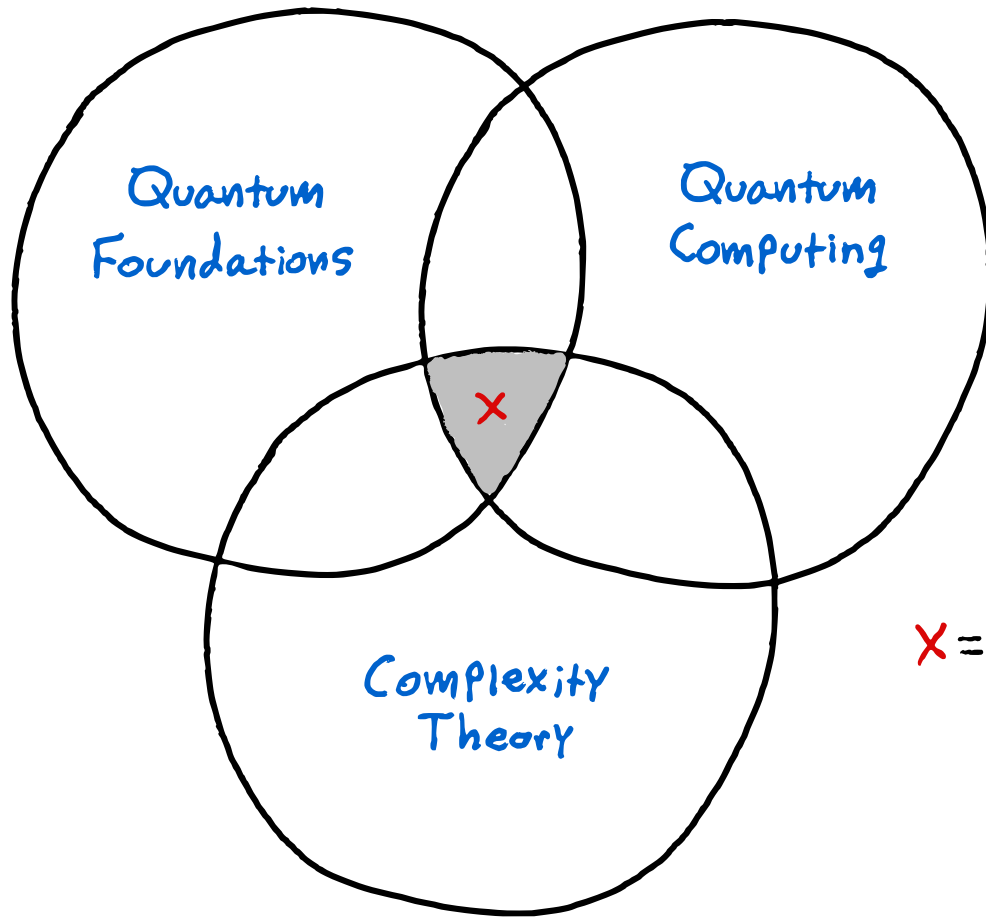
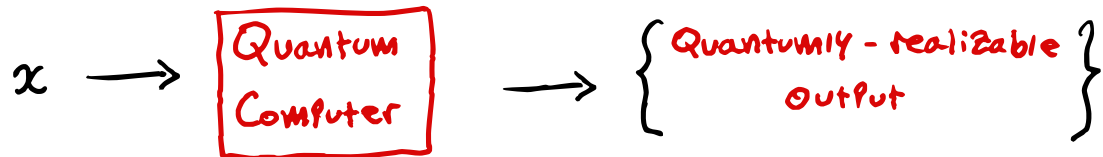
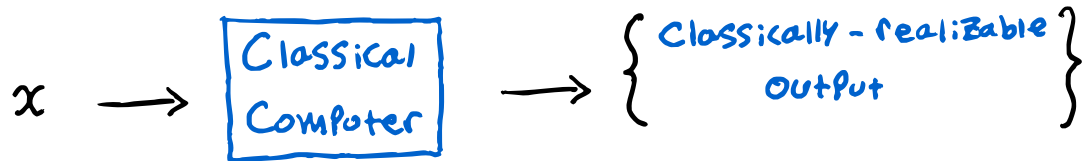


Mixed State Quantum Computation and the Necessity of Entanglement for BQP Tasks

Matthew Fox



X = this talk



"QUANTUM COMPUTATIONAL ADVANTAGE"

$\Leftrightarrow$

$$\left\{ \begin{array}{c} \text{Classically - realizable} \\ \text{output} \end{array} \right\} \subsetneq \left\{ \begin{array}{c} \text{Quantumly - realizable} \\ \text{output} \end{array} \right\}$$

"QUANTUM COMPUTATIONAL ADVANTAGE"

$\Leftrightarrow$

Classical Complexity Class $\subsetneq$ Quantum Complexity Class

(BPP, MIP, NC^o, ...)

