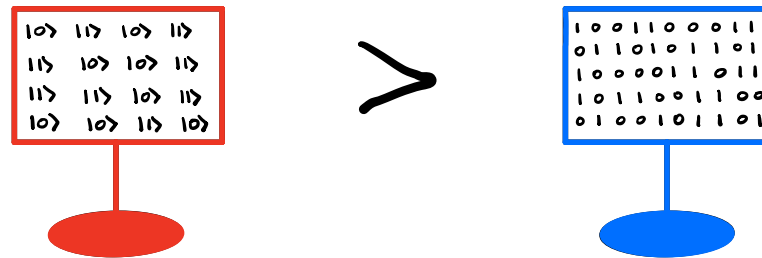


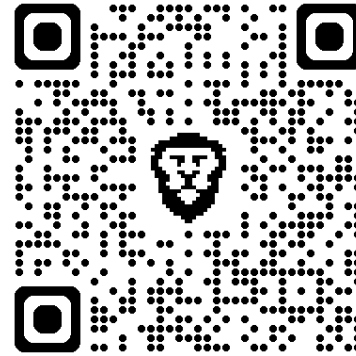
Post-Selected A Criterion for $\wedge$ Quantum Advantage



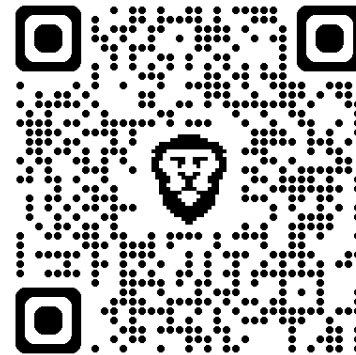
Matthew Fox

University of Colorado Boulder

Paper ~➡



Slides ~➡





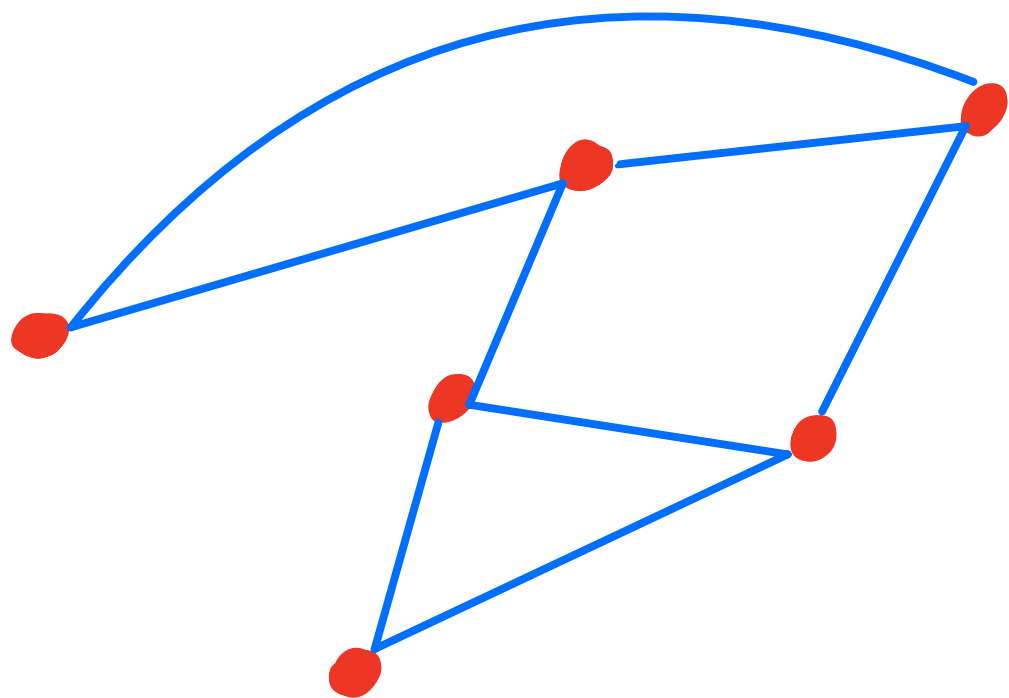
Chaitanya
Karamchedu
(UMD)



Daniel
Gottesman
(UMD)

Part I

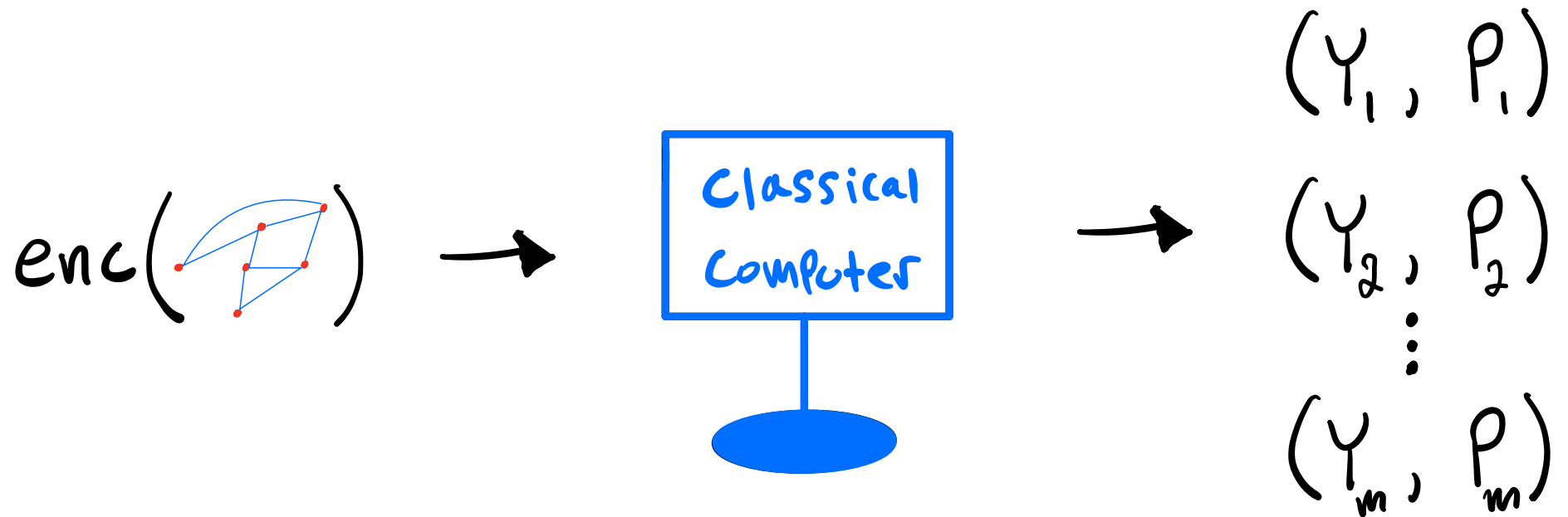
Classical and Quantum Computers



$$\text{enc}\left(\begin{array}{c} \text{Diagram} \end{array}\right) = 10010110111$$

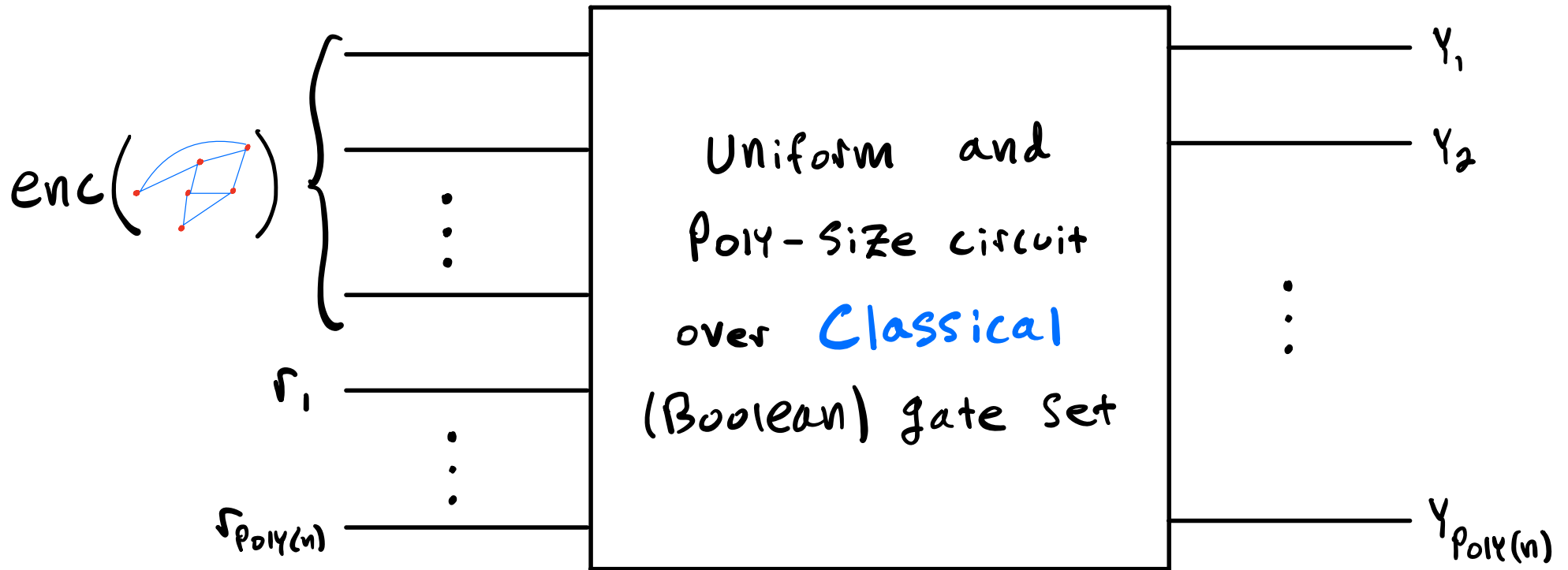
$$\in \{0, 1\}^n$$

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



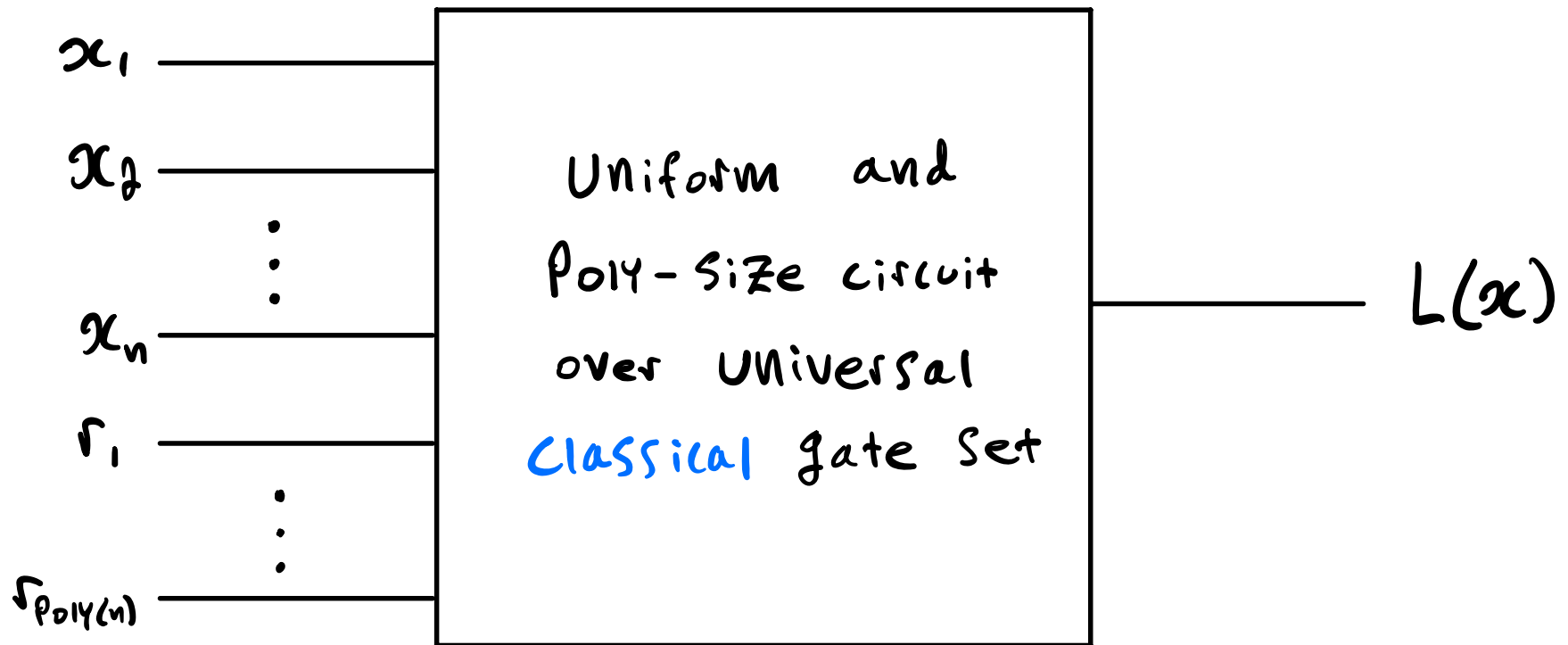
$$Y_i \in \{0,1\}^{poly(n)}, \quad P_i = P_r[Y_i]$$

Efficient **Classical** Computer:



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

Def: $L \in \text{BPP}$ iff $\exists$ efficient **Classical** computer **C** over Universal **Classical** gate set such that $\forall x \in \{0,1\}^*$,
 $\Pr[\text{C}(x) = L(x)] \geq 2/3$.



