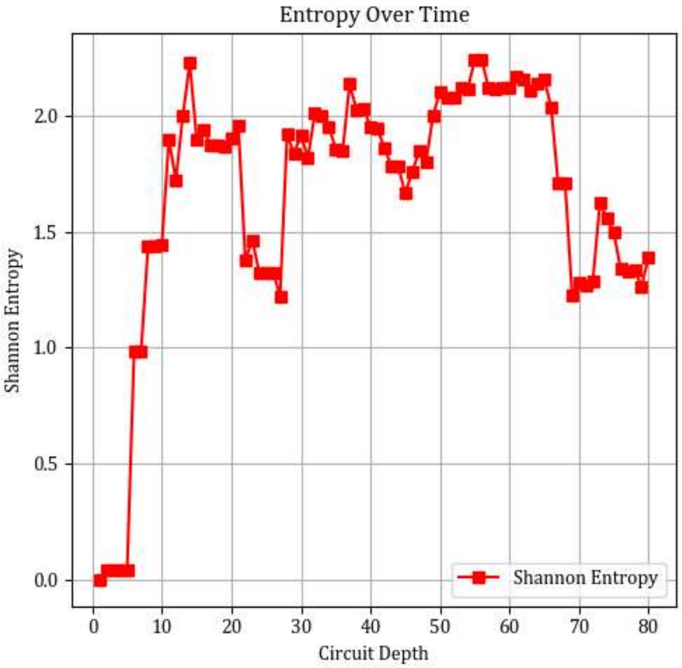
- What we really want is to examine naturally peaked interferometers
- Peaked random circuits are exponentially rare! [1] Postselection impossible to analyze numerically
- But with linear optics the system size is smaller and unitaries scale with direct product! Vague intuition for why it would be simpler

1 **Theorem 2.2** (Probability of finding peaked circuits in an well-spread circuit ensemble). *Let P_δ be the probability of finding a δ-peaked circuit in a well-spread ensemble. Then $P_\delta = O(\frac{1}{\delta^2 2^n})$.*

Single-shot instances

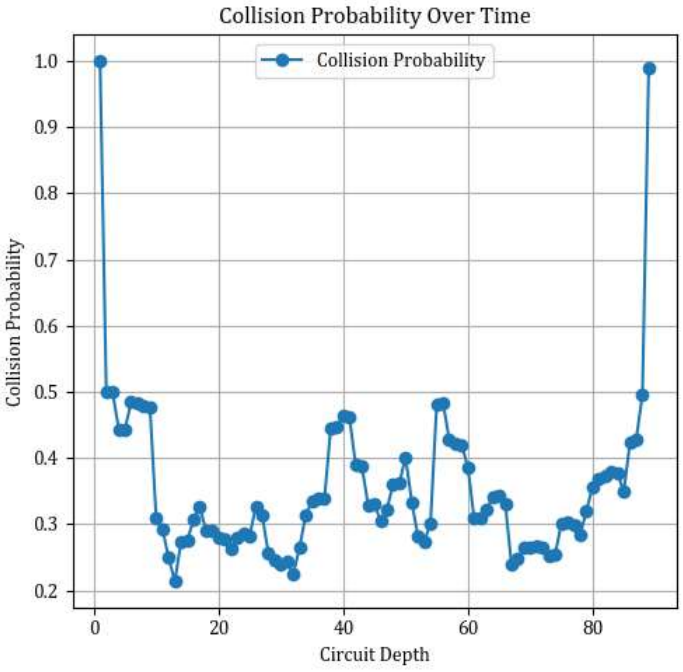
Collision probability and entropy of a post-selected circuit

