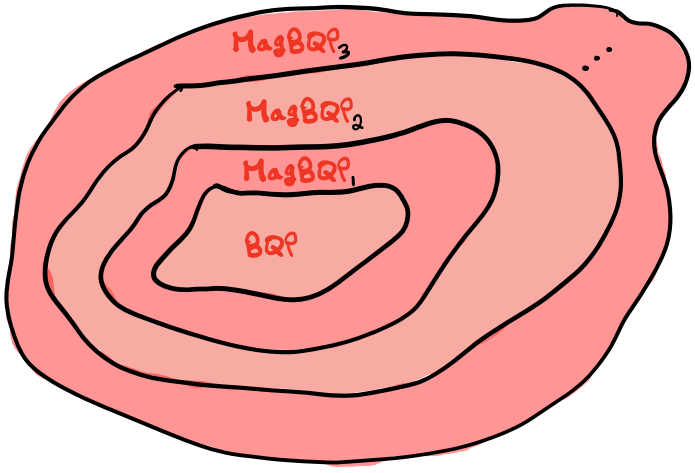
The Computational Power of Eliminating Relative Phases



Matthew Fox

University of Colorado Boulder



Chai Karamchedu (UMD)



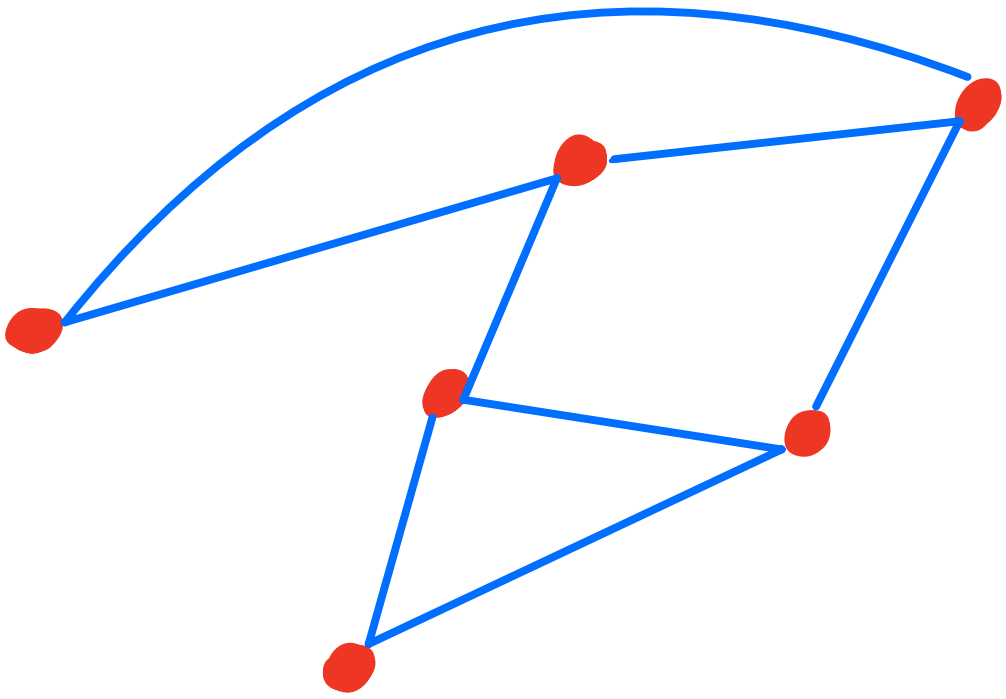
Cari Miller (UMD, NIST)

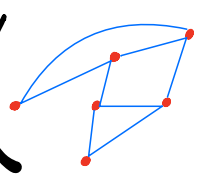


Nicole Yunger Halpern (UMD, NIST)

