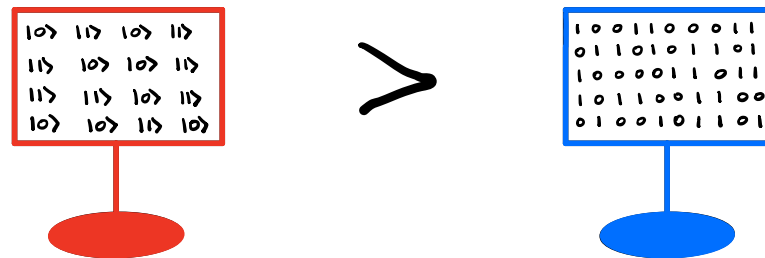
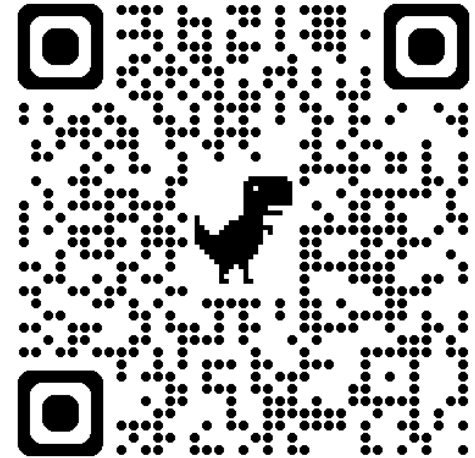


A Criterion for Quantum Advantage

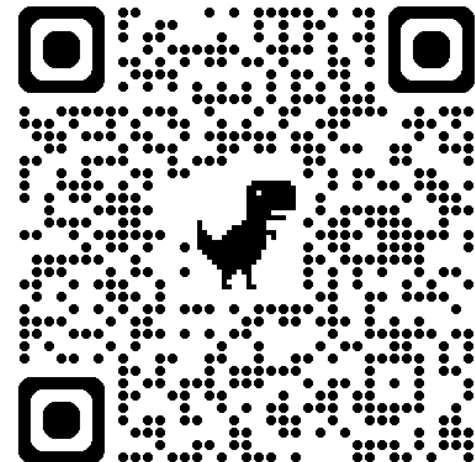


Matthew Fox

Paper



Slides





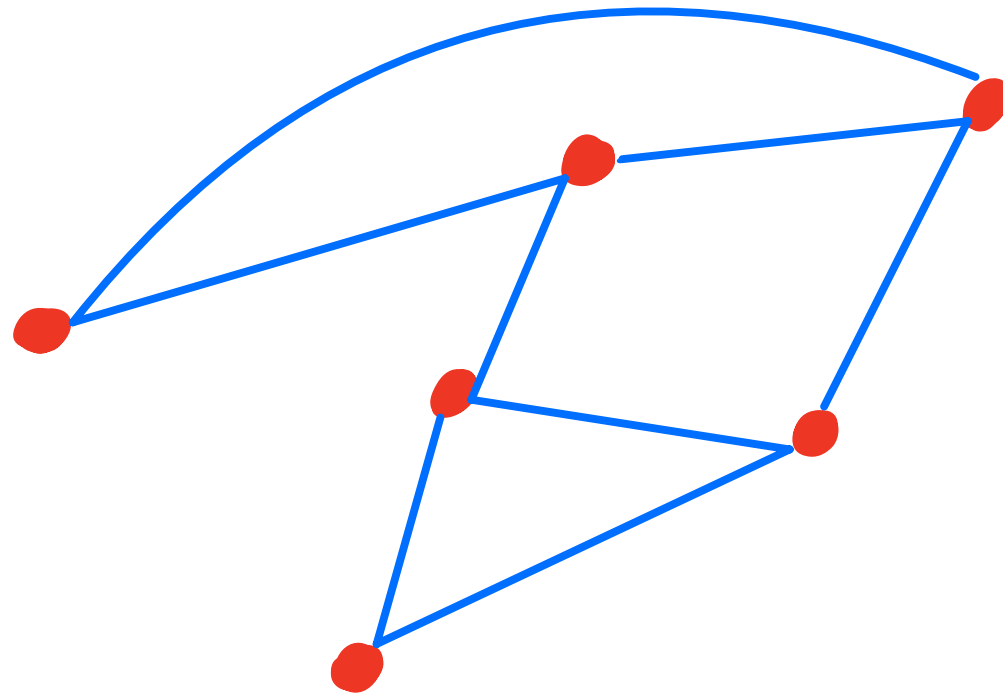
Chaitanya
Karamchedu
(UMD)



Daniel
Gottesman
(UMD)

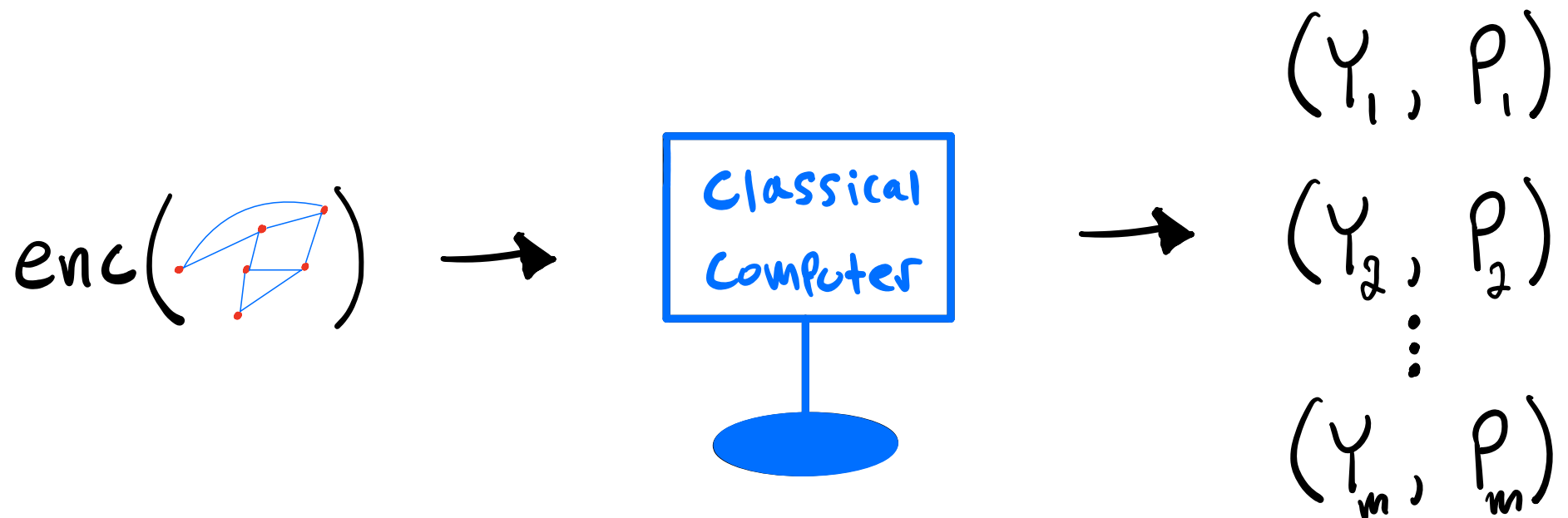
Part I

Classical and Quantum Computers



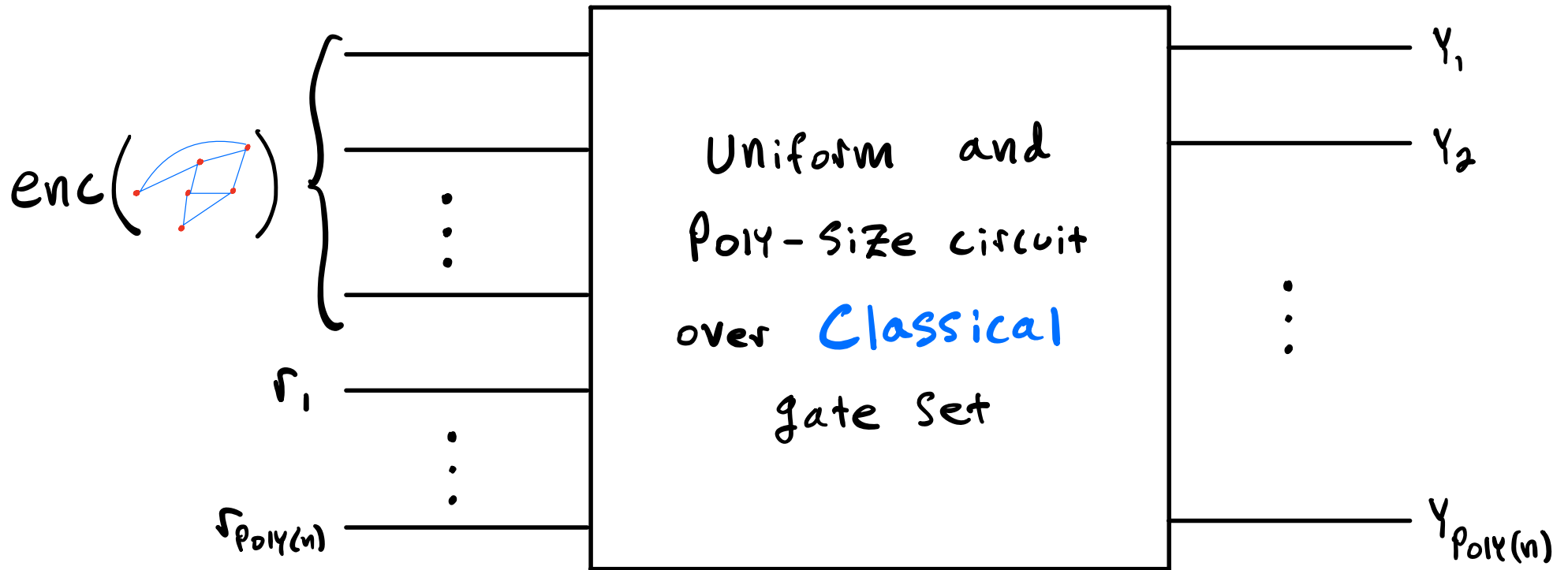
$$\text{enc}\left(\begin{array}{c} \text{Diagram} \end{array}\right) = 1001011011$$