(BQP, MIP*, QNC^o, DQC1, ...)

BPP v.s. BQP

Bounded-error Probabilistic Polynomial-time (BPP)

Def: BPP-machine $A: \{0,1\}^* \rightarrow \{0,1\}^*$ is a Probabilistic Polynomial time Turing machine.

→ "efficient classical algorithm" (Extended Church-Turing Thesis)

Def: For language $L \subseteq \{0,1\}^*$,

$\exists$ BPP-machine A s.t. $\forall x \in \{0,1\}^*$,

$L \in \text{BPP} \iff$

• $x \in L \Rightarrow \Pr[A(x) = 1] \geq 2/3$

• $x \notin L \Rightarrow \Pr[A(x) = 0] \geq 2/3$

Bounded-error Quantum Polynomial-time (BQP)

Def: **BQP-Circuit** $Q: \{0,1\}^* \rightarrow \{0,1\}^*$ is a (uniform) family $(Q_n)_{n \in \mathbb{N}}$ of polynomial size quantum circuits.

→ "efficient quantum algorithm" (Extended Church-Turing-Deutsch Thesis).

Def: For $L \subseteq \{0,1\}^*$,

$\exists$ **BQP-Circuit** Q s.t. $\forall x \in \{0,1\}^*$

$L \in \text{BQP} \iff$

$$\bullet x \in L \Rightarrow \Pr[Q(x)=1] \geq 2/3$$

$$\bullet x \notin L \Rightarrow \Pr[Q(x)=0] \geq 2/3$$

$Q(x) =$ result of measuring first qubit of $Q_{|x|}|x\rangle$.

$$\text{BPP} \stackrel{?}{=} \text{BQP}$$

i.e. (roughly)

$$\begin{array}{ccc} \text{efficient Classical} & \stackrel{?}{=} & \text{efficient Quantum} \\ \text{Computation} & & \text{Computation} \end{array}$$

$BPP \stackrel{?}{=} BQP$ is hard.

Perhaps easier is the question:

If $BPP \neq BQP$, then why?

ENTANGLEMENT!

(In) SUFFICIENCY OF ENTANGLEMENT

Thm. (Gottesman-Knill):

$$\text{CLIFFORD CIRCUITS} \subseteq \text{BPP}.$$

Thm. (Vidal):

Any evolution

$$|\psi\rangle \rightarrow U_1 |\psi\rangle \rightarrow \dots \rightarrow U_L \dots U_1 |\psi\rangle$$

is simulable by a **BPP-machine** provided $\forall \ell \in \{1, \dots, L\}$,

$$\chi(U_L \dots U_1 |\psi\rangle) = O(\text{poly}).$$

Cor:

Entanglement insufficient for **BPP** $\neq$ **BQP**.

NECESSITY OF ENTANGLEMENT

Cor:

If no **BPP-machine** can simulate

$$|\psi\rangle \rightarrow \mathcal{U}_1|\psi\rangle \rightarrow \dots \rightarrow \mathcal{U}_d \dots \mathcal{U}_1|\psi\rangle,$$

then $\exists d \in \{1, \dots, d\}$ s.t.

$$\chi(\mathcal{U}_d \dots \mathcal{U}_1|\psi\rangle) \neq O(\text{poly}).$$

So it seems:

If **BPP** $\neq$ **BQP**, then (a large amount of) entanglement is necessary.

NECESSITY OF ENTANGLEMENT?

Thm. (Braunstein et al.):

Let σ be any mixed state. For $\varepsilon > 0$ sufficiently small,

$$\rho_\varepsilon = (1-\varepsilon) \frac{1}{N} I_N + \varepsilon \sigma \quad \text{separable.}$$

Cor. (Jozsa-Linden):

"Separable Mixed States require the same number of parameters for their description as do general mixed states."

IS ENTANGLEMENT NECESSARY?

- $(Q_n)_{n \in \mathbb{N}} = \text{BQP-circuit}$
- $(\rho_x)_{x \in \{0,1\}^*} = \text{Collection of mixed and separable states}$
- $\forall x \in \{0,1\}^*$ and $\forall \ell \in \{1, \dots, d\}$, $Q_{1|x\ell} = U_\ell \dots U_1$ s.t.
 $(U_\ell \dots U_1) \rho_x (U_1^\dagger \dots U_\ell^\dagger)$ separable.