Part I

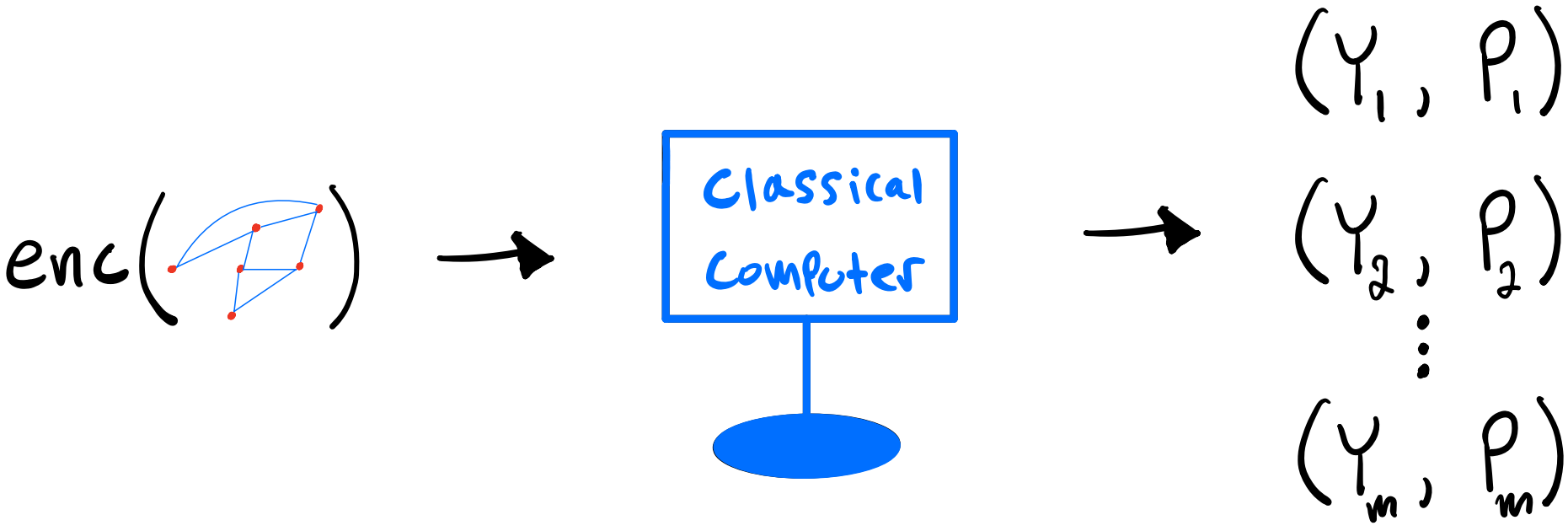
Classical and Quantum Computers



$$\text{enc}\left(\text{  }\right) = 1001011\,0111$$

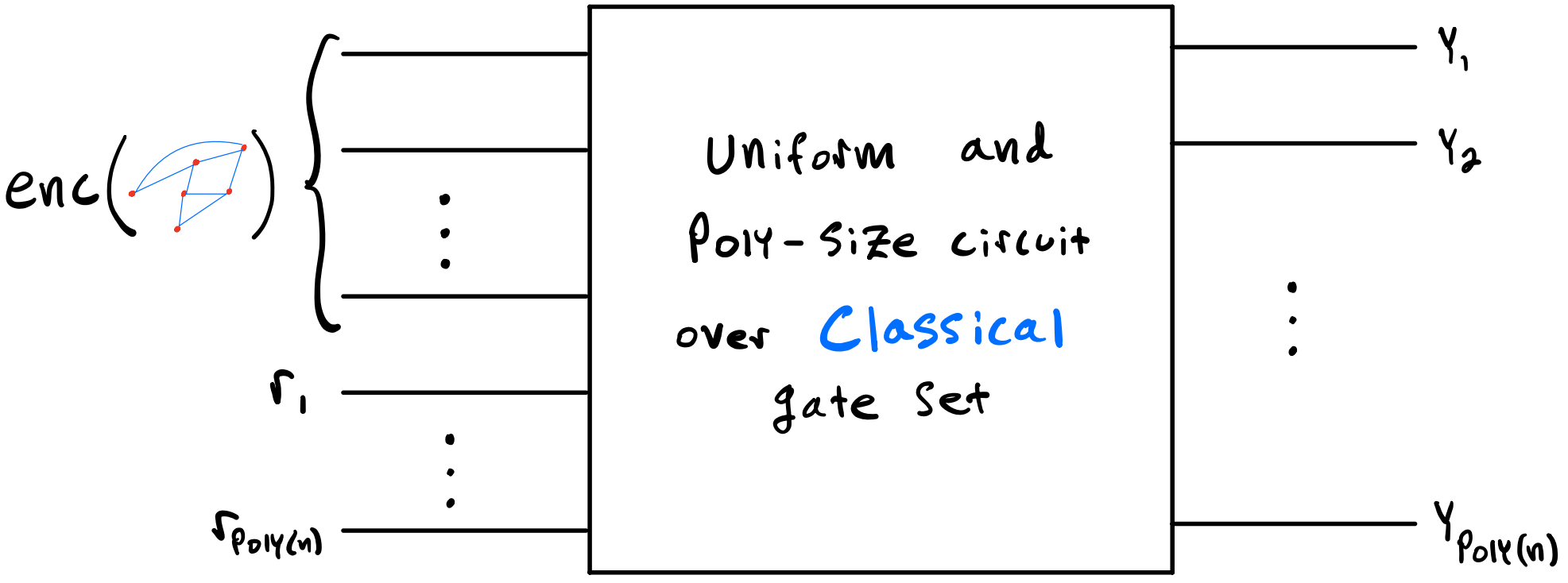
$$\in \{0,1\}^n$$

$$\subset \{0,1\}^*$$



$$y_i \in \{0,1\}^{poly(n)}, \quad p_i = Pr[y_i]$$

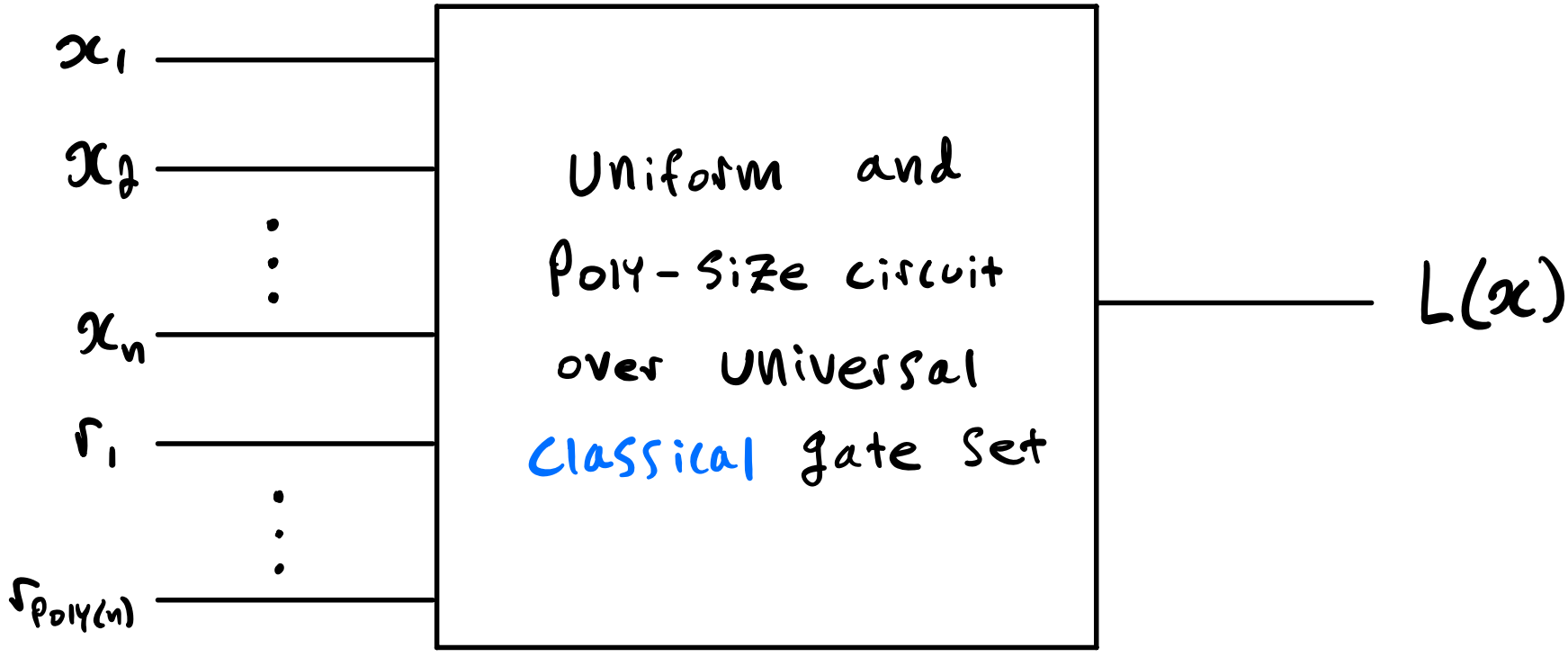
Efficient Classical Computer:

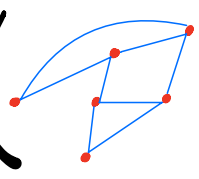


$$r_1, \ldots, r_{poly(n)} \sim \text{Uniform}(\{0,1\})$$

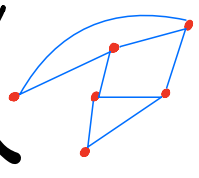
Def: $L \in$ BPP iff $\exists$ efficient Classical Computer C over Universal Classical gate set such that $\forall x \in \{0,1\}^*$,

$$Pr[C(x) = L(x)] \geq 2/3 .$$



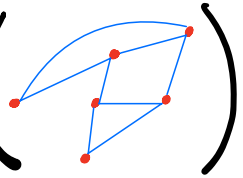
$\mathrm{enc}($  $) = 1001011\,0111$

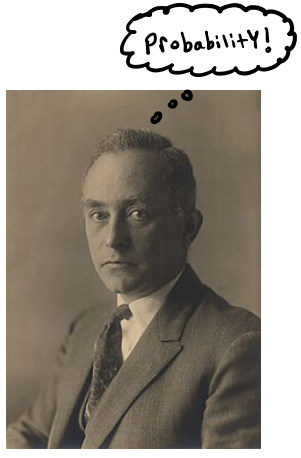
encode in quantum system

$\mathrm{Qenc}($  $) =$ 

$= |1001011\,0111\rangle$

$\in (\mathbb{C}^{2^n}, \langle \cdot | \cdot \rangle)$

$Qenc($  $)$ → Quantum Computer → $\sum_{z \in \{0,1\}^n} \beta_z |z\rangle$



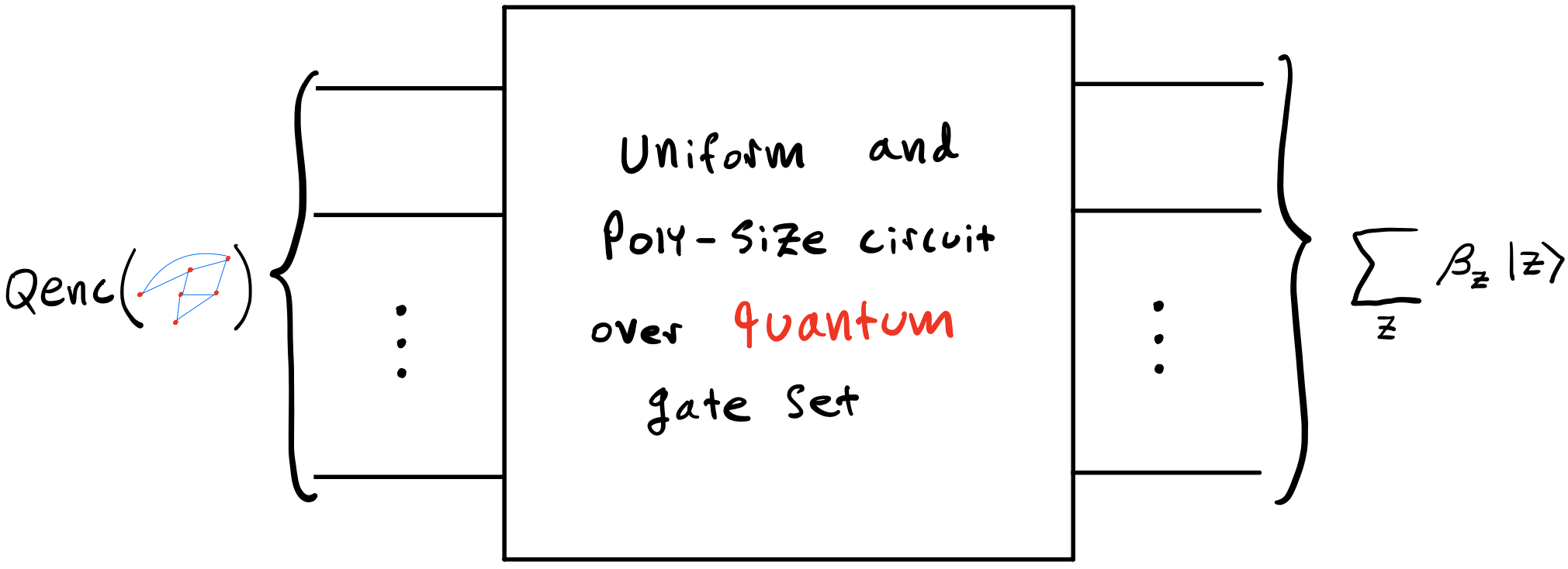
- $Pr[Y] = |\langle Y| \sum_z \beta_z |z\rangle|^2$

  $= |\beta_Y|^2$



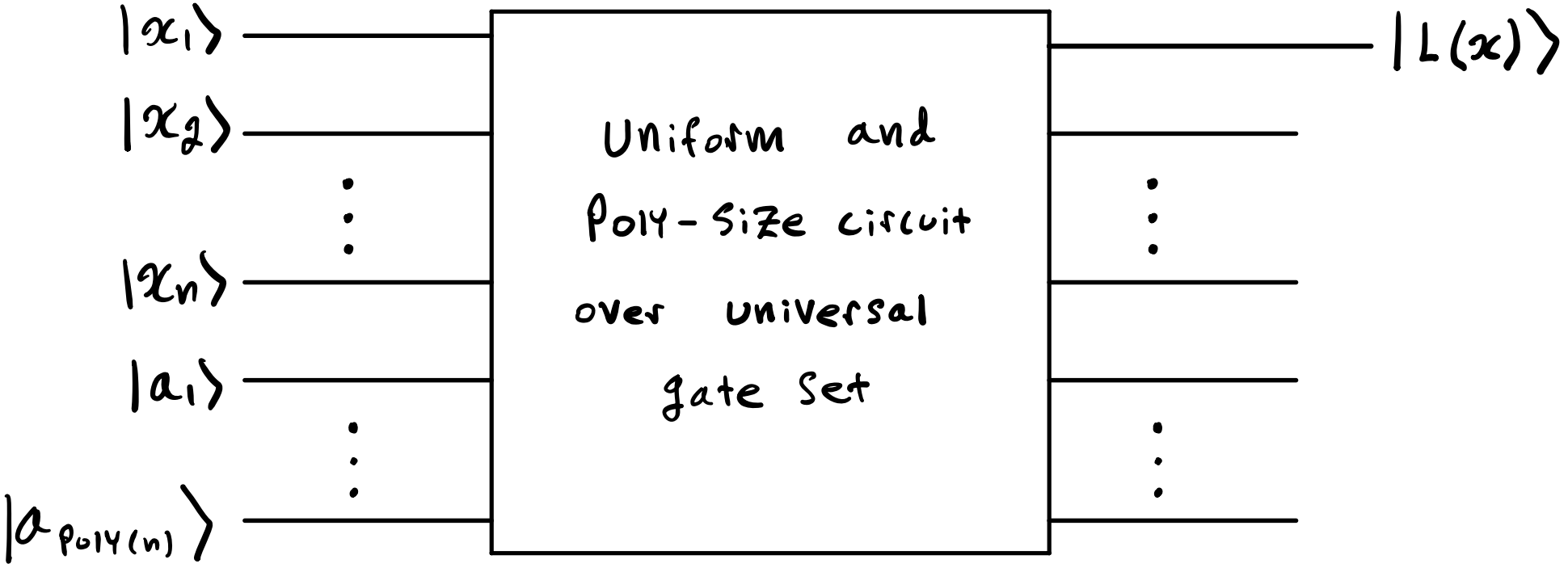
- Quantum Computer : $(\mathbb{C}^{2^n}, \langle \cdot | \cdot \rangle) \to (\mathbb{C}^{2^n}, \langle \cdot | \cdot \rangle)$

Efficient Quantum Computer:



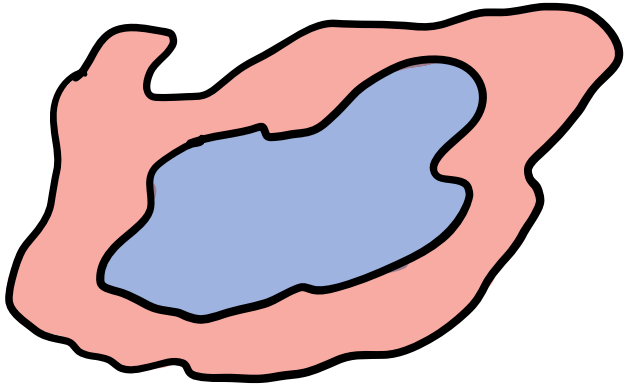
Def: $L \in$ BQP iff $\exists$ efficient quantum computer Q over a universal gate set such that $\forall x \in \{0,1\}^*$,

$$Pr[Q(x)_1 = L(x)] \geq 2/3 .$$



Fact: $BPP \subseteq BQP$

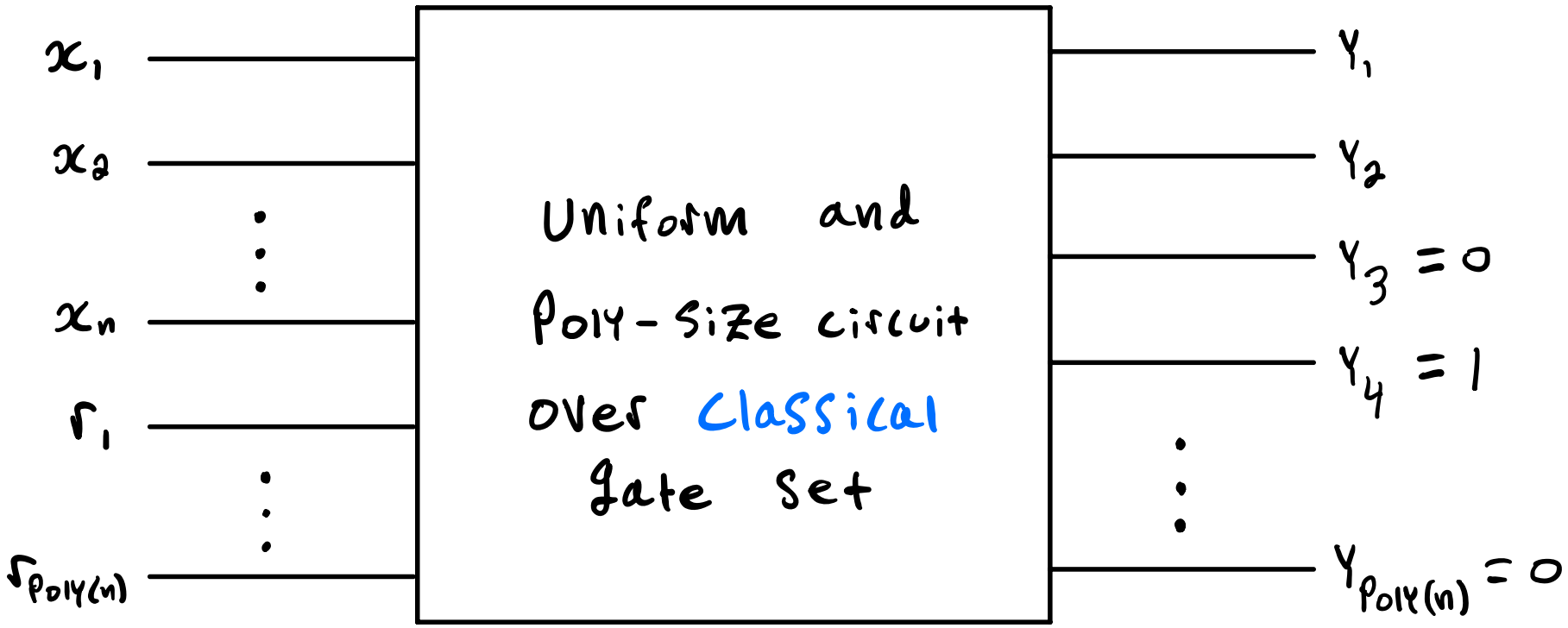
Conj: $BPP \subsetneq BQP$



Part II

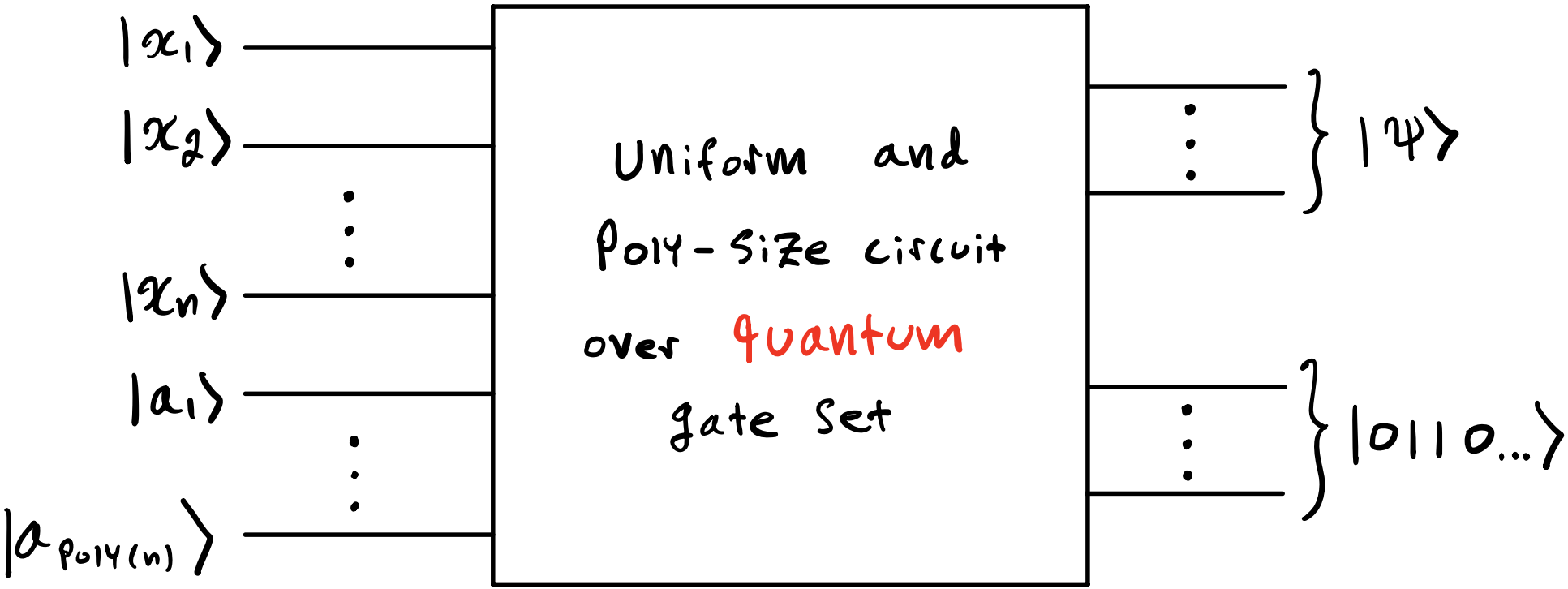
Post-Selection

Efficient Post-selected Classical Computer:



PostBPP

Efficient Post-selected Quantum Computer:



PostBQP



BPP



PostBPP



BQP



PostBQP

Bouland, 2018

Facts:

- $\mathrm{P}^{\mathrm{PostBPP}} \subseteq \Sigma_3\mathrm{P}$ (HHT, 1997)
- $\mathrm{PostBQP} = \mathrm{PP}$ (Aaronson, 2005)
- $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ (Toda, 1991)

Corollary:

$\mathrm{PostBPP} = \mathrm{PostBQP} \rightarrow \mathrm{PH} \subseteq \Sigma_3\mathrm{P}$

Upshot:

Quantum Mechanics ⇝ BQP

Modified Quantum Mechanics ⇝ New Complexity Classes!

Some Examples

Post-Selection (Aaronson '05) ⇝ PostBQP

Hidden Variables (Aaronson '05) ⇝ DQP

Non-Collapsing Measurements (Aaronson et al. '14) ⇝ PDQP

Quantum Cloning (Bao et al. '16) ⇝ CBQP

Rewindable Measurements (Hiromasa et al. '23) ⇝ RwBQP

Part III

Phase Erasure and MagBQP

Def: The **Mag gate** is the "phase erasure" map

$$\text{Mag}: \underbrace{\sum_x \alpha_x |x\rangle}_{|\psi\rangle} \longmapsto \underbrace{\sum_x |\alpha_x|\, |x\rangle}_{\text{Mag}(|\psi\rangle) = |\text{Mag}(\psi)\rangle}.$$

Observation: The Mag gate is non-linear (and therefore unphysical).

Proof:

$$\text{Mag}(e^{i\theta}|\psi\rangle) = \text{Mag}(|\psi\rangle)$$

$$\neq e^{i\theta}\,\text{Mag}(|\psi\rangle).$$

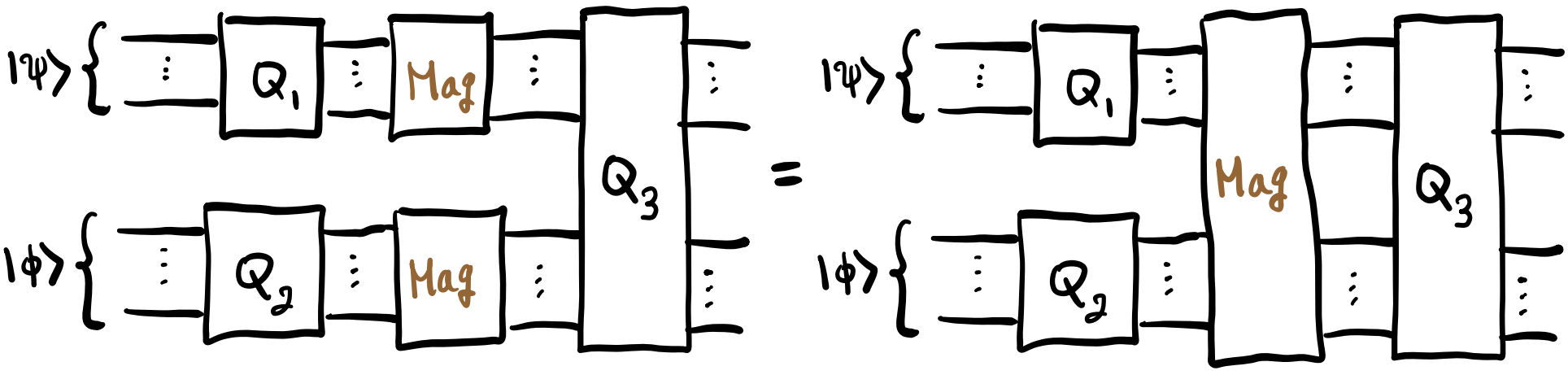
Observation: The Mag gate respects $\otimes$:

$$\mathrm{Mag}(|\psi\rangle \otimes |\phi\rangle) = \mathrm{Mag}(|\psi\rangle) \otimes \mathrm{Mag}(|\phi\rangle) .$$