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



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

Efficient **Classical** Computer:



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

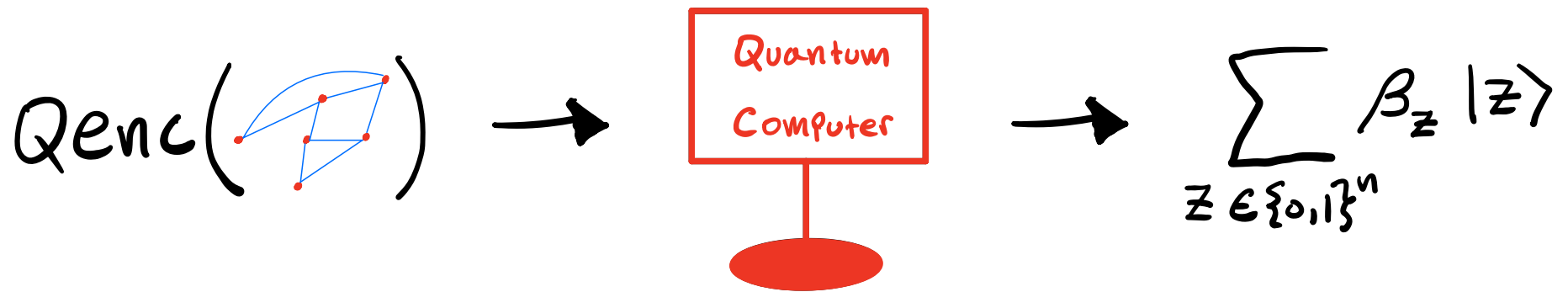
$$\text{enc}\left(\begin{array}{c} \text{graph} \end{array}\right) = 10010110111$$


 encode in
 quantum system

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

$$= |10010110111\rangle$$

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



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

$$= |\beta_Y|^2$$

Probability!

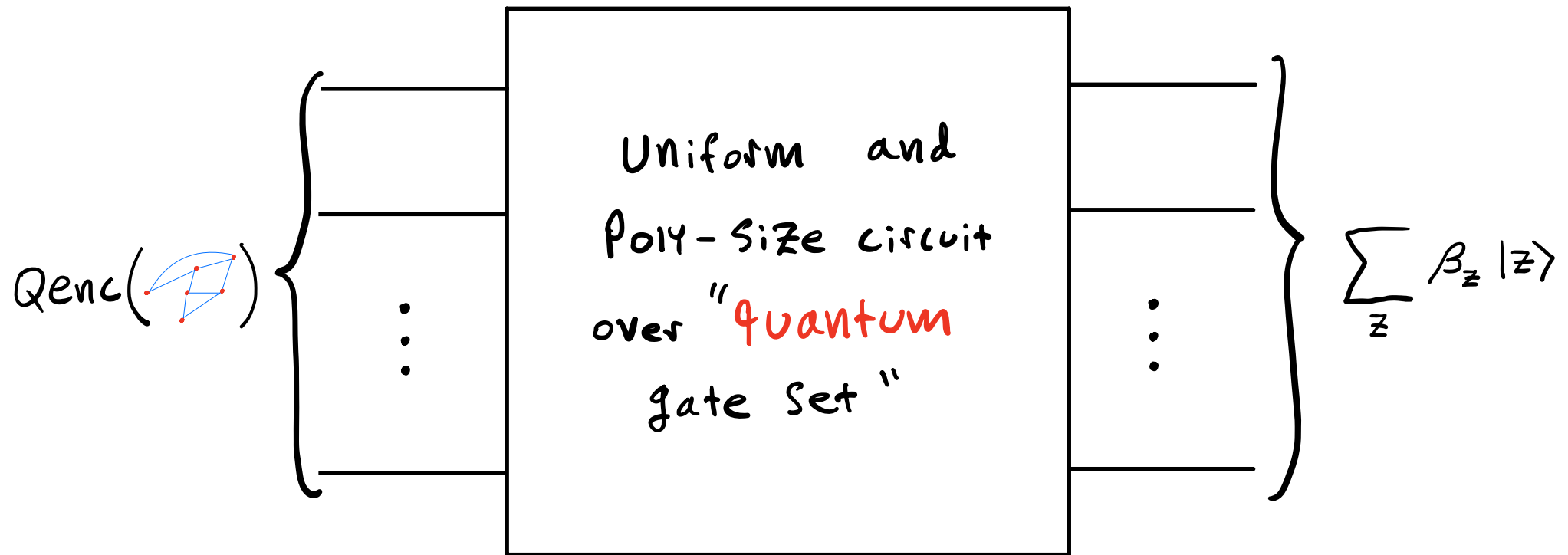


- $$\text{Quantum Computer} : (\mathbb{C}^{2^n}, \langle \cdot | \cdot \rangle) \rightarrow (\mathbb{C}^{2^n}, \langle \cdot | \cdot \rangle)$$

Unitary!

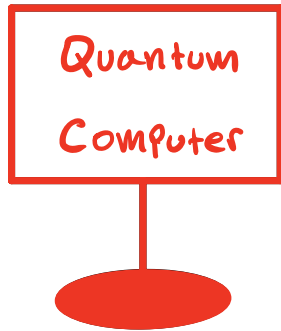


Efficient **Quantum** Computer:



Part II

Quantum Gate Sets and Universality



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



Quantum Computers
are Unitary Operators!

Def:

• $M \in \mathbb{C}^{d \times d}$ unitary iff

$$M^\dagger := (M^*)^T = M^{-1}.$$

• $U(d) := \{M \in \mathbb{C}^{d \times d} \mid M \text{ unitary}\}$

• $SU(d) := U(d) \cap SL(d; \mathbb{C})$

Def: An **entangling gate** $\mathcal{E}$ is an operator in $SU(4)$ that is neither

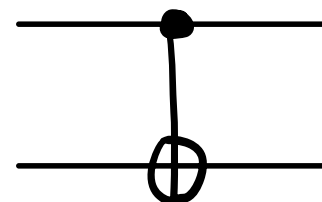
- in $SU(2) \otimes SU(2)$,
- a representative of $\pi \in S_2$.

Formally,

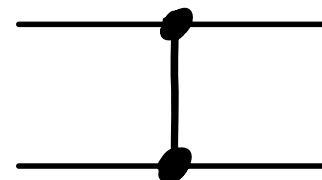
$$\mathcal{E} \notin N_{SU(4)}(SU(2) \otimes SU(2)).$$

Ex:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

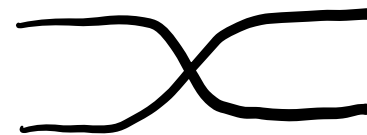


$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$



Non-Ex:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



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

Ex:

$$\text{Clifford} = \{H, S, \text{CNOT}\},$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Ex:

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

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}.$$

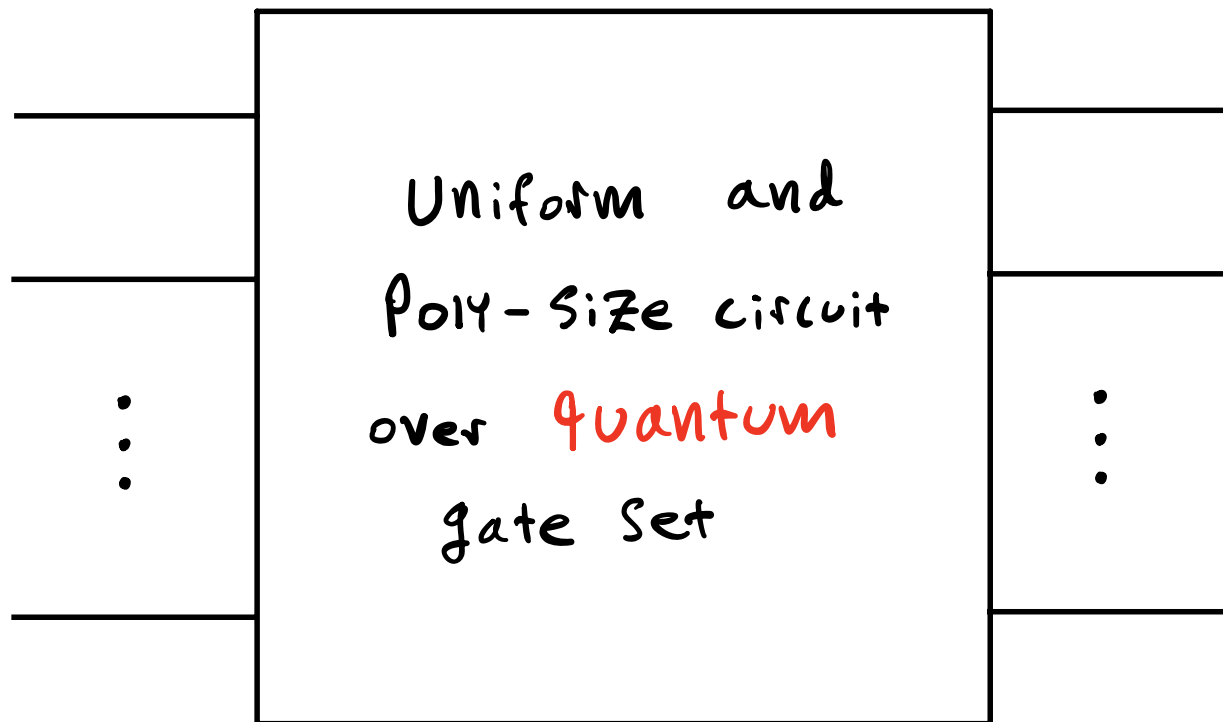
- Unlike Clifford, Clifford + T is universal for quantum computation.

