**Title:** A Criterion for Post-Selected Quantum Advantage

**Speakers:** Matthew Fox

**Collection/Series:** Quantum Information

**Subject:** Quantum Information

**Date:** May 14, 2025 - 11:00 AM

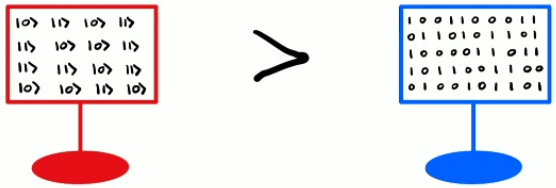
**URL:** https://pirsa.org/25050025

**Abstract:**

Assuming the polynomial hierarchy is infinite, we prove a sufficient condition for determining if uniform and polynomial size quantum circuits over a non-universal gate set are not efficiently classically simulable in the weak multiplicative sense. Our criterion exploits the fact that subgroups of SL(2; C) are essentially either discrete or dense in SL(2; C). Using our criterion, we give a new proof that both instantaneous quantum polynomial (IQP) circuits and conjugated Clifford circuits (CCCs) afford a quantum advantage. We also prove that both commuting CCCs and CCCs over various fragments of the Clifford group afford a quantum advantage, which settles two questions of Bouland, Fitzsimons, and Koh. Our results imply that circuits made of just U \otimes U-conjugated CZ gates afford a quantum advantage for almost all single-qubit unitaries U.

# Post-Selected

# A Criterion for ^ Quantum Advantage




Matthew Fox

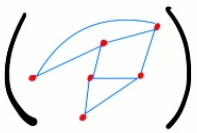
University of Colorado Boulder

Paper ⇝

Slides ⇝

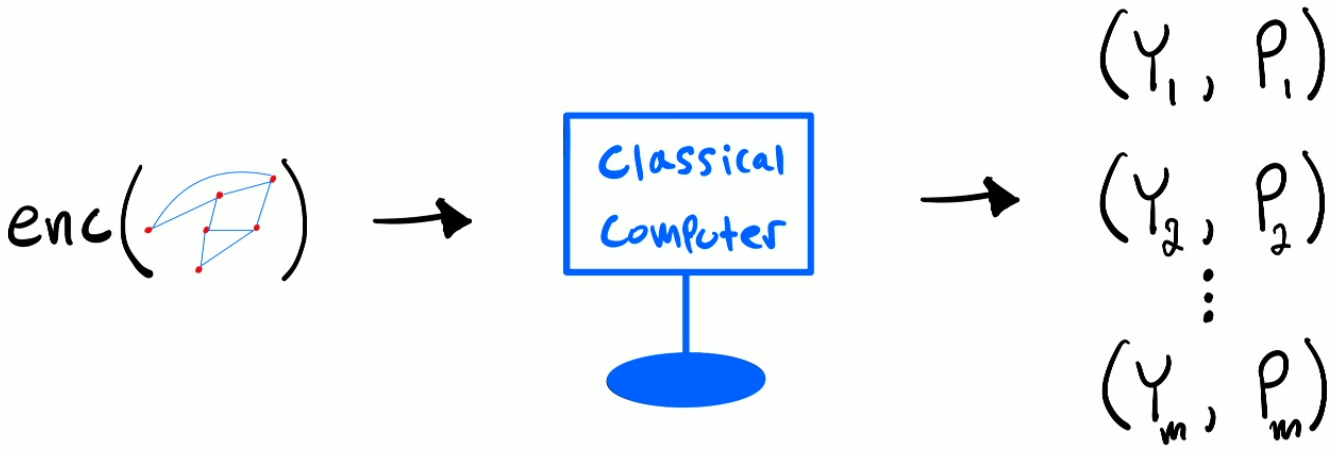
# Part I

## Classical and Quantum Computers

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

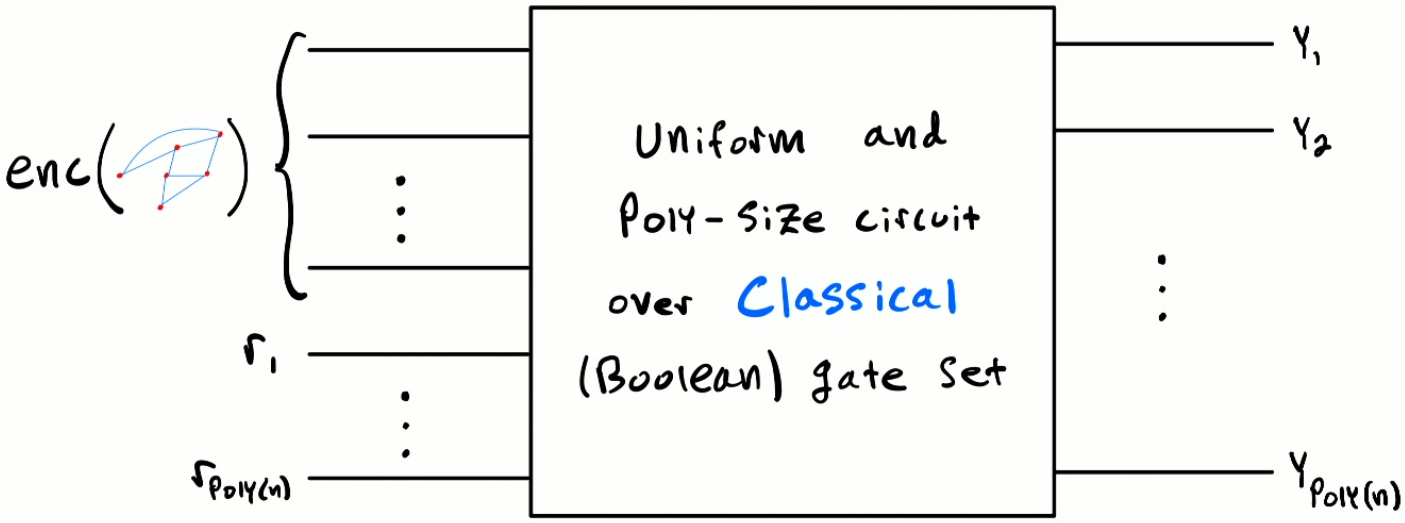
$$\in \{0,1\}^n$$

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




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

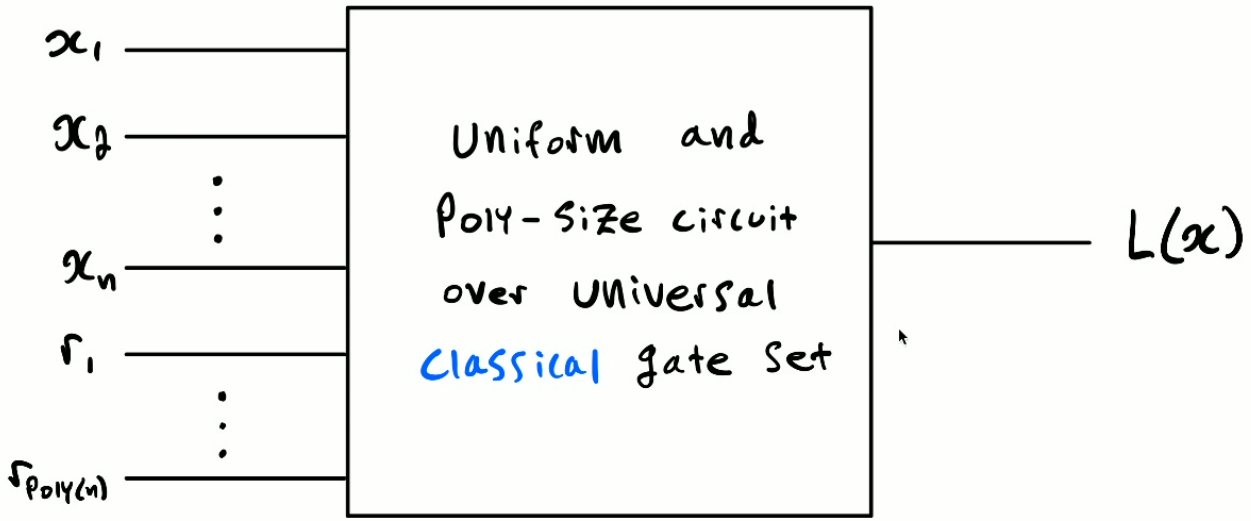
# Efficient Classical Computer:

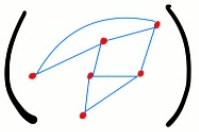



$$r_1, \ldots, r_{poly(n)} \sim \text{Uniform}(\{0,1\})$$

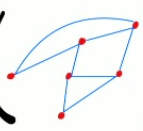
**Def:** $L \in$ BPP iff $\exists$ efficient Classical computer $C$ over Universal Classical gate set such that $\forall x \in \{0,1\}^*$,

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



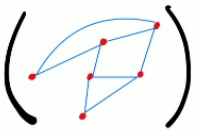
$enc($  $) = 1001011011$

encode in quantum system

$Qenc($  $) =$ 

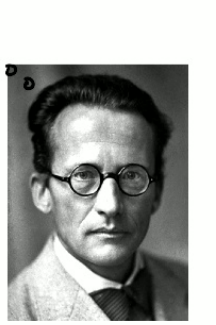
$= |1001011011\rangle$

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

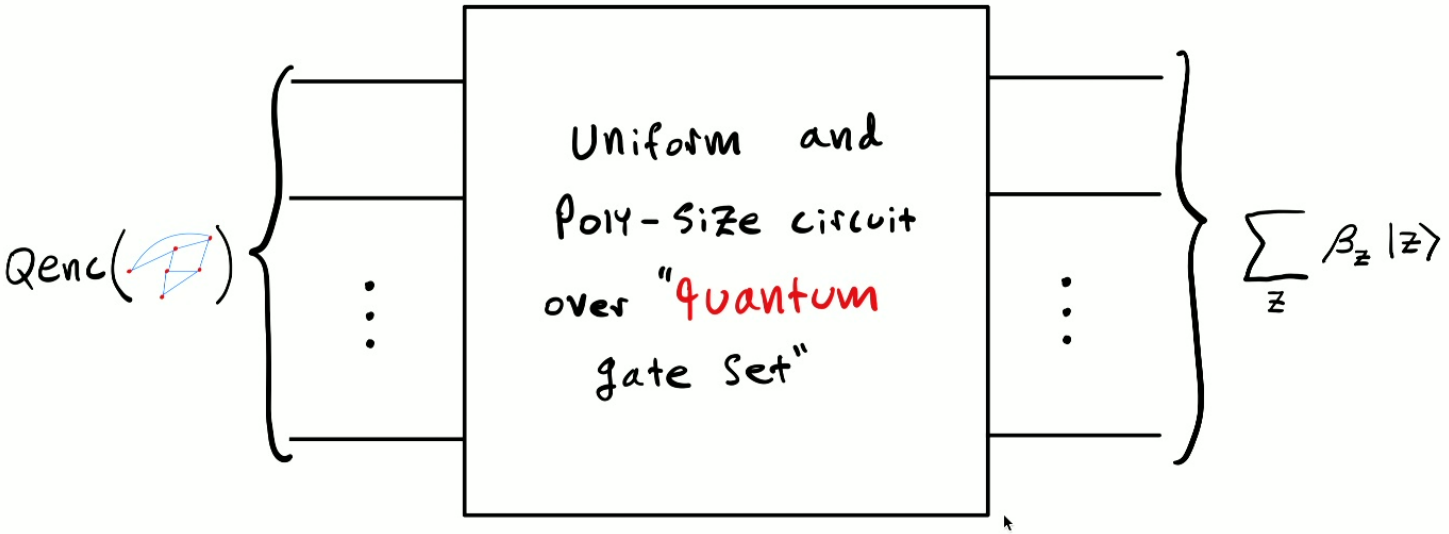
$Qenc($  $) \rightarrow$ Quantum Computer $\rightarrow \sum_{z \in \{0,1\}^n} \beta_z |z\rangle$

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


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



# Efficient Quantum Computer:



**Def:** A quantum gate set $S$ is a finite collection of $SU(2)$ gates, together with at least one entangling gate $\mathcal{E}$.

**Ex:**

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

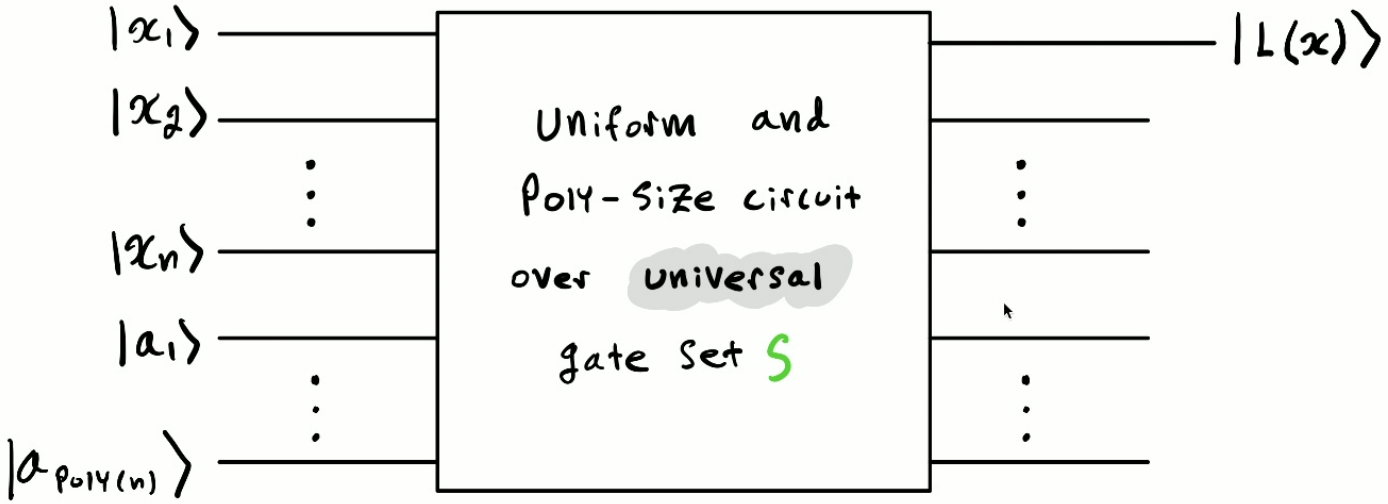
**Def:** A quantum gate set $S$ is universal iff

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

is dense in $SU(2)$.