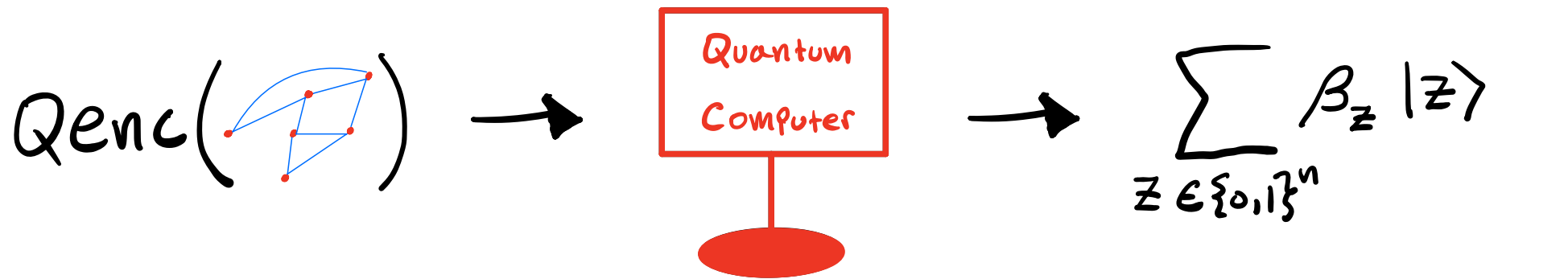
$$\text{enc}\left(\begin{array}{c} \text{graph} \end{array}\right) = 10010110111$$


 encode in
 quantum system

$$\text{Qenc}\left(\begin{array}{c} \text{graph} \end{array}\right) = \begin{array}{cccccccccccc} \bullet & & \bullet & & \bullet & & \bullet & & \bullet & & \bullet & & \bullet & & \bullet & & \bullet & & \bullet & & \bullet \end{array}$$

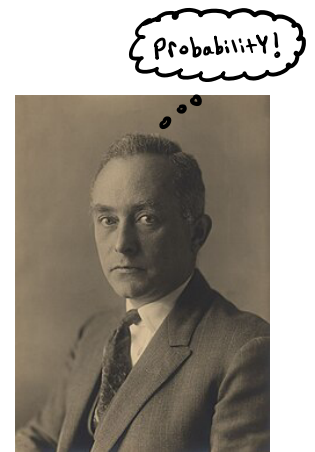
$$= |10010110111\rangle$$

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



- $$P_r[Y] = \left| \langle Y | \sum_{\mathbf{z}} \beta_{\mathbf{z}} |\mathbf{z}\rangle \right|^2$$

$$= |\beta_Y|^2$$

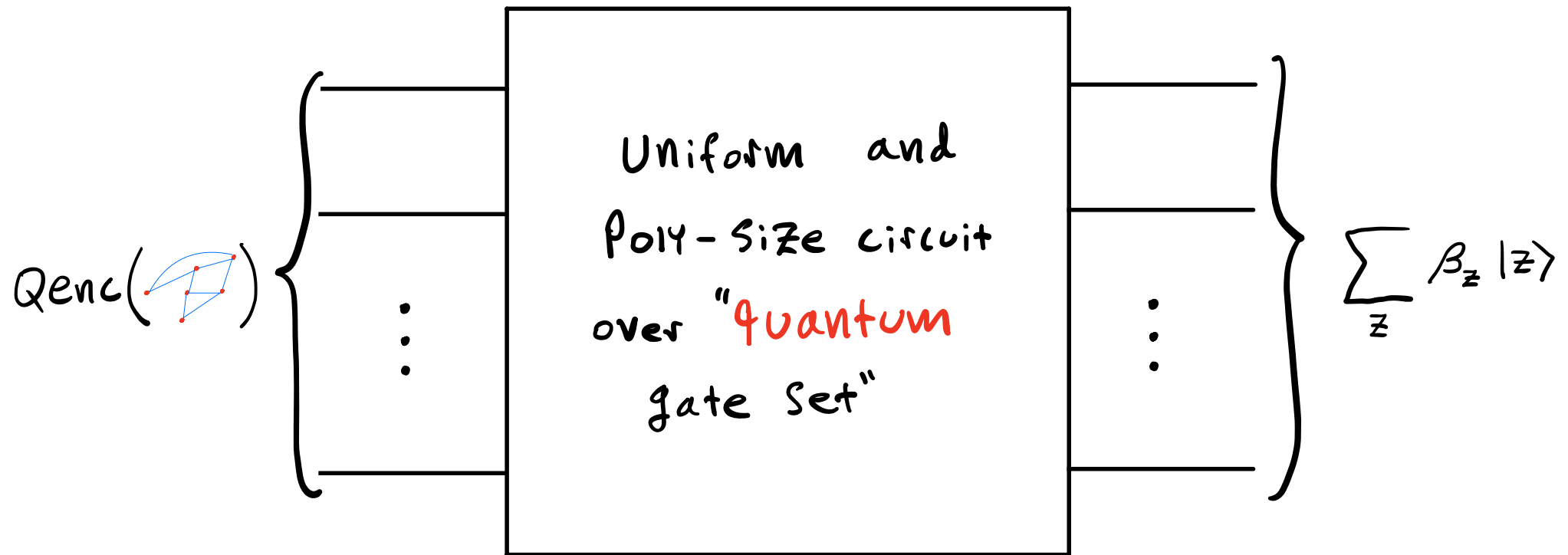


- $$\text{Quantum Computer} : (\mathbb{C}^{2^n}, \langle \cdot | \cdot \rangle) \rightarrow (\mathbb{C}^{2^n}, \langle \cdot | \cdot \rangle)$$

Unitary!



Efficient **Quantum** Computer:



Def: A Quantum Gate Set S is a finite collection of $SU(2)$ gates, together with at least one entangling gate E .

Ex:

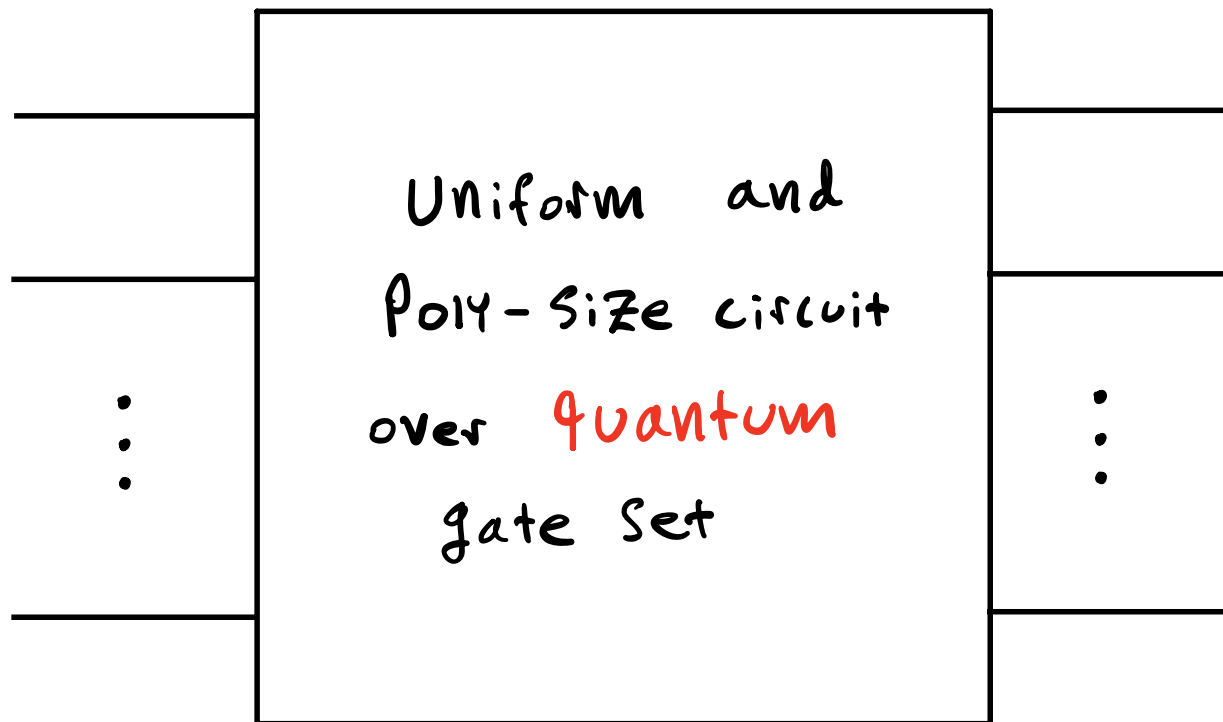
- Clifford = $\{H, S, CNOT\}$
- Clifford + T

Def: A quantum gate set S is
universal iff

$$\langle S \cap \text{SU}(2) \rangle = \text{group generated by } S \cap \text{SU}(2)$$

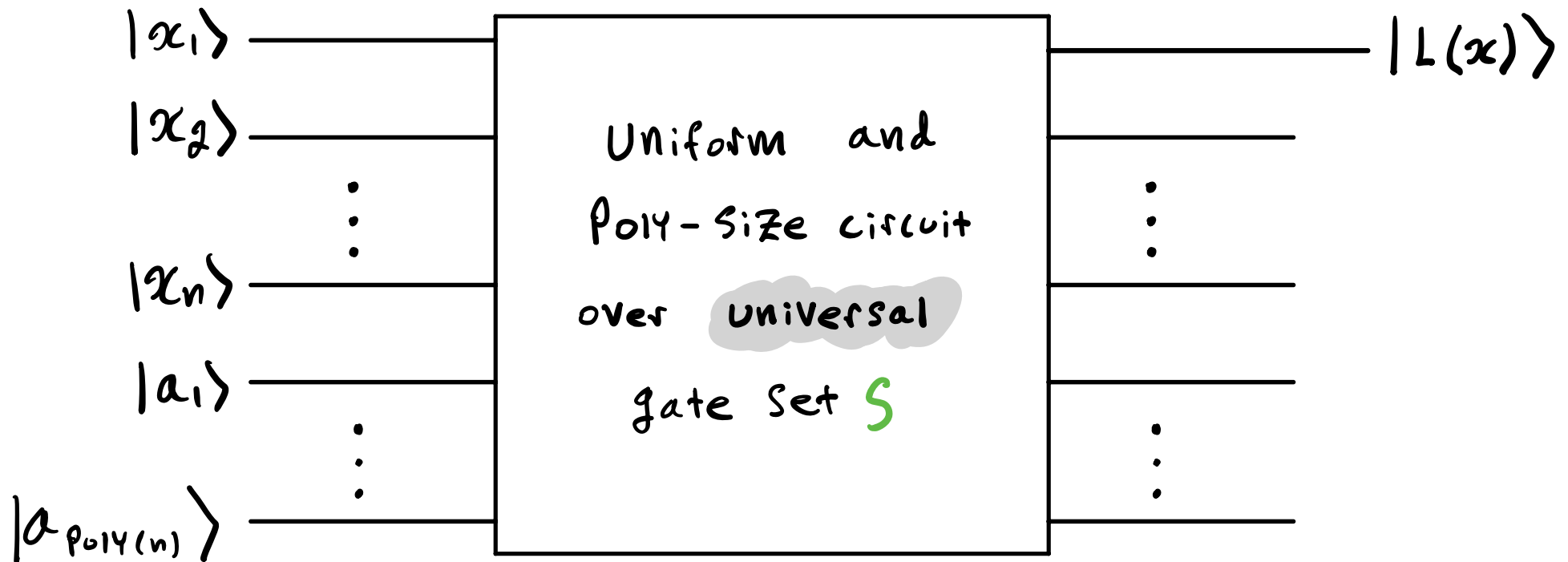
is dense in $\text{SU}(2)$.

Efficient Quantum Computer:



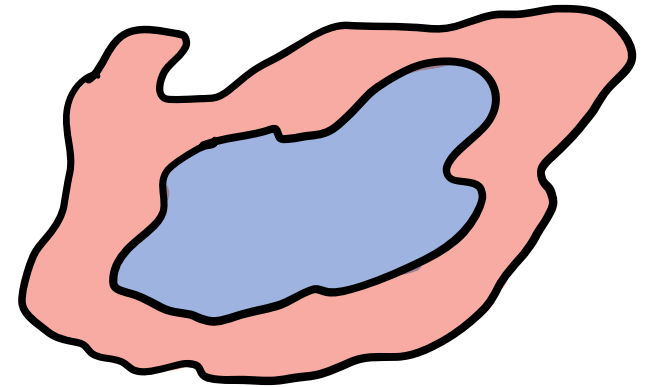
Def: $L \in \text{BQP}$ iff $\exists$ efficient quantum computer Q over a universal gate set S such that $\forall x \in \{0,1\}^*$,