Def: A quantum gate set S is
universal iff

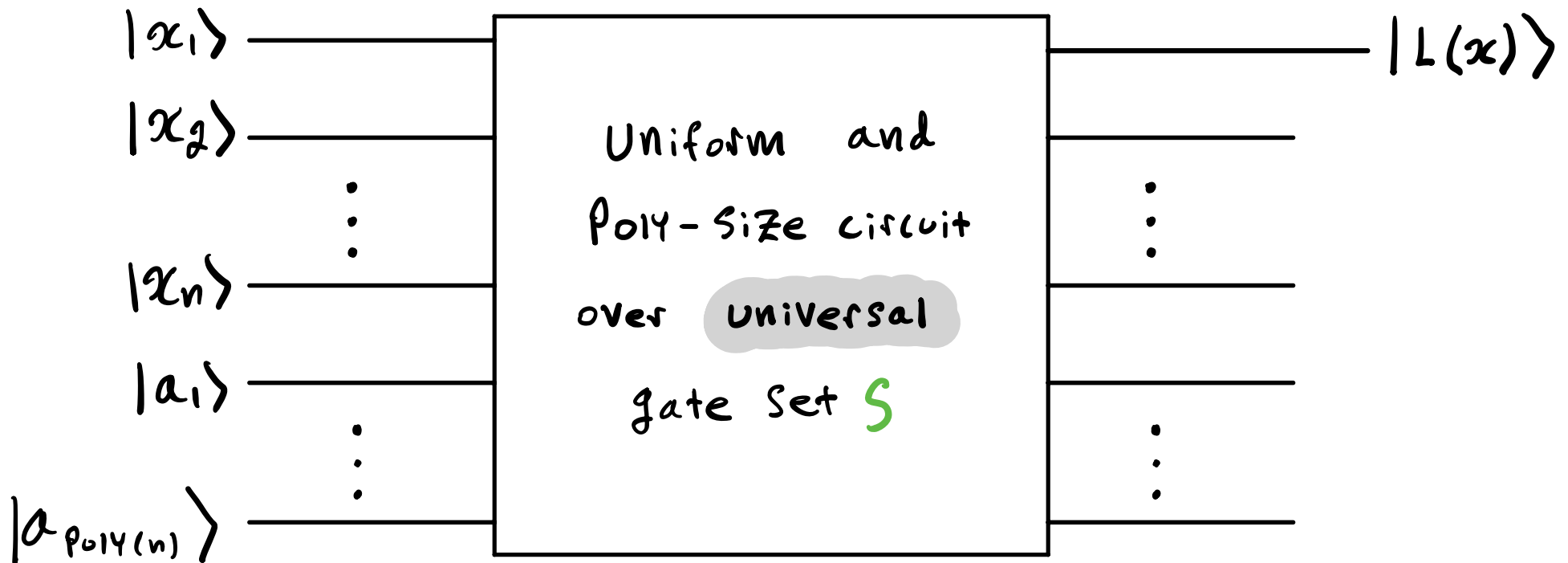
$$\langle S \cap \text{SU}(2) \rangle = \text{group generated by } S \cap \text{SU}(2)$$

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

Efficient Quantum Computer:

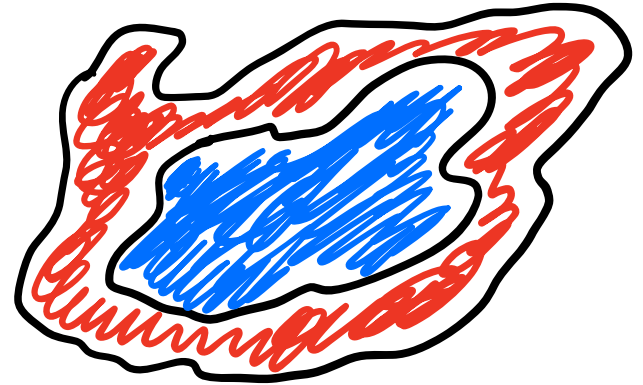


Def: $L \in \text{BQP}$ iff $\exists$ efficient quantum computer Q over a universal gate set S such that $\forall x \in \{0,1\}^*$,
 $\Pr [Q(x) = L(x)] \geq 2/3$.



Fact: $BPP \subseteq BQP$

Conj: $BPP \subsetneq BQP$



Part III

Quantum Advantage

"Quantum Advantage"



$\exists$  Such that $\forall$ 

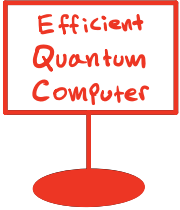
$P_r[\cdot]$ and $P_r[\cdot]$ are

"Sufficiently different".

Def:

- Say C Simulates Q to within multiplicative error $\epsilon \geq 0$ iff $\forall x, y:$

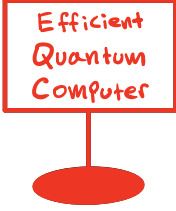
$$\frac{1}{1+\epsilon} \Pr[Q(x)=y] \leq \Pr[C(x)=y] \leq (1+\epsilon) \Pr[Q(x)=y]$$

- Say $Q =$  affords an ϵ -quantum advantage

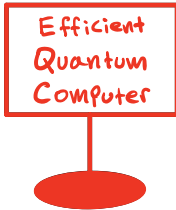
iff $\forall C =$ , C cannot simulate Q to

within multiplicative error ϵ .

Theorem [AA 2010, BTS 2010]:

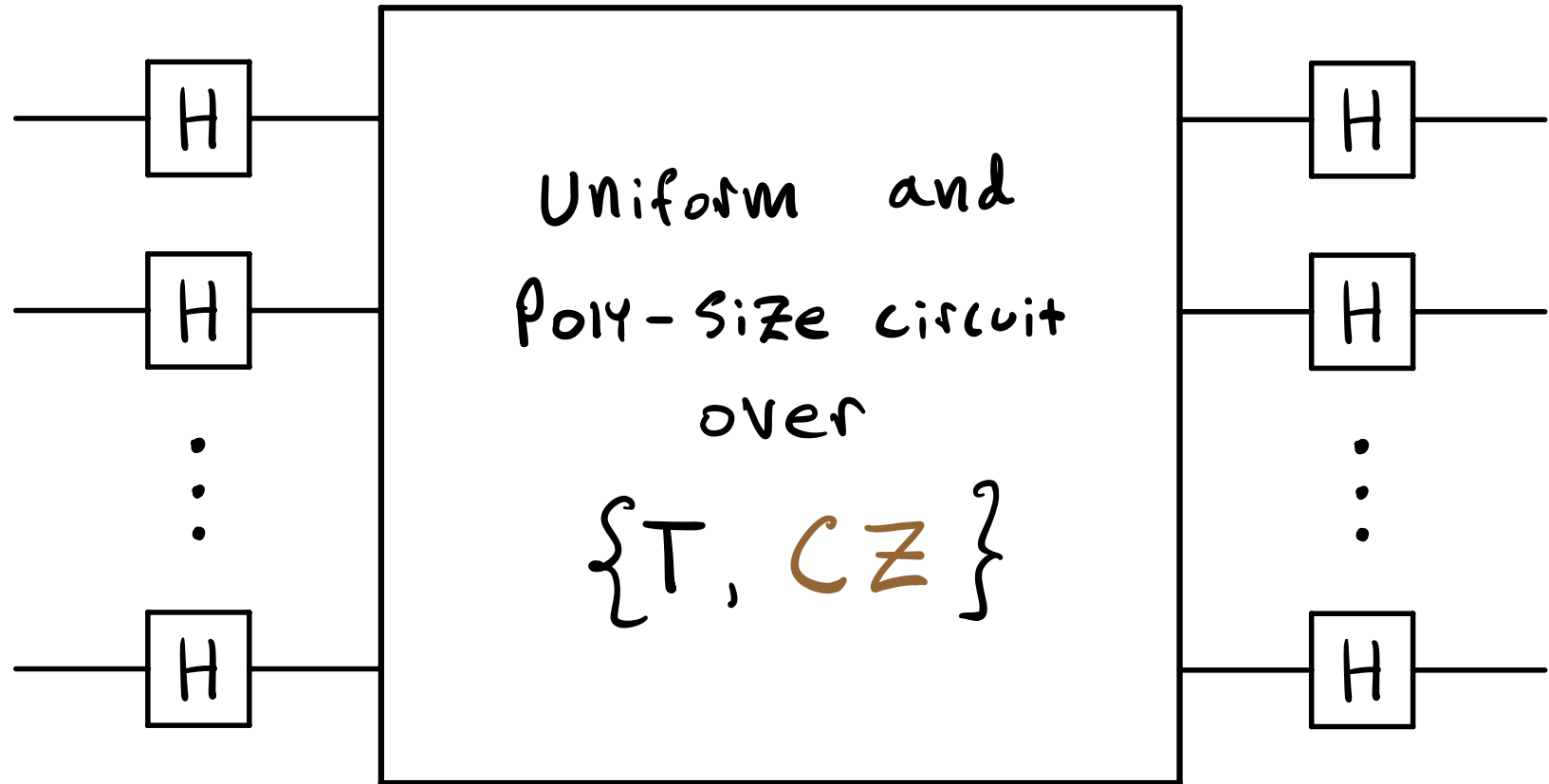
If PH is infinite, then  over
any universal gate set S afford
a $(\sqrt{2} - 1)$ -quantum advantage.