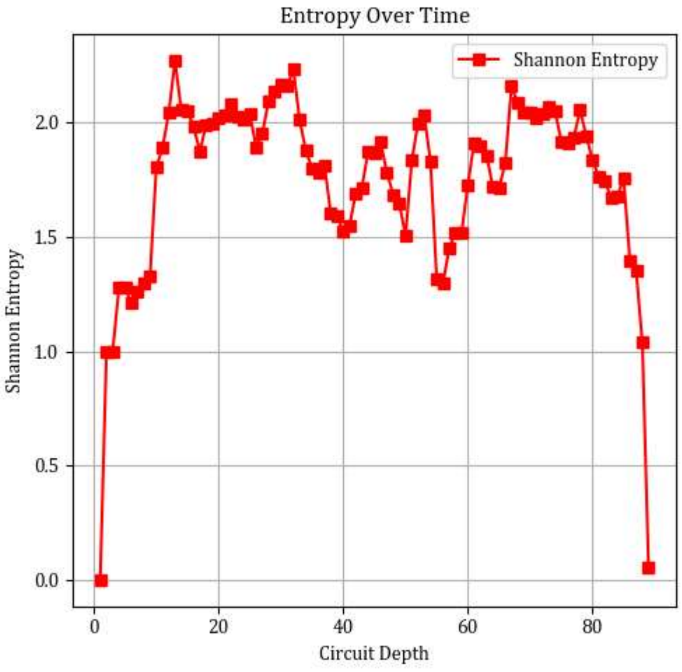




Single-shot instances

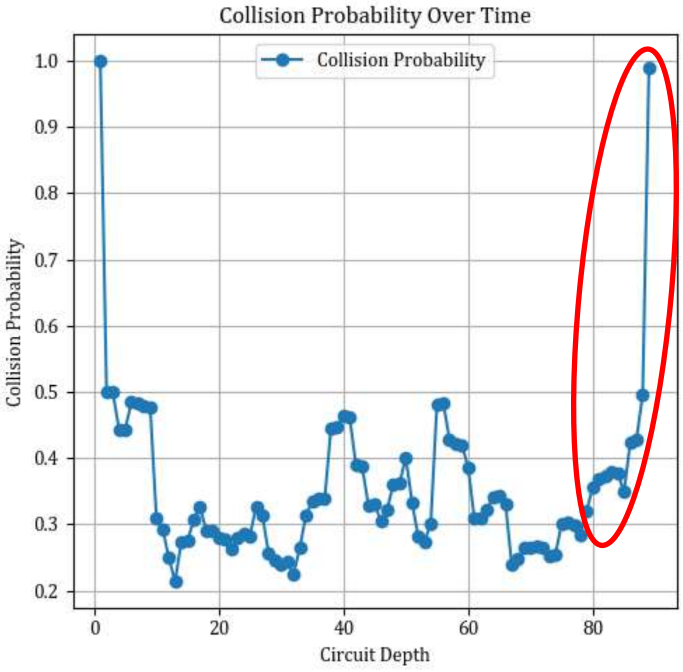
Collision probability and entropy of an explicitly-peaked circuit