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



Fact: $BPP \subseteq BQP$

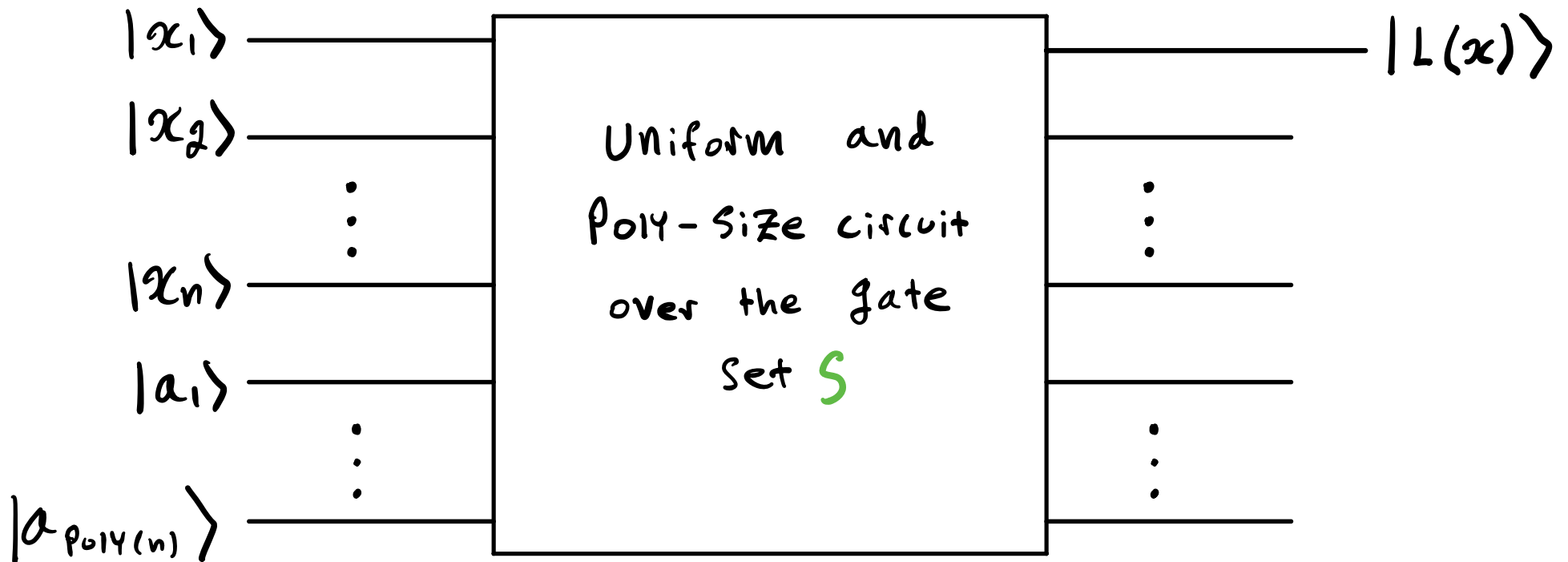
Conj: $BPP \subsetneq BQP$



Part II

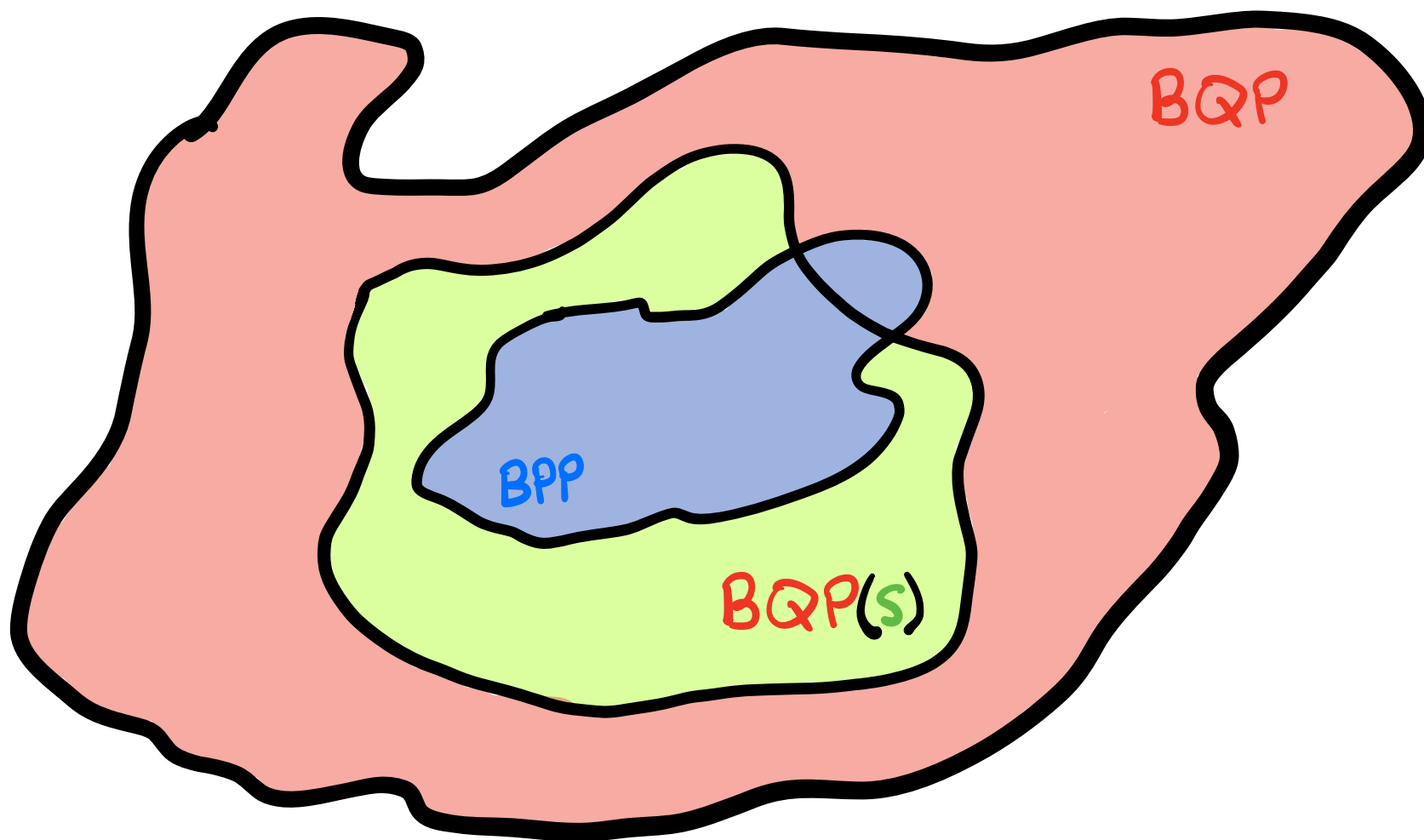
Non-Universal Quantum Computation

Def: $L \in \text{BQP}(S)$ iff $\exists$ efficient quantum computer Q over the gate set S such that $\forall x \in \{0,1\}^*$,
 $\Pr[Q(x) = L(x)] \geq 2/3$.

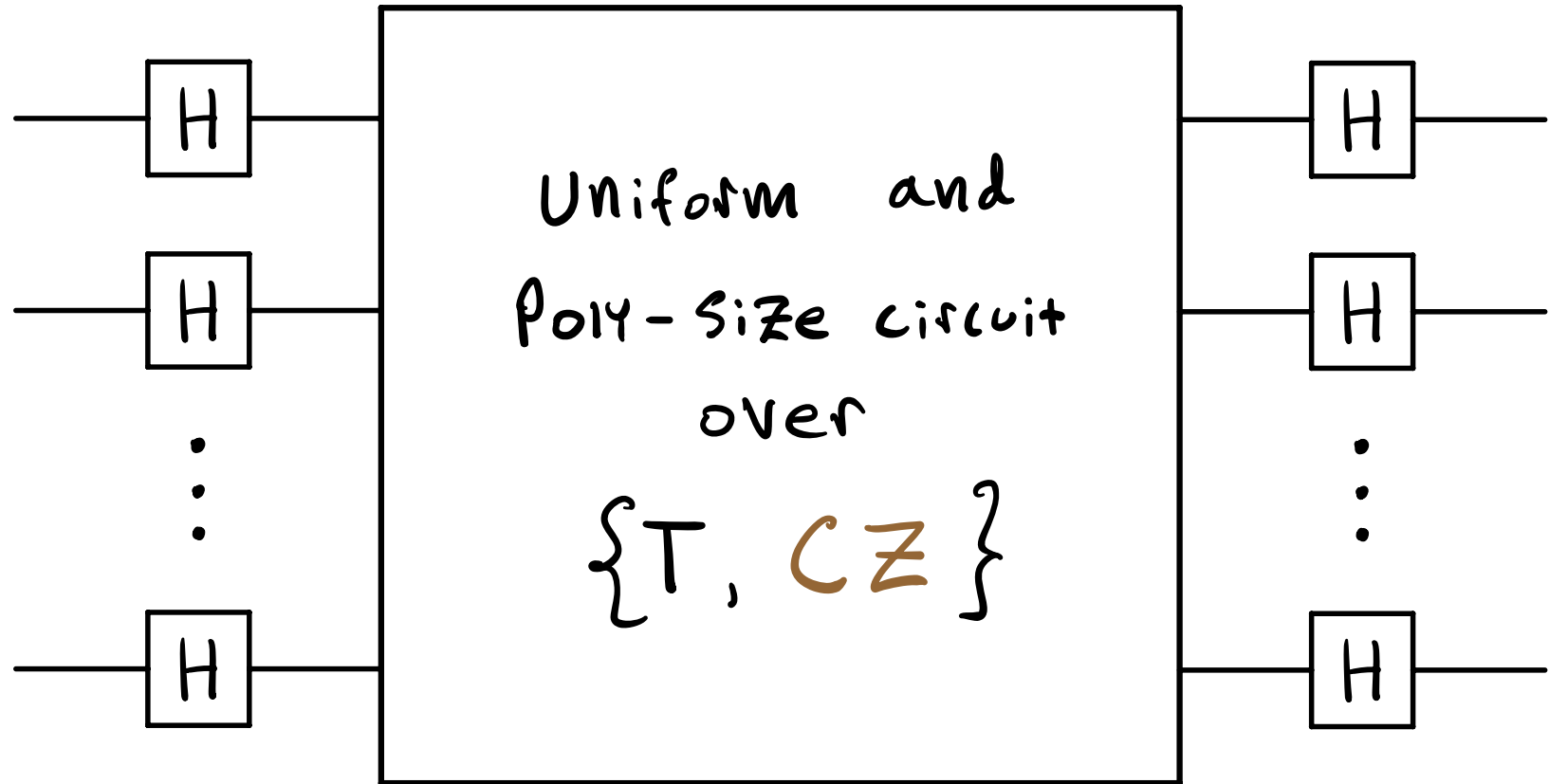


Facts:

- $\forall S, \text{BQP}(S) \subseteq \text{BQP}$
- $\forall \text{ universal } S, \text{BQP}(S) = \text{BQP}$
- $\exists \text{ non-universal } S \text{ s.t. } \text{BQP}(S) = \text{BQP}$
- $\exists \text{ non-universal } S \text{ s.t. } \text{BQP}(S) \subseteq \text{BPP}$

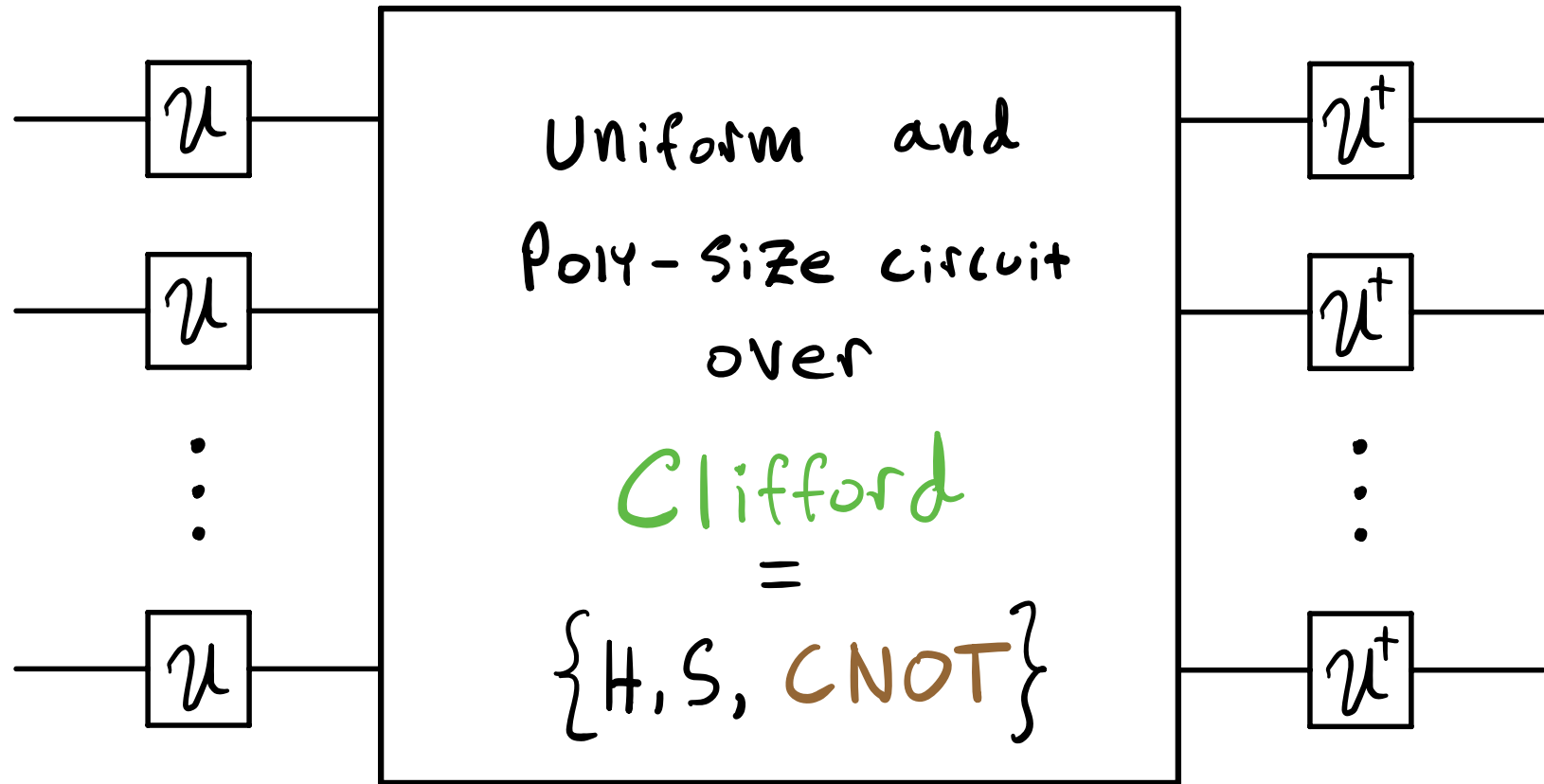


Instantaneous Quantum Polynomial



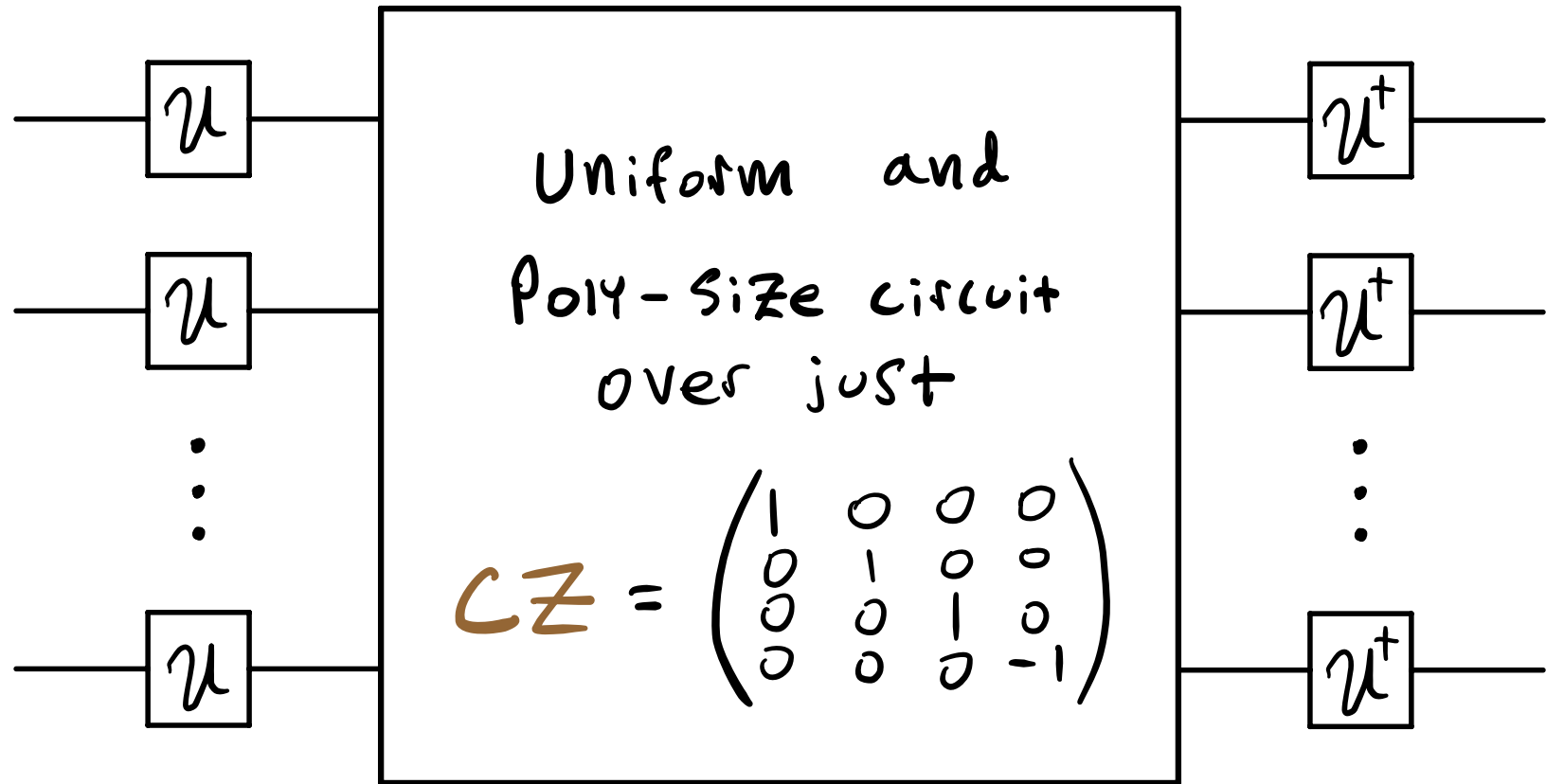
$$S_{\text{IQP}} = \{HTH, H \otimes H CZ H \otimes H\}$$

