

Title: Cayley path and quantum supremacy: Average case $\#P$ -Hardness of random circuit sampling

Speakers: Ramis Movassagh

Series: Perimeter Institute Quantum Discussions

Date: May 20, 2020 - 4:00 PM

URL: <http://pirsa.org/20050022>

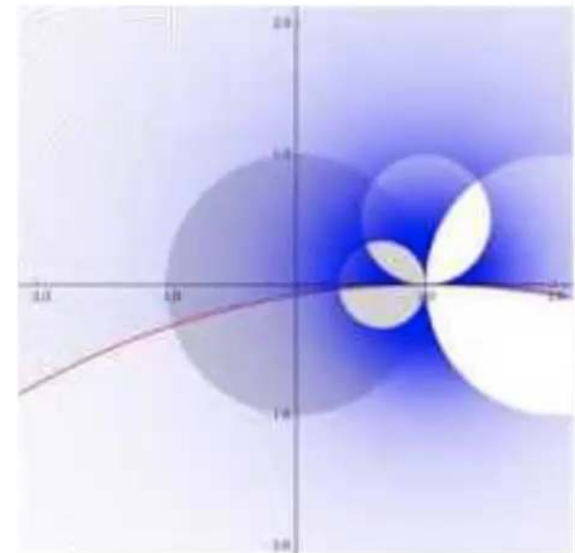
Abstract: Given the large push by academia and industry (e.g., IBM and Google), quantum computers with hundred(s) of qubits are at the brink of existence with the promise of outperforming any classical computer. Demonstration of computational advantages of noisy near-term quantum computers over classical computers is an imperative near-term goal. The foremost candidate task for showing this is Random Circuit Sampling (RCS), which is the task of sampling from the output distribution of a random circuit. This is exactly the task that recently Google experimentally performed on 53-qubits.

Stockmeyer's theorem implies that efficient sampling allows for estimation of probability amplitudes. Therefore, hardness of probability estimation implies hardness of sampling. We prove that estimating probabilities to within small errors is $\#P$ -hard on average (i.e. for random circuits), and put the results in the context of previous works.

Some ingredients that are developed to make this proof possible are construction of the Cayley path as a rational function valued unitary path that interpolate between two arbitrary unitaries, an extension of Berlekamp-Welch algorithm that efficiently and exactly interpolates rational functions, and construction of probability distributions over unitaries that are arbitrarily close to the Haar measure.

Cayley Path and Quantum Supremacy

Ramis Movassagh
IBM Research



arXiv: [1909.06210](https://arxiv.org/abs/1909.06210)

Quantum computers are here...

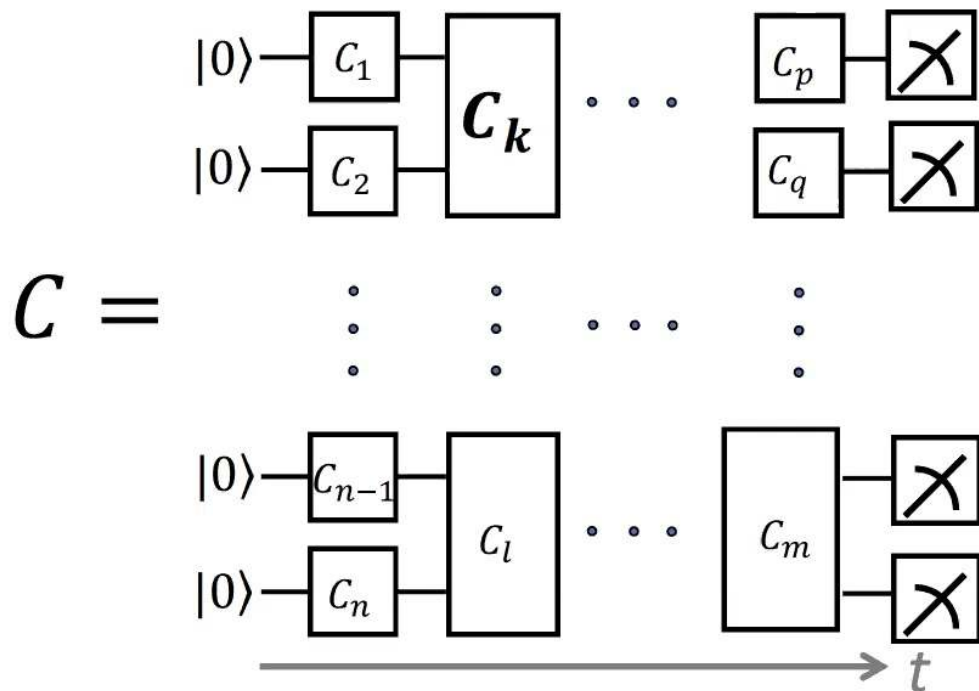
- NISQ capable of a computational task that is practically impossible on classical computers?
- Milestone– violate Extended Church-Turing thesis
- Lead candidate: **Random Circuit Sampling (RCS)**
 - Google experimental demonstrations

Arute+ Nature (2019), S Boixo+ Nature Phys. (2018)

IBM Q : quantum computer



Architecture \mathcal{A} : Distribution $\mathcal{H}_{\mathcal{A}}$



Problem Statement

$$C = C_m C_{m-1} \dots C_2 C_1$$

C_k : Random Unitary (Haar) $\forall k$

Prove: Classical sampling from the output distribution is *hard*

Problem Statement

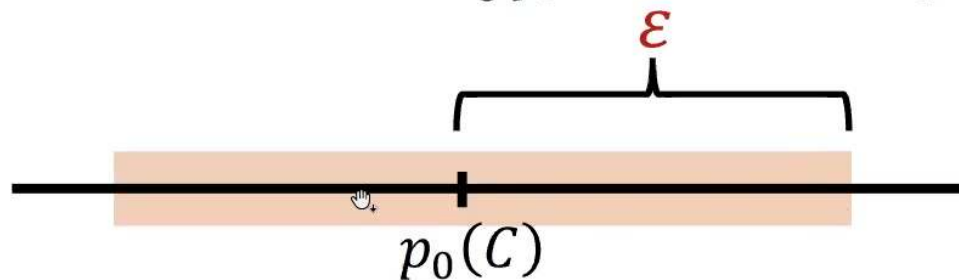
Quantum Supremacy Conjecture: There is no classical randomized algorithm that performs RCS efficiently.