Proof:

$$\begin{aligned}
\mathrm{Mag}(|\psi\rangle \otimes |\phi\rangle) &= \sum_{x,y} |\alpha_x \beta_y| \, |x,y\rangle \\
&= \sum_{x,y} |\alpha_x| |\beta_y| \, |x,y\rangle \\
&= \mathrm{Mag}(|\psi\rangle) \otimes \mathrm{Mag}(|\phi\rangle) .
\end{aligned}$$

Corollary:



(Relevant for the quiz later)

Observation: The Mag gate is expansive:

$$|\langle \mathrm{Mag}(\psi) \,|\, \mathrm{Mag}(\phi)\rangle| \geq |\langle \psi | \phi \rangle| .$$

Proof:

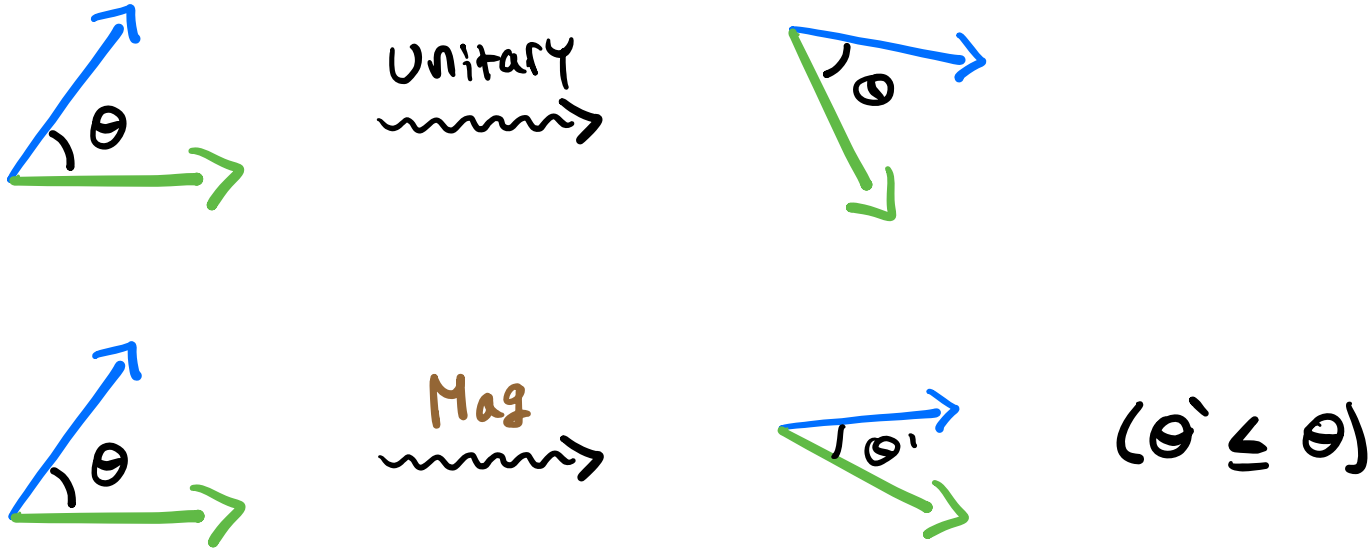
$$|\langle \mathrm{Mag}(\psi) \,|\, \mathrm{Mag}(\phi)\rangle| = \sum_x |\alpha_x \beta_x|$$

$$\geq \left| \sum_x \alpha_x \beta_x \right|$$

$$= |\langle \psi | \phi \rangle| .$$

Corollary:

Mag gates cannot help distinguish quantum states any more than unitaries can.

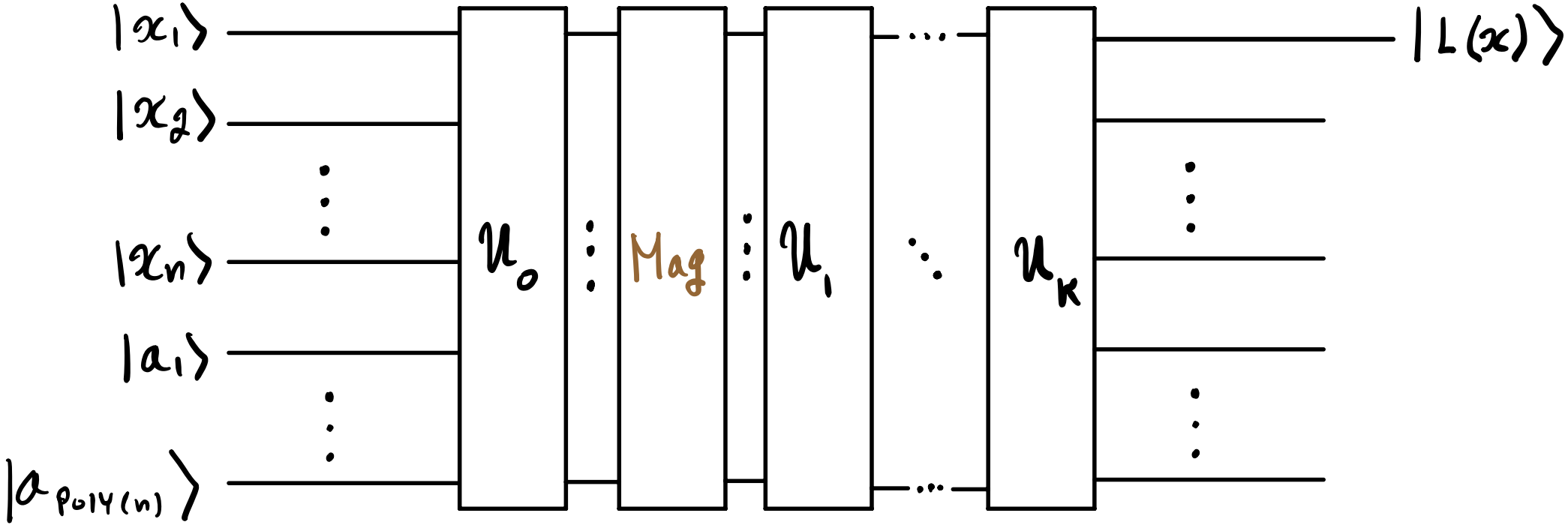


Part IV

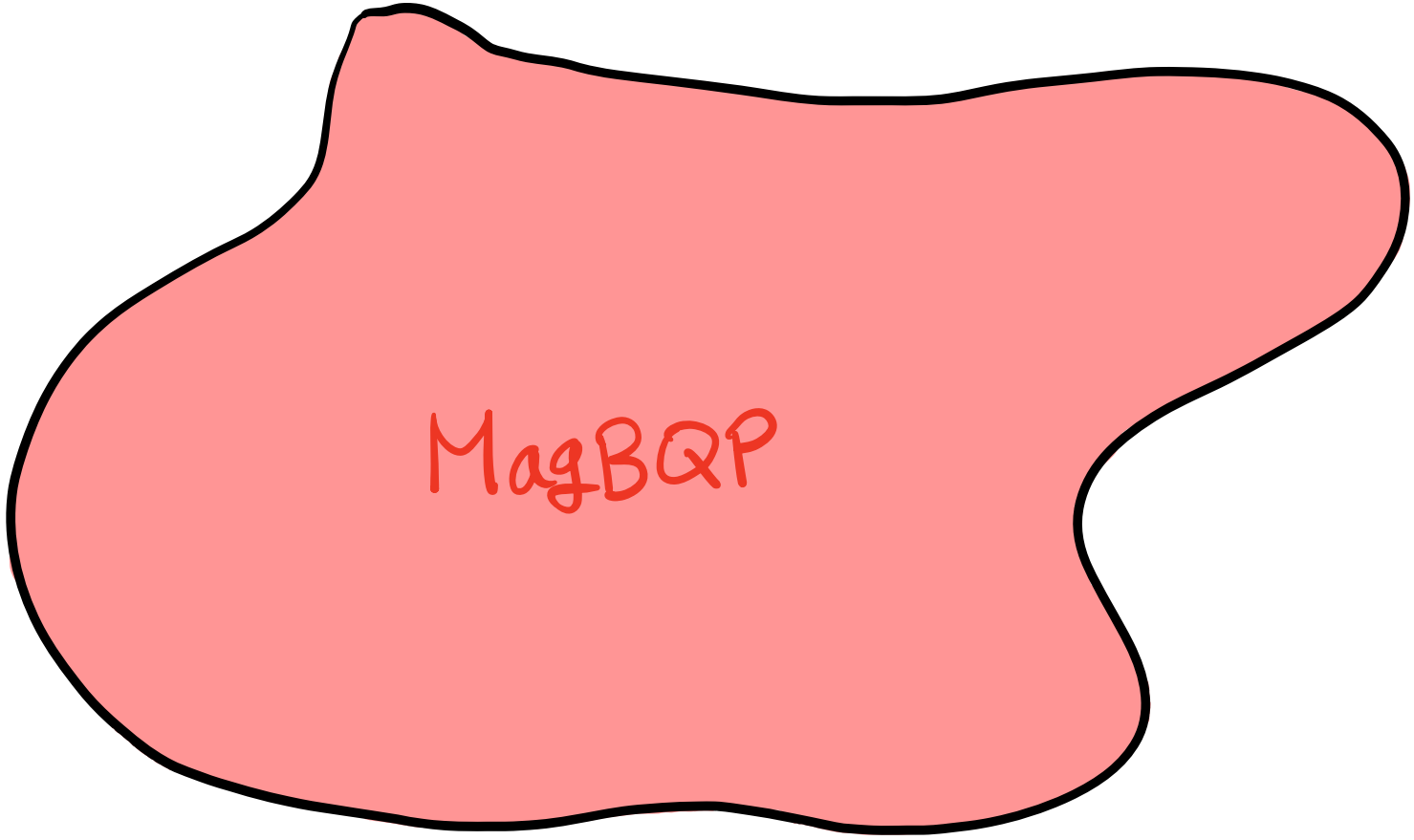
The Computational Power of Eliminating Relative Phases

Def: $L \in \text{MagBQP}_K$ iff $\exists$ uniform and poly-size circuit family Q over a universal gate set + Mag gate s.t. $\forall x \in \{0,1\}^*$,

- $Q(x)$ uses $\leq K$ Mag gates
- $\Pr[Q(x)_1 = L(x)] \geq 2/3$.