Conjugated Clifford Circuits



$$S_{ccc}(U) = \{U H U^\dagger, U S U^\dagger, U \otimes U \text{ CNOT } U^\dagger \otimes U^\dagger\}$$

Conjugated CZ Circuits



$$S_{CZ}(U) = \{U \otimes U \, CZ \, U^\dagger \otimes U^\dagger\}$$

Part III

Pigs Can't Fly

(the Polynomial hierarchy is infinite)

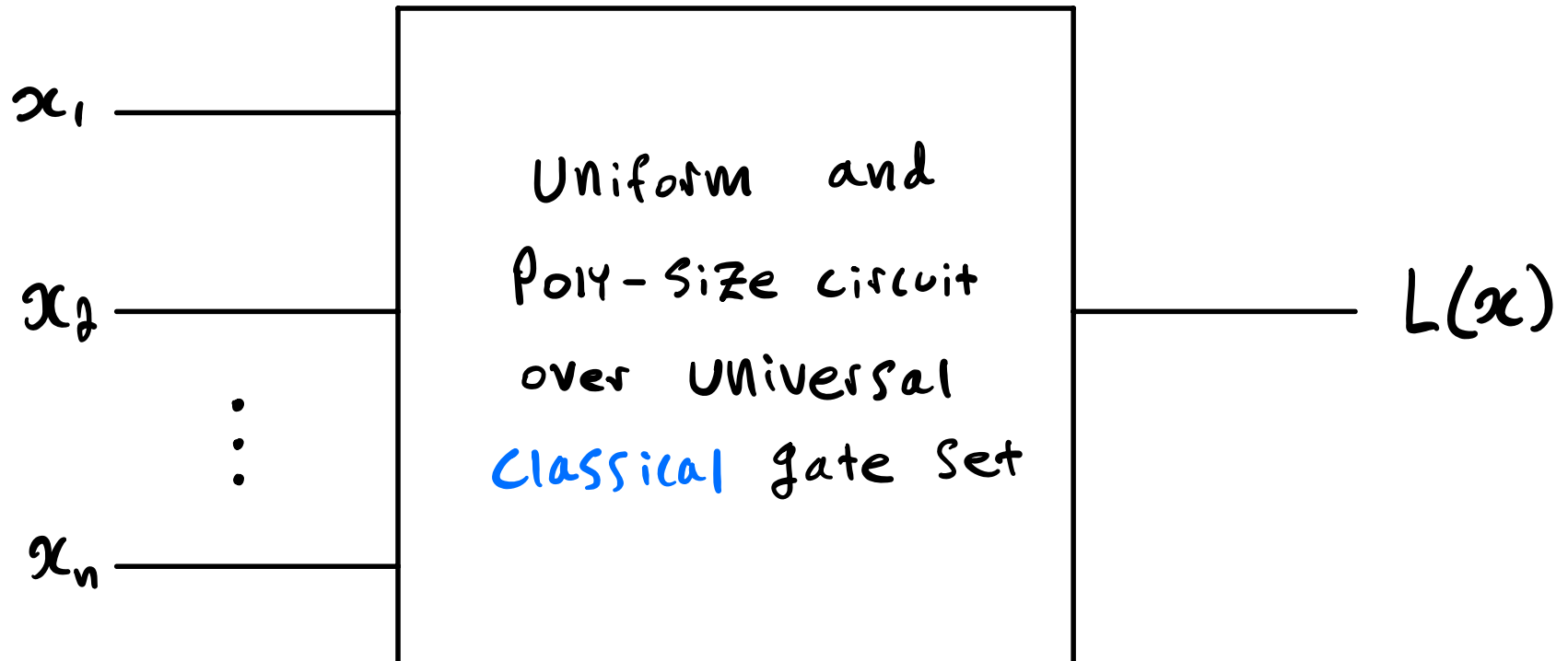
Def:

$L \in P$ iff $\exists$ deterministic



C

s.t. $\forall x \in \{0,1\}^*$, $C(x) = L(x)$.



Def:

$L \in NP$ iff $\exists$ deterministic  C
and a polynomial P s.t. $\forall x \in \{0,1\}^*$,
 $\exists y \in \{0,1\}^{P(|x|)}$ s.t. $C(x, y) = L(x)$.

Def:

$L \in \Sigma_k^P$ iff $\exists$ deterministic



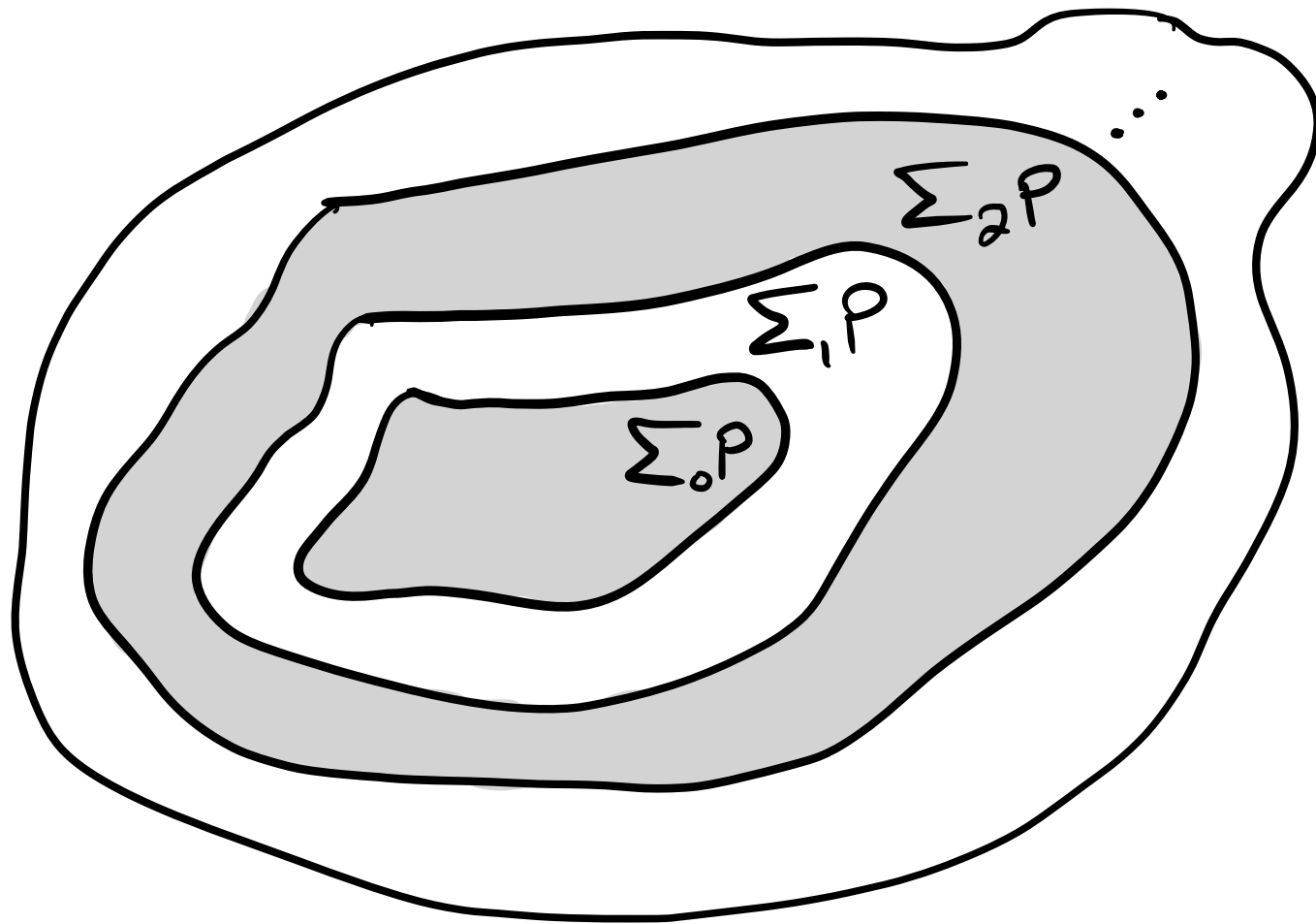
C

and polynomials $P_1, \dots, P_k$ s.t. $\forall x \in \{0,1\}^*$,

$$\exists y_1 \in \{0,1\}^{P_1(|x|)} \quad \forall y_2 \in \{0,1\}^{P_2(|x|)}$$

$$\exists y_3 \in \{0,1\}^{P_3(|x|)} \quad \dots \quad \exists \forall y_k \in \{0,1\}^{P_k(|x|)}$$

$$\text{s.t. } C(x, y_1, y_2, \dots, y_k) = L(x).$$



Def: $PH := \bigcup_{k \geq 0} \Sigma_k P$ ("Polynomial Hierarchy")

Facts:

- $P = NP$ iff $\Sigma_0 P = \Sigma_1 P$.
- For $k \neq l$, $\Sigma_k P = \Sigma_l P$ iff $PH = \Sigma_k P$.

“the PH collapses”

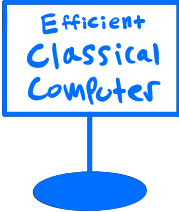
“the PH is not infinite”

Part IV

Quantum Advantage

"Quantum Advantage"



$\exists$  Such that $\forall$ 

$P_r[\cdot]$ and $P_r[\cdot]$ are

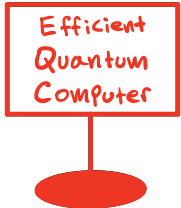
"Sufficiently different".

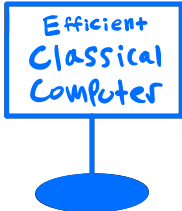
Def:

- Say C Simulates Q to within weak

Multiplicative error $\epsilon \geq 0$ iff $\forall x, y:$

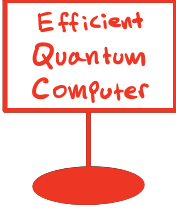
$$\frac{1}{1+\epsilon} \Pr[Q(x)=y] \leq \Pr[C(x)=y] \leq (1+\epsilon) \Pr[Q(x)=y]$$

- Say $Q =$  affords a weak ϵ -quantum advantage

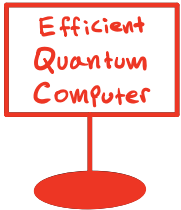
iff $\forall C =$ , C cannot simulate Q to

within weak multiplicative error ϵ .