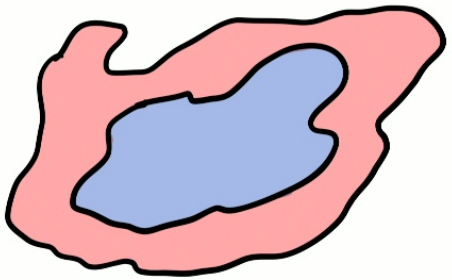
**Def:** $L \in BQP$ iff $\exists$ efficient quantum computer $Q$ over a universal gate set $S$ such that $\forall x \in \{0,1\}^*$,

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



Fact: $BPP \subseteq BQP$

Conj: $BPP \subsetneq BQP$

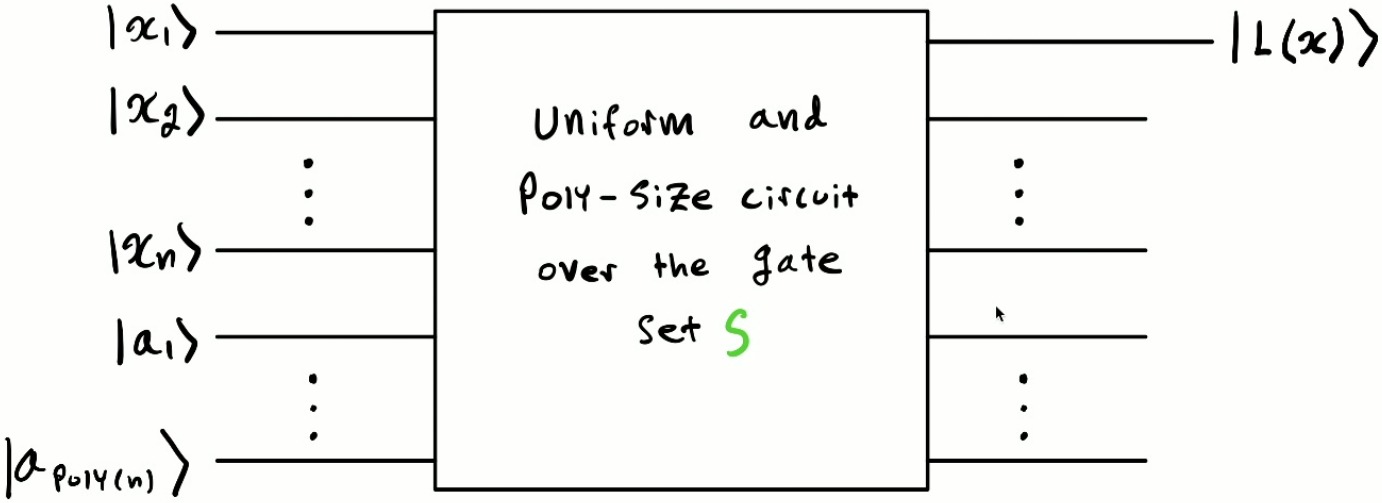


# Part II

## Non-Universal Quantum Computation

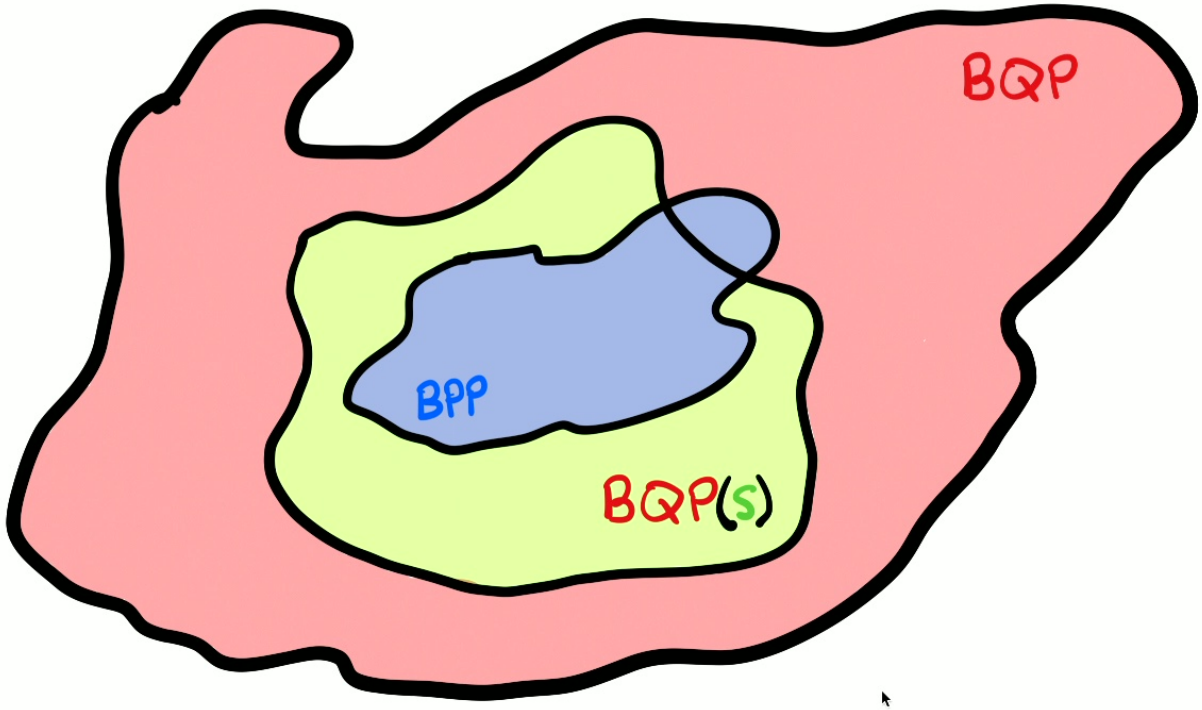
**Def:** $L \in BQP(S)$ iff $\exists$ efficient quantum computer $Q$ over the gate set $S$ such that $\forall x \in \{0,1\}^*$,

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

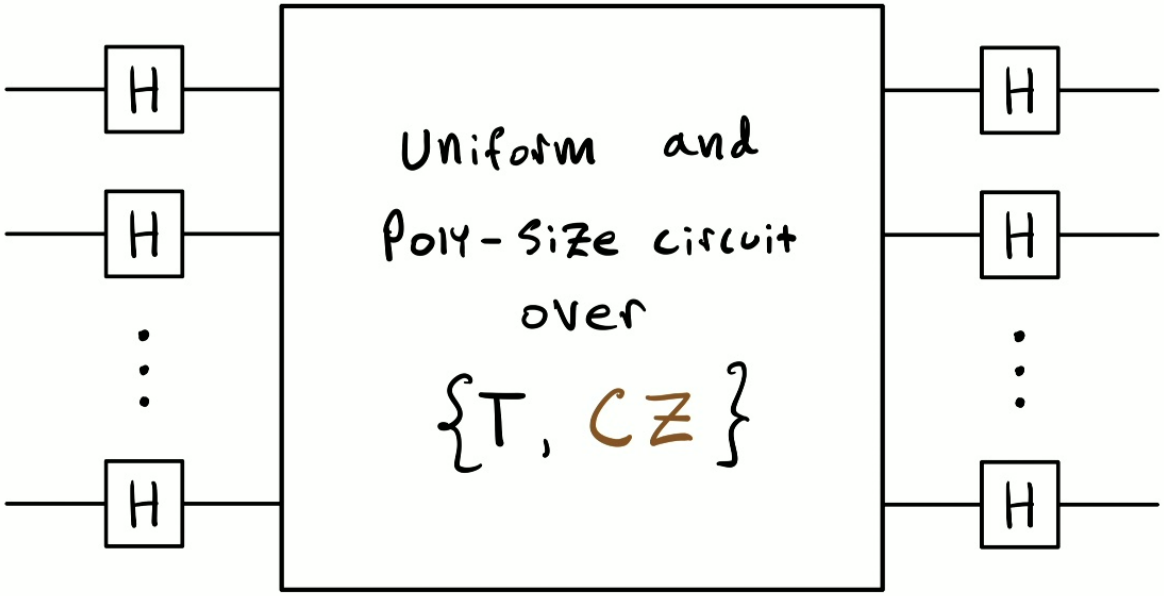


Facts:

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

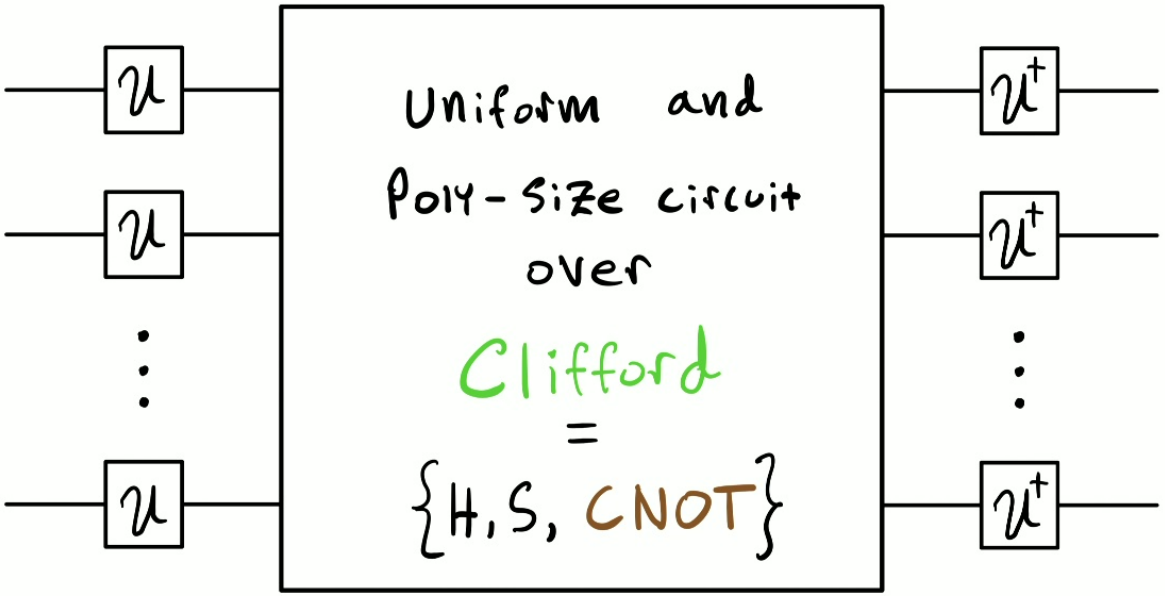

BQP
BPP
BQP(S)

# Instantaneous Quantum Polynomial



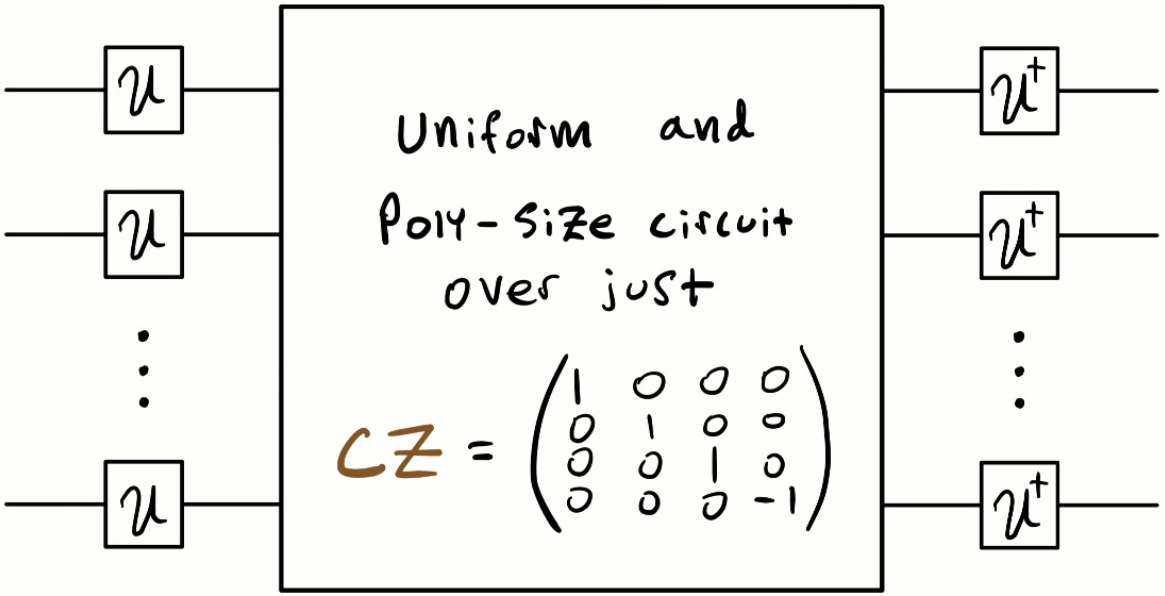

$$S_{IQP} = \{HTH,\ H \otimes H\ CZ\ H \otimes H\}$$

# Conjugated Clifford Circuits




$$S_{ccc}(U) = \{UHU^\dagger,\ USU^\dagger,\ U\otimes U\ CNOT\ U^\dagger\otimes U^\dagger\}$$

# Conjugated CZ Circuits



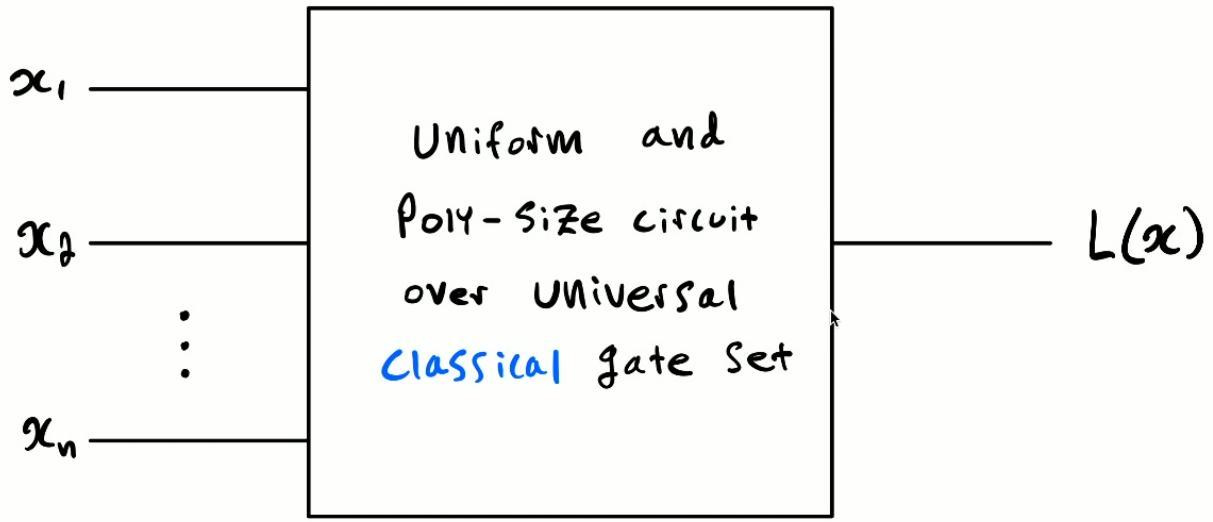

$$S_{CZ}(\mathcal{U}) = \{\mathcal{U}\otimes\mathcal{U}\ CZ\ \mathcal{U}^\dagger\otimes\mathcal{U}^\dagger\}$$