Q. (Jozsa-Linden, Aaronson, Yoganathan,...):

$$L_Q := \left\{ x \mid \Pr \left[\begin{array}{c} \text{First qubit of} \\ Q_{1|x\ell} \rho_x Q_{1|x\ell}^\dagger \text{ is } |1\rangle \end{array} \right] \geq \frac{2}{3} \right\} \text{ in BPP?}$$

"CLASSICAL QUANTUM STATES"

Caveat: L_Q even in BQP ?

• For general $(\rho_x)_{x \in \{0,1\}^*}$, NO!

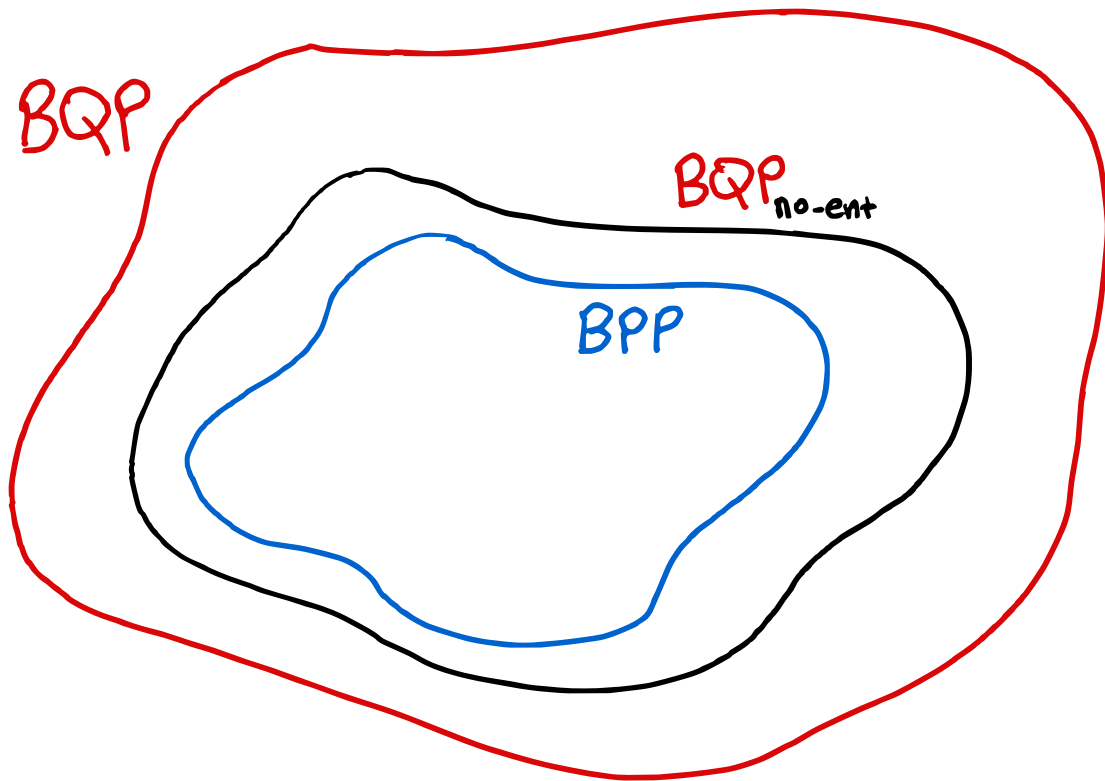
Thm:

$$L_Q \in BQP \iff$$

$\exists$ BPP -machine A s.t. $\forall x \in \{0,1\}^*$,

$$\rho_x = \sum_y P_r[A(x)=y] |Y_X Y|.$$

$\rightarrow$ Need $(\rho_x)_{x \in \{0,1\}^*}$ to be BPP -realizable.