Theorem (AA 2010, BTS 2010):

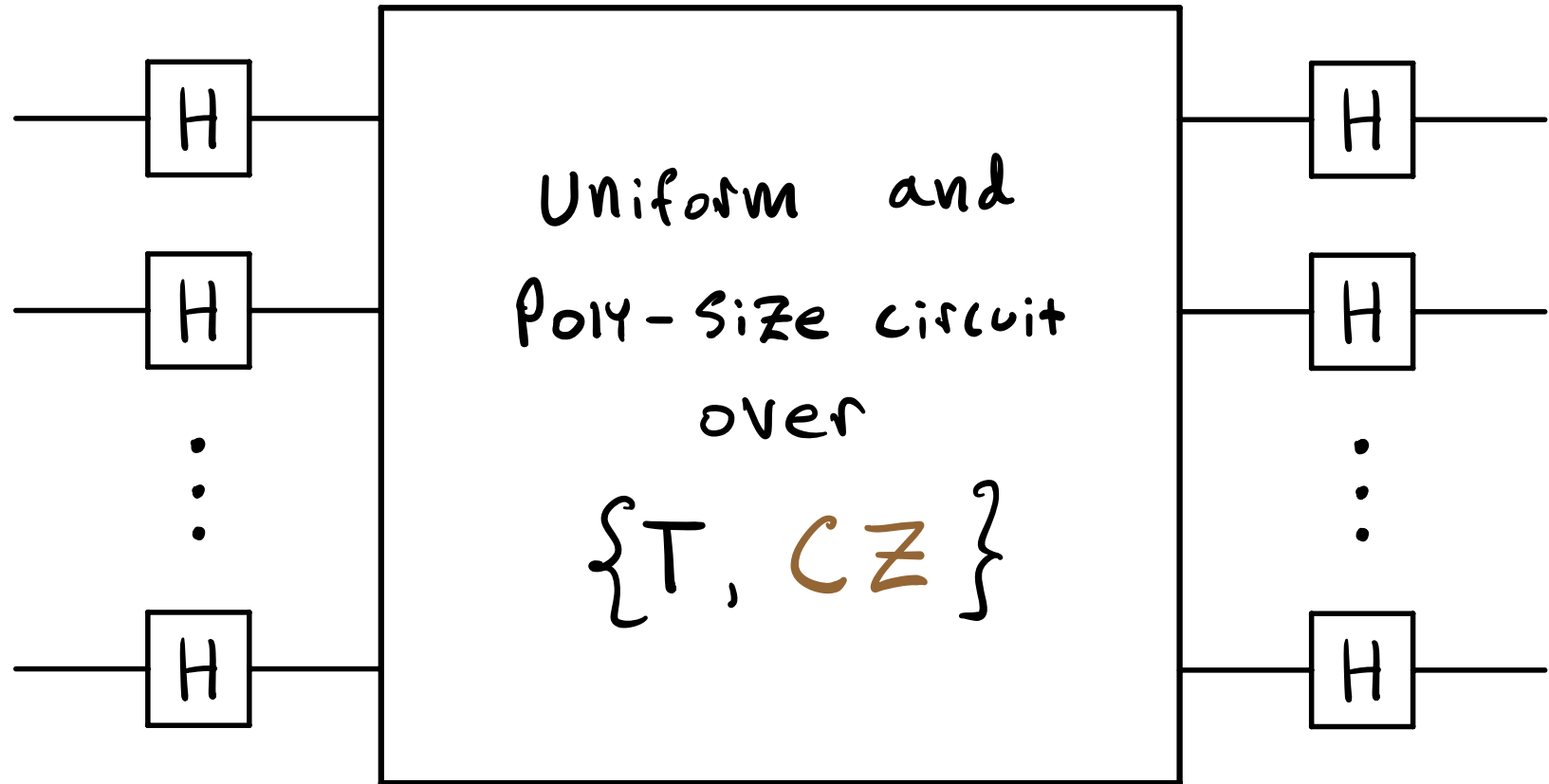
If PH is infinite, then  over
any universal gate set S afford a
weak $(\sqrt{2} - 1)$ -quantum advantage.

Key Idea: Post-Selection!

Q: If PH is infinite, Can  over a
NON-universal gate set afford a weak
 ϵ -quantum advantage, $\epsilon > 0$?

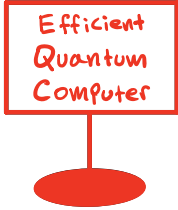
A: YES!


Instantaneous Quantum Polynomial



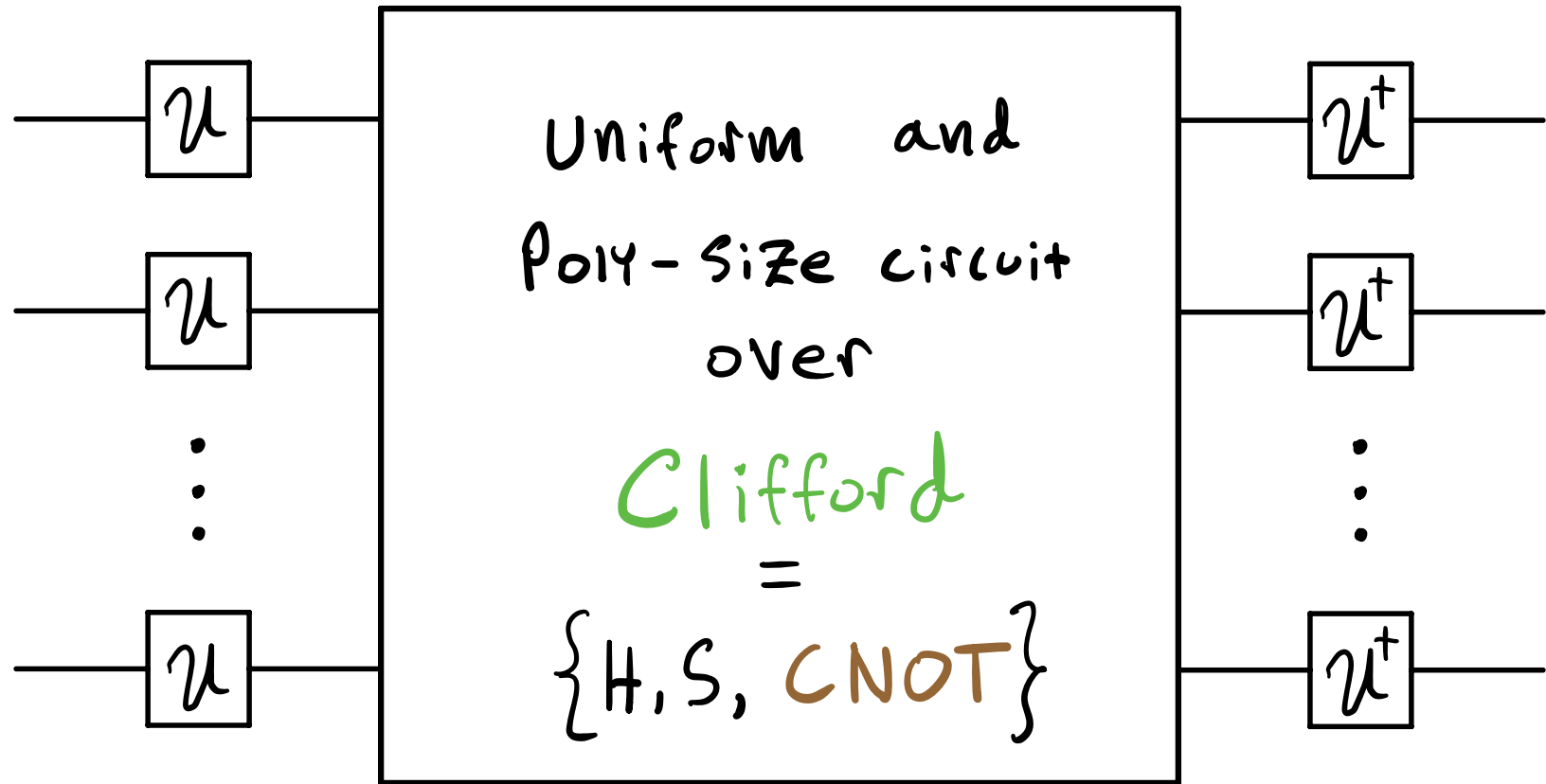
$$S_{IQP} = \{HTH, H \otimes H CZ H \otimes H\}$$

Theorem (BJS, 2010):

If PH is infinite, then  over S_{IQP} afford a weak $(\sqrt{2} - 1)$ -quantum advantage.

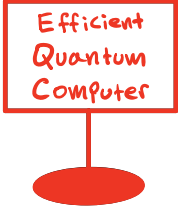
Key Idea: Post-Selection!

Conjugated Clifford Circuits



$$S_{ccc}(U) = \{U H U^\dagger, U S U^\dagger, U \otimes U \text{ CNOT } U^\dagger \otimes U^\dagger\}$$

Theorem (BFK, 2016):

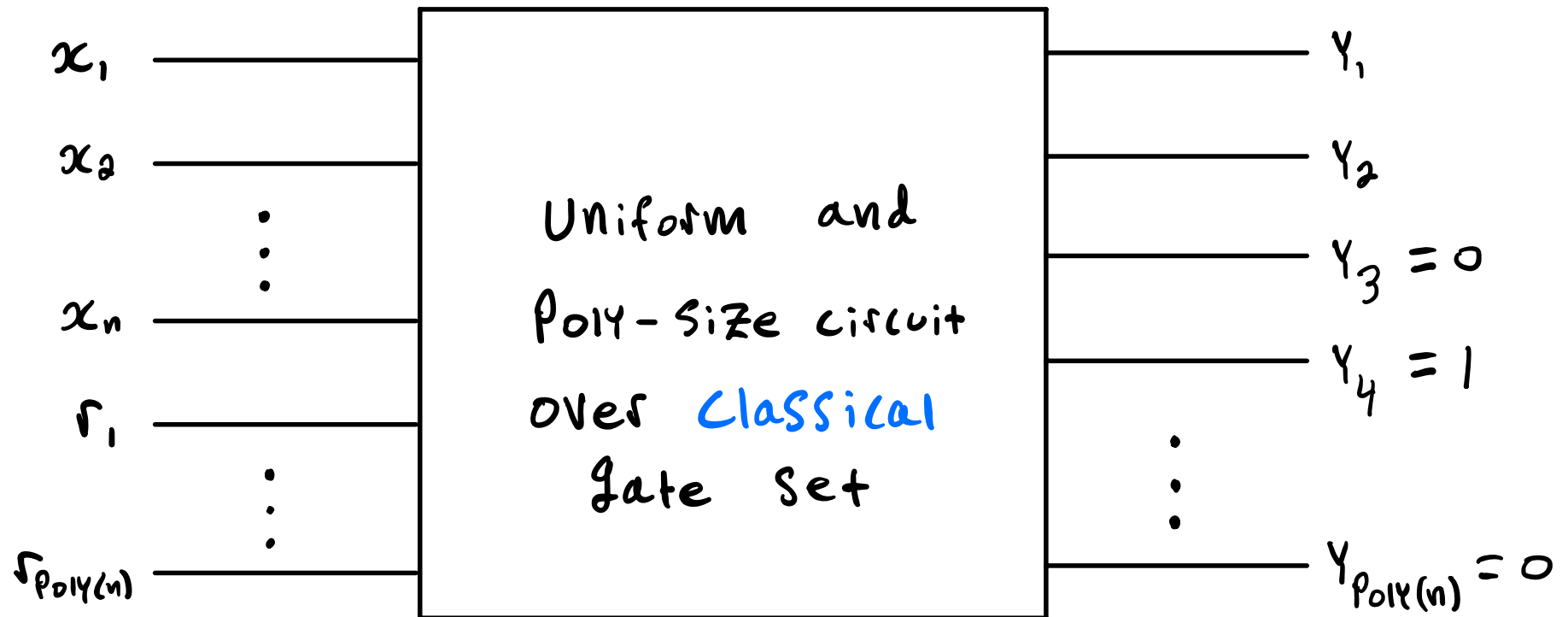
If PH is infinite, then  over $S_{ccc}(U)$ afford a weak $(\sqrt{2}-1)$ -quantum advantage for almost all $U \in SU(2)$.

Key Idea: Post-Selection!

Part V

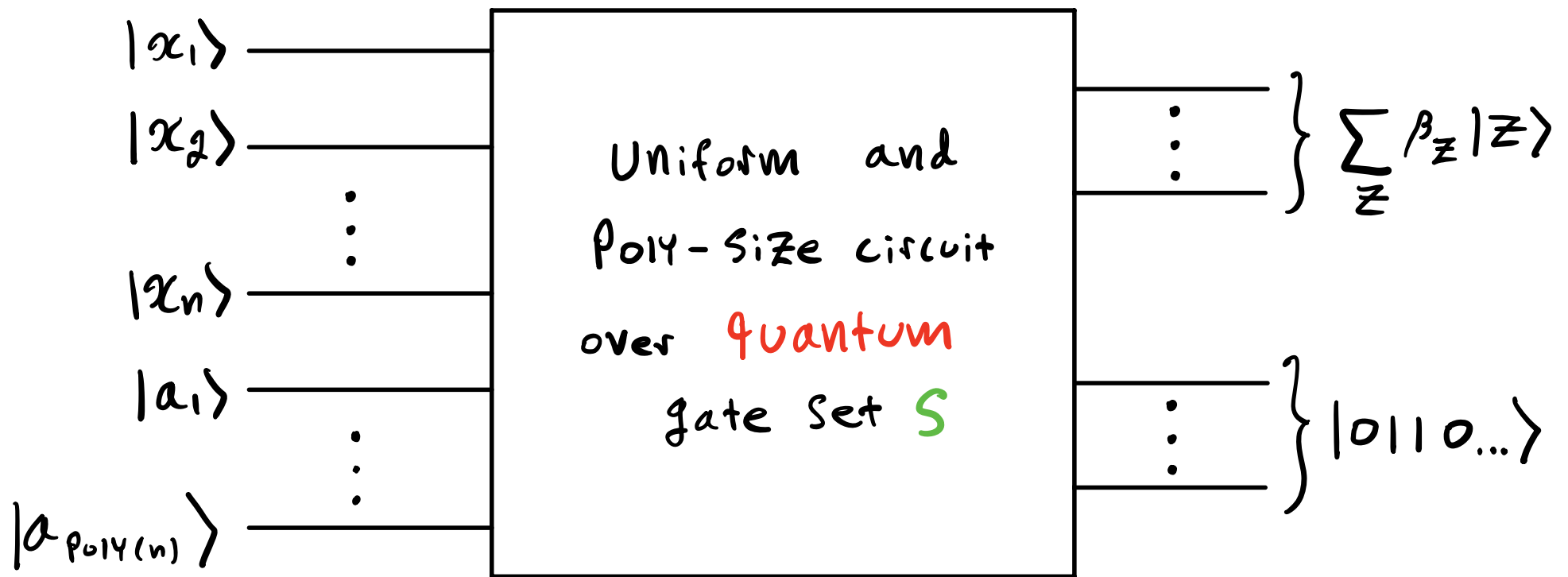
Post-Selection

Efficient Post-selected Classical Computer:



PostBPP

Efficient Post-Selected Quantum Computer:



$\text{PostBQP}(S)$, PostBQP



BPP



PostBPP



BQP



PostBQP

(Bouland, 2018)

Facts:

$$\bullet P^{\text{PostBPP}} \subseteq \Sigma_3 P$$

(HHT, 1997)

$$\bullet \text{PostBQP} = \text{PP}$$

(Aaronson, 2005)

$$\bullet \text{PH} \subseteq P^{\text{PP}}$$

(Toda, 1991)

Corollary:

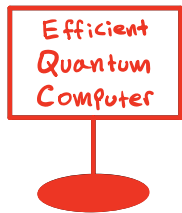
$$\text{PostBPP} = \text{PostBQP} \rightarrow \text{PH} \subseteq \Sigma_3 P$$

Theorem (AA 2010, BTS 2010):

If

- $PH \not\subseteq \Sigma_3P$
- $\text{PostBQP}(S) = \text{PostBQP},$

then

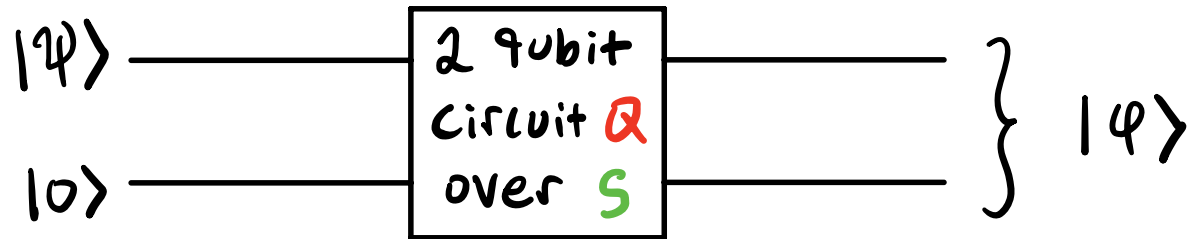


over S afford a weak $(\sqrt{2}-1)$ -

quantum advantage.