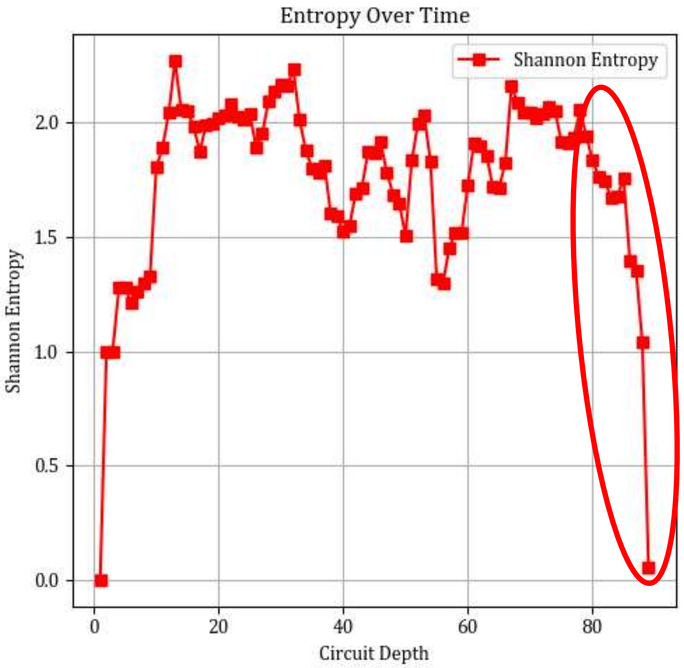




Single-shot instances

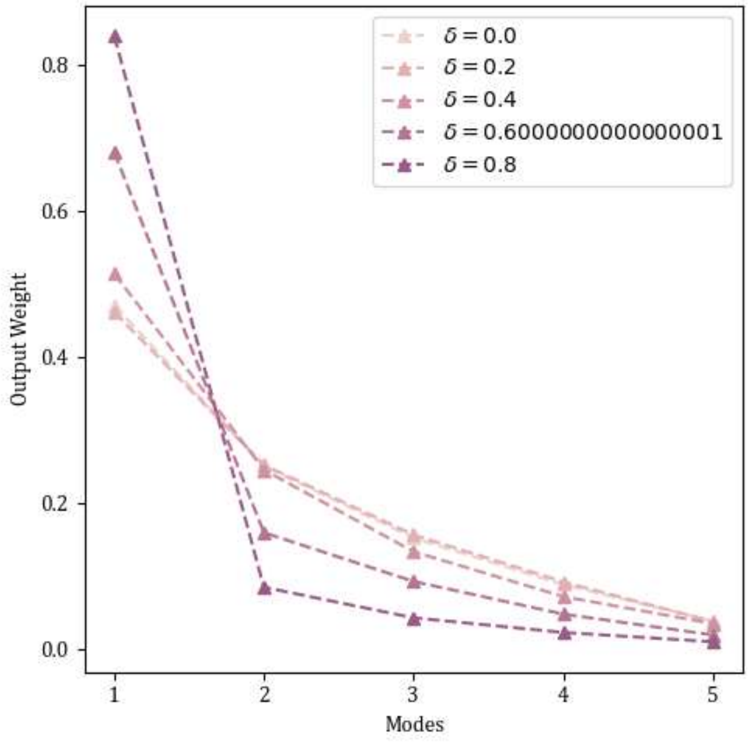
Collision probability and entropy of an explicitly-peaked circuit





Distribution of peakedness

Probability of photon occupation in each mode, generated for $\delta = 0, 0.2, 0.4, 06, 0.8$



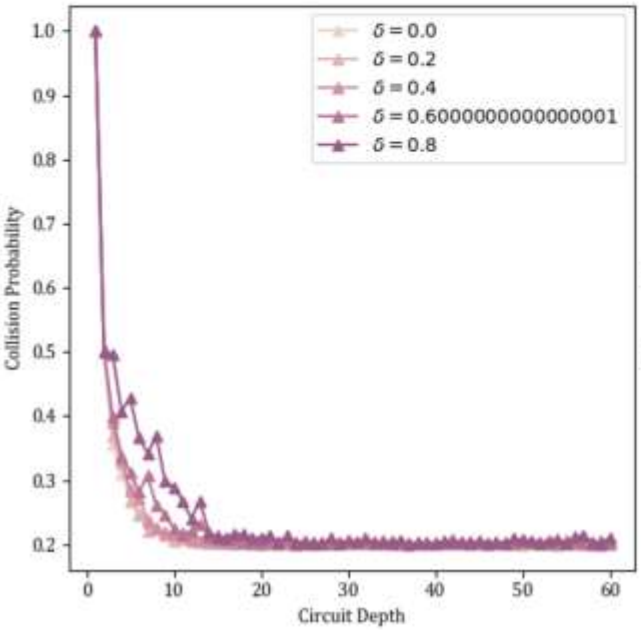
Additional Metrics

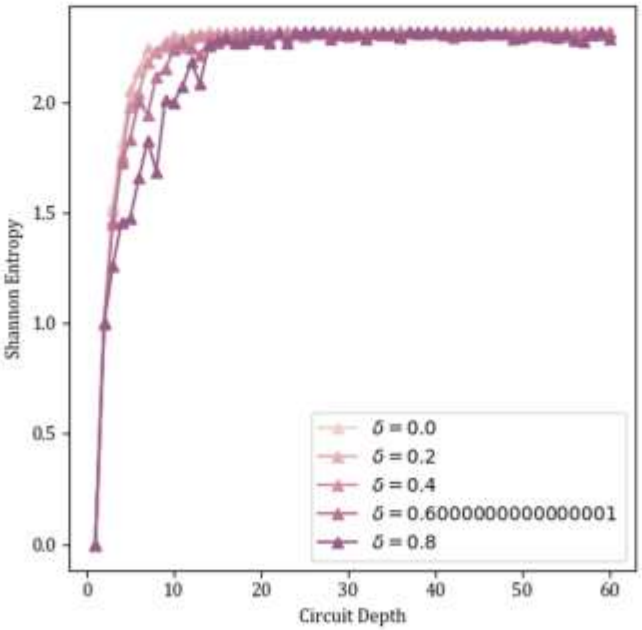
Collision probability (π) and Shannon entropy (S) as a function of circuit depth

For probability distribution P,

$$\pi = \sum_{s} P(s)^2$$

$$S = -\sum_{s} P(s) \log P(s)$$





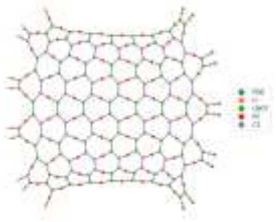
Summary

1. Our experiment(s) combine the linear optical setup of Boson Sampling with the efficiently verifiable properties of peaked circuits.
2. We use an interferometer setup to generate random networks.
3. We then use stochastic gradient descent to optimize over the peaking layer of the constructed circuit.
4. Finally, we examine the entropy and collision probability over time of post selected random beamsplitter networks.