Prove: There exists an architecture \mathcal{A} such that **estimating**

$$p_0(C) \equiv |\langle 0^n | C | 0^n \rangle|^2 \pm \varepsilon$$

is *#P-Hard* for $C \sim \mathcal{H}_{\mathcal{A}}$ (i.e., on average)

#P-Hard: harder than *NP*



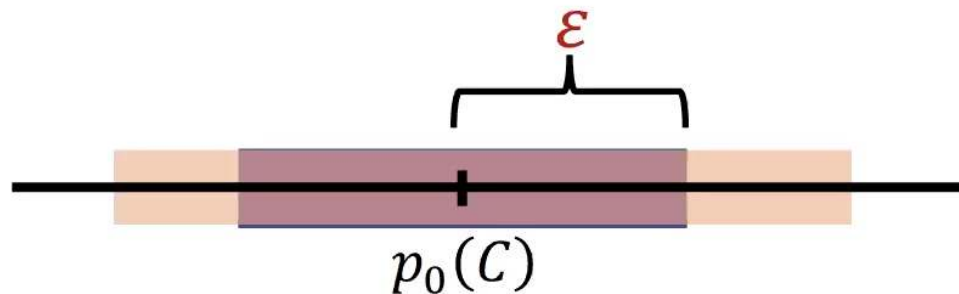
Today we prove:

1. There exists an architecture \mathcal{A} such that

$$p_0(C) \equiv |\langle 0^n | C | 0^n \rangle|^2$$

is *#P-Hard* for $C \sim \mathcal{H}_{\mathcal{A}}$ (i.e., on average)

2. Estimating to ε –neighborhood is also *#P-Hard*



Average Case Hardness of $p_0(C)$

(Traditionally) Reduction idea for average case hardness [Lipton '98]:

(1) There exists a 'worst case' circuit for which :

Bremner-Josza-Sheperd (2011)

Terhal-DiVincenzo (2004)

$$p_0 \equiv |\langle 0^n | C | 0^n \rangle|^2 \text{ is } \#P\text{-Hard (harder than NP)}$$

(2) Deform the circuit from worst to 'average case':

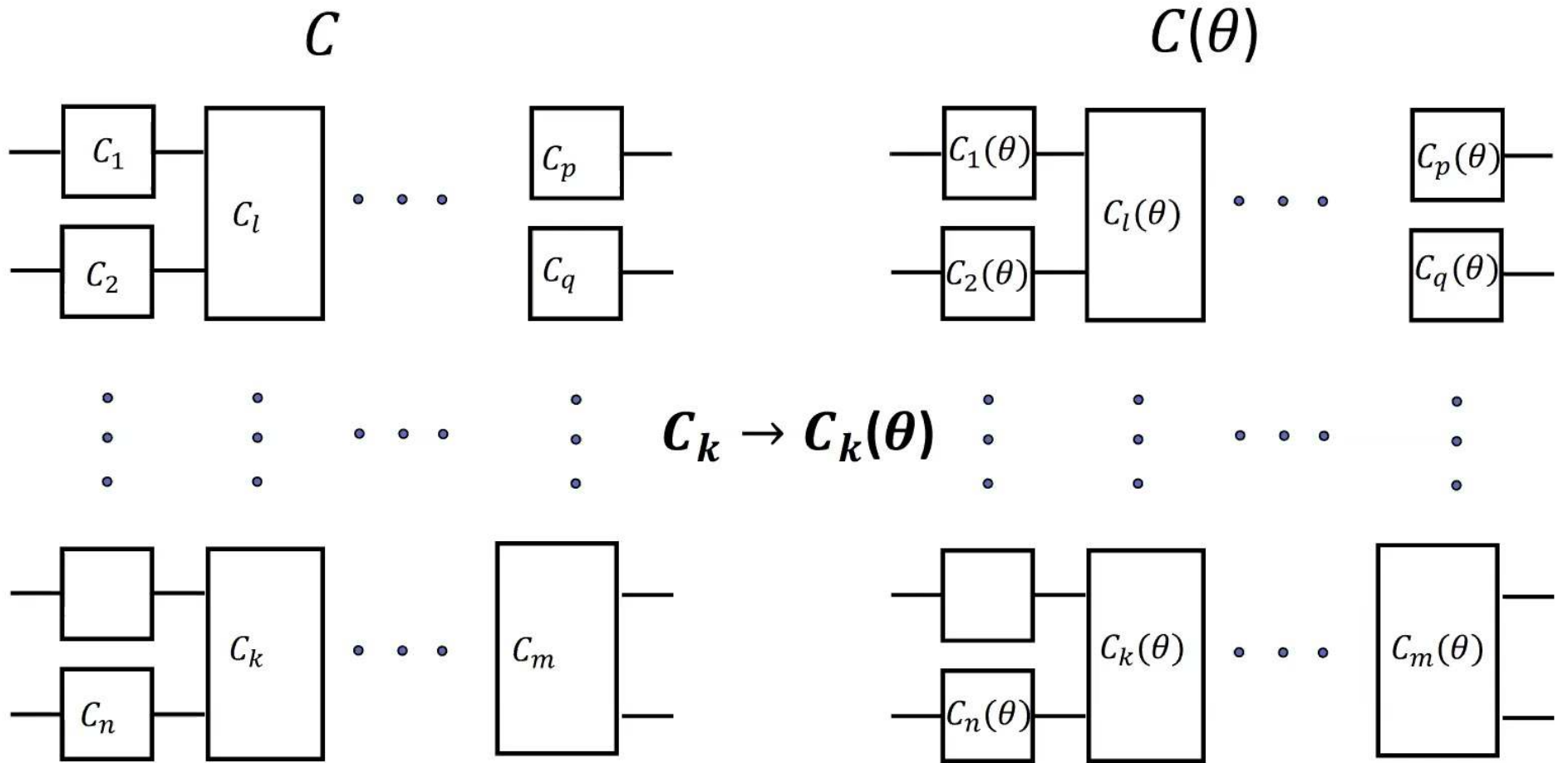
$$C \quad \longrightarrow \quad C(\theta)$$

