Lecture 19

Refs
[Bremner Jozsa Shepherd 10]
[Terhal DiVincenzo 02]
[Fenner Green Homer Zhang 03]
[Aaronson 04]

Today:
1. Facts from complexity theory
2. Hardness of exactly simulating quantum computation
3. Hardness of approximately simulating QC

---

1. Facts from complexity theory

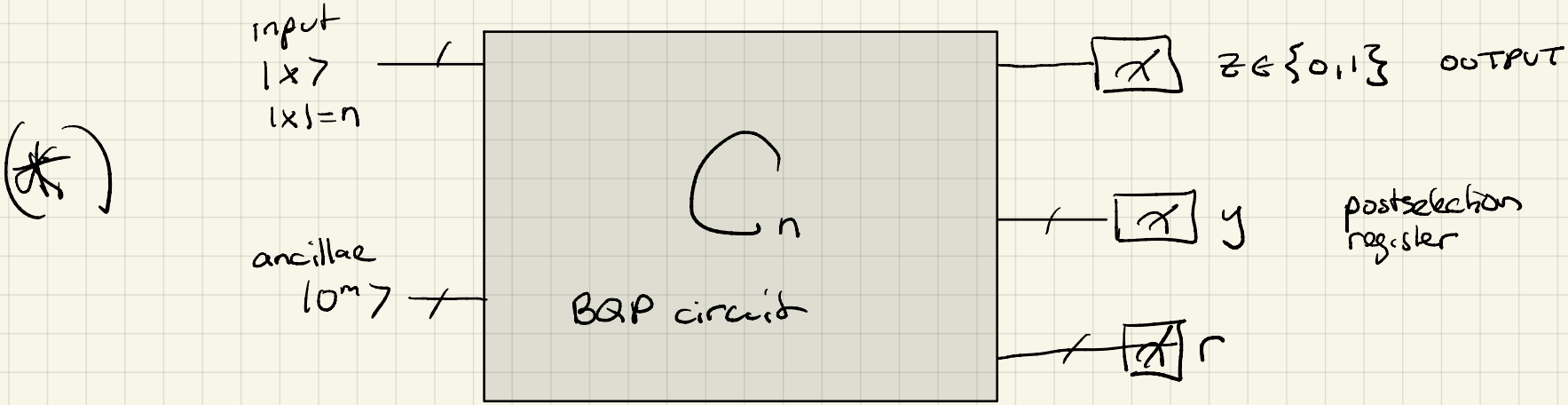
The polynomial hierarchy $PH = \bigcup_{k=0,1,2,\dots} \Sigma_k$

where
$$\Sigma_0 = P$$
$$\Sigma_1 = NP$$
$$\Sigma_2 = NP^{NP}$$
NP verifier can call an NP oracle

$$\vdots$$
$$\Sigma_k = NP^{\Sigma_{k-1}}$$
$$\vdots$$

If $\Sigma_i = \Sigma_{i+1}$ for some i then $PH = \Sigma_i$ and this "polynomial hierarchy collapse" is thought to be extremely unlikely.

postselected circuits



PostBQP

A decision problem $L \in$ postBQP if $\exists$ a uniformly generated polynomial-size circuit family $\{C_n\}_n$ s.t

$$x \in L \Rightarrow \Pr[z=1 \mid y=0] \geq 2/3$$
$$x \notin L \Rightarrow \Pr[z=1 \mid y=0] \leq 1/3$$

Can likewise define postBPP by replacing the BQP circuit with a BPP circuit.

Can also define post A for any restricted family A of BQP circuits.

Fact Quantum postselection >> classical postselection

$$P^{\text{postBPP}} \subseteq \Sigma_3$$ [Han, Hemaspaandra, Thierauf 97]

$$P^{\text{postBQP}} \supseteq PH$$ [Aaronson 2005] + Toda's Thm

$\Rightarrow$ If postBPP contains postBQP then PH collapses!

② Classical hardness of exact simulation [see Bremner Jozsa Shepherd 10]

Claim: Suppose A is a restricted circuit family such that

$$\text{post}\,A = \text{postBQP}$$

Suppose that $\exists$ an efficient randomized classical alg. that, given a circuit in A, samples from the distribution

$$p(z, y, r)$$ (see (*))

Then PH collapses.