Key Idea: Post-Selection!

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

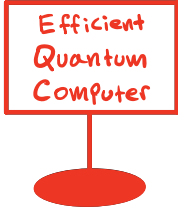
A: YES!


Instantaneous Quantum Polynomial



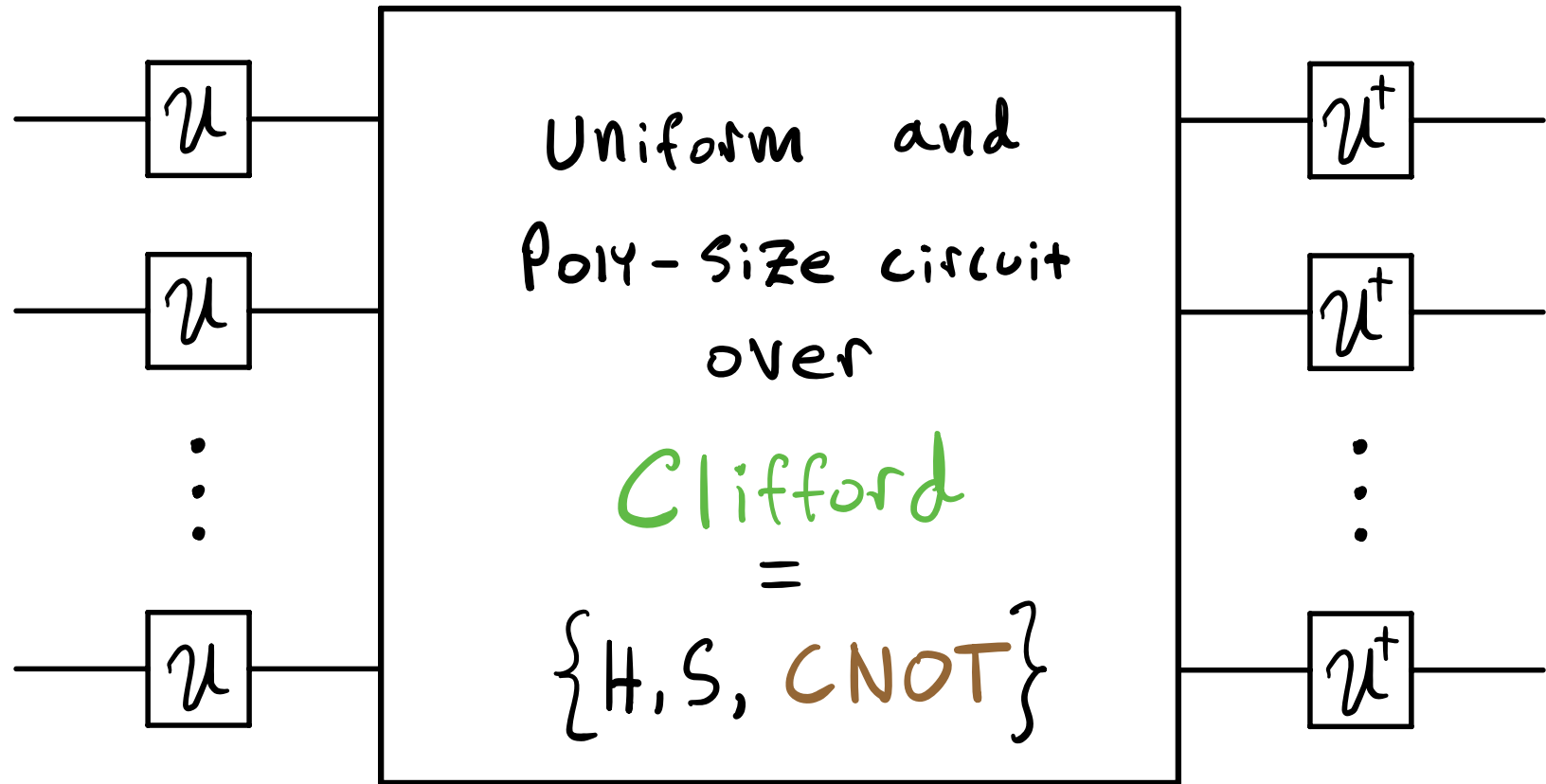
$$S_{\text{IQP}} = \{HTH, H \otimes H \text{ CZ } H \otimes H\}$$

Theorem [BJS, 2010]:

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

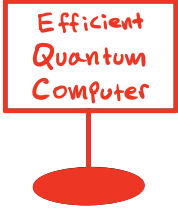
Key Idea: Post-Selection!

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]:

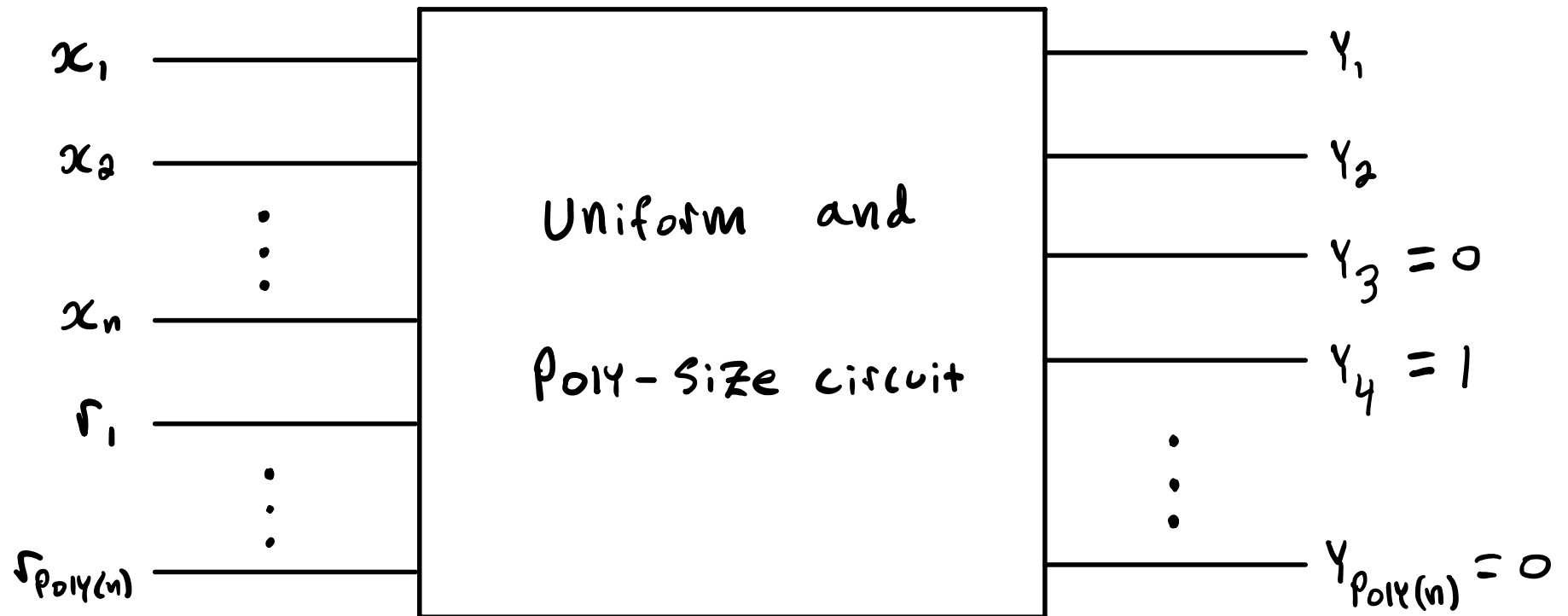
If PH is infinite, then  over $S_{ccc}(U)$ afford a $(\sqrt{2} - 1)$ -quantum advantage for most $U \in SU(2)$.

Key Idea: Post-Selection!