$$p_0 \equiv |\langle 0^n | C | 0^n \rangle|^2 \quad \longrightarrow \quad p_0(\theta) \equiv |\langle 0^n | C(\theta) | 0^n \rangle|^2$$

where $\theta \in \mathbb{R}$ and :

$$C(1) \quad \Rightarrow \quad p_0(1) \text{ is } \textit{worst-case} \text{ instance } (\#P\text{-Hard})$$

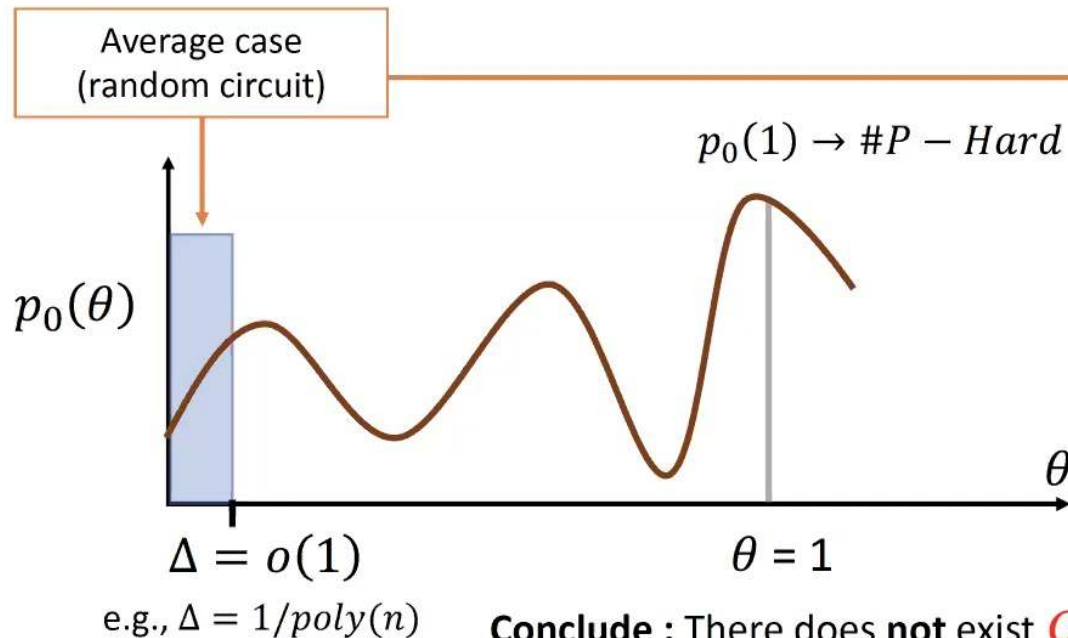
$$C(0) \in \mathcal{H}_{\mathcal{A}} \Rightarrow p_0(0) \text{ is } \textit{average case} \text{ instance}$$



(Traditionally) Reduction idea for average case hardness [Lipton '98]:

Deform circuit from worst to 'average case':

$$p_0(\theta) \equiv |\langle 0^n | C(\theta) | 0^n \rangle|^2 \quad \text{Polynomial of low degree (e.g. poly}(n))$$



* Assume: classical efficient algorithm \mathcal{O} calculates $p_0(\theta)$ with high probability

* Call \mathcal{O} $d+1$ times: To get $(\theta_i, p(\theta_i))$.

* Write $p_0(\theta)$ exactly and efficiently!

* Extrapolate to $p_0(1)$, which is $\#P$ -hard

X Contradiction X

Conclude : There does not exist \mathcal{O} that can efficiently calculate $p_0(\theta)$ for $\theta \in [0, \Delta]$

The key question is...

How are we to deform $C \rightarrow C(\theta)$ such that

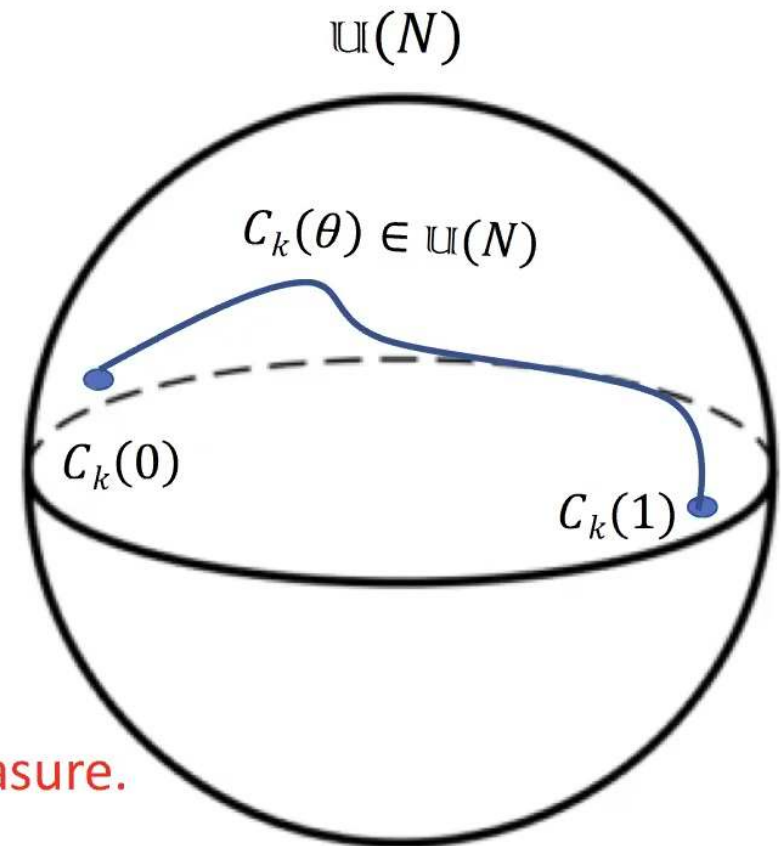
$$p_0(\theta) \equiv |\langle 0^n | C(\theta) | 0^n \rangle|^2$$