Part VI

Gadgets and $SL(2; \mathbb{C})$

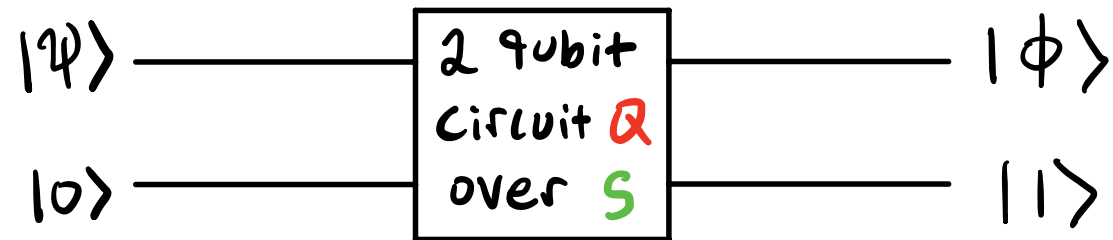


of course

$$|\psi\rangle \otimes |0\rangle \xrightarrow{Q} |\psi\rangle$$

Unitary
(always)



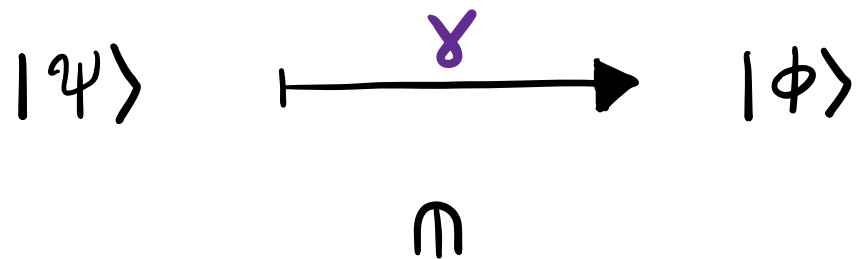
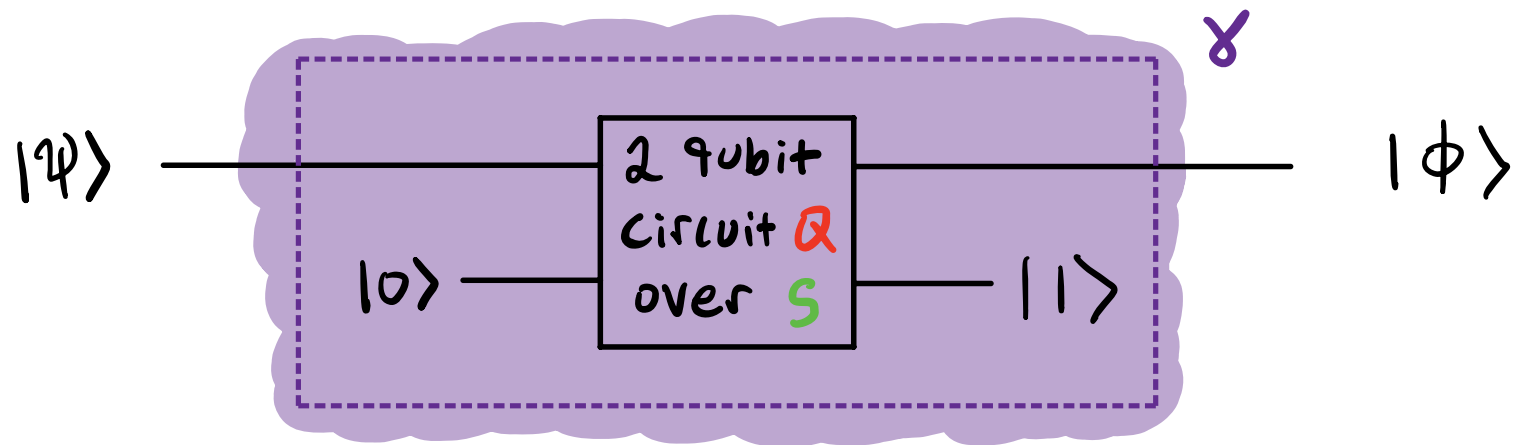


Post-Select!

However

$$|\psi\rangle \otimes |0\rangle \xrightarrow{Q} |\phi\rangle \otimes |1\rangle$$

non-Unitary
(generally)

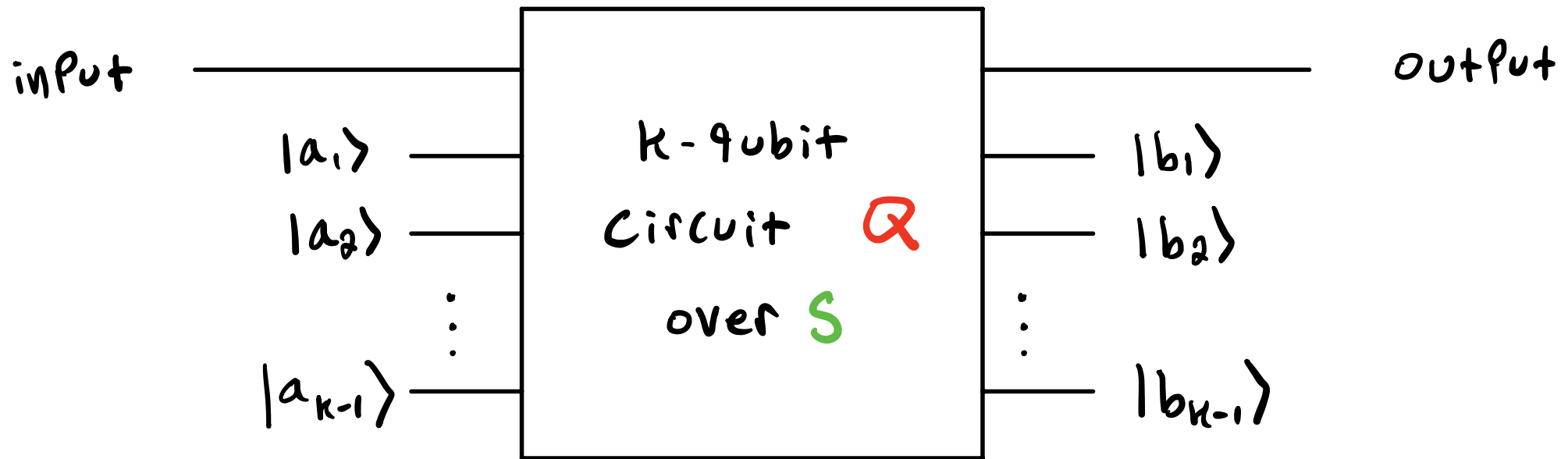


$$SL(2; \mathbb{C}) \setminus SU(2)$$

(generally)

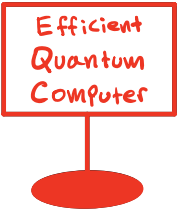
Def:

A k -qubit Post-selection gadget γ over S is



where $a_i, b_j \in \{0, 1\}$.

Facts:

- $\gamma \in SL(2; \mathbb{C})$. Often, $\gamma \notin SU(2)$.
- Circuits over $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ over S are Post-Selected  over S .

Theorem (FKG, 2024):

$\exists \Gamma$ over S s.t. $\langle \Gamma \rangle$ dense in $SL(2; \mathbb{C})$



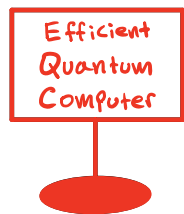
$$\text{Post+BQP}(S) = \text{Post+BQP}.$$

Theorem (AA 2010, BTS 2010):

If

- $PH \not\subseteq \Sigma_3P$
- $\text{PostBQP}(S) = \text{PostBQP},$

then



over S afford a weak $(\sqrt{2}-1)$ -

quantum advantage.

Theorem (FKG, 2024):

If

- $PH \not\subseteq \Sigma_3 P$

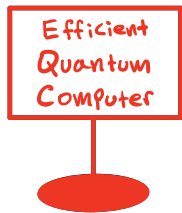
$\exists \Gamma$ over S s.t.

$\langle \Gamma \rangle$ dense in $SL(2; \mathbb{C})$

- ~~$PostBQP(S) = PostBQP$~~



then

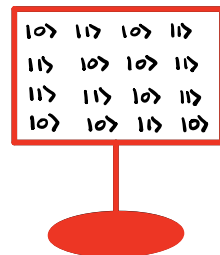


over S afford a weak $(\sqrt{2}-1)$ -

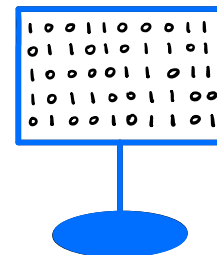
quantum advantage.

Part VII

A Criterion for Post-Selected Quantum Advantage



>



Q: When is $\langle \Gamma \rangle$ dense in $SL(2; \mathbb{C})$?

Theorem (Sullivan, 1985):

If $\langle \Gamma \rangle$ is non-elementary,
non-discrete, and strictly loxodromic,
then $\langle \Gamma \rangle$ is dense in $SL(2; \mathbb{C})$.

Theorem (FKG, 2024):

If

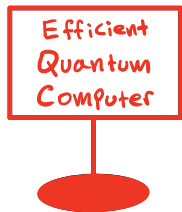
- $PH \not\subseteq \Sigma_3P$

$\exists \Gamma$ over S s.t.

$\langle \Gamma \rangle$ dense in $SL(2; \mathbb{C})$

- ~~$PostBQP(S) = PostBQP$~~ 

then



over S afford a weak $(\sqrt{2}-1)$ -

quantum advantage.

Theorem (FKG, 2024):

$\exists \Gamma$ over S s.t. $\langle \Gamma \rangle$
is non-elem, non-discrete
and strictly isodromic

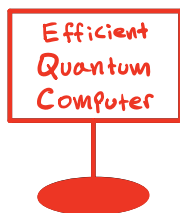
If

- $PH \not\subseteq \Sigma_3 P$

- ~~$PostBQP(S) = PostBQP$~~

~~$\exists \Gamma$ over S s.t.
 $\langle \Gamma \rangle$ dense in $SL(2; \mathbb{C})$~~

then



over S afford a weak $(\sqrt{2}-1)$ -

quantum advantage.

$\langle \Gamma \rangle$ is...

... non-elementary if " Γ can do more than $SU(2)$ "

... non-discrete if $\langle \Gamma \rangle$ is "topologically interesting"

... strictly loxodromic if $\exists \gamma \in \Gamma$ s.t. $\text{tr}(\gamma) \in \mathbb{C} \setminus \mathbb{R}$.