Contributions

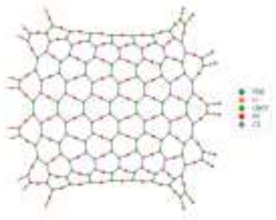
1. First framework to delve into peaked + linear optical systems.
2. Replicate experimental results from [AZ24].
3. Observe new behavior such as peaked interferometers converging to the same statistical values as random linear optical ones.
4. Code: https://github.com/michelled01/Peaked-circuits

Future Work



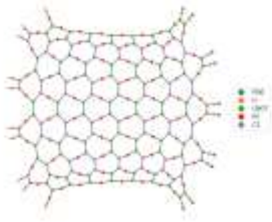
- [Yuxuan & I] Efficiently supporting larger simulation spaces
- [Nirkhe] At what depth do t-designs form in linear optical settings?
- Do linear optical networks anticoncentrate? If so, at what depth?
- Reflection matrices ⇒ higher frequency of Grover-like circuits?
- Orthogonal gates ⇒ better peaking?
- Calculating the operator norm between regions of explicitly peaked circuits

Future Work



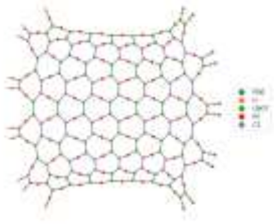
- [Yuxuan & I] Efficiently supporting larger simulation spaces
- [Nirkhe] At what depth do t-designs form in linear optical settings? [CHH+24] section 5.2.1
- Do linear optical networks anticoncentrate? If so, at what depth? [DHJB22]
- Reflection matrices ⇒ higher frequency of Grover-like circuits?
- Orthogonal gates ⇒ better peaking?
- Calculating the operator norm between regions of explicitly peaked circuits

Future Work

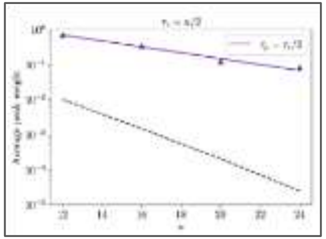


- [Yuxuan & I] Efficiently supporting larger simulation spaces
- [Nirkhe] At what depth do t-designs form in linear optical settings? [CHH+24] section 5.2.1
- Do linear optical networks anticoncentrate? If so, at what depth? [DHJB22]
- Reflection matrices ⇒ higher frequency of Grover-like circuits?
- Orthogonal gates ⇒ better peaking?
- Calculating the operator norm between regions of explicitly peaked circuits

Future Work



- [Yuxuan & I] Efficiently supporting larger simulation spaces
- [Nirkhe] At what depth do t-designs form in linear optical settings? [CHH+24] section 5.2.1
- Do linear optical networks anticoncentrate? If so, at what depth? [DHJB22]
- Reflection matrices ⇒ higher frequency of Grover-like circuits?
- Orthogonal gates ⇒ better peaking?



- Calculating the operator norm between regions of explicitly peaked circuits [AZ24]

References

- [AA10] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. 2010.
- [AZ24] Scott Aaronson and Yuxuan Zhang. On verifiable quantum advantage with peaked circuit sampling, 2024.
- [BGL23] Sergey Bravyi, David Gosset, and Yinchen Liu. Classical simulation of peaked shallow quantum circuits, 2023.
- [BBW25] Marcello Benedetti, Harry Buhrman, and Jordi Weggemans. Complement sampling: Provable, verifiable and nisqable quantum advantage in sample complexity, 2025.
- [CHH+24] Chi-Fang Chen, Jeongwan Haah, Jonas Haferkamp, Yunchao Liu, Tony Metger, and Xinyu Tan. Incompressibility and spectral gaps of random circuits, 2024.
- [DHJB22] Alexander M. Dalzell, Nicholas Hunter-Jones, and Fernando G. S. L. Brandão. Random quantum circuits anticoncentrate in log depth.
- [BGL23b] Sergey Bravyi, David Gosset, and Yinchen Liu. Classical simulation of peaked shallow quantum circuits, 2023.
- [SSA+21] Aakarshitha Suresh, Abdullah Ash Saki, Mahabubul Alam, Rasit o Topalaglu, and Swaroop Ghosh. A quantum circuit obfuscation methodology for security and privacy, 2021.

Thanks for listening!