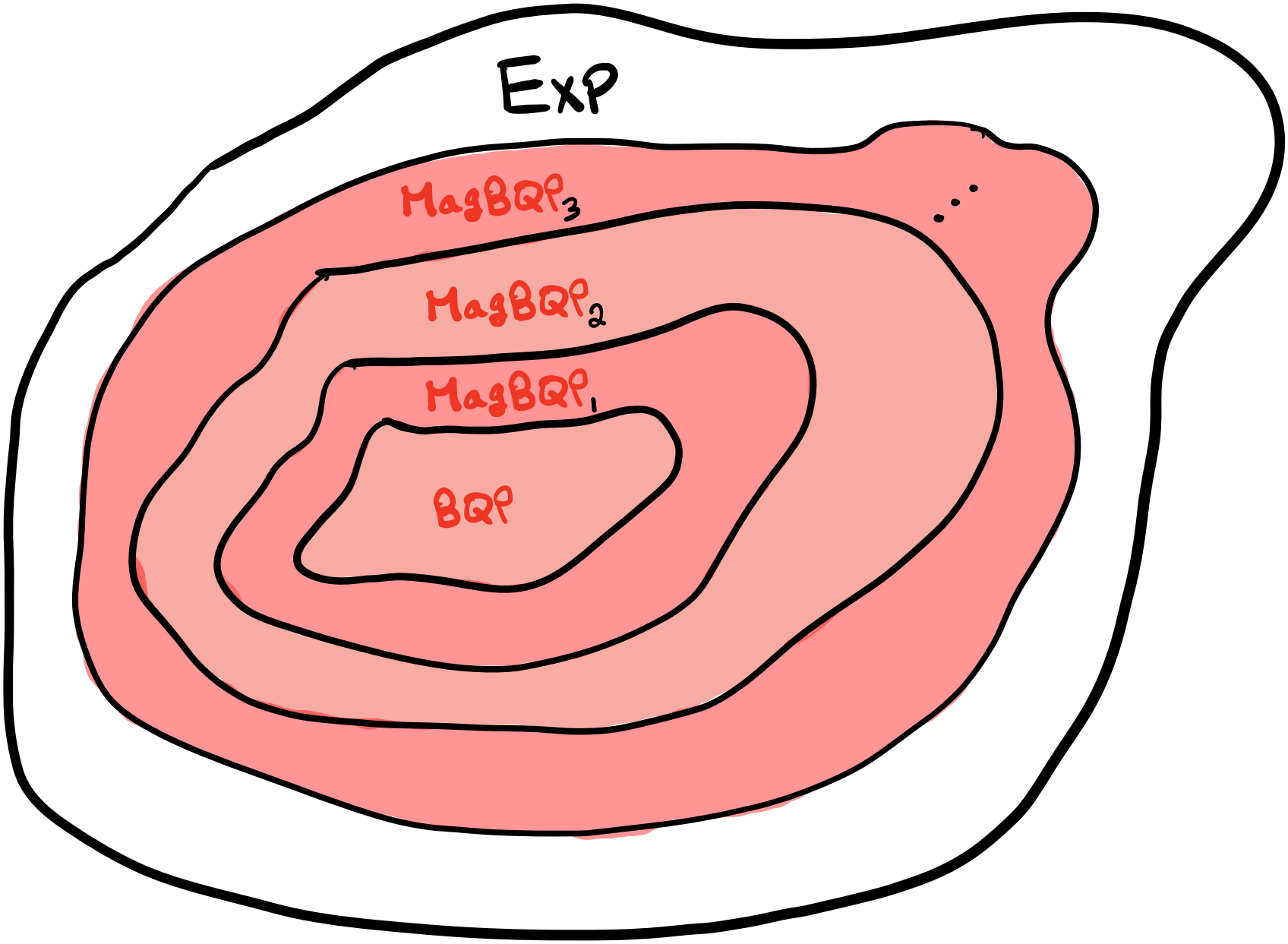


Def: $\mathrm{MagBQP} := \bigcup_{k \geq 0} \mathrm{MagBQP}_k$.



Basic Facts (a.k.a. "The Quiz")

- $BQP = MagBQP_0$
- $\forall k,\ MagBQP_k \subseteq MagBQP_{k+1}$
- $MagBQP \subseteq Exp$
- $\forall k,\ MagBQP_k$ admits Probability amplification
- $\forall k,\ MagBQP_k$ independent of underlying universal gate set (Solovay-Kitaev works)


EXP
MagBQP$_3$
MagBQP$_2$
MagBQP$_1$
BQP

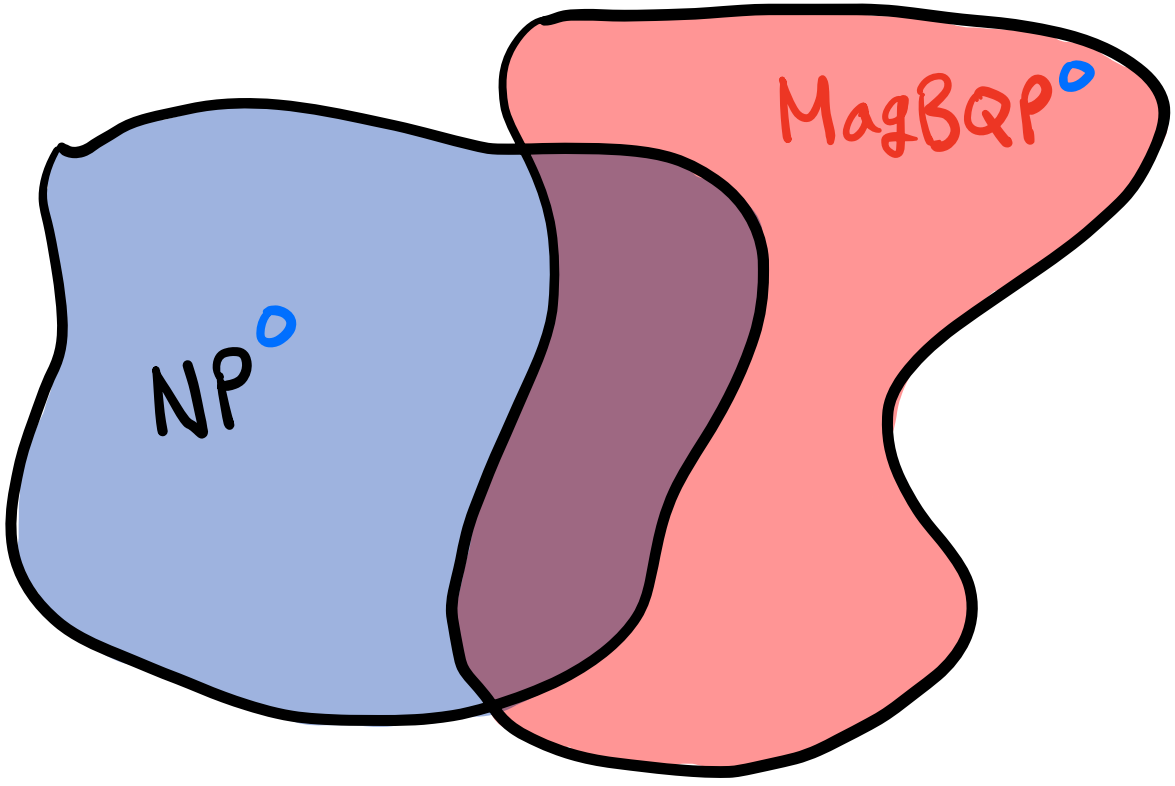
 = No AI used (save checking result)

 = AI used in Proof (ask how!)



Results:

$\exists$ oracle O s.t. $NP^O \not\subseteq MagBQP^O$.





Proof Idea: Mag gates do not change Grover lower bound for the unstructured search problem.

Def: The unstructured search problem (USP) is:

Input: Oracle access to $f:[N] \to \{0,1\}$ s.t. $\exists!\, x$ s.t. $f(x)=1$.

Output: x.

Thm (Bennett et al. '97): On an efficient quantum computer, USP takes $\Omega(\sqrt{N})$ queries.

Idea (Ambainis, '00):



- Suppose Q solves USP. Then, for f and g with $x = f^{-1}(1)$ and $y = g^{-1}(1)$, $x \neq y$:

$$|0^n\rangle \xrightarrow{Q,f} |\psi_x^1\rangle \xrightarrow{Q,f} \cdots \xrightarrow{Q,f} |\psi_x^T\rangle \approx |x\rangle$$

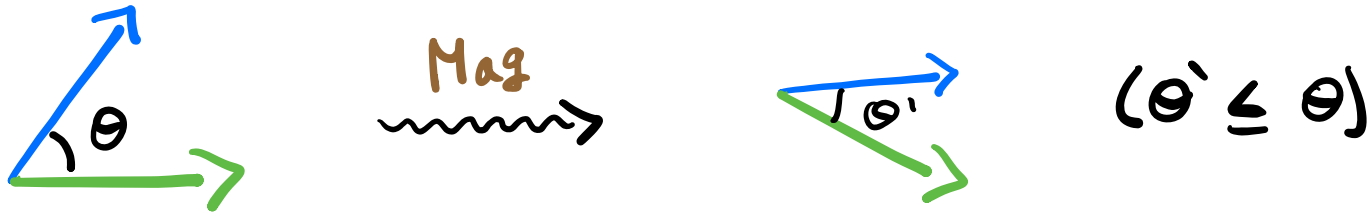
$$|0^n\rangle \xrightarrow{Q,g} |\psi_y^1\rangle \xrightarrow{Q,g} \cdots \xrightarrow{Q,g} |\psi_y^T\rangle \approx |y\rangle$$

- Therefore, the states $|\psi_x^i\rangle$ and $|\psi_y^i\rangle$ become increasingly distinguishable as $i \to T$.

- Unitaries can't distinguish quantum states, so the oracle calls are responsible, and it takes $T = \Omega(\sqrt{N})$ queries to distinguish.