Part IV

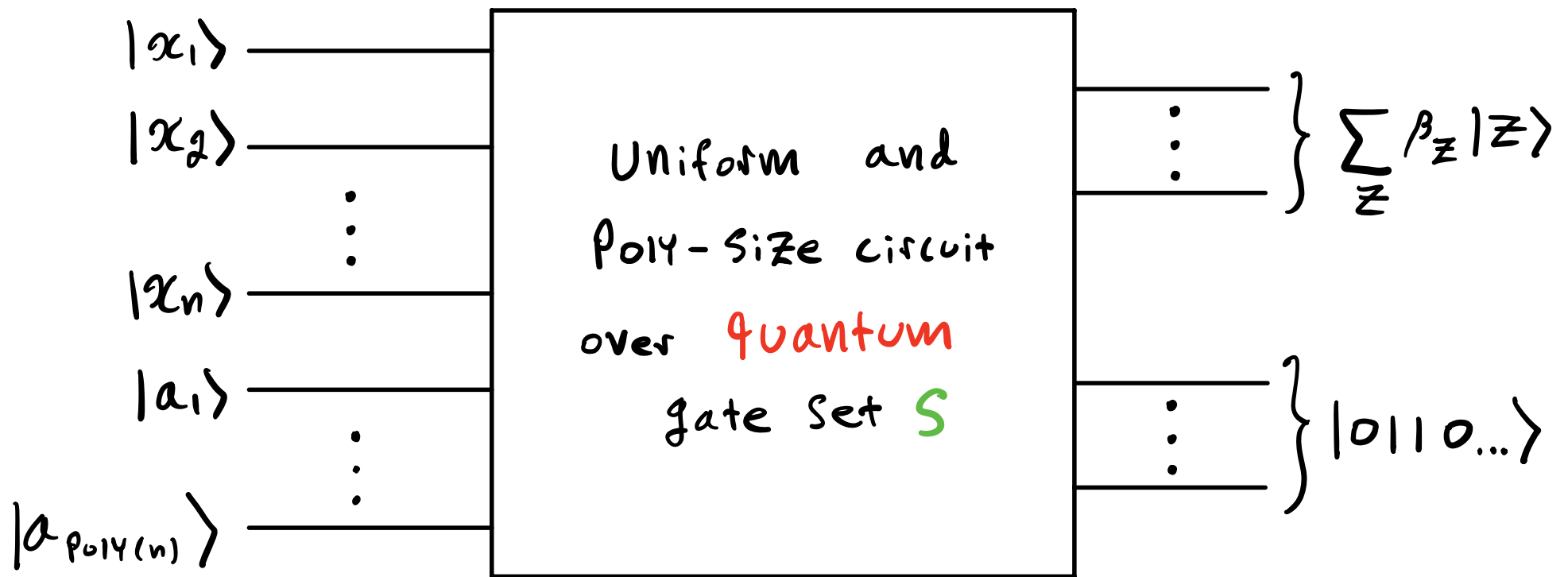
Post-Selection

Efficient Post-selected Classical Computer:



PostBPP

Efficient Post-Selected Quantum Computer:



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

Facts:

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

Corollary:

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

Theorem [AA 2010, BTS 2010]:

If

- $PH \not\subseteq P^{\Sigma_3 P}$

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

then

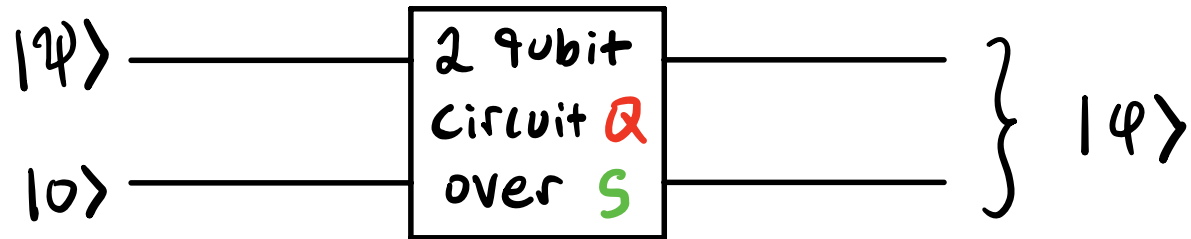
Efficient
Quantum
Computer



over S afford a $(\sqrt{2}-1)$ -quantum
advantage.

Part V

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

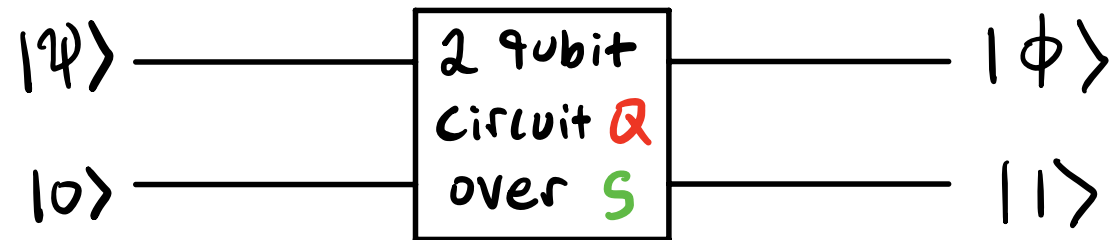


of course

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

Unitary
(always)



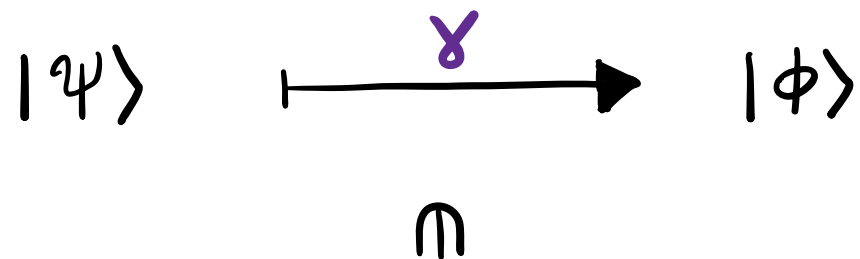
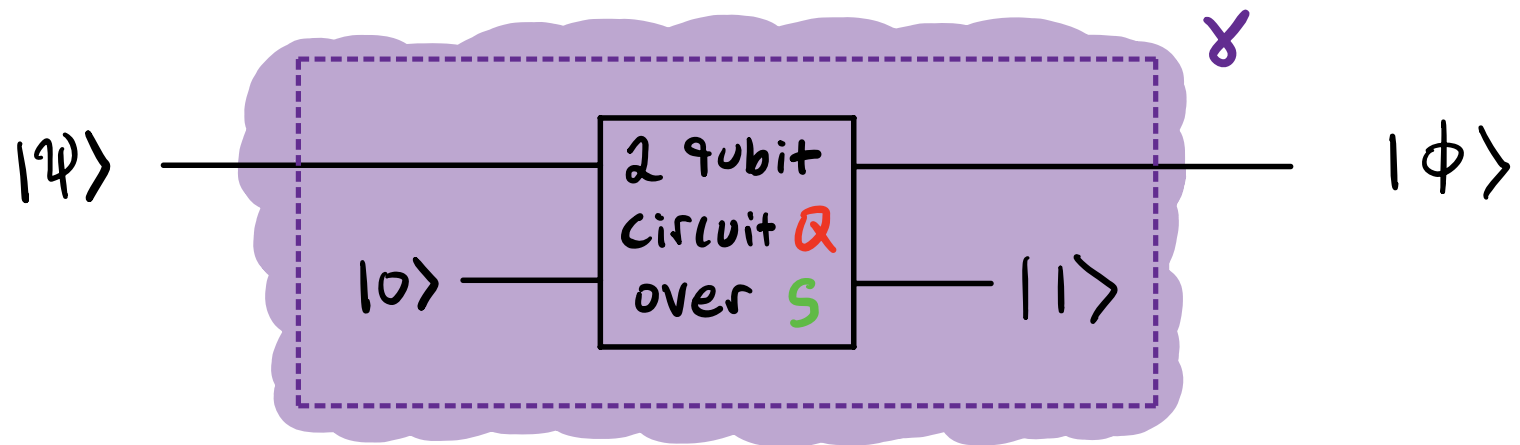


Post-Select!

However

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

non-unitary
(generally)

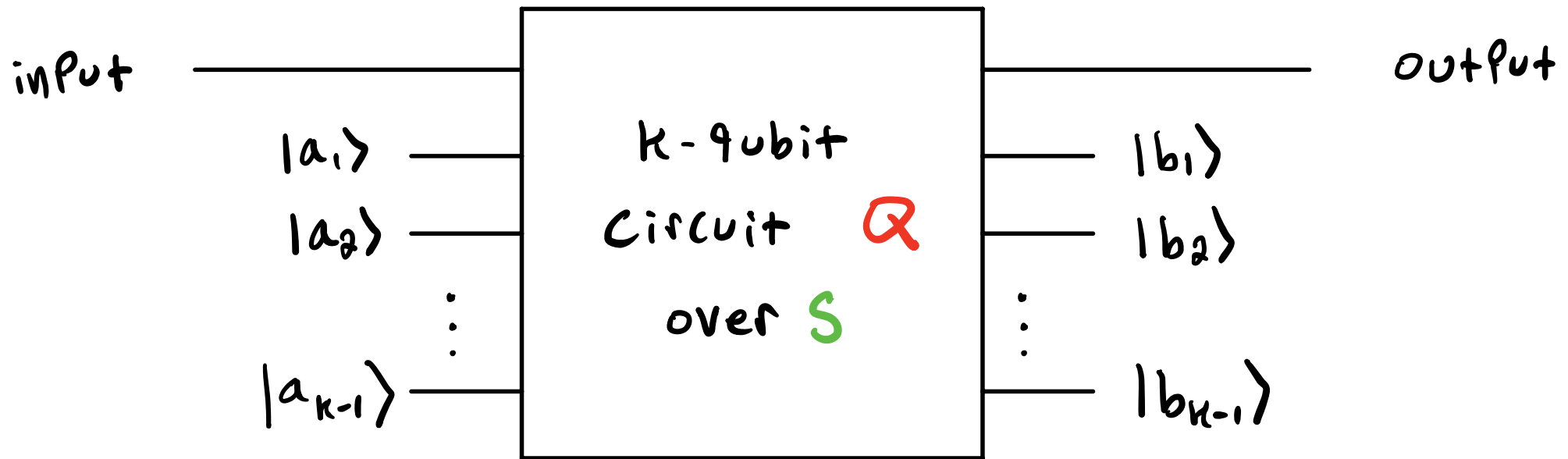


$$SL(2; \mathbb{C}) \setminus SU(2)$$

(generally)

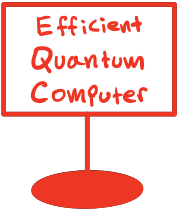
Def:

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



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

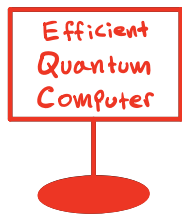
Theorem [AA 2010, BTS 2010]:

If

- $PH \not\subseteq P^{\Sigma_3 P}$

- $PostBQP(S) = PostBQP,$

then



over S afford a $(\sqrt{2}-1)$ -quantum
advantage.