**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. $\forall x \in \{0,1\}^*$,

$$\exists y \in \{0,1\}^{p(|x|)} \text{ s.t. } C(x,y) = L(x).$$

**Def:**

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

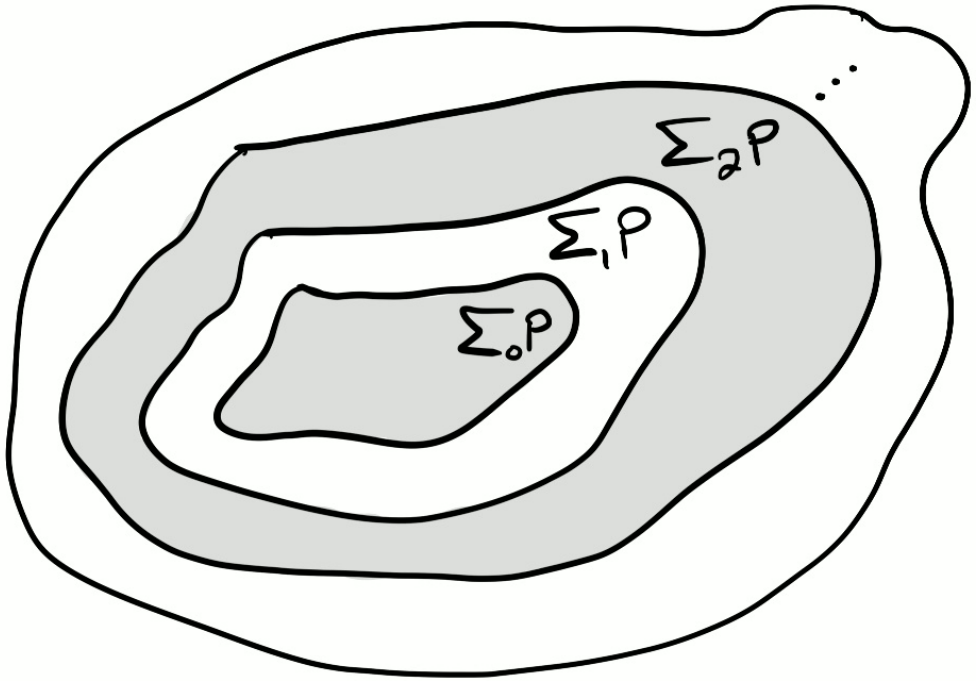
$C$

and polynomials $p_1, \ldots, p_k$ s.t. $\forall x \in \{0,1\}^*$,

$$\exists y_1 \in \{0,1\}^{p_1(|x|)} \quad \forall y_2 \in \{0,1\}^{p_2(|x|)}$$

$$\exists y_3 \in \{0,1\}^{p_3(|x|)} \ldots \quad \exists / \forall \, y_k \in \{0,1\}^{p_k(|x|)}$$

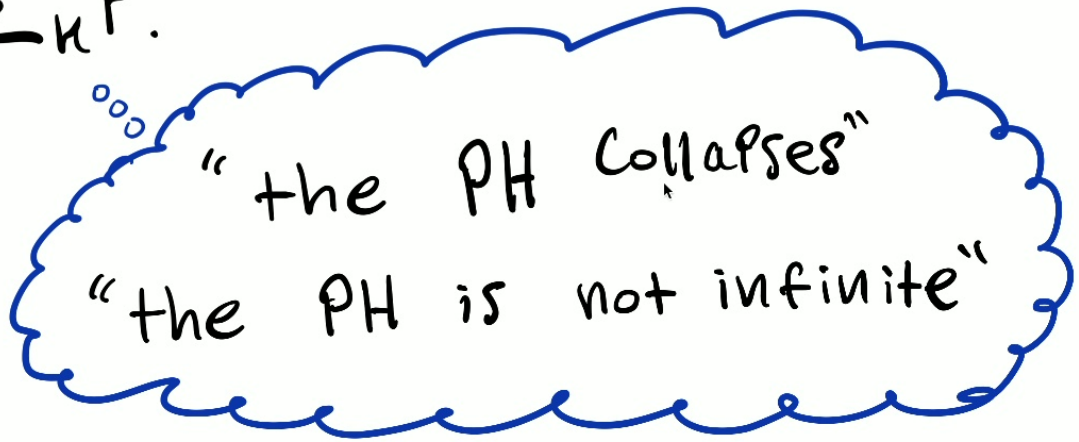
s.t. $C(x, y_1, y_2, \ldots, y_k) = L(x)$.




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

## Facts:

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



# Part IV

## Quantum Advantage

"Quantum Advantage"

$\Leftrightarrow$

$\exists$ 

such that $\forall$ 


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

"Sufficiently different".

**Def:**

- Say $C$ simulates $Q$ to within weak multiplicative error $\varepsilon \geq 0$ iff $\forall x, y$:

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

- Say $Q =$ 

affords a weak $\varepsilon$-quantum advantage iff $\forall C =$ 

, $C$ cannot simulate $Q$ to within weak multiplicative error $\varepsilon$.

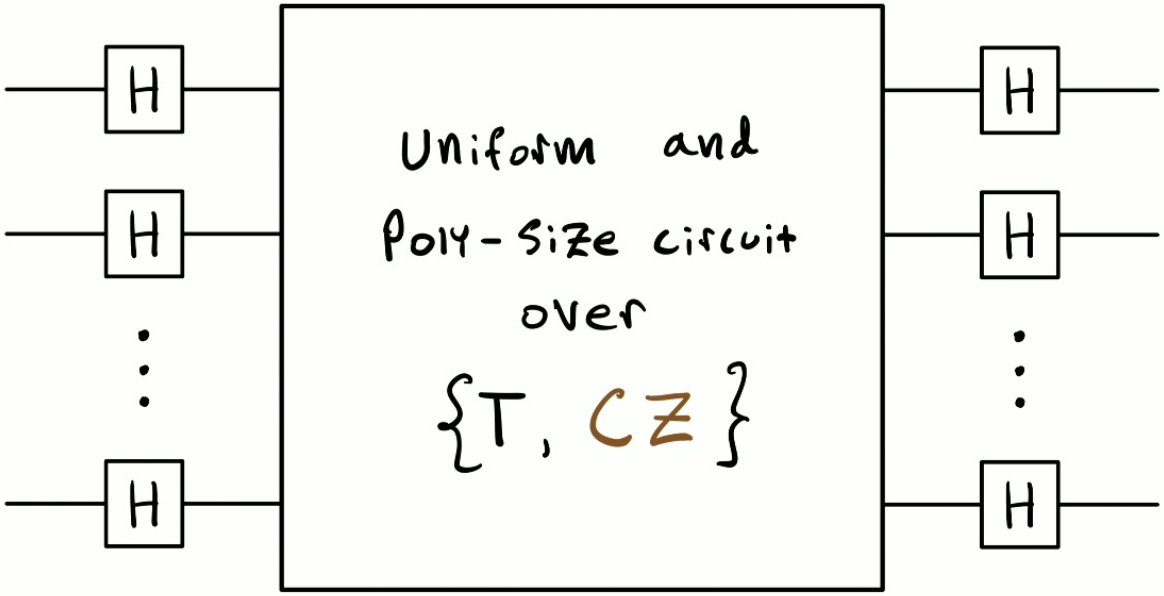
**Theorem (AA 2010, BJS 2010):**

If PH is infinite, then 

over any universal gate set $S$ afford a weak $(\sqrt{2}-1)$-quantum advantage.