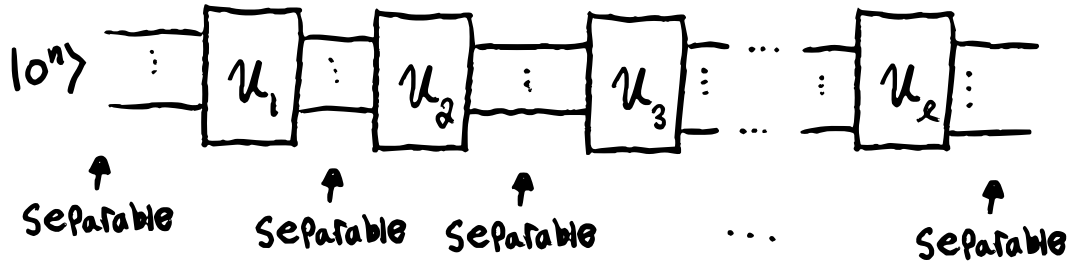


$BQP_{\text{no-ent}}$ = "BQP with no entanglement"

Non-Entangling Circuits

Def. (Yoganathan):

$Q_n = U_d \dots U_1$ non-entangling iff $\forall l \in \{1, \dots, d\}$,
 $U_l \dots U_1 |0^n\rangle$ Product State.

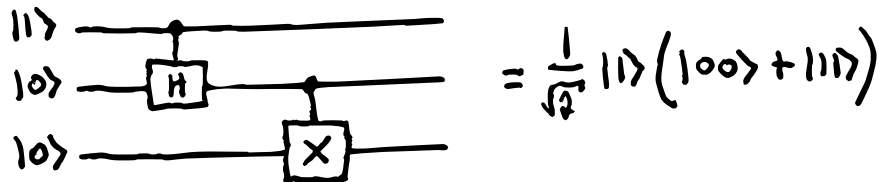
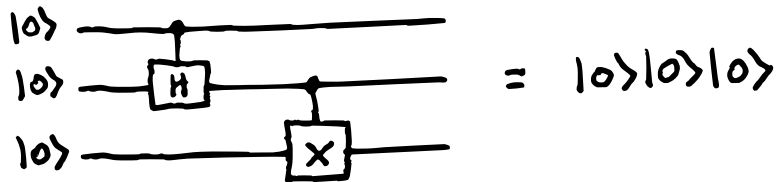


Non-ENTANGLING CIRCUITS

- IMO, not in the spirit of Jozsa et al.'s question!
- Q_n not necessarily non-entangling for generic BPP State

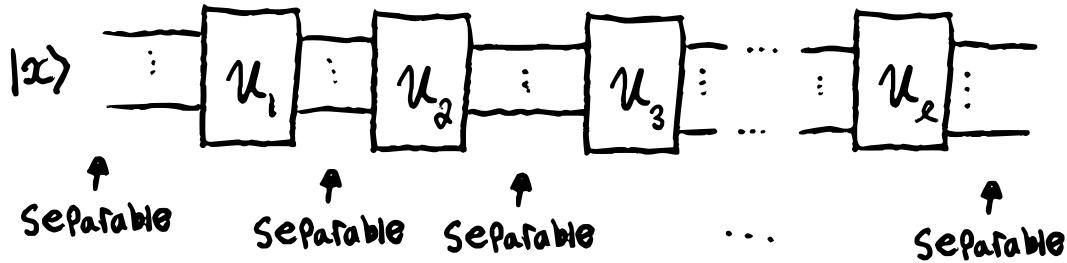
$$\rho_x = \sum_Y P_r[A(x)=Y] |YXY\rangle$$

- E.g.



Non-ENTANGLING CIRCUITS

Def: $Q_n = U_d \dots U_1$ non-entangling iff $\forall i \in \{1, \dots, d\}$ and $\forall x \in \{0, 1\}^n$
 $U_d \dots U_1 |x\rangle$ Product state