Theorem [FKG, 2024]:

If

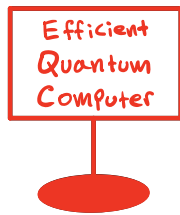
- $PH \not\subseteq P^{\Sigma_3 P}$

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

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



then

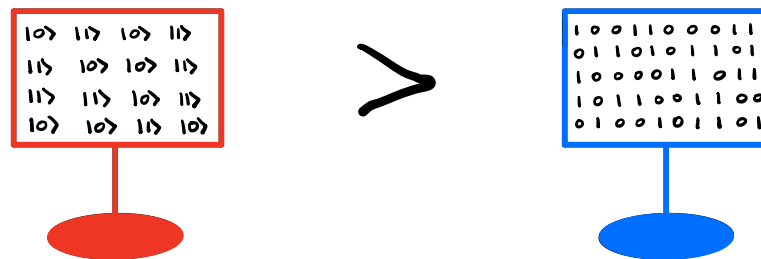


over S afford a $(\sqrt{2}-1)$ -quantum

advantage.

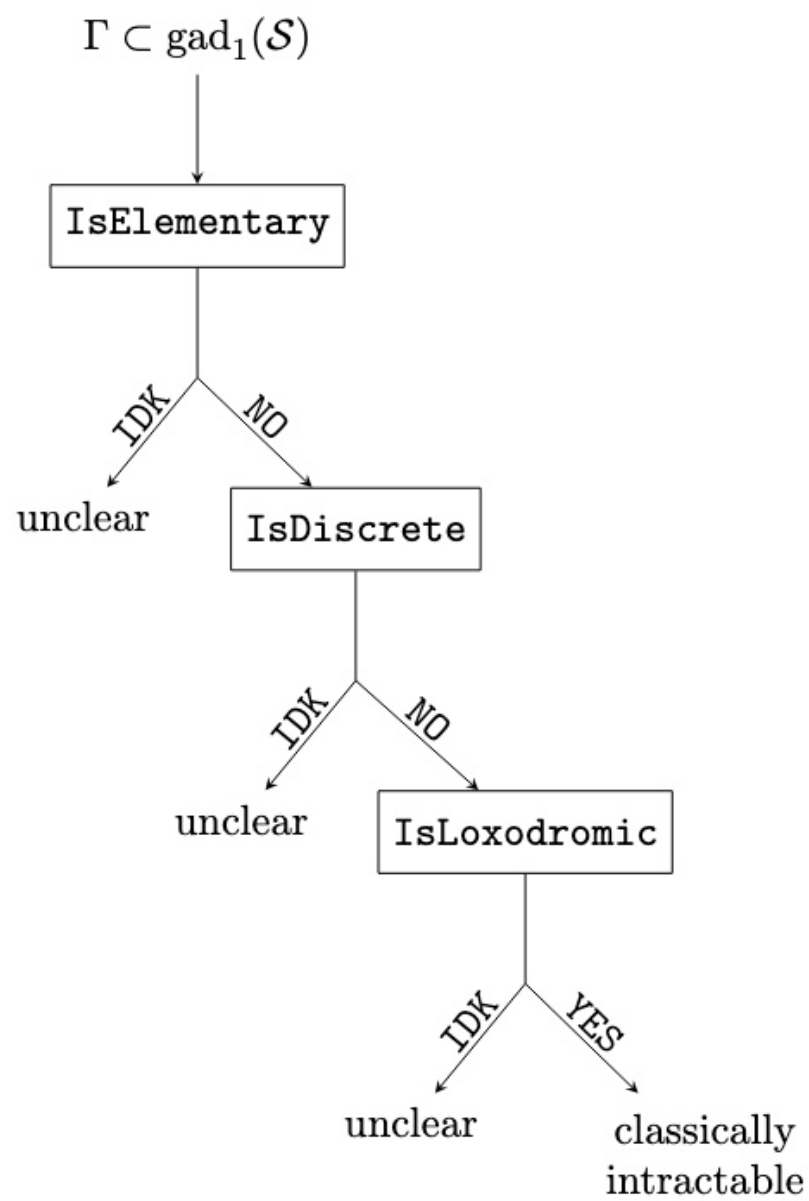
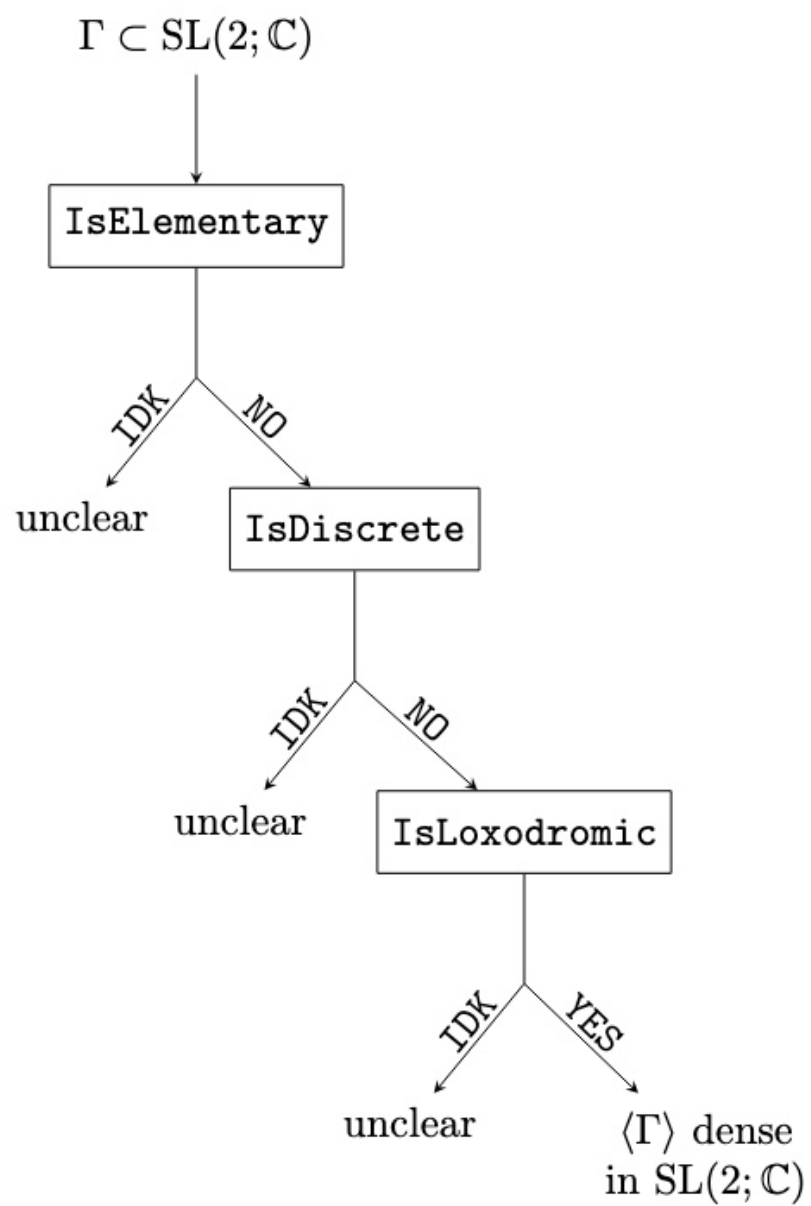
Part VI

A Criterion for Quantum Advantage



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

A: Look at traces of Γ !



Algorithm 1 IsElementary

```
1: Input: Finite set  $\Gamma \subset \mathrm{SL}(2; \mathbb{C})$  such that  $\langle \Gamma \rangle \leq \mathrm{SL}(2; \mathbb{C})$ 
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
```