**Key Idea:** Post-Selection!

# Instantaneous Quantum Polynomial




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

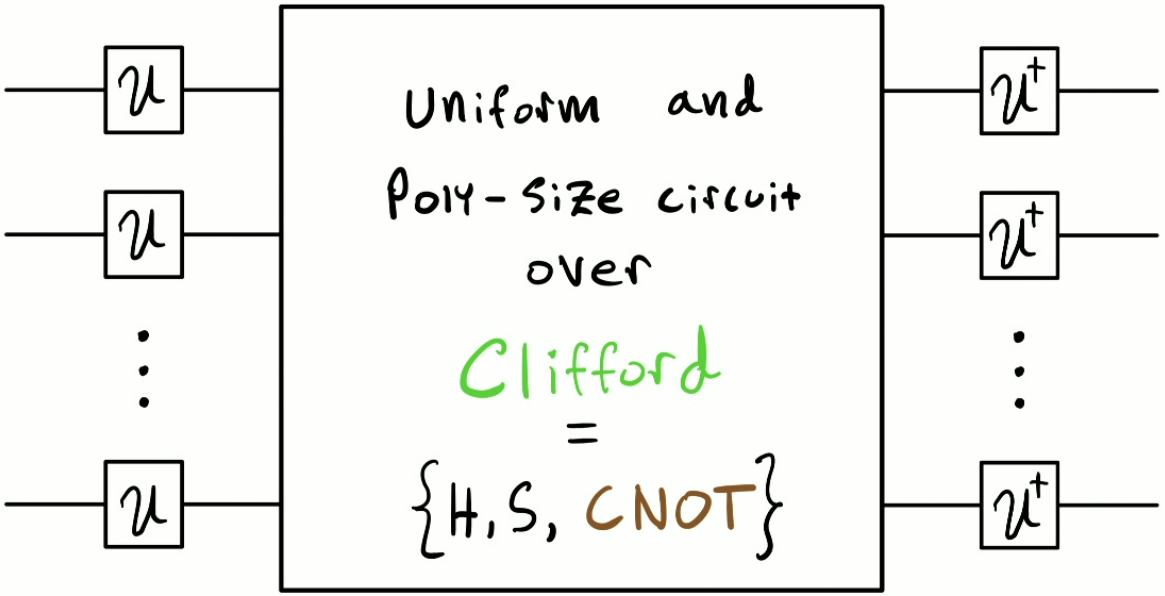
## Theorem (BJS, 2010):

If PH is infinite, then 

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

## Key Idea: Post-Selection!

# Conjugated Clifford Circuits




$$S_{ccc}(U) = \{UHU^\dagger,\ USU^\dagger,\ U\otimes U\ CNOT\ U^\dagger\otimes U^\dagger\}$$

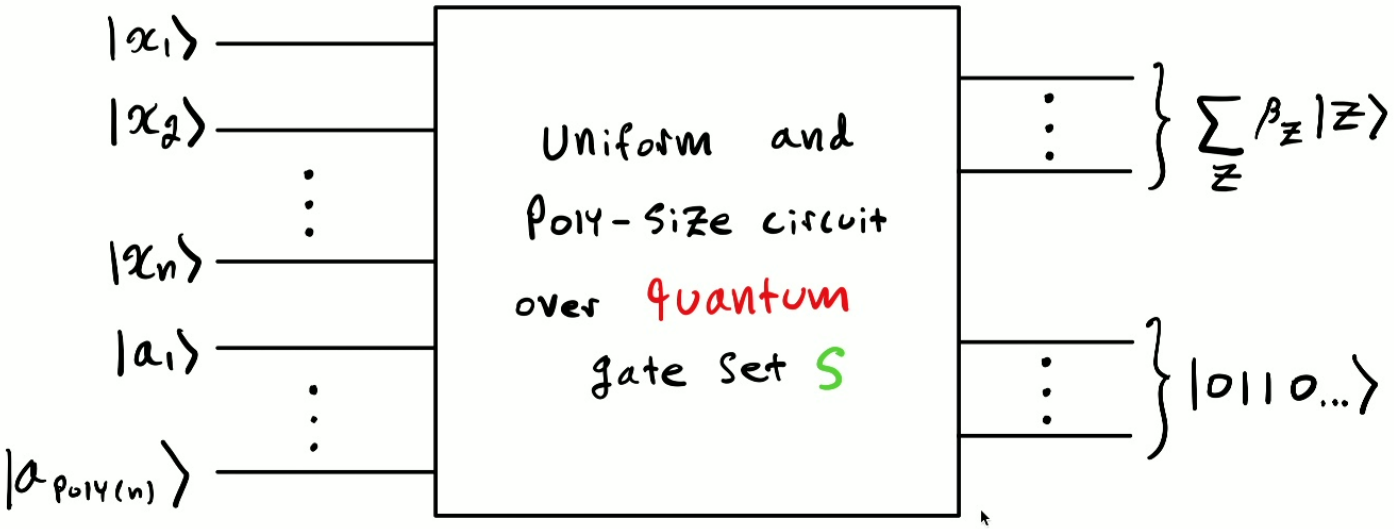
**Theorem (BFK, 2016):**

If PH is infinite, then 

over $S_{ccc}(\mathcal{U})$ afford a weak $(\sqrt{2}-1)$-quantum advantage for almost all $\mathcal{U} \in SU(2)$.

**Key Idea:** Post-Selection!

Efficient Post-selected Quantum Computer:




PostBQP(S), PostBQP

BPP

PostBPP


BQP

PostBQP

(Bouland, 2018)

## Facts:

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

## Corollary:

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

# Part VI

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

## Theorem (AA 2010, BJS 2010):

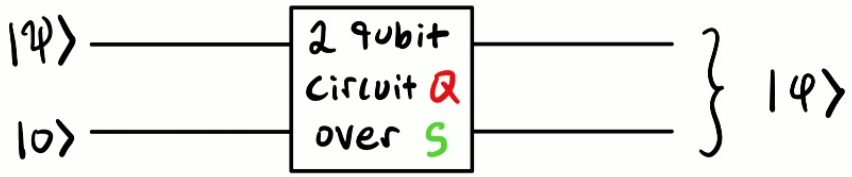
If

- $PH \not\subseteq \Sigma_3 P$
- $\text{Post-BQP}(S) = \text{Post-BQP}$,

then


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

quantum advantage.