Let

$$\beta(g) = \text{tr}^2(g) - 4$$

$$\gamma(g, h) = \text{tr}(ghg^{-1}h^{-1}) - 2$$

Algorithm 1 IsElementary

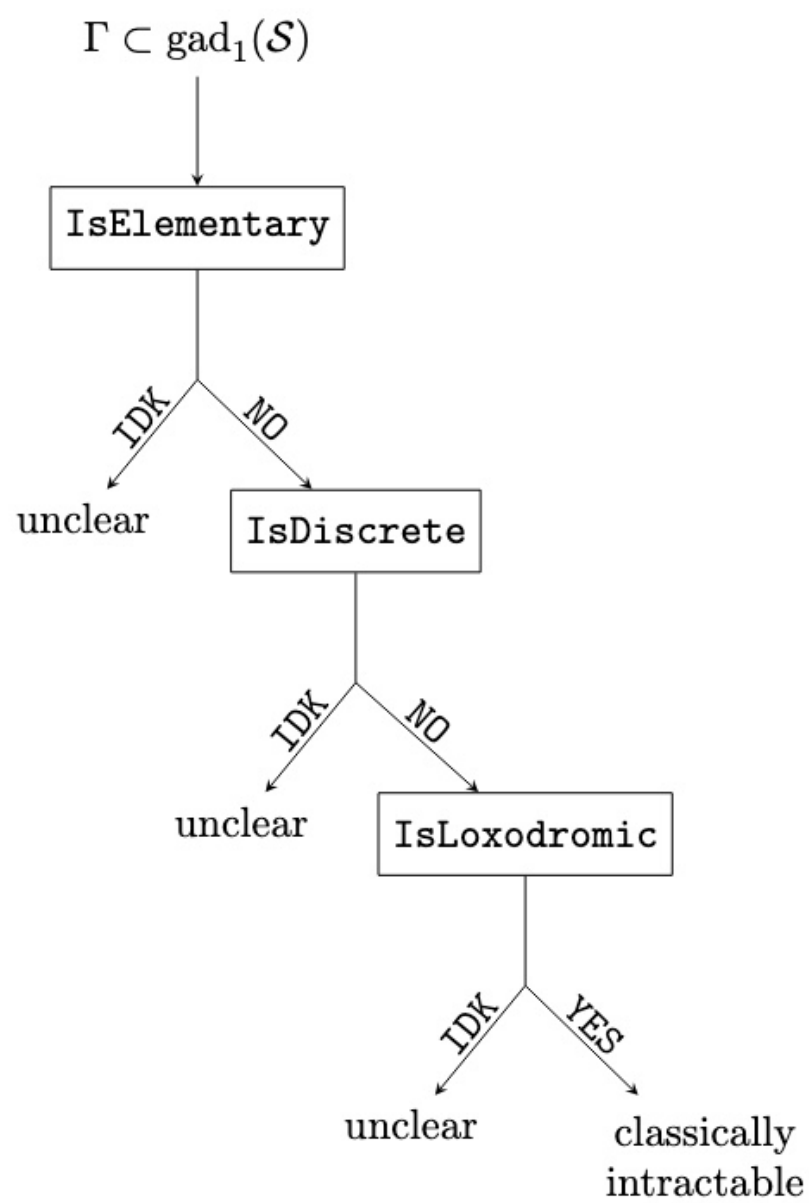
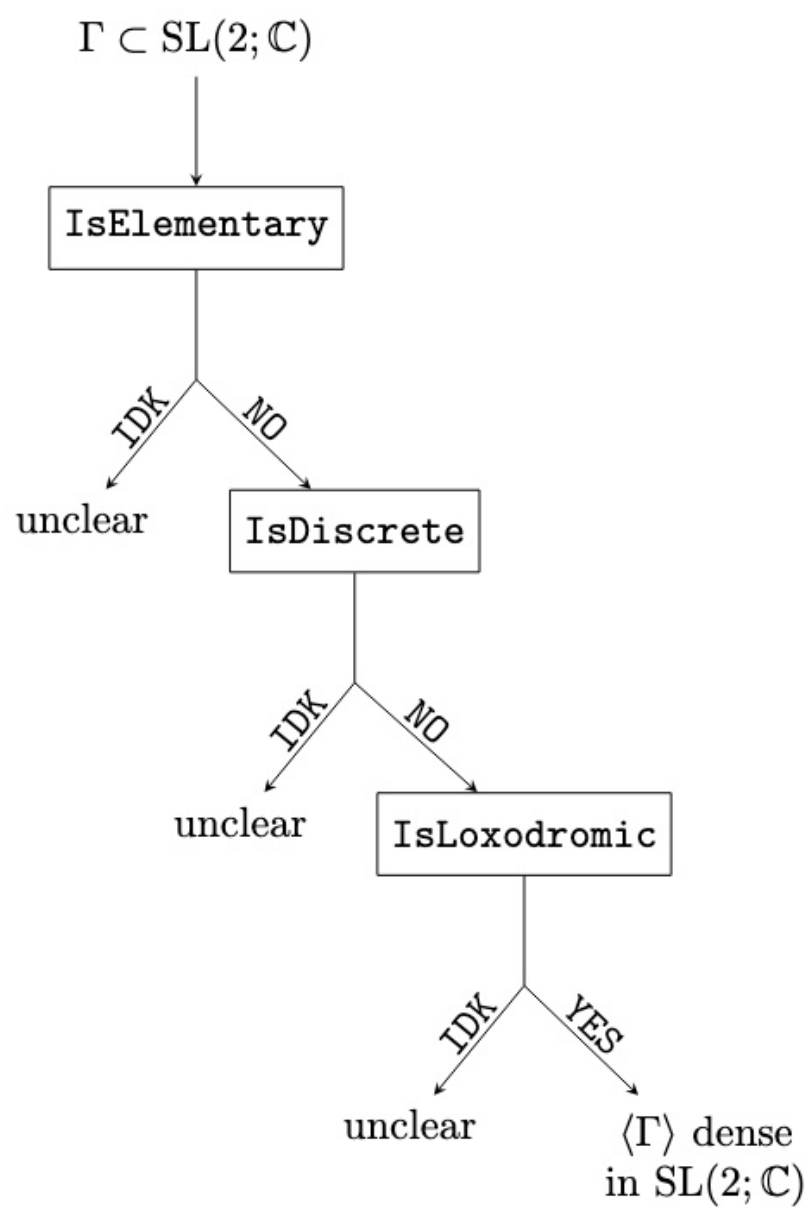
```
1: Input: Finite set  $\Gamma \subset \text{SL}(2; \mathbb{C})$  such that  $\langle \Gamma \rangle \leq \text{SL}(2; \mathbb{C})$ 
2: Output: NO if  $\langle \Gamma \rangle$  is non-elementary, IDK (“I don’t know”) otherwise
3: for  $g, h \in \Gamma$  do
4:   if  $\beta(g) \notin [-4, 0]$  or  $\beta(h) \notin [-4, 0]$  or  $\gamma(g, h) \notin [-\beta(g)\beta(h)/4, 0]$  then
5:     if  $\gamma(g, h) \neq 0$  then
6:       if  $\beta(g) \neq \gamma(g, h)$  or  $\beta(h) \neq -4$  then
7:         if  $\beta(g) \neq -4$  or  $\beta(h) \neq \gamma(g, h)$  then
8:           if  $\beta(g) \neq -4$  or  $\beta(h) \neq -4$  then
9:             return NO
10: return IDK
```

Algorithm 2 IsDiscrete

```
1: Input: Finite set  $\Gamma \subset \text{SL}(2; \mathbb{C})$  such that  $\langle \Gamma \rangle \leq \text{SL}(2; \mathbb{C})$ 
2: Output: NO if  $\langle \Gamma \rangle$  is non-discrete, IDK otherwise
3: for  $g, h \in \Gamma$  do
4:   if IsElementary( $\{g, h\}$ ) = NO and  $|\text{tr}^2(g) - 4| + |\text{tr}(ghg^{-1}h^{-1}) - 2| < 1$  then
5:     return NO
6:   if  $\text{tr}(ghg^{-1}h^{-1}) \neq 1$  and  $|\text{tr}^2(g) - 2| + |\text{tr}(ghg^{-1}h^{-1}) - 1| < 1$  then
7:     return NO
8:   if  $\text{tr}(ghg^{-1}h^{-1}) = 1$  and  $\text{tr}^2(g) \neq 2$  and  $|\text{tr}^2(g) - 2| \leq 1/2$  then
9:     return NO
10:  if  $\text{tr}^2(g) \neq 1$  and  $|\text{tr}^2(g) - 1| + |\text{tr}(ghg^{-1}h^{-1})| < 1$  then
11:    return NO
12:  if  $\text{tr}^2(g) = 1$  and  $|\text{tr}(ghg^{-1}h^{-1})| \leq 1/2$  and  $\text{tr}(ghg^{-1}h^{-1}) \neq 0$  then
13:    return NO
14:  if  $\text{tr}^2(g) = 1$  and  $|\text{tr}(ghg^{-1}h^{-1}) - 1| \leq 1/2$  and  $\text{tr}(ghg^{-1}h^{-1}) \neq 1$  then
15:    return NO
16:  if  $\text{tr}(ghg^{-1}h^{-1}) \neq 1$  and  $|\text{tr}^2(g) - \text{tr}(ghg^{-1}h^{-1})| + |\text{tr}(ghg^{-1}h^{-1}) - 1| < 1$  then
17:    return NO
18:  if  $\text{tr}(ghg^{-1}h^{-1}) = 1$  and  $\text{tr}^2(g) \neq 1$  and  $|\text{tr}^2(g) - 1| \leq 1/2$  then
19:    return NO
20: return IDK
```

Algorithm 3 IsLoxodromic

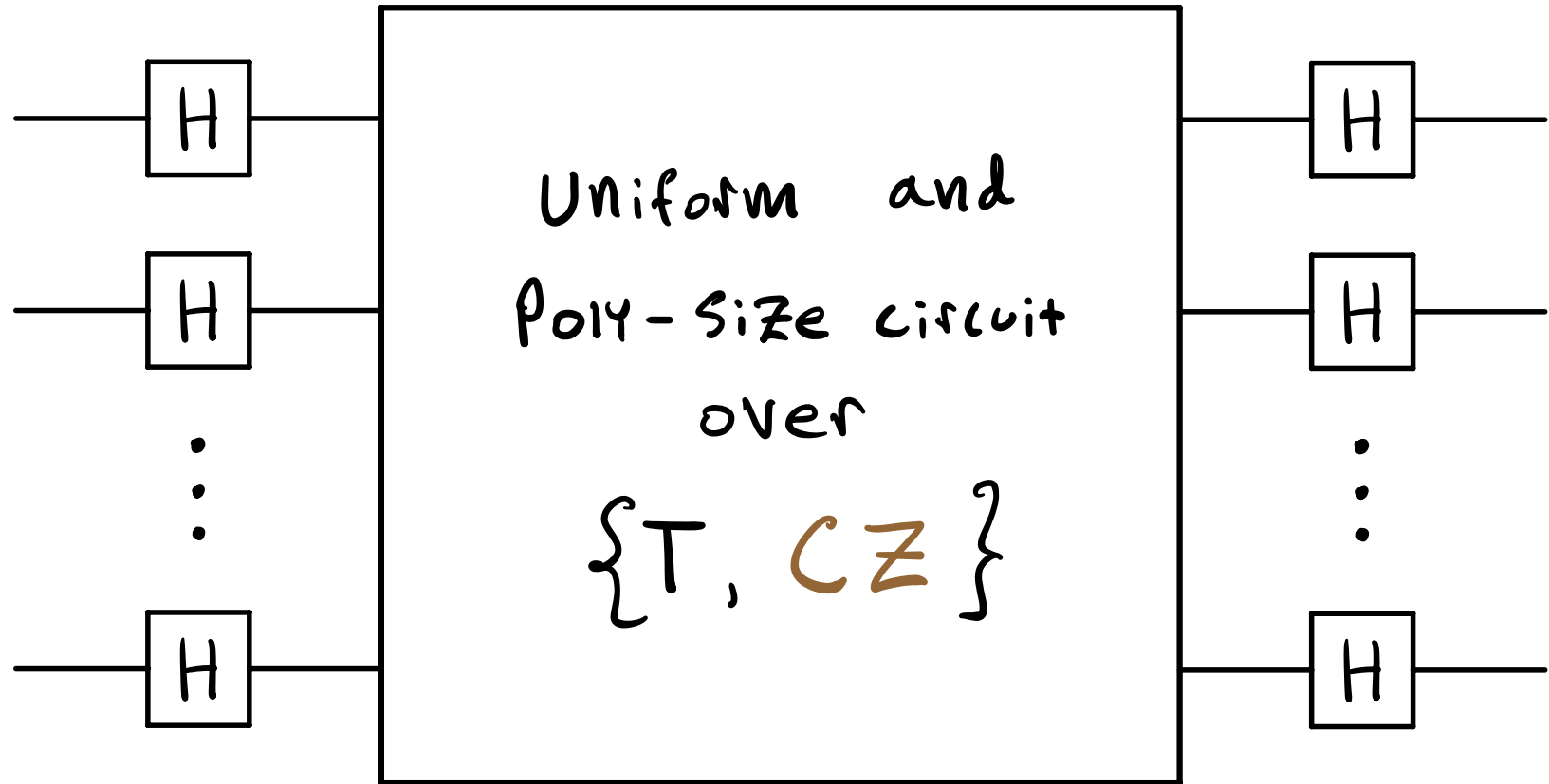
1: **Input:** Finite set $\Gamma \subset \mathrm{SL}(2; \mathbb{C})$ such that $\langle \Gamma \rangle \leq \mathrm{SL}(2; \mathbb{C})$
2: **Output:** YES if $\langle \Gamma \rangle$ is strictly loxodromic, IDK otherwise
3: **for** $g \in \Gamma$ **do**
4: **if** $\mathrm{tr}(g) \in \mathbb{C} \setminus \mathbb{R}$ **then**
5: return YES
6: return IDK



Part VII

Applications

Instantaneous Quantum Polynomial



$$S_{IQP} = \{HTH, H \otimes H CZ H \otimes H\}$$

Theorem (FKG, 2024):

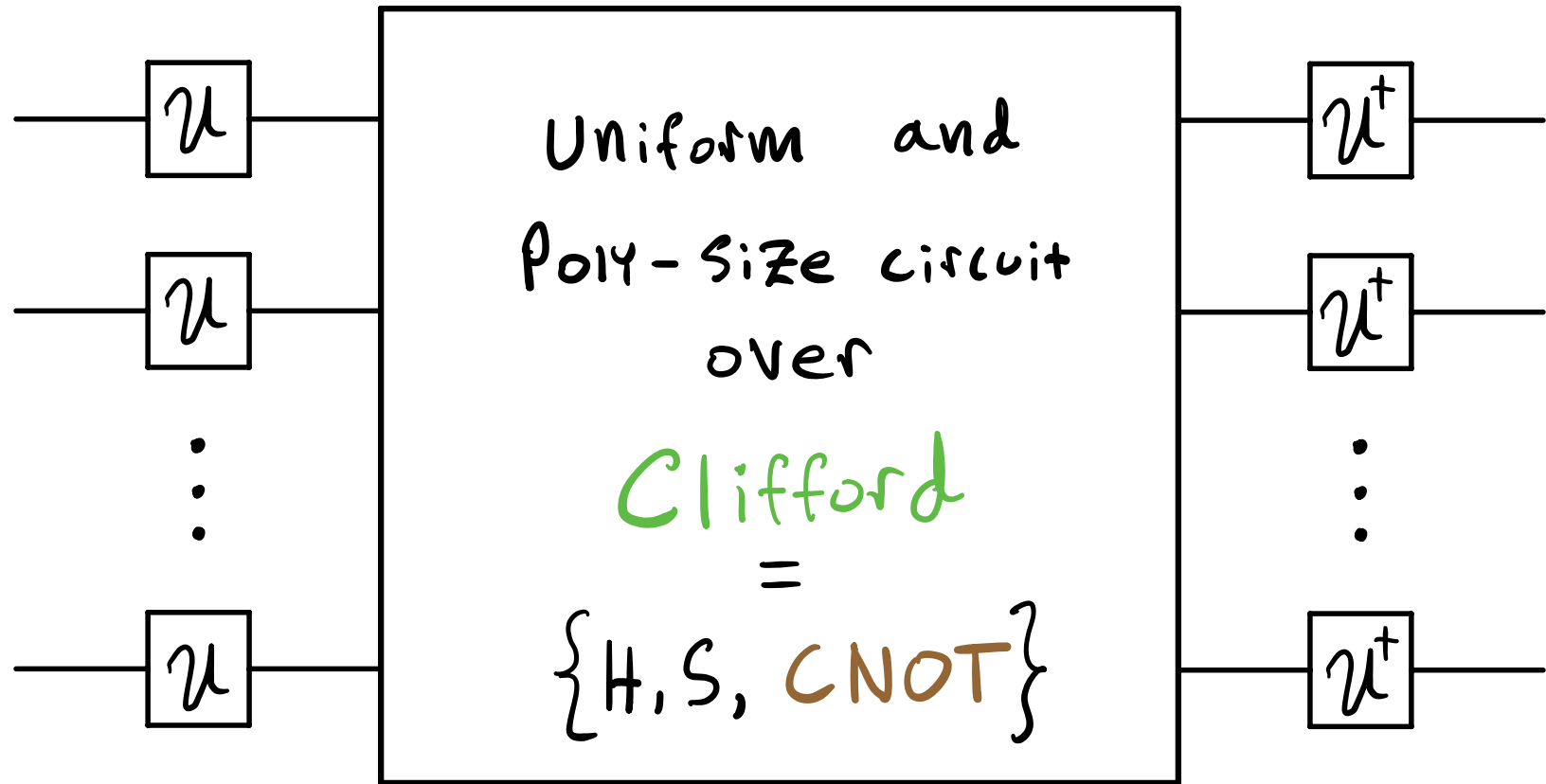
The following gadgets over S_{IQP} generate a dense subgroup of $SL(2; \mathbb{C})$:

$$\gamma_1 = \text{---} \boxed{H} \text{---} \boxed{T} \text{---} \boxed{H} \text{---}$$

$$\gamma_2 = \begin{array}{c} \text{---} \boxed{H} \text{---} \boxed{T} \text{---} \bullet \text{---} \boxed{H} \text{---} |0\rangle \\ |0\rangle \text{---} \boxed{H} \text{---} \boxed{T^4} \text{---} \bullet \text{---} \boxed{H} \text{---} \end{array}$$

$$\gamma_3 = \begin{array}{c} \text{---} \boxed{H} \text{---} \bullet \text{---} \boxed{H} \text{---} \\ |0\rangle \text{---} \boxed{H} \text{---} \boxed{T} \text{---} \bullet \text{---} \boxed{H} \text{---} |0\rangle \end{array}$$