is a **low degree polynomial or algebraic function?**

$$C_k(1) = C_k$$

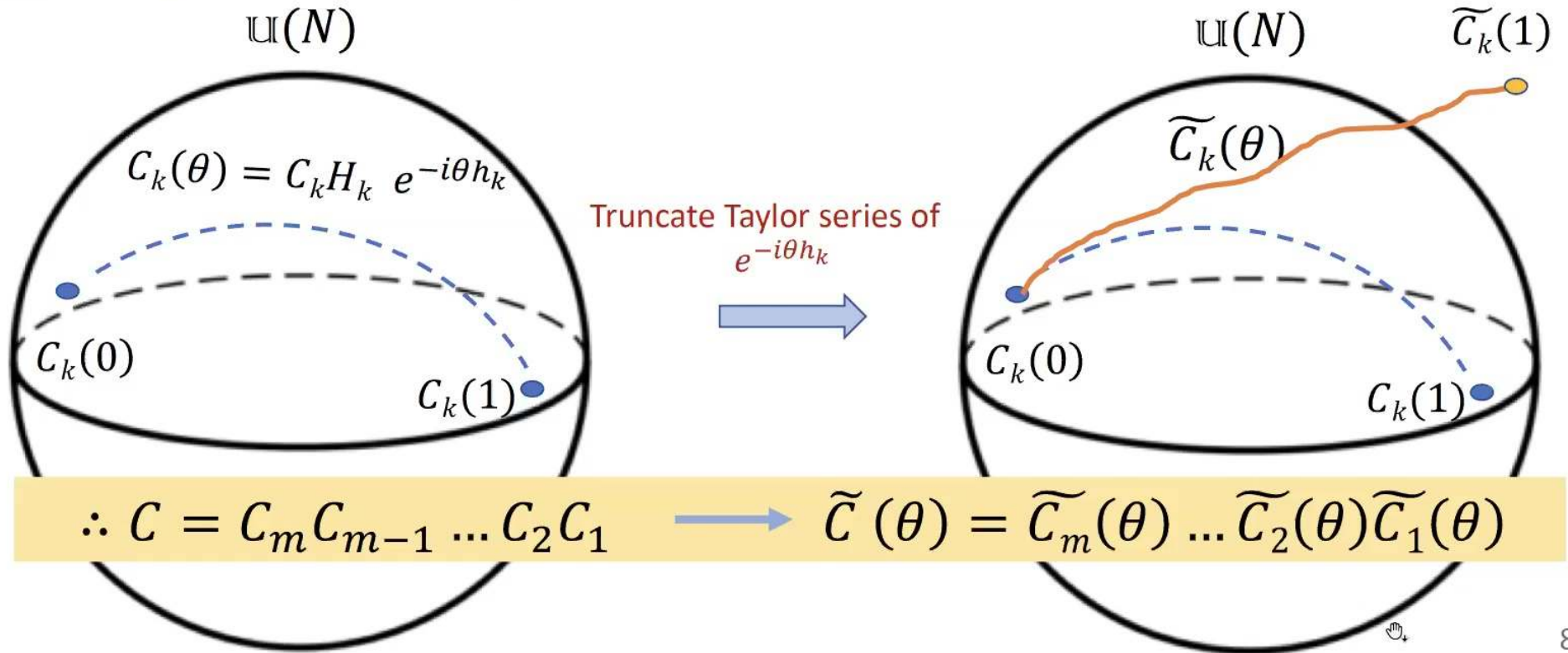
$$H_k \in Haar \Rightarrow C_k(0) = C_k H_k \in Haar$$

By definition of Haar measure.



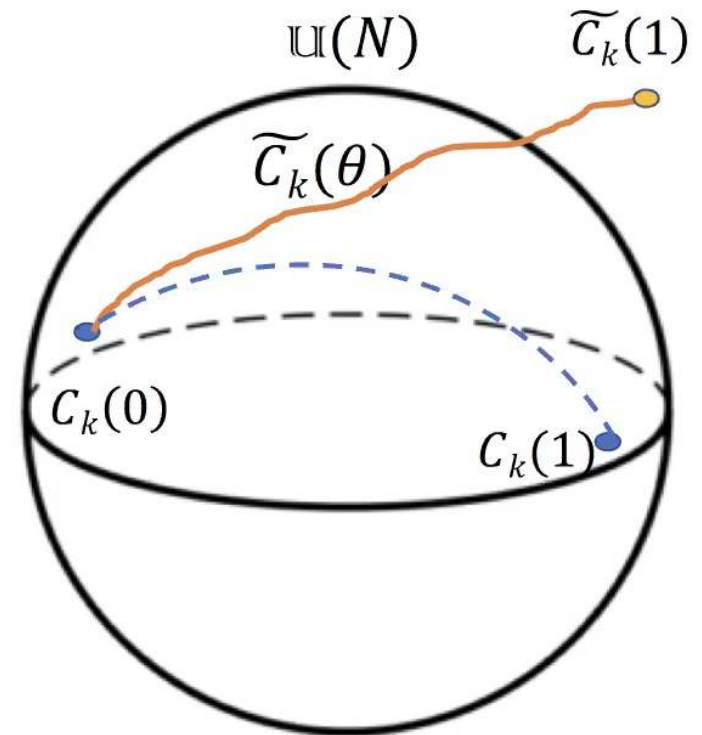
On the complexity and verification of quantum random circuit sampling