Non-ENTANGLING BQP

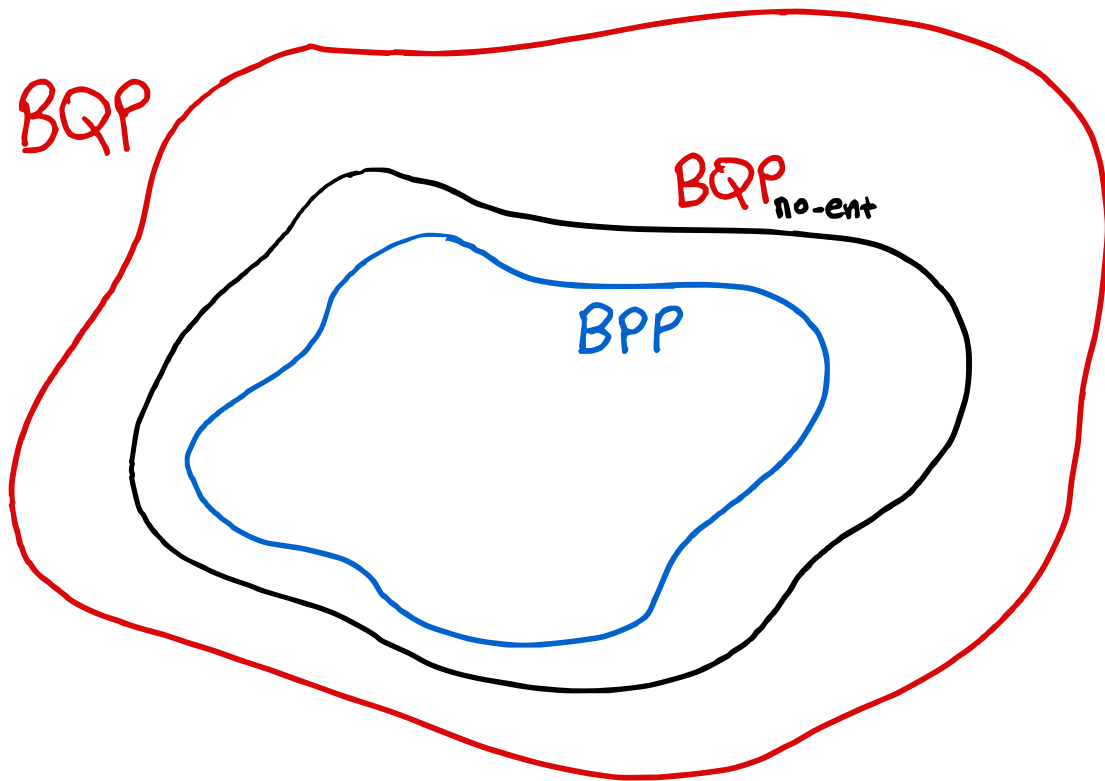
Def: For $L \subseteq \{0,1\}^*$,

$L \in \text{BQP}_{\text{no-ent}}$ $\iff$ $\exists$ BPP-realizable Collection $(\rho_x)_{x \in \{0,1\}^*}$
and $\text{BQP}_{\text{no-ent}}$ -Circuit Q s.t. $\forall x \in \{0,1\}^*$,

- $x \in L \Rightarrow \Pr[Q(\rho_x) = 1] \geq 2/3$
- $x \notin L \Rightarrow \Pr[Q(\rho_x) = 0] \geq 2/3$

Note:

$$\text{BPP} \subseteq \text{BQP}_{\text{no-ent}} \subseteq \text{BQP}$$



$BQP_{\text{no-ent}}$ = "BQP with no entanglement"

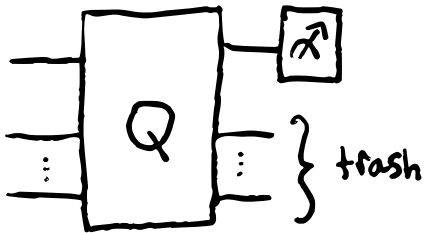
$$\text{BPP} \stackrel{?}{=} \text{BQP}_{\text{no-ent}}$$

(If Yes, then if $\text{BPP} \neq \text{BQP}$, entanglement is necessary.)

SAMPLING PROBLEMS

LANGUAGES:

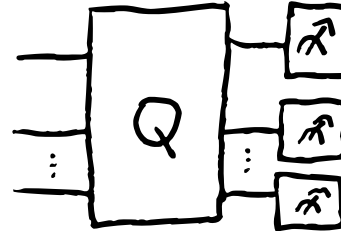
$$L \subseteq \{0,1\}^*$$



BPP, BQP, ...

SAMPLING:

$$S = \bigcup_{x \in \{0,1\}^*} \mathcal{D}_x$$



SampBPP, SampBQP, ...

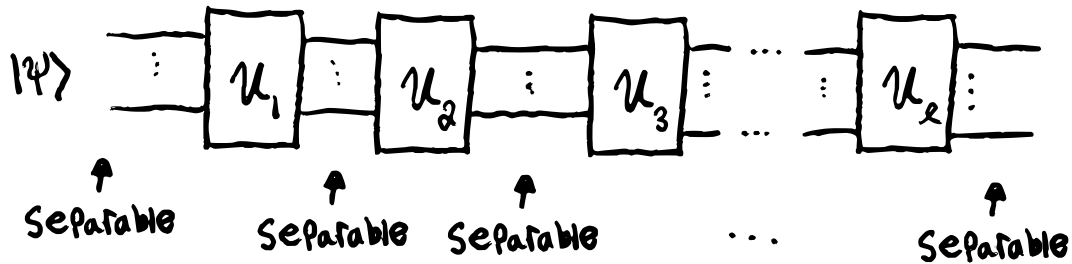
$$\text{SampBPP} \stackrel{?}{=} \text{SampBQP}_{\text{no-ent}}$$