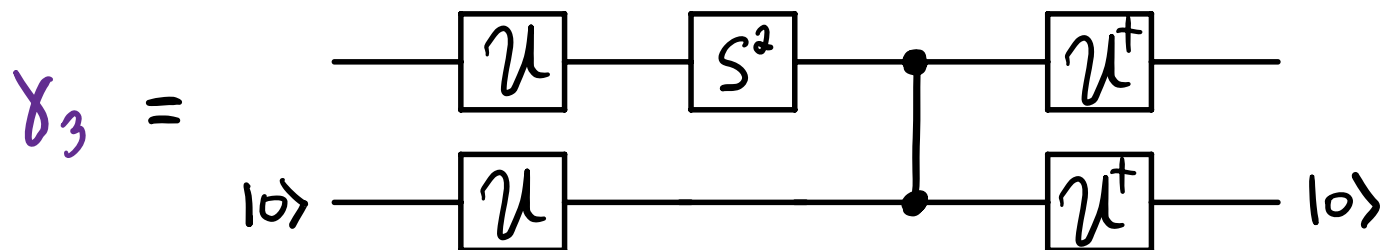
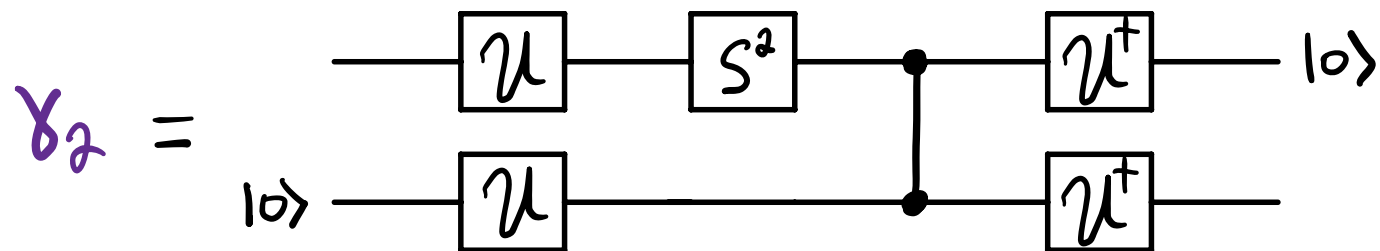
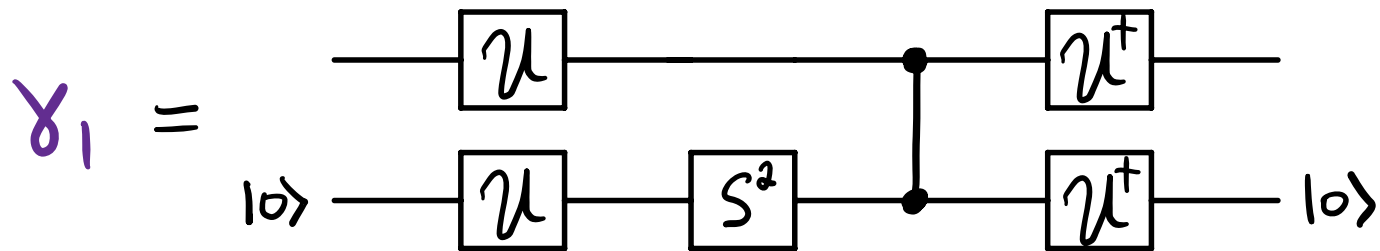
Conjugated Clifford Circuits

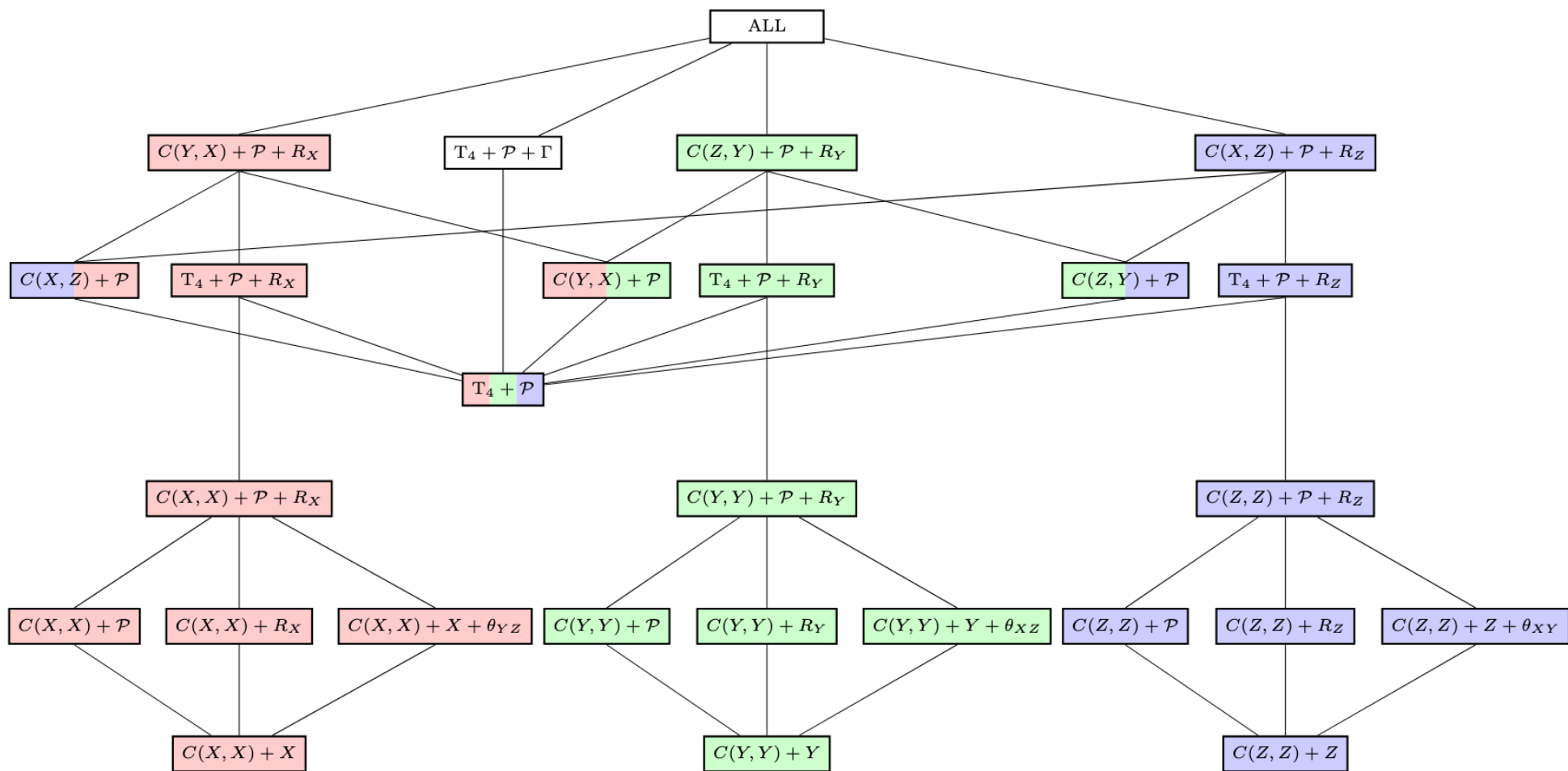


$$S_{ccc}(U) = \{U H U^\dagger, U S U^\dagger, U \otimes U \text{ CNOT } U^\dagger \otimes U^\dagger\}$$

Theorem (FKG, 2024):

The following gadgets over $S_{\text{cc}}(U)$ generate a dense subgroup of $SL(2; \mathbb{C})$ for almost all $U \in SU(2)$:



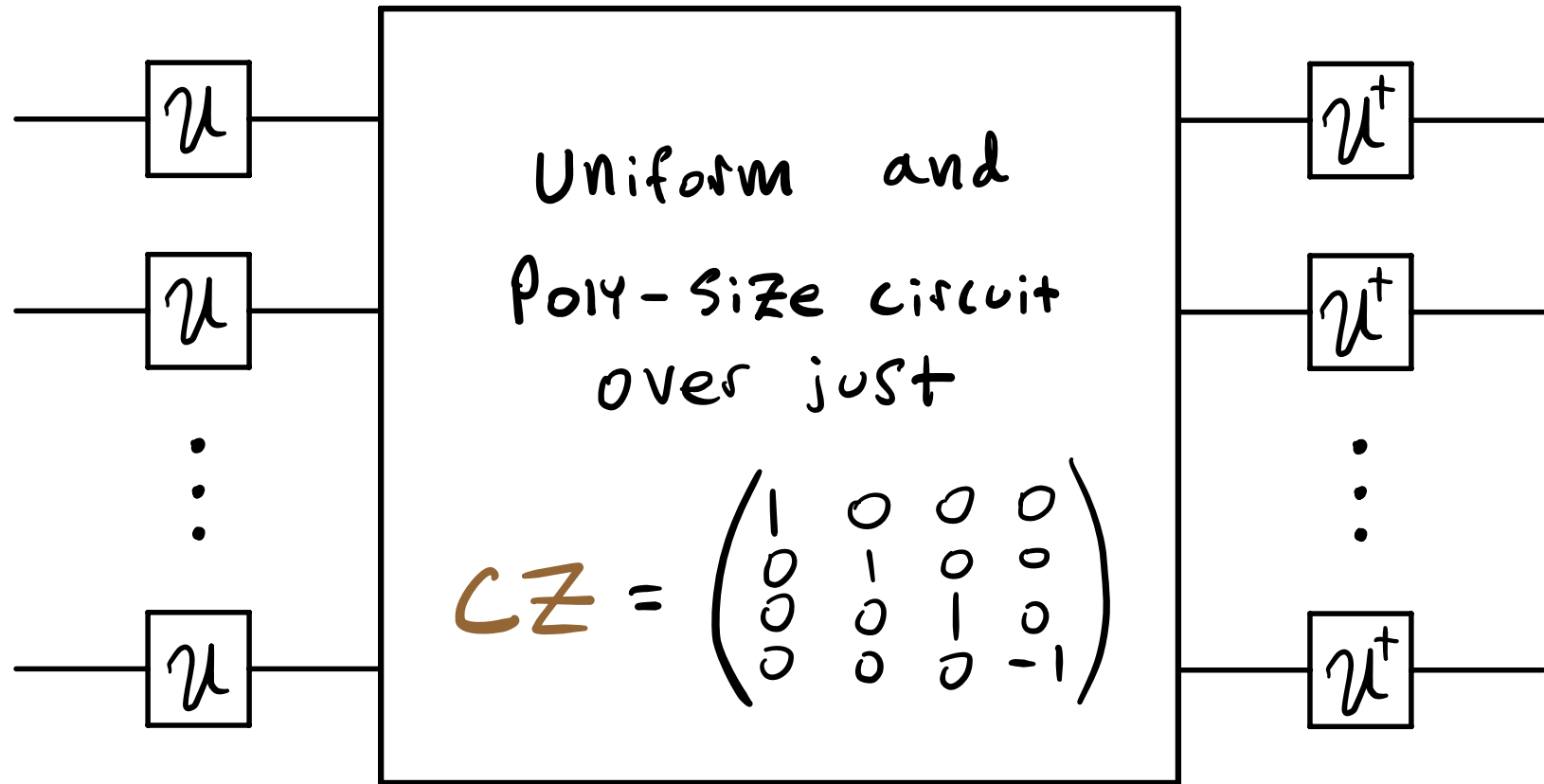


(GS, 2022)

Theorem (FKG, 2024):

CCCs over any Clifford fragment afford a weak $(\sqrt{2}-1)$ -**quantum** advantage.

Conjugated CZ Circuits



$$S_{CZ}(U) = \{U \otimes U \, CZ \, U^\dagger \otimes U^\dagger\}$$

Theorem (FKG, 2024):

If PH is infinite, then  over $S_{\mathbb{C}\mathbb{Z}}(\mathcal{U})$
afford a weak $(\sqrt{2}-1)$ -quantum advantage



$$U \neq e^{i\alpha} R_Z(\phi) C R_Z(\lambda)$$

where

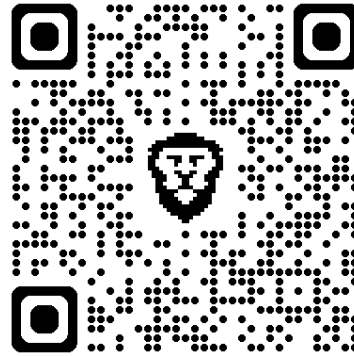
$$\alpha, \phi, \lambda \in [0, 2\pi), C \in \langle H, S \rangle.$$

Some Open Questions

- Is strict isodromy necessary?
- Existence of inverse gadgets?
- Hardness classification of CCCs over Clifford subgroups (in progress).
- Criterion for additive error?

Thank You!

Paper ~➡



Slides ~➡