But Mag gates don't help distinguish quantum states either!

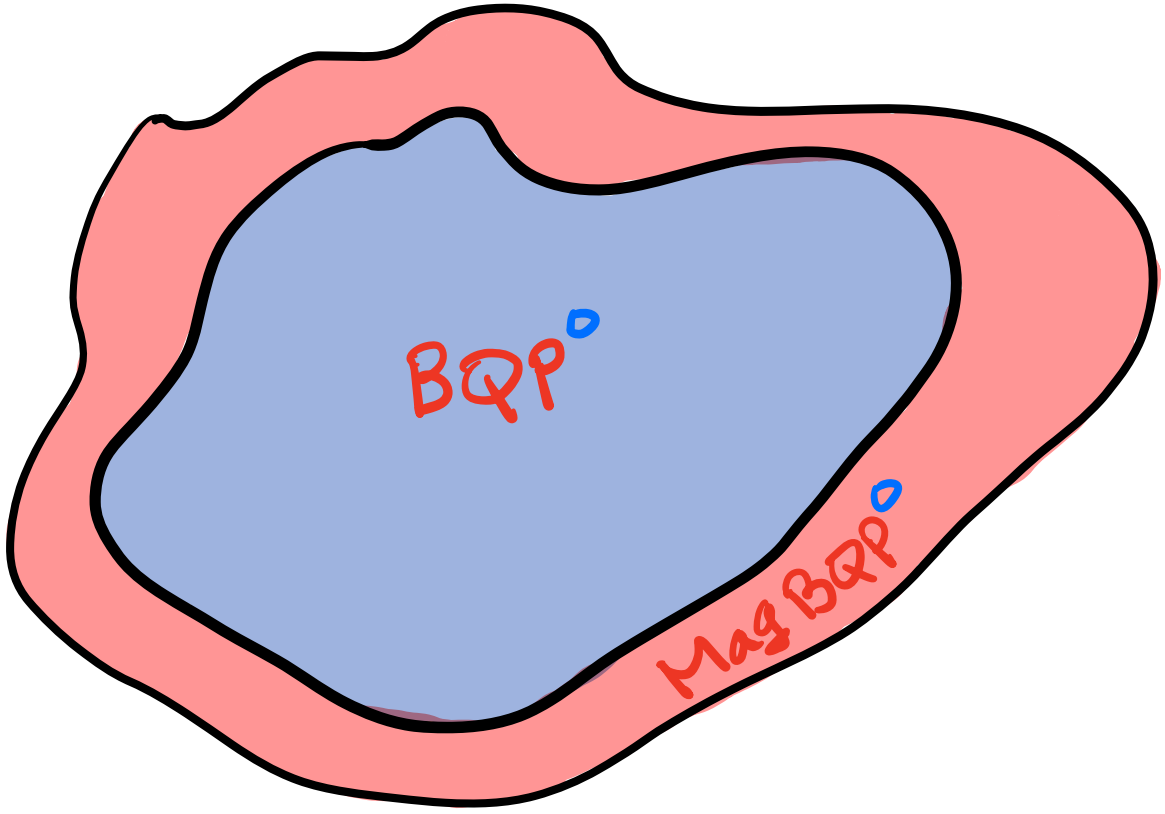


Corollary: Even with Poly(n) Mag gates, a MagBQP computer takes $\Omega(\sqrt{N})$ queries to solve USP.



Result:

$\exists$ oracle O s.t. $\mathrm{BQP}^O \neq \mathrm{MagBQP}_1^O$.





Proof Idea: Mag gates help solve Collision problem, which no BQP computer can do.

Def: The **Collision Problem** is:

Input: Oracle access to $f:\{0,1\}^n \to \{0,1\}^n$ that is either 1-1 or 2-1.

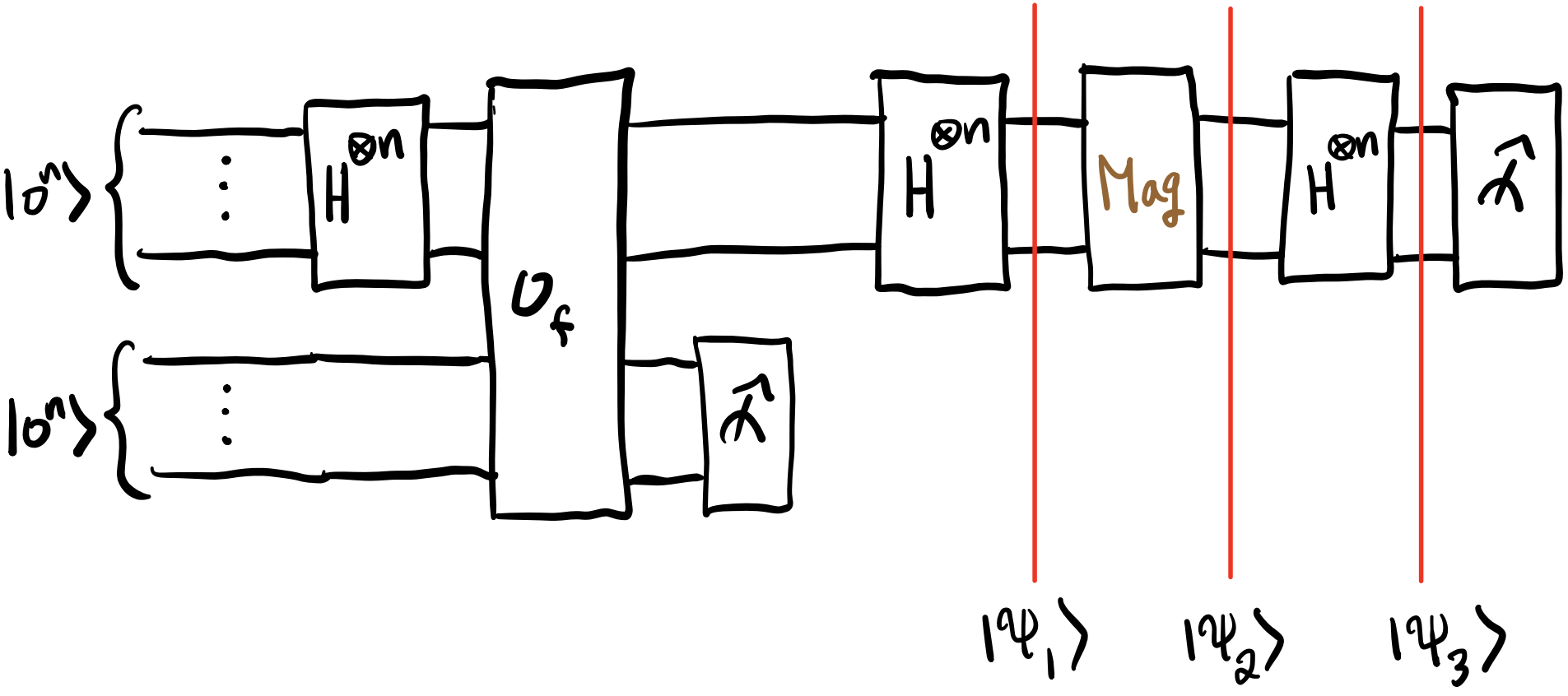
output: Decide which.

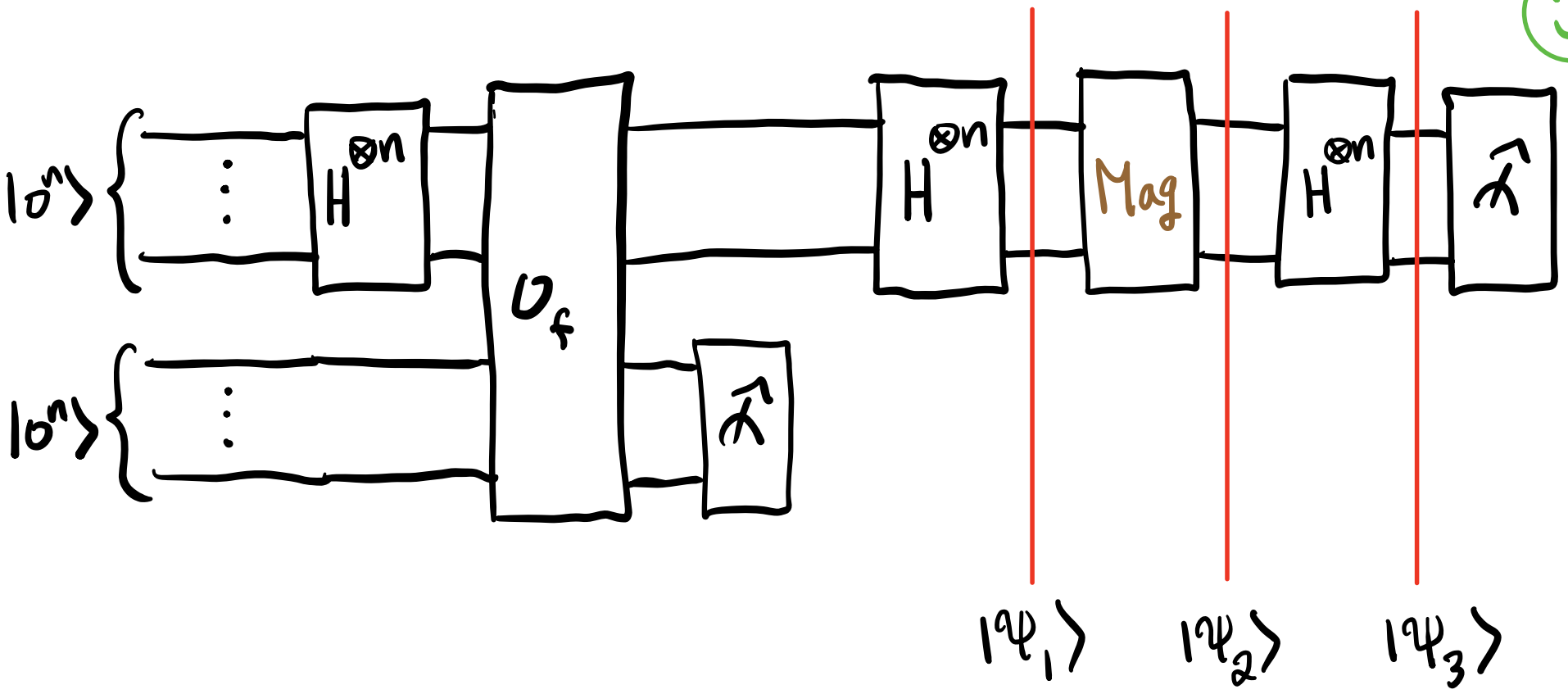
Thm (Aaronson, '01): On an efficient quantum computer, Collision takes $\Omega(2^{n/5})$ queries.