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

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

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
```

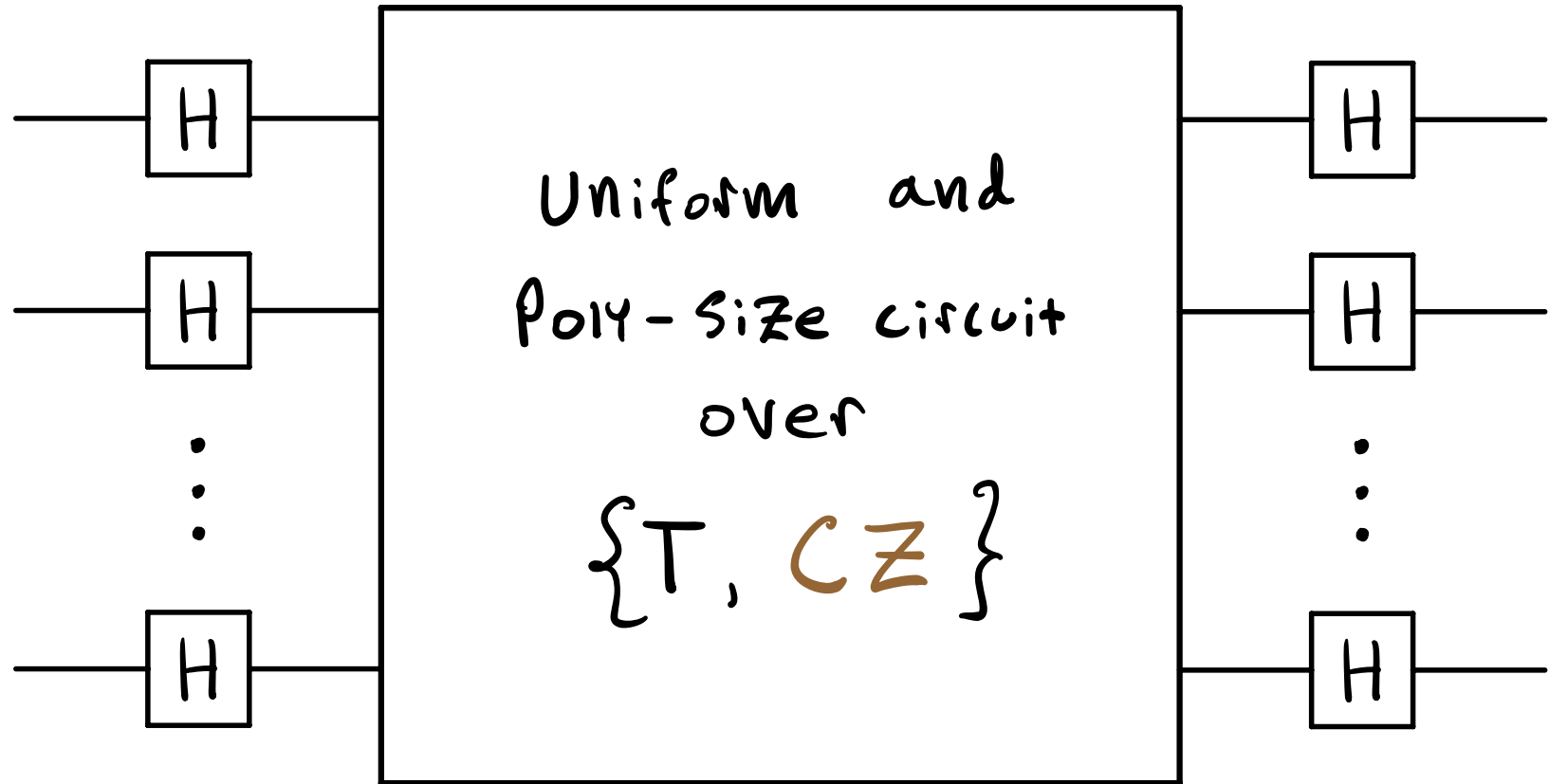
Algorithm 3 IsLoxodromic

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]:

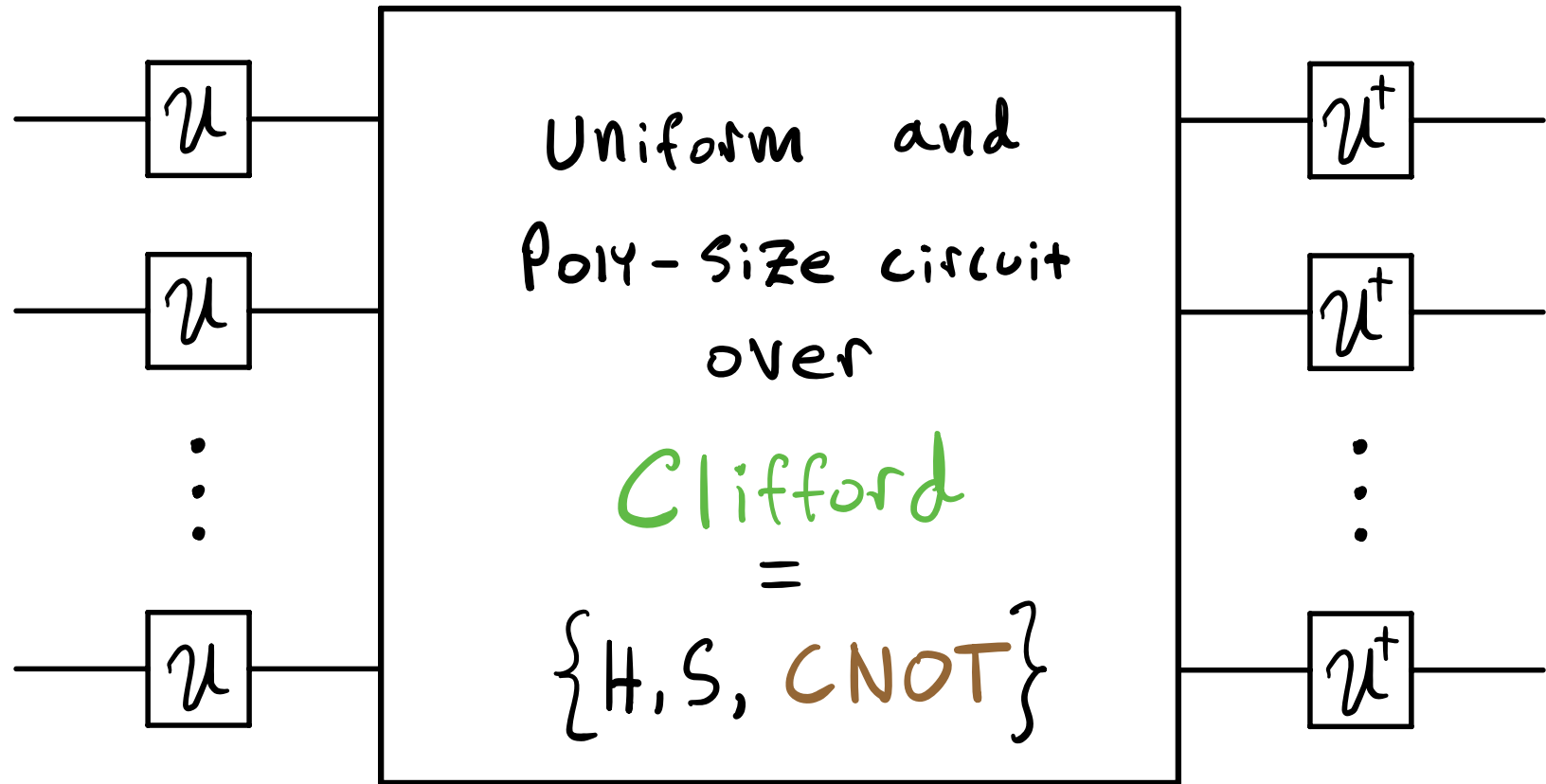
The following gadgets over S_{IQP} generate a dense subgroup of $SL(2; \mathbb{C})$:

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

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

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

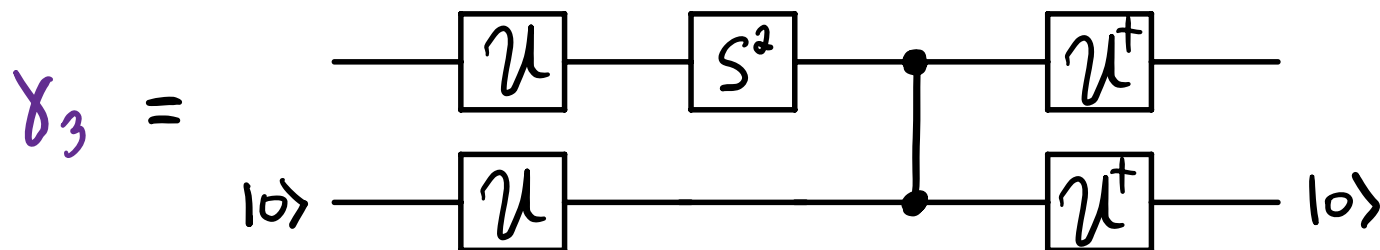