Thm:

$$\text{SampBPP} = \text{SampBQP}_{\text{no-ent}} \implies \text{BPP} = \text{BQP}_{\text{no-ent}}$$

INTERMEDIATE RESULTS

- $Q = (Q_n)_{n \in \mathbb{N}}$ **BQP**_{no-ent} - **Circuit** s.t. each $Q_n = U_d \dots U_1$
 Satisfies $\forall$ Product States $|\psi\rangle$ and $\forall l \in \{1, \dots, d\}$,
 $U_d \dots U_1 |\psi\rangle$ Product State.



INTERMEDIATE RESULTS

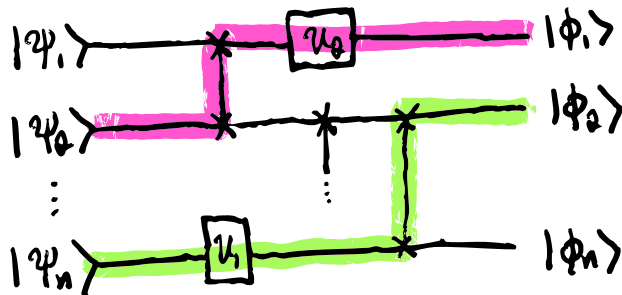
Thm: Sampling log registers of Q is in **SampBPP**.

Proof Idea: (for measuring one qubit, log case similar)

- $Q_n \in N(U(\mathbb{Q})^{\otimes n})$ (normalizer)

- $N(U(\mathbb{Q})^{\otimes n}) = U(\mathbb{Q})^{\otimes n} \rtimes \text{SWAP}_n$

• "Traceback Algorithm":



$$|\phi_1\rangle = U_2 |\psi_2\rangle$$

$$|\phi_2\rangle = U_1 |\psi_n\rangle$$

⋮

- In general, $|\phi_i\rangle = U_d \dots U_1 |\psi_{\pi(i)}\rangle$, $\pi \in S_n$, $U_1, \dots, U_d \in U(\mathbb{Q})$.

INTERMEDIATE RESULTS

- Therefore, $\exists \tilde{Q}_n \in U(2)^{\otimes n}$ s.t. $\forall x \in \{0,1\}^n$
 $Q_n |x_1 \dots x_n\rangle = \tilde{Q}_n |x_{\pi(1)} \dots x_{\pi(n)}\rangle$.

- On **BPP-realizable** input

$$\rho_x = \sum_Y \Pr[A(x) = Y] |Y\rangle\langle Y|$$

$$Q_n : \rho_x \mapsto \tilde{Q}_n \left(\sum_Y \Pr[A(x) = Y] |\pi(Y)\rangle\langle\pi(Y)| \right) \tilde{Q}_n^\dagger$$

- So,

$$\Pr[\text{first qubit} = |1\rangle] = \sum_{i \in \{0,1\}} |\langle 1 | \tilde{Q}_n^{(1)} | i \rangle|^2 \Pr(Y_{\pi(1)} = i)$$

INTERMEDIATE RESULTS

$$Pr[\text{first qubit} = |1\rangle] = \sum_{i \in \{0,1\}} |\langle 1 | \tilde{Q}_n^{(1)} | i \rangle|^2 Pr(Y_{\pi(1)} = i)$$

Algorithm:

Given x, Q_n

→ Sample $K \sim A(\pi(x))$

→ Sample $r \sim [0, 1]$

→ if $K=0$ and $r < |\langle 1 | \tilde{Q}_n^{(1)} | 0 \rangle|^2$:
output 1

→ if $K=1$ and $r < |\langle 1 | \tilde{Q}_n^{(1)} | 1 \rangle|^2$:
output 1

→ else:

output 0

OPEN QUESTIONS

- Many "log-Size" Sampling Problems in $\text{SampBQP}_{\text{no-ent}}$ are in SampBPP . Are all of them?
- More generally, $\text{SampBPP} \stackrel{?}{=} \text{SampBQP}_{\text{no-ent}}$.
- If not, does $\text{BPP} \stackrel{?}{=} \text{BQP}_{\text{no-ent}}$.

THANK You!