Result: With one Mag gate, an efficient quantum computer can solve collision with $O(1)$ queries.

Proof Sketch:





$$|\psi_1\rangle = \sum_{\substack{x \in f^{-1}(y) \\ w \in \{0,1\}^n}} (-1)^{x \cdot w} |w\rangle, \quad y \sim \mathrm{Im}(f)$$

$|\psi_1\rangle$ very sensitive to $|f^{-1}(y)|$!

1-1:

$$|\psi_2\rangle = \sum_{w \in \{0,1\}^n} |w\rangle$$

$$|\psi_3\rangle = H^{\otimes n} |\psi_2\rangle$$

$$= |0^n\rangle.$$

Measure

$$\Pr[0^n] = 1.$$

2-1:



$$|\psi_2\rangle = \sum_{\substack{w \in \{0,1\}^n \\ w \cdot (x_1 \oplus x_2) = 0}} |w\rangle$$

$$|\psi_3\rangle = H^{\otimes n} |\psi_2\rangle$$

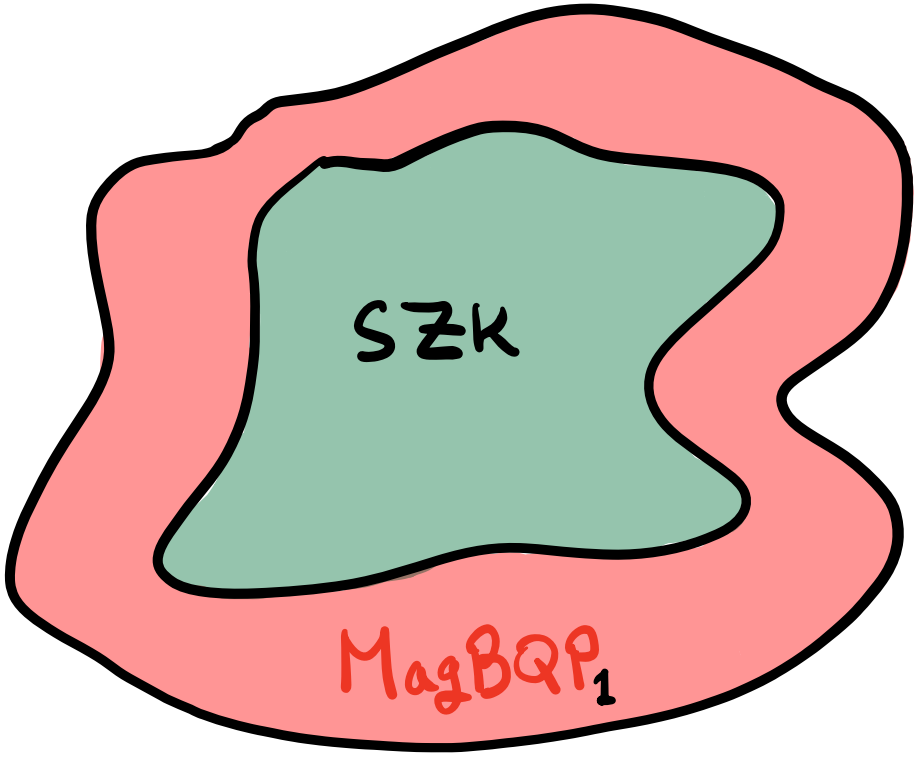
$$= \frac{1}{\sqrt{2}} \left(|0^n\rangle + |x_1 \oplus x_2\rangle \right).$$

Measure

$$\Pr[0^n] = 1/2.$$



Result: $SZK \subseteq MagBQP_1$.



Def: The **Statistical difference Problem (SDP):**

Input: Circuits $C_0, C_1 : \{0,1\}^n \to \{0,1\}^m$ that, on input $x \sim \{0,1\}^n$, give distributions $\mathcal{D}_0, \mathcal{D}_1$, respectively.

Output:
- YES if $TVD(\mathcal{D}_0, \mathcal{D}_1) \geq 2/3$
- NO if $TVD(\mathcal{D}_0, \mathcal{D}_1) \leq 1/3$.

Def (Sahai-Vadhan, '03):

$L \in SZK$ iff it is (Karp) reducible to SDP.

Thm (Okamoto, '00): $coSZK = SZK$.

Ex: GI ∈ SZK

- Given G_0, G_1, let C_0 and C_1 be circuits that, on a random input, output a random permutation of G_0 and G_1, respectively.
- If $G_0 \cong G_1$, then

$$TVD(\mathcal{D}_0, \mathcal{D}_1) = 0.$$

- If $G_0 \not\cong G_1$, then

$$TVD(\mathcal{D}_0, \mathcal{D}_1) = 1.$$



Proof Idea for SZK ⊆ MagBQP$_1$:

Given SDP instance $C_0, C_1 : \{0,1\}^n \to \{0,1\}^m$, Prepare

$$|\Phi_b\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^m} e^{i\theta(y)} \sqrt{N_b(y)}\, |y\rangle$$

where

- $b \in \{0,1\}$
- $N_b(y) = |C_b^{-1}(y)|$
- θ is any fnc.



Then,

$$|\Psi_b\rangle := \mathrm{Mag}(|\Phi_b\rangle)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^m} \sqrt{N_b(y)} \; |y\rangle$$

$$= \sum_{y \in \{0,1\}^m} \sqrt{\mathcal{D}_b(y)} \; |y\rangle .$$

So,

- $\mathcal{D}_0 \approx \mathcal{D}_1 \rightarrow |\Psi_0\rangle \approx |\Psi_1\rangle$
- $\mathcal{D}_0 \not\approx \mathcal{D}_1 \rightarrow |\Psi_0\rangle \not\approx |\Psi_1\rangle$

} State discrimination task doable in BQP.

How to Prepare

$$|\Phi_b\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^m} e^{i\theta(y)} \sqrt{N_b(y)}\, |y\rangle \quad ?$$

Take a (random) walk!

Fact: For $\sigma_1, \ldots, \sigma_N \sim \{-1, 1\}$, $X = \sum_i \sigma_i$ has

$$\mathbb{E}[|X|] \approx \sqrt{N}.$$

To Prepare $|\Phi_b\rangle$:

- Define "random looking" $f:\{0,1\}^n \to \{0,1\}$.
- Prepare

$$\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle |C_b(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_y \sum_{x \in C_b^{-1}(y)} (-1)^{f(x)} |x\rangle |y\rangle .$$

- Hadamard x-register and apply Mag

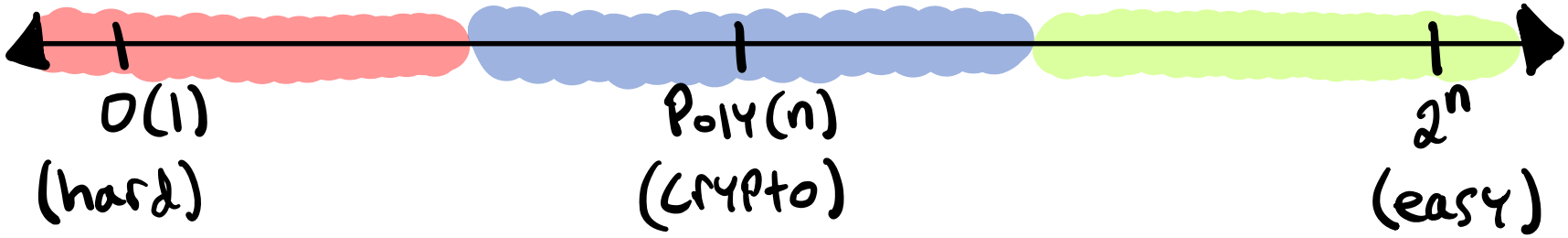
$$\frac{1}{\sqrt{2^n}} \sum_{y,z} \left| \sum_{x \in C_b^{-1}(y)} (-1)^{f(x)+x\cdot z} \right| |z\rangle |y\rangle$$

Sum of $N_b(y) = |C_b^{-1}(y)|$

"random" signs, so is $\approx \sqrt{N_b(y)}$

Corollary:

$\sqrt{\frac{n}{\log n}}$-GapSVP $\in$ MagBQP_1 (Goldreich–Goldwasser).

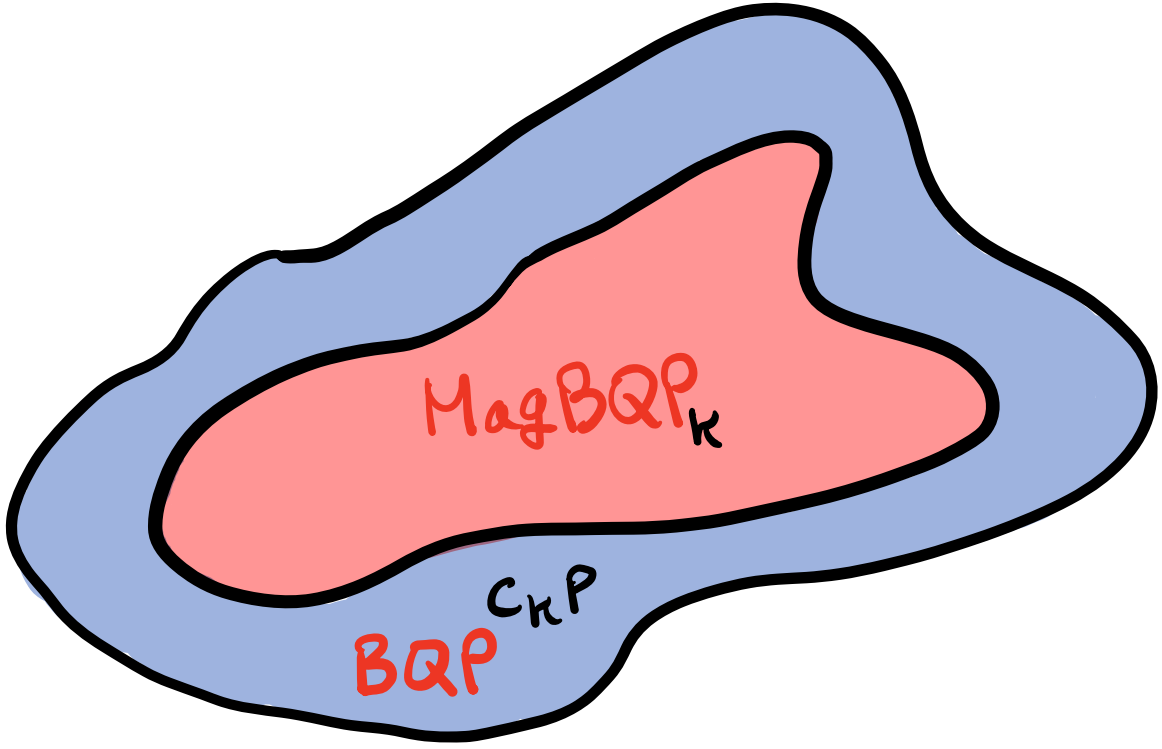


"Bennett Diagram"

⇝ A single Mag late destroys security guarantee of many lattice-based crypto protocols!