Adam Bouland¹, Bill Fefferman^{1,2*}, Chinmay Nirkhe¹ and Umesh Vazirani¹



On the complexity and verification of quantum random circuit sampling

Adam Bouland¹, Bill Fefferman^{1,2*}, Chinmay Nirkhe¹ and Umesh Vazirani¹



Define h_k such that $H_k^\dagger = e^{-ih_k}$ for some $h_k = h_k^\dagger$

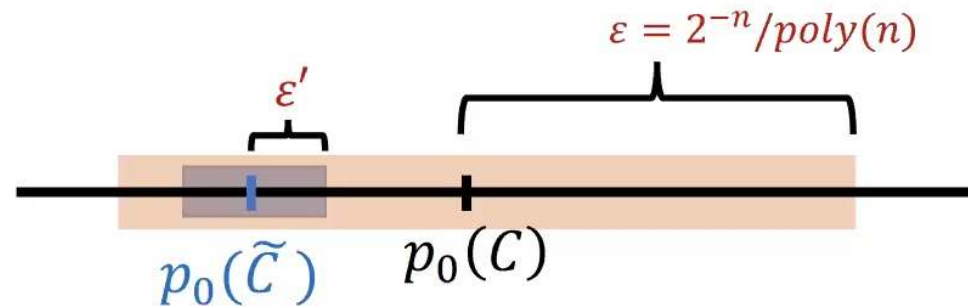
Use : $C_k(\theta) = C_k H_k \boxed{e^{-i\theta h_k}} \approx C_k H_k \boxed{\left\{ \sum_{j=0}^L \frac{(-i\theta h_k)^j}{j!} \right\}} \equiv \widetilde{C}_k(\theta)$

Non-Unitary gates

$\therefore C = C_m C_{m-1} \dots C_2 C_1 \longrightarrow \widetilde{C}(\theta) = \widetilde{C}_m(\theta) \dots \widetilde{C}_2(\theta) \widetilde{C}_1(\theta)$

Non-Unitary circuit

- Recall the goal is:



- Bouland *et al* (*Nature Physics* 2018) show

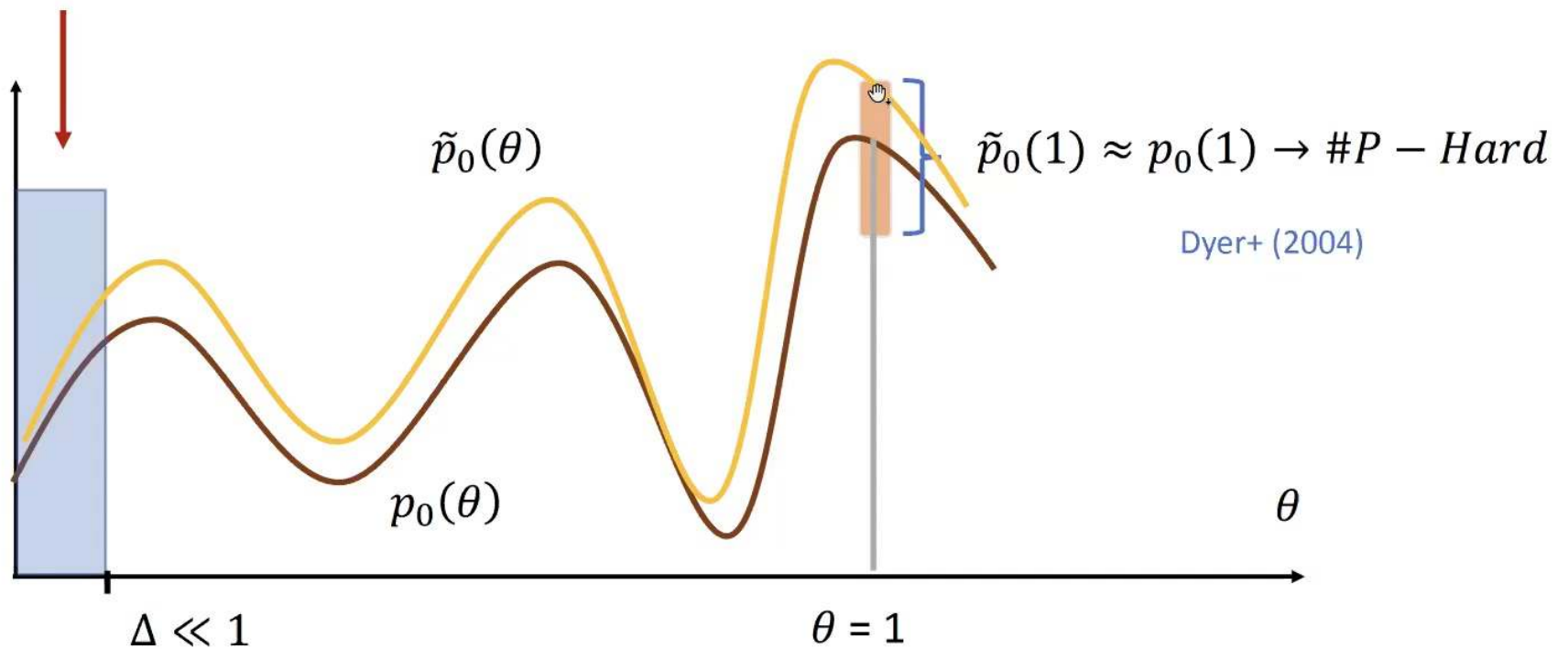
- The distribution over $\tilde{C}(\theta)$ is close to the distribution over $C(\theta)$
- Calculating $p_0(\tilde{C})$ is #P-Hard on average
- They claim an $\varepsilon' = \exp(-\text{poly}(n))$ robustness, which we prove *unnatural*:

➤ Spoiler: If one inputs a *circuit* then degree of polynomial is $\exp(+\text{poly}(n))$!!