Pf: Take the efficient (BPP) circuit that samples

$$p(z,y,r)$$

and then postselect on y. This gives a postBPP circuit that exactly simulates the postselected q. circuit.

$$\text{postBQP} = \text{postA} \subseteq \text{postBPP} \Rightarrow PH \subseteq \Sigma_3$$

//

restricted circuit families A s.t. postA = postBQP can be much less powerful than BQP

Examples

A = depth 3 circuits [Terhal DiVincenzo 2002]

A = IQP circuits [Bremner Jozsa Shepherd 2010]

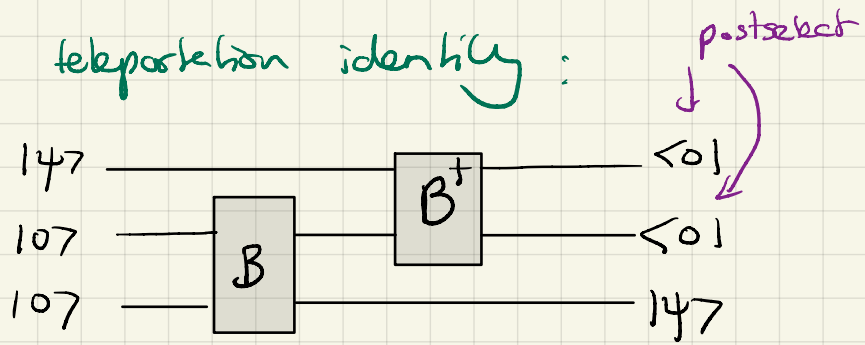
A = QAOA circuits [Farhi Harrow 2016]

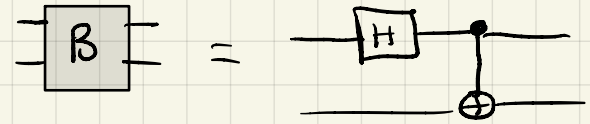
⋮

Depth-3 circuits ([Terhal DiVincenzo 02], version here follow [Fenner Green Homer Zhang 03])

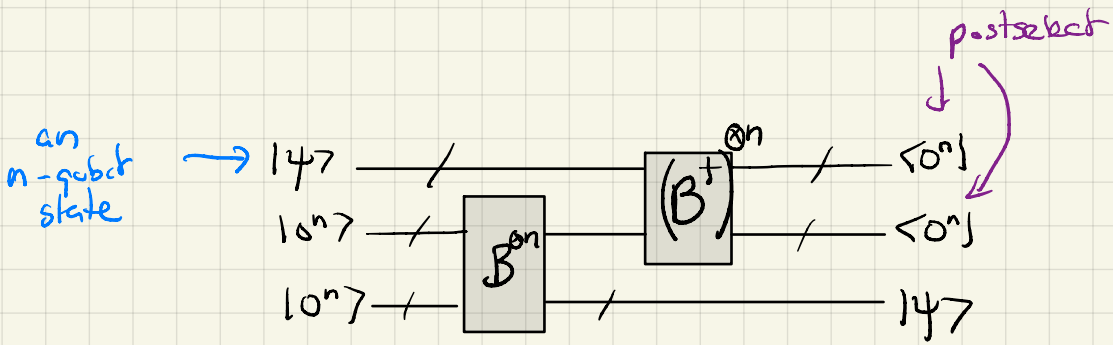
Want to show postselected (depth 3) = postBQP

postselected teleportation identity:

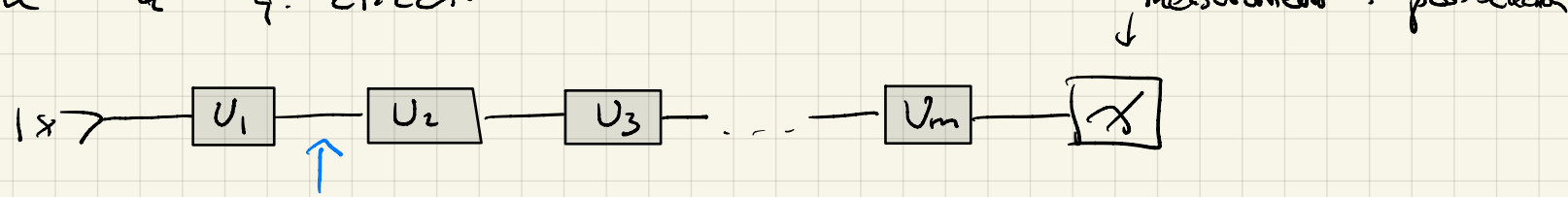




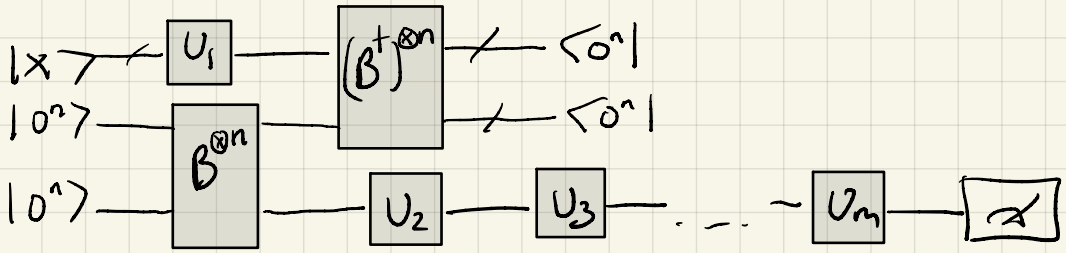
An n qubit state can be teleported using n parallel copies of the above:



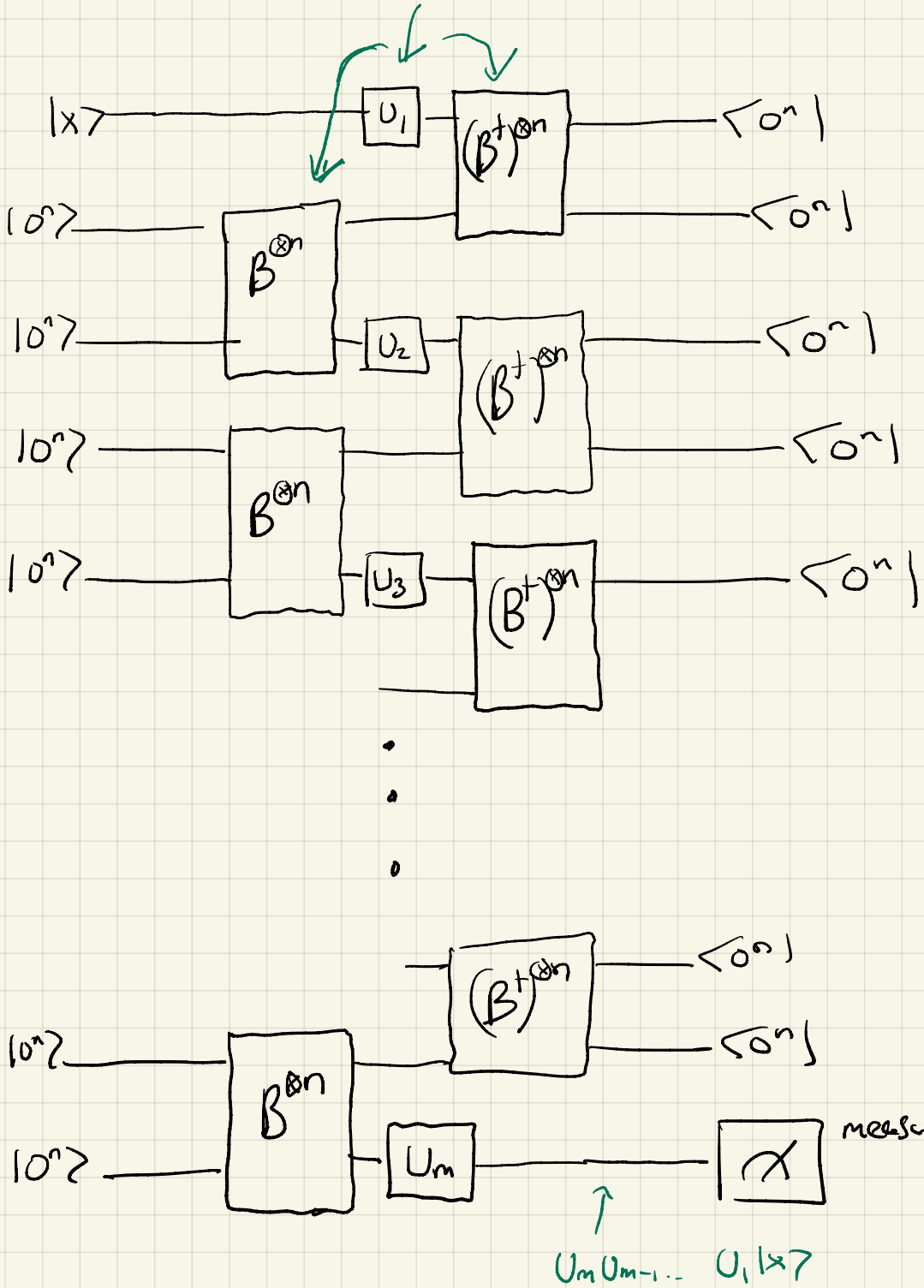
Suppose we have a q. circuit



We can insert postselected teleportation after the 1st gate to get an equivalent circuit:



Now insert postselected teleportation after 2nd, 3rd, ..., m-1st gates:



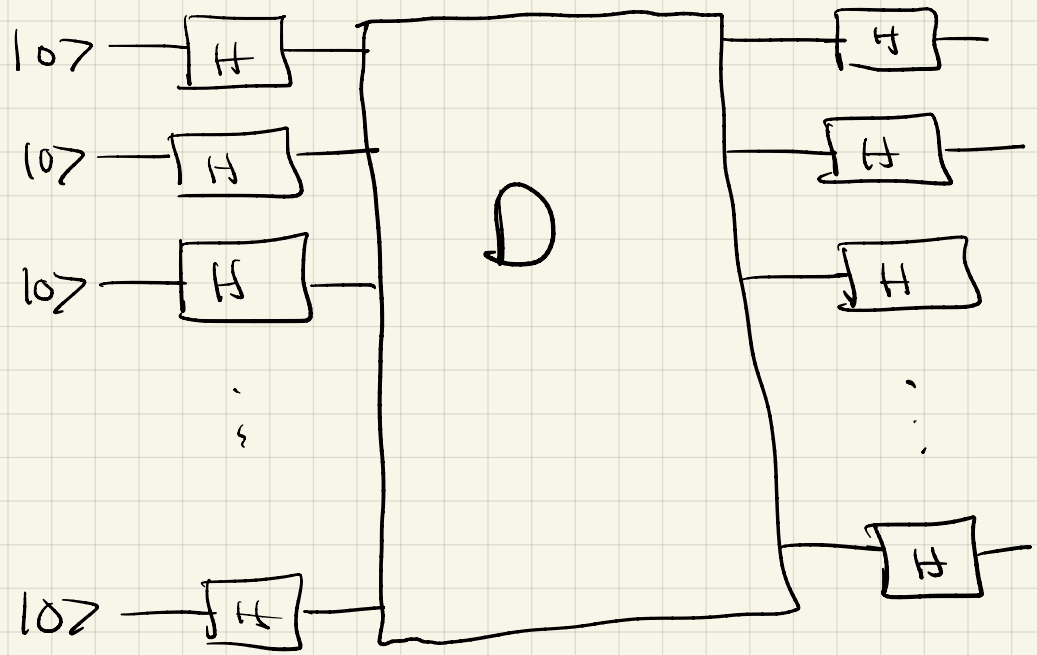
This is a depth-3 postselected circuit that simulates the given postselected circuit with m gates.

$\Rightarrow$ no efficient classical alg can exactly sample from output of depth 3 poly-size q. circuits, unless PH collapses.

(depth 2 circuits can be efficiently simulated, see homework)

IQP circuits

"Instantaneous Quantum polynomial time" [Brenner Jozsa Shepherd 2010]



where

$$D = \left(\prod_{j<k} e^{\frac{i\pi}{8} \omega_{jk} Z_j Z_k} \right) \left(\prod_{\ell=1}^{n} e^{\frac{i\pi}{8} V_\ell Z_\ell} \right)$$

2-qubit gates

single qubit z rotations

$$\omega_{jk}, V_\ell \in \{0, 1, 2, \ldots, 7\}$$