Result: $\mathrm{MaqBQP}_k \subseteq \mathrm{BQP}^{\mathrm{C}_k\mathrm{P}}$, where $\mathrm{C}_k\mathrm{P}$ is the kth level of the Counting hierarchy ($\mathrm{C}_0\mathrm{P}=\mathrm{P}$, $\mathrm{C}_k\mathrm{P}=\mathrm{P}^{\mathrm{P}^{\mathrm{C}_{k-1}\mathrm{P}}}$).



Proof Idea: Use GapP characterization of PP and BQP.

Def: $f \in \mathrm{GapP}$ iff $\exists$ poly-time NTM M s.t.

$$f = \begin{pmatrix} \#\text{ accepting} \\ \text{paths of } M \end{pmatrix} - \begin{pmatrix} \#\text{ rejecting} \\ \text{paths of } M \end{pmatrix}.$$

Thm. (Fenner-Fortnow-Kurtz, '94):

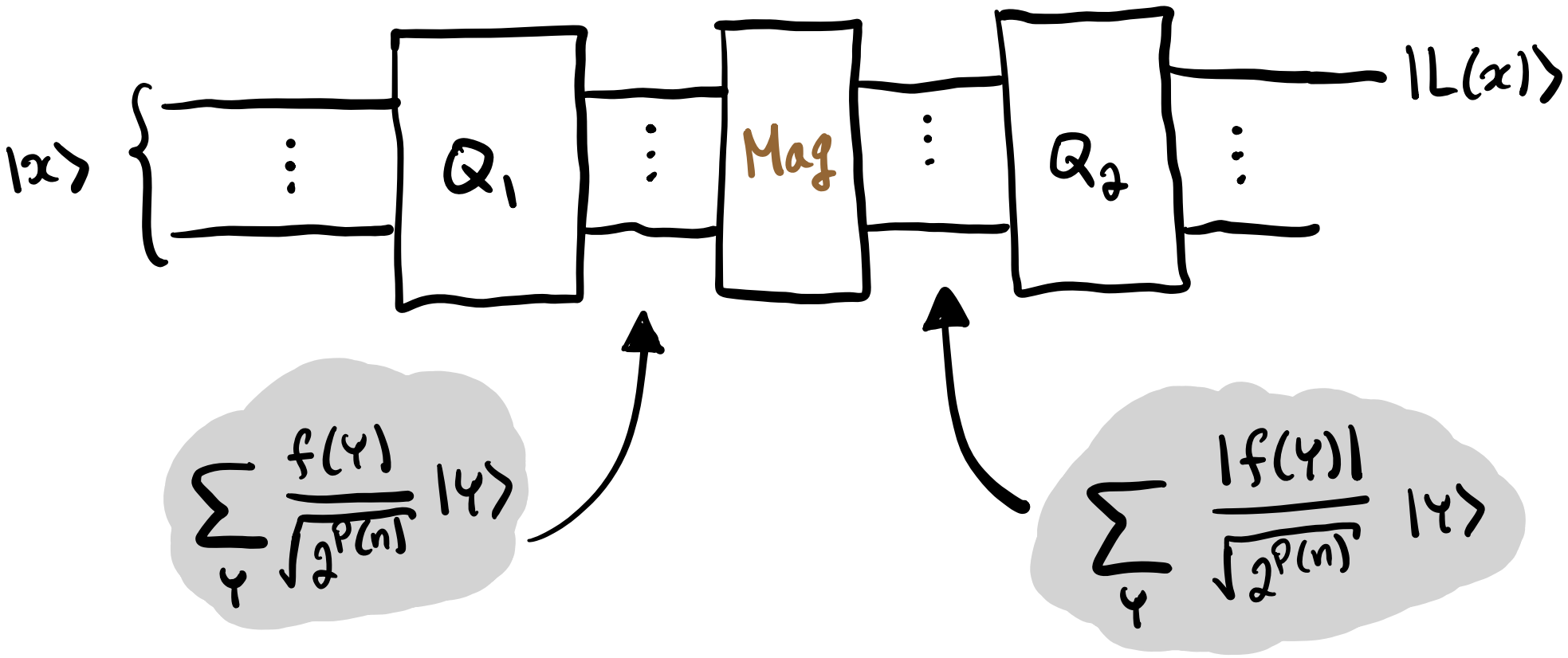
$L \in \mathrm{PP}$ iff $\exists f \in \mathrm{GapP}$ s.t. $\forall x,\ x \in L \Leftrightarrow f(x) > 0$.

Thm (Fortnow-Rogers, '98):

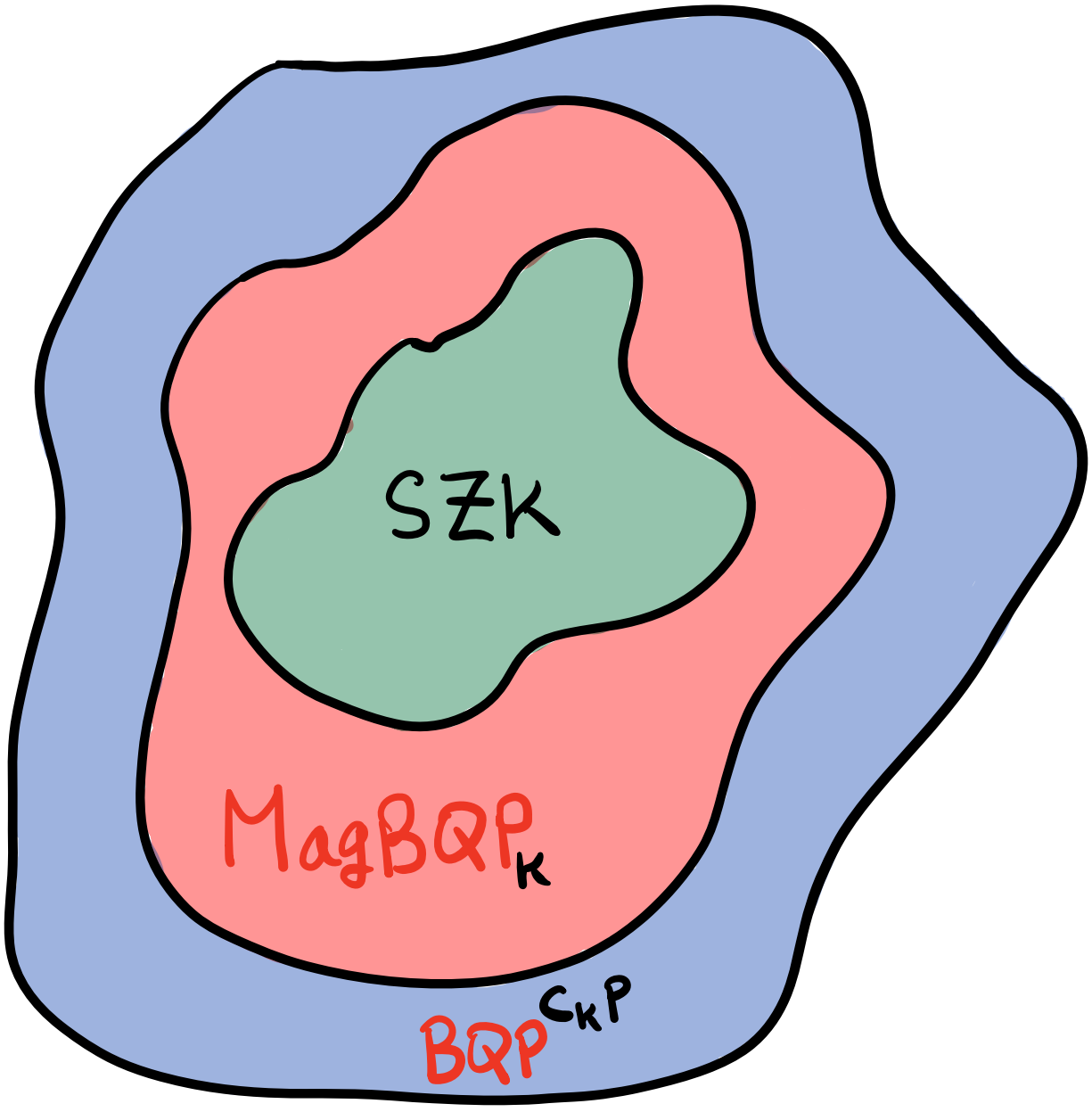
$\forall$ quantum states $|\psi\rangle = \sum_y \alpha_y |y\rangle$ realized by an efficient quantum computer, $\exists$ GapP f and poly p s.t.

$$\alpha_y = \frac{f(y)}{\sqrt{2^{p(n)}}}.$$

If $L \in \mathrm{MagBQP}_1$, then



- To simulate Mag, suffices to decide sign of $f \in \mathrm{GapP}$. But that's PP!
- $\mathrm{MagBQP}_1 \subseteq \mathrm{BQP}^{\mathrm{PP}}$ (Relativized version gives $\mathrm{MagBQP}_k \subseteq \mathrm{BQP}^{\mathrm{C_kP}}$)


SZK
MagBQP$_k$
BQP^{C_kP}

Open Questions:

- Can we break LWE with $\mathrm{Poly}(n)$ Mag gates?

  ⇝ If so, Post-quantum crypto not secure in world with Mag gates.

- $\mathrm{PostMagBQP}_k \stackrel{?}{=} \mathrm{C_{k+1}P}$.

  ⇝ If so, then generalizes Aaronson's $\mathrm{PostBQP} = \mathrm{PP}$ to all levels of the CH.

  ⇝ Also suggests simulating 2 Mag gates with 1 Mag gate implies CH collapse.

Thank You!

Questions?