So they need to assume that the classical algorithm takes as input the specific non-unitary circuits

[for more: Appendix A in Napp *et al* 2020)]

$O : (\theta_i, p(\theta_i) \pm \epsilon_i)$ for $\theta_i \in [0, \Delta]$



Let: $p(\theta) \equiv p_0(\theta) - \tilde{p}_0(\theta)$

(Paturi's Lemma) Suppose $p(\theta)$ is a degree d polynomial and that $|p(\theta)| \leq \varepsilon$ for $\theta \in [0, \Delta]$ then

$$|p(1)| \leq \varepsilon e^{2d(1+\Delta^{-1})}$$

Recall $\Delta = 1/\text{poly}(n)$: $|p_0(1) - \tilde{p}_0(1)| \leq \varepsilon e^{2d(1+\Delta^{-1})}$

[Bouland et al: truncation]

$$\leq e^{O(mn - L \ln L)} e^{2d(1+\Delta^{-1})} \quad \text{SYSTEMATIC!!!}$$

$$\leq e^{O(mn - L \ln L)} e^{2(2Lm)(1+\Delta^{-1})}$$

$$\therefore L \geq O(\exp(4m \Delta^{-1})) \quad !!$$

$$\leq e^{O(mn + L(4m\Delta^{-1} - \ln L))} \longrightarrow \infty \quad 12$$

Cayley path and Quantum Supremacy

[arXiv:1909.06210](https://arxiv.org/abs/1909.06210)

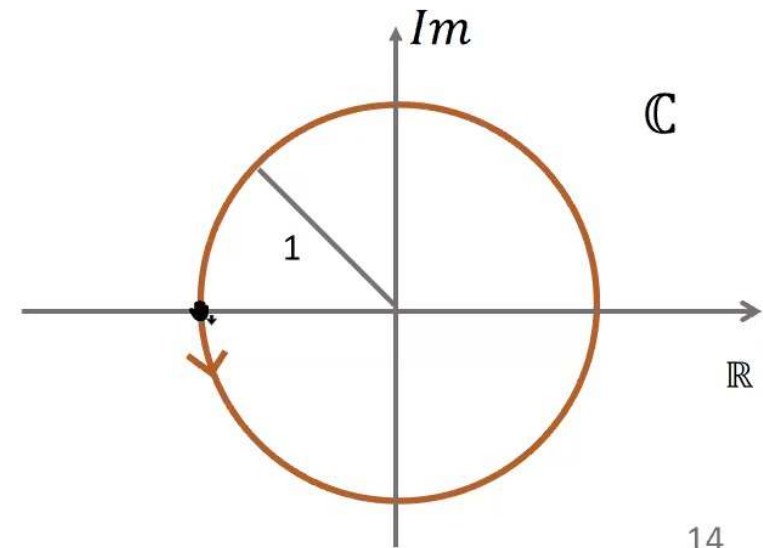
Cayley Function :

$$f(x) = \frac{1+ix}{1-ix}$$

where $f(-\infty) \equiv -1$



f
bijection



14

Efficient unitary-valued path between any two unitary matrices:

$$H \text{ unitary:} \quad H = f(h), \quad h = h^\dagger$$

$$H^\dagger = f(-h)$$

Procedure

Given **worst case** circuit with m gates:

$$C_1, C_2, \dots, C_m$$

Generate corresponding m **random Haar gates**:

$$H_1, H_2, \dots, H_m$$

Easy and efficient.



$C_k(\theta)$ is rational function valued unitary matrix

By eigenvalue decomposition $H_k = f(h_k)$:

$$h_k = \sum_{\alpha=1}^N h_{\alpha} |\psi_{\alpha}\rangle \langle \psi_{\alpha}|, \quad N \in \{2,4\}$$

We find that

$$C_k(\theta) = C_k H_k f(-\theta h_k) = \frac{1}{q(\theta)} \sum_{\alpha=1}^N p_{\alpha}(\theta) (C_k |\psi_{\alpha}\rangle \langle \psi_{\alpha}|)$$

$$q(\theta) = \prod_{\alpha=1}^N (1 + i\theta h_{\alpha})$$

$$p_{\alpha}(\theta) = f(h_{\alpha})(1 - i\theta h_{\alpha}) \prod_{\beta \in [N] \setminus \alpha} (1 + i\theta h_{\beta})$$

Entries of $C_k(\theta)$ are rational functions of degree (N, N)

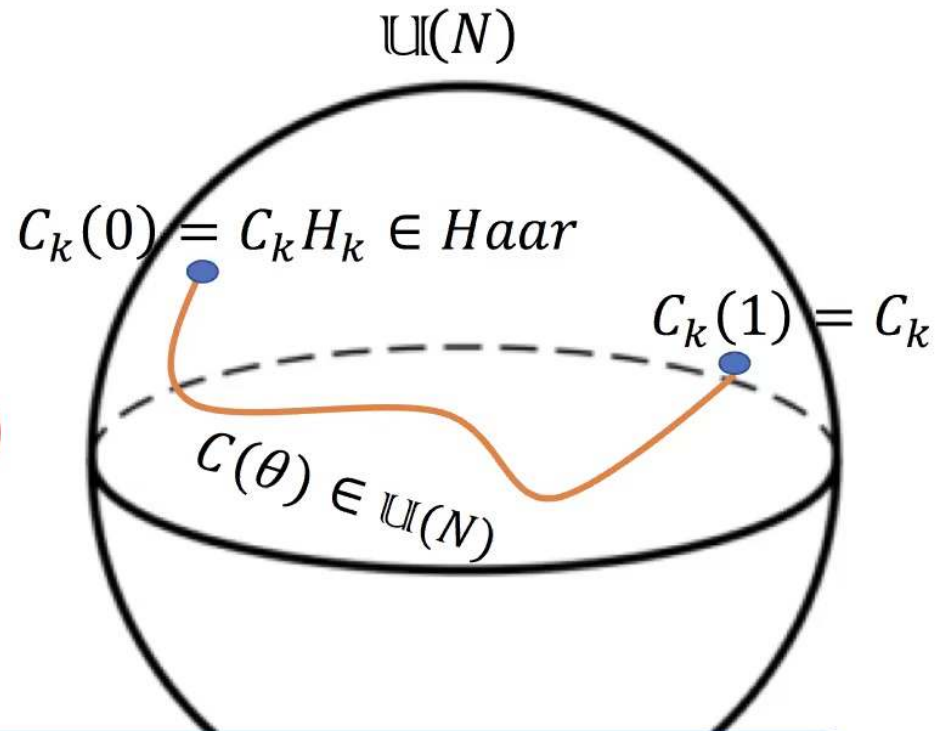
$$C = C_m C_{m-1} \dots C_k \dots C_2 C_1$$