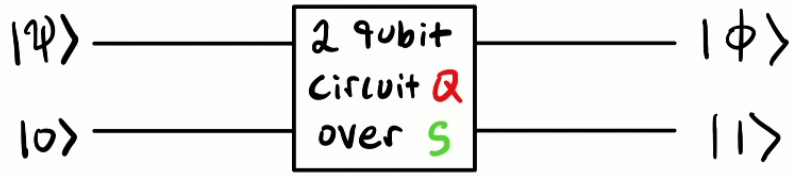



of course

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

unitary

(always)



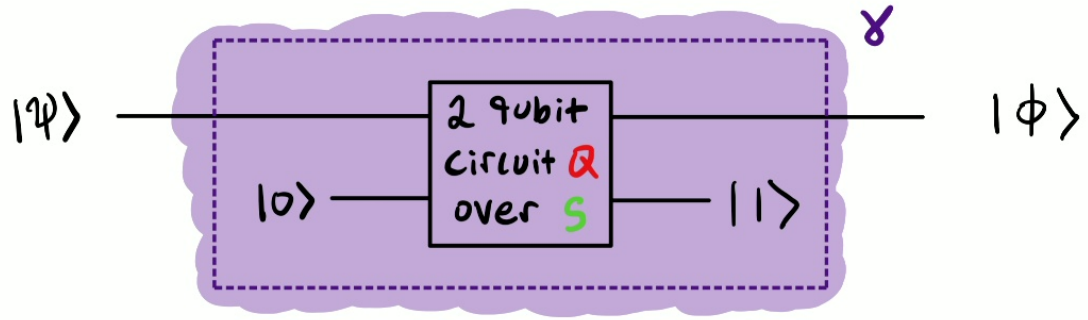

Post-select!

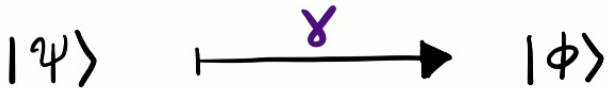
However

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

non-unitary

(generally)



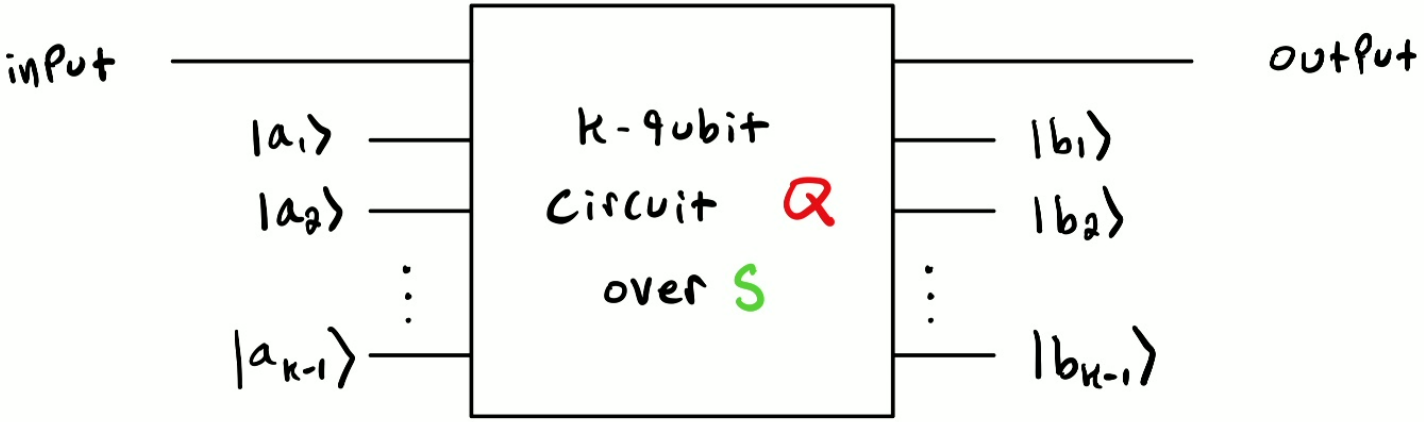

$\Pi$

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

(generally)

## Def:

A k-qubit post-selection gadget $\gamma$ 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 $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ over $S$ are Post-selected 

over $S$.

Theorem (FKG, 2024):

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

$\rightarrow$

$\mathrm{Post}\cdot\mathrm{BQP}(S) = \mathrm{Post}\cdot\mathrm{BQP}$.

## Theorem (FKG, 2024):

If

- $PH \not\subseteq \Sigma_3 P$
- ~~$\text{Post}BQP(S) = \text{Post}BQP$~~,

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

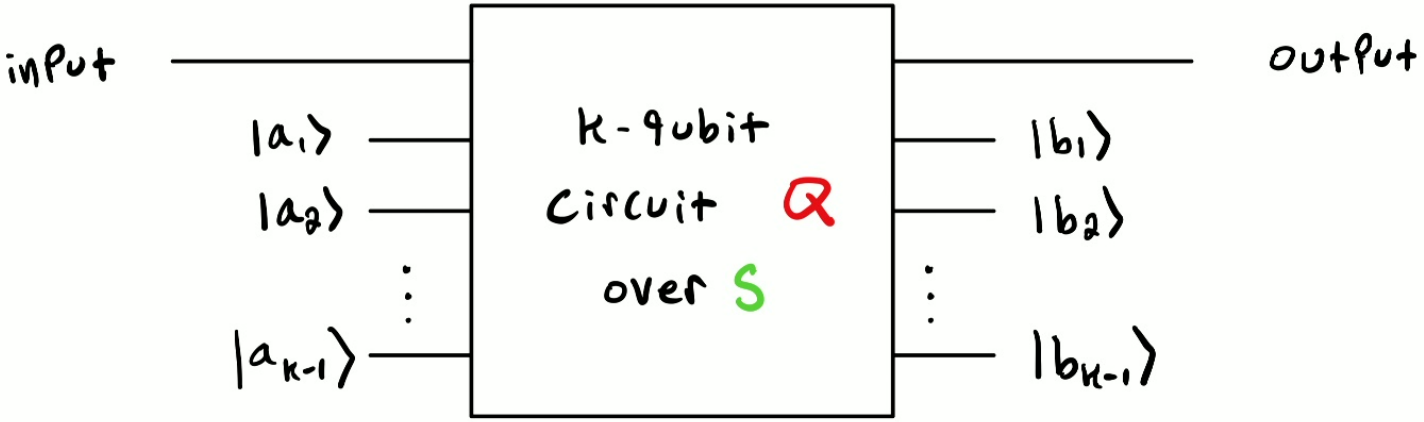
then


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

quantum advantage.

## Def:

A k-qubit post-selection gadget $\gamma$ over $S$ is




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

## Theorem (FKG, 2024):

If

- $PH \not\subseteq \Sigma_3 P$
- ~~$\mathrm{Post}\cdot BQP(S) = \mathrm{Post}\cdot BQP$,~~

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

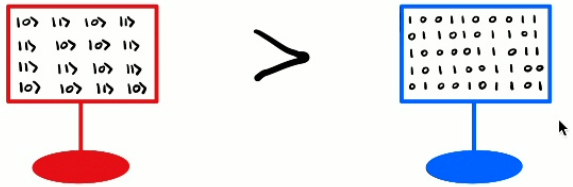
then


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

quantum advantage.