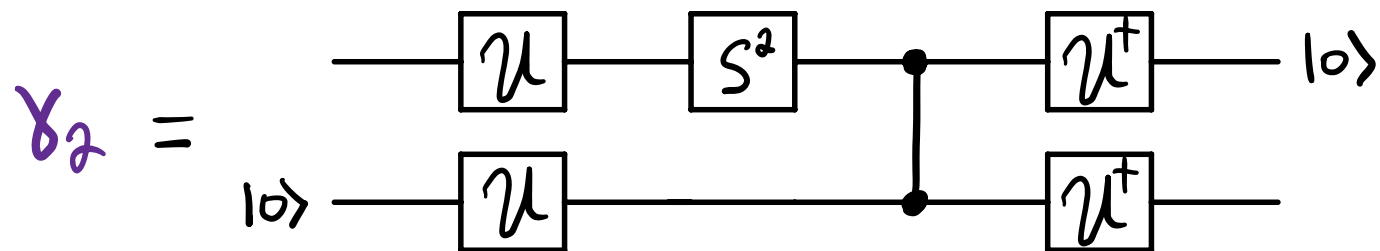
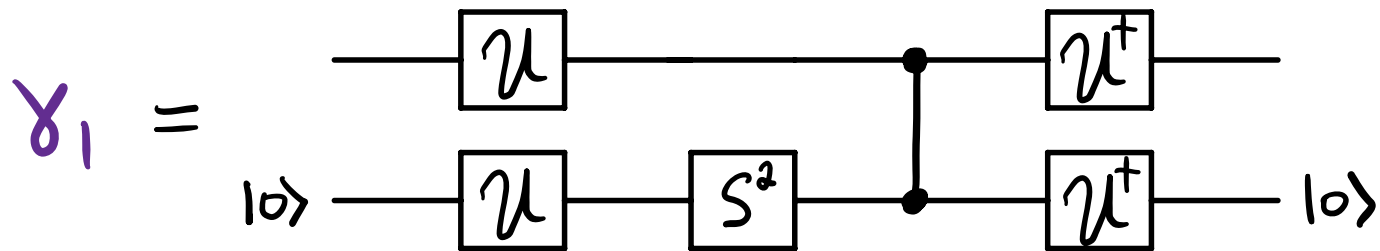
Conjugated Clifford Circuits

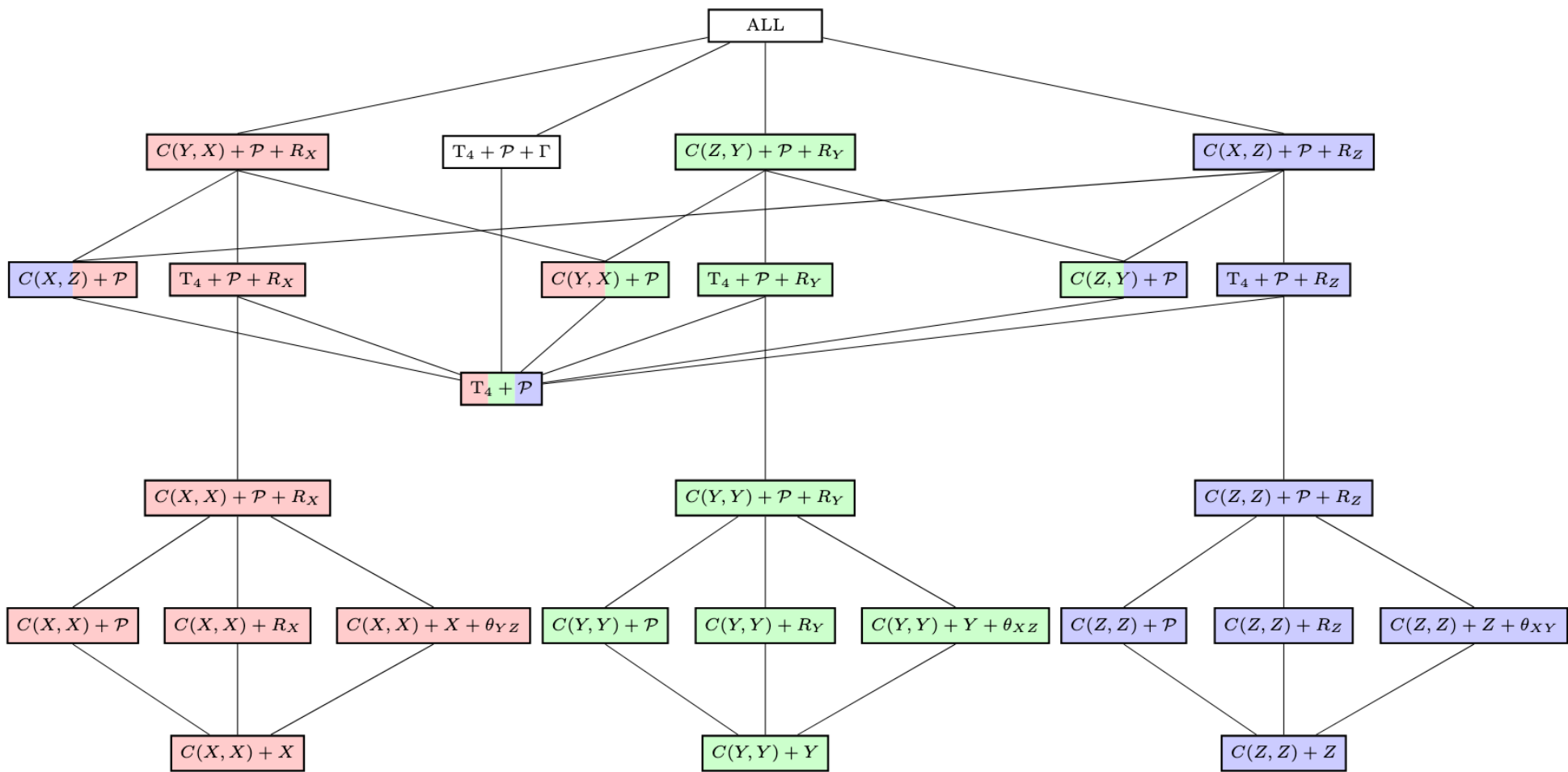


$$S_{ccc}(U) = \{U H U^\dagger, U S U^\dagger, U \otimes U \text{ CNOT } U^\dagger \otimes U^\dagger\}$$

Theorem [FKG, 2024]:

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

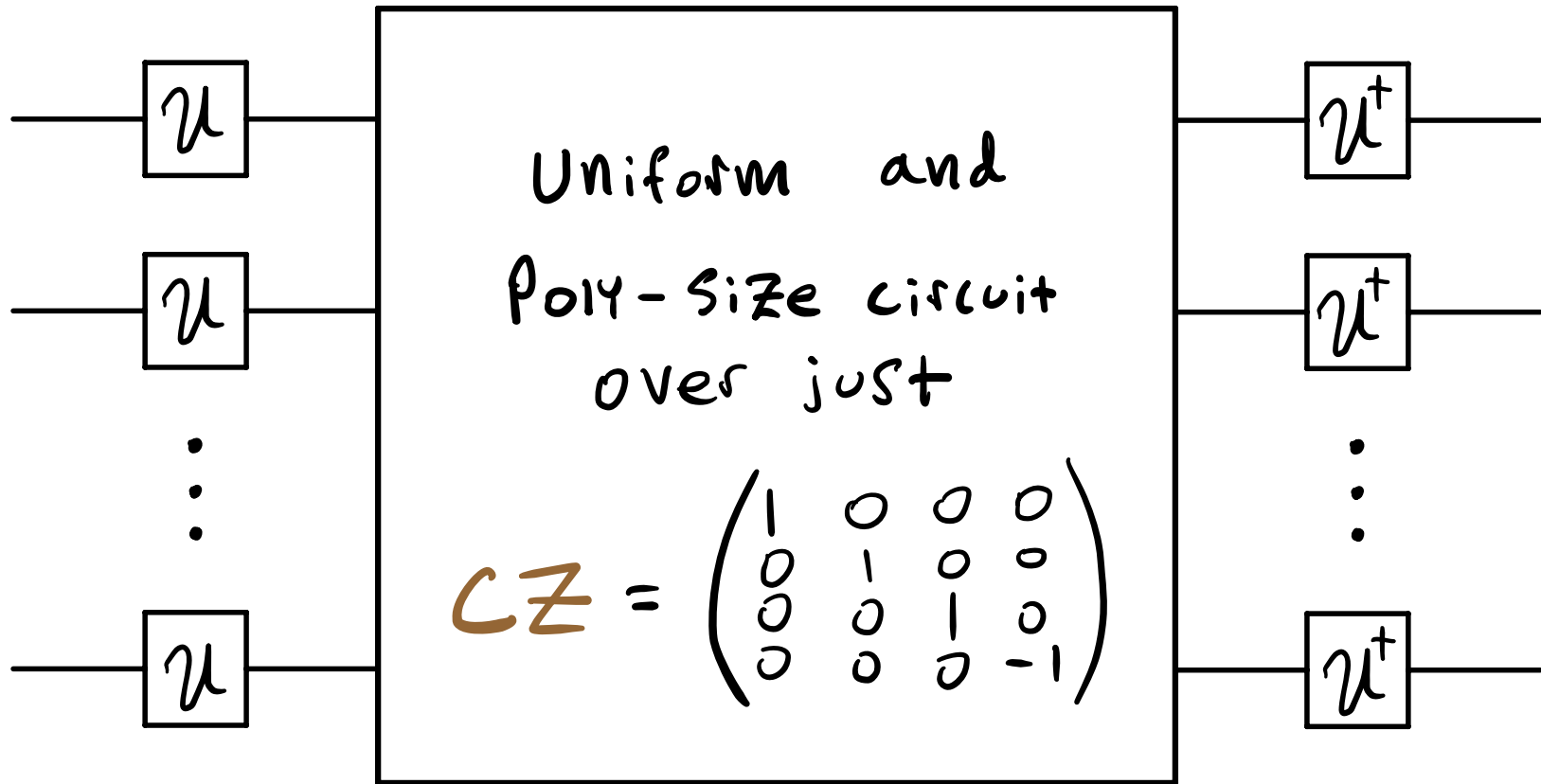




Theorem [FKG, 2024]:

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



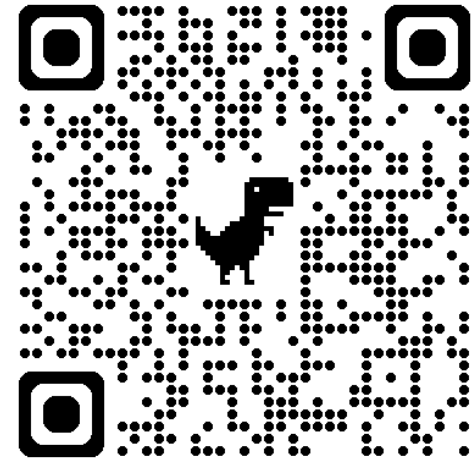
$$U \neq e^{i\alpha} R_Z(\phi) C R_Z(\lambda)$$

where

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

|Thank You!>

Paper



Slides