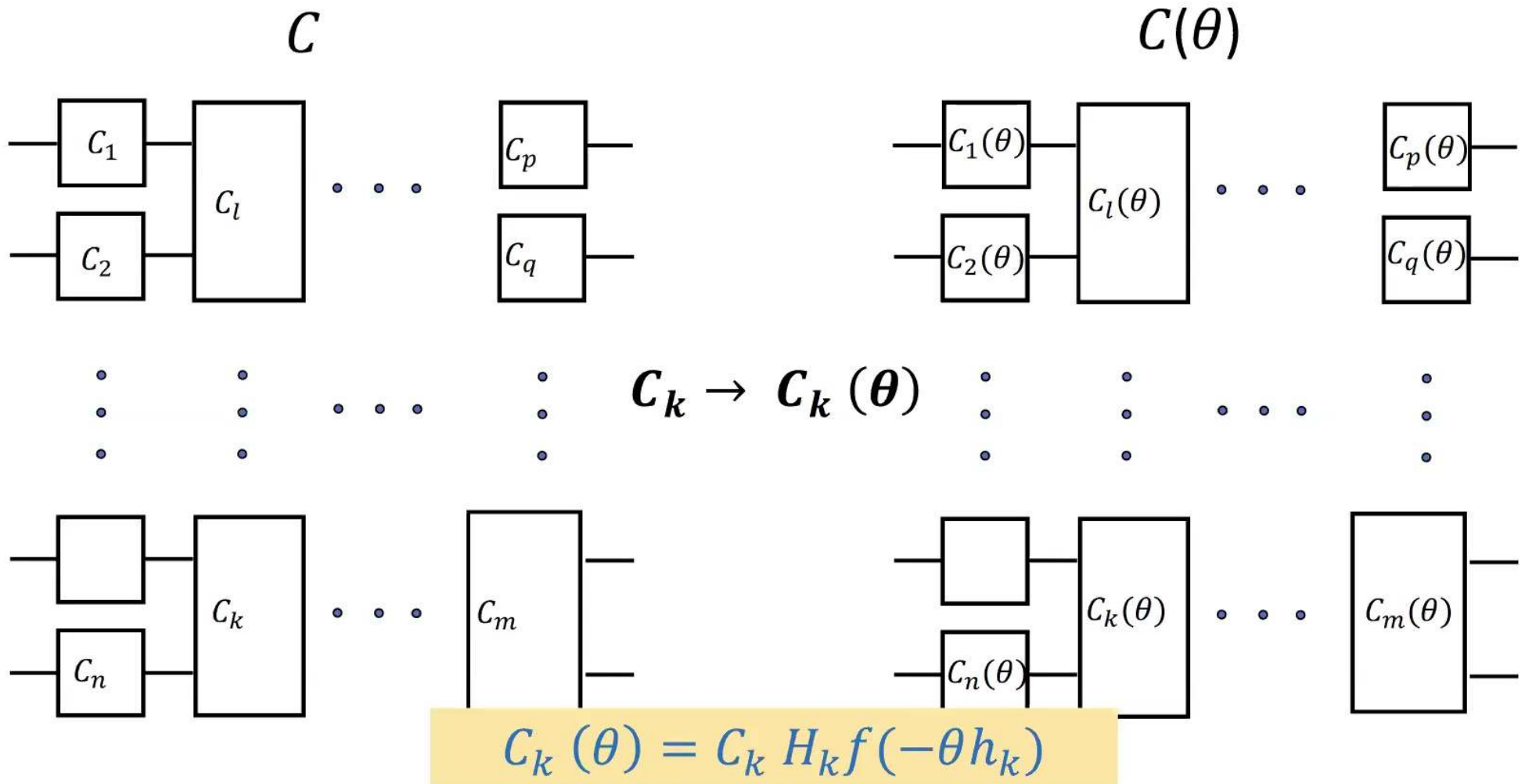
$$C_k(\theta) = C_k H_k f(-\theta h_k)$$

Entries are rational functions of degree (N,N)

$$C \longrightarrow C(\theta)$$

Entries of $C(\theta)$ are rational function of degree (mN, mN)





$$p_0(C) \equiv |\langle 0^n | C | 0^n \rangle|^2$$



$$p_0(\theta) \equiv |\underbrace{\langle 0^n | C(\theta) | 0^n \rangle}_{(1,1)\text{-entry of } C(\theta)}|^2$$

(1,1)- entry of $C(\theta)$

$p_0(\theta)$ is a rational function of degree $(2mN, 2mN)$

One slide on further technical ingredients

Crucial to reconstruct $p_0(\theta)$ with high probability despite noise.

Algorithm (Berlekemp-Welch for rational functions)

Suppose $F(\theta)$ is (k_1, k_2) rational function. Given $(\theta_1, f(\theta_1)), \dots, (\theta_n, f(\theta_n))$, find a rational function $F(\theta)$ of degree (k_1, k_2) exactly by evaluating it at $n > k_1 + k_2 + 2t$ points despite t errors in the evaluation points.

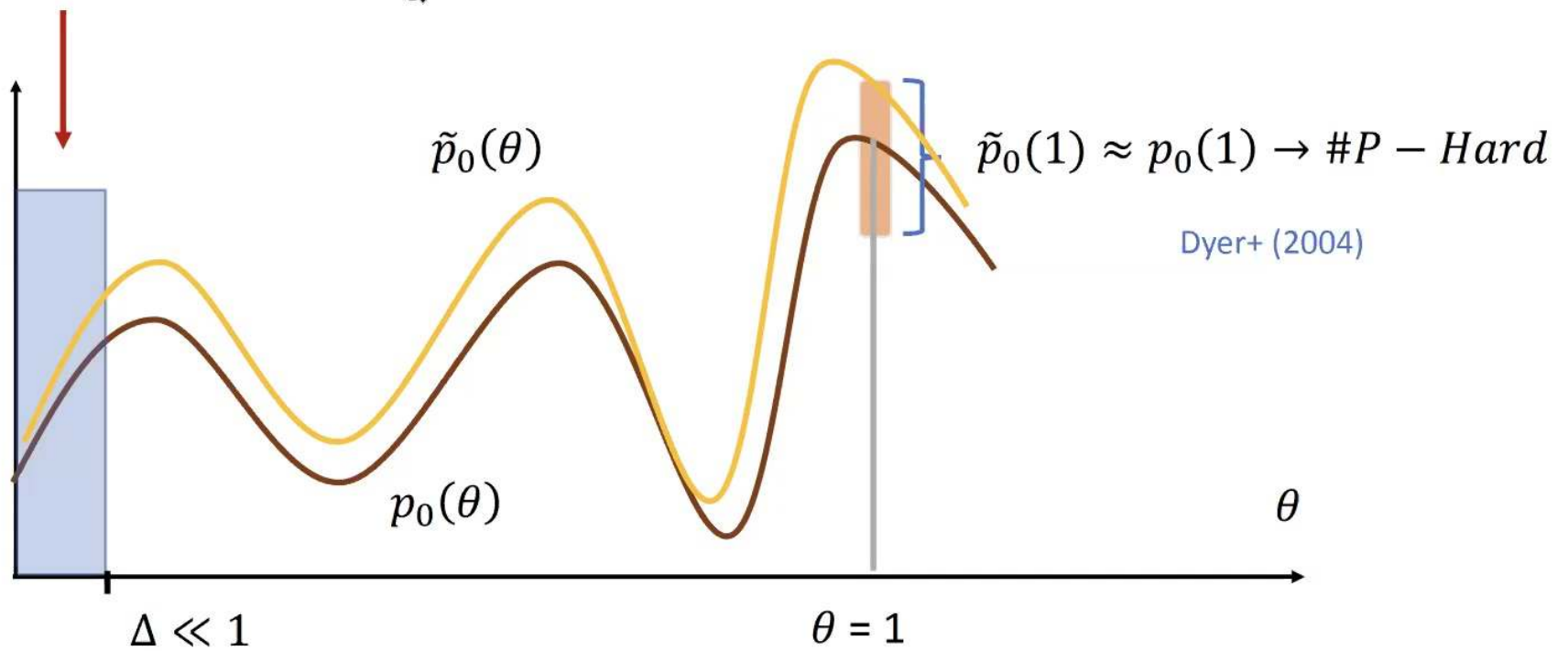
To prove supremacy: Also Crucial that the circuit is close to $\mathcal{H}_{\mathcal{A}}$

Theorem : Consider $(N \times N)$ operator $f(h)f(-\theta h)$ for $\theta \ll 1$. This operator is $O(\sqrt{\theta})$ close in TVD to the Haar measure. Therefore, a circuit with m gates is $O(m\sqrt{\theta})$ close to $\mathcal{H}_{\mathcal{A}}$ in total variational distance (TVD).

Average-case hardness:

Theorem: Let \mathcal{A} be an architecture such that computing $p_0(C)$ is $\#P$ -Hard in the worst case. Then it is $\#P$ -Hard to compute $\frac{3}{4} + 1/\text{poly}(n)$ of the probabilities $p_0(C)$ over $\mathcal{H}_{\mathcal{A}}$.

$O : (\theta_i, p(\theta_i) \pm \epsilon_i)$ for $\theta_i \in [0, \Delta]$



Theorem (Robustness): It is $\#P - \text{Hard}$ to compute p_0 over $\mathcal{H}_{\mathcal{A}}$ to within $\varepsilon = 2^{-\Theta(m\Delta^{-1})}$ additive error.

In practice:

□ $\varepsilon = 2^{-O(n^2)}$ for constant depth circuits

□ $\varepsilon = 2^{-O(n^3)}$ for a quantum circuit on a $\sqrt{n} \times \sqrt{n}$ grid and depth \sqrt{n}

(Google Circuit)

Supremacy Conjecture: It is $\#P - \text{Hard}$ to compute p_0 over $\mathcal{H}_{\mathcal{A}}$ to within $\varepsilon = \frac{2^{-n}}{\text{poly}(n)}$ additive error.

Open questions

- Improving robustness to $2^{-n}poly(1/n)$ proves the supremacy conjecture.
- Supremacy conjecture even true for constant depth circuits?! (Napp et al 2019)
- Cayley path for:
 - Quantum computing by interpolation
 - Cryptography and circuit hiding; Blind quantum computing
- Cayley path optimal in some sense?
- Proof not based on interpolation?

Open questions

- Improving robustness to $2^{-n}poly(1/n)$ proves the supremacy conjecture.
- Supremacy conjecture even true for constant depth circuits?! (Napp et al 2019)
- Cayley path for:
 - Quantum computing by interpolation
 - Cryptography and circuit hiding; Blind quantum computing
- Cayley path optimal in some sense?
- Proof not based on interpolation?

I salute you for your interest and attention!



Cartoon picture from VectorStock