# 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

- $PH \not\subseteq \Sigma_3 P$
- ~~$\text{Post-BQP}(S) = \text{Post-BQP}$,~~

then


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

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

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

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

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

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

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

Let

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

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

**Algorithm 1** `IsElementary`

**Input:** Finite set $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$ such that $\langle\Gamma\rangle \leq \mathrm{SL}(2;\mathbb{C})$
**Output:** `NO` if $\langle\Gamma\rangle$ is non-elementary, `IDK` ("I don't know") otherwise
**for** $g, h \in \Gamma$ **do**
  **if** $\beta(g) \notin [-4, 0]$ or $\beta(h) \notin [-4, 0]$ or $\gamma(g, h) \notin [-\beta(g)\beta(h)/4, 0]$ **then**
    **if** $\gamma(g, h) \neq 0$ **then**
      **if** $\beta(g) \neq \gamma(g, h)$ or $\beta(h) \neq -4$ **then**
        **if** $\beta(g) \neq -4$ or $\beta(h) \neq \gamma(g, h)$ **then**
          **if** $\beta(g) \neq -4$ or $\beta(h) \neq -4$ **then**
            return `NO`
return `IDK`

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

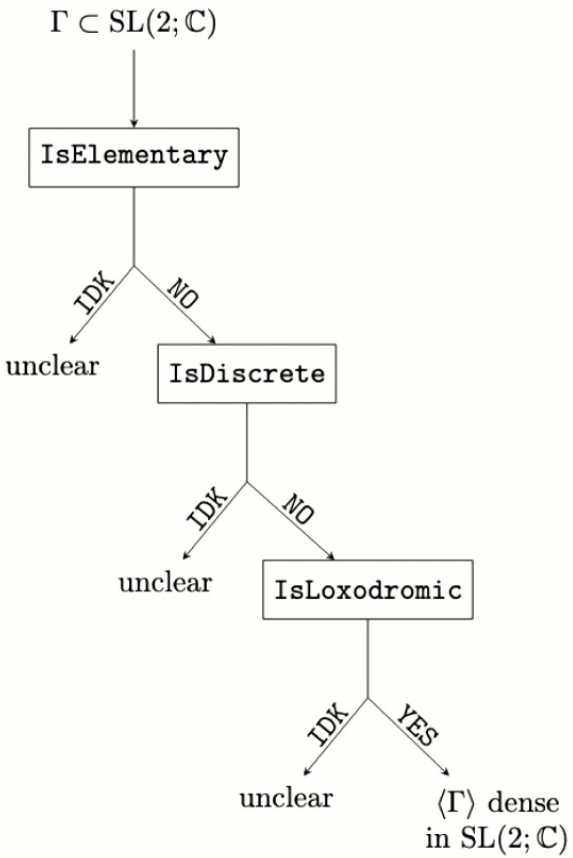
... non-elementary if "$\Gamma$ can do more than $SU(2)$"

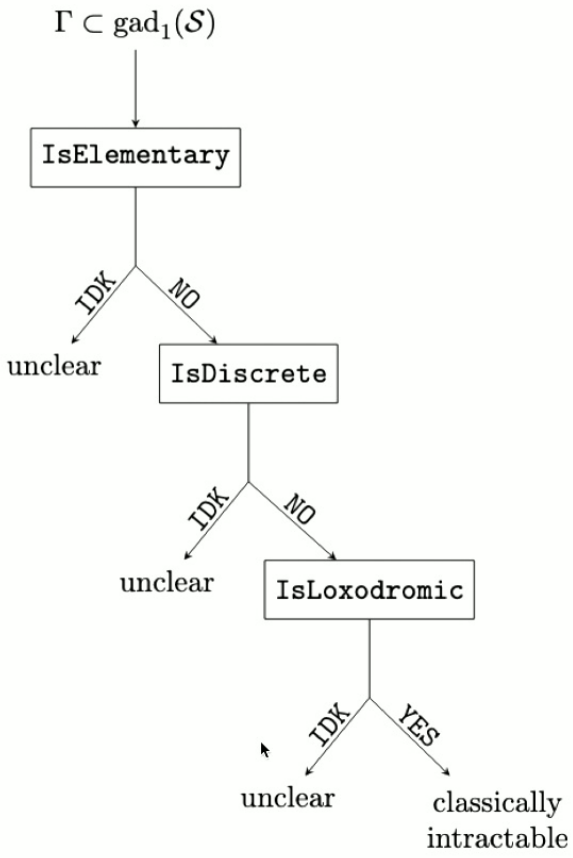
... non-discrete if $\langle \Gamma \rangle$ is "topologically interesting"

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

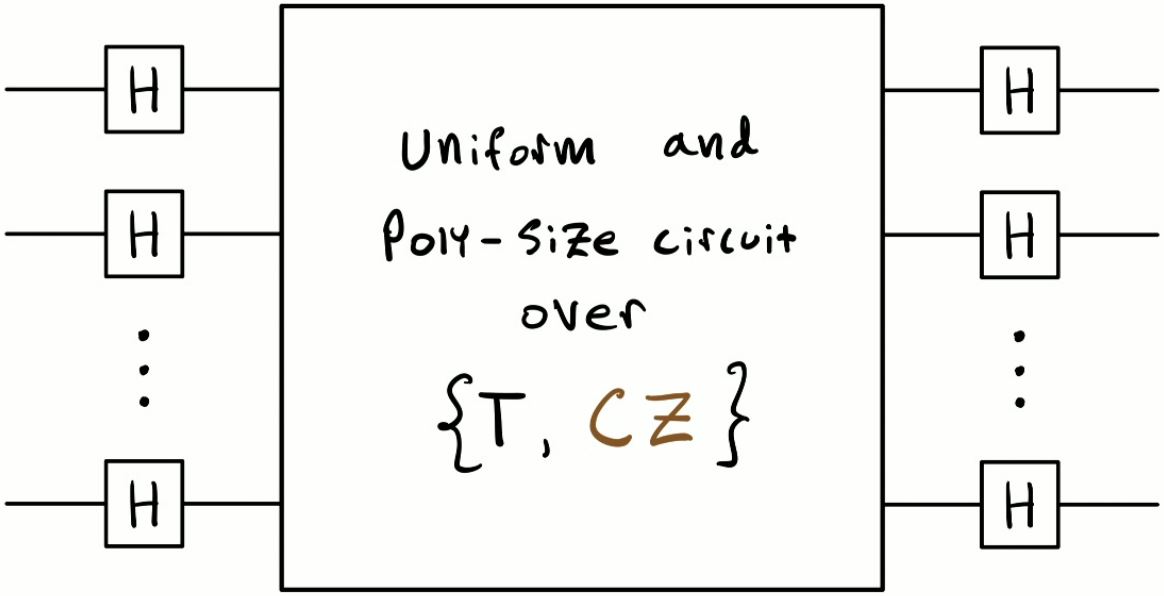
**Algorithm 2** `IsDiscrete`

**Input:** Finite set $\Gamma \subset \mathrm{SL}(2;\mathbb{C})$ such that $\langle \Gamma \rangle \leq \mathrm{SL}(2;\mathbb{C})$
**Output:** `NO` if $\langle \Gamma \rangle$ is non-discrete, `IDK` otherwise
**for** $g, h \in \Gamma$ **do**
  **if** `IsElementary`$(\{g,h\}) =$ `NO` and $\left|\mathrm{tr}^2(g) - 4\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1}) - 2\right| < 1$ **then**
    return `NO`
  **if** $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$ and $\left|\mathrm{tr}^2(g) - 2\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1}) - 1\right| < 1$ **then**
    return `NO`
  **if** $\mathrm{tr}(ghg^{-1}h^{-1}) = 1$ and $\mathrm{tr}^2(g) \neq 2$ and $\left|\mathrm{tr}^2(g) - 2\right| \leq 1/2$ **then**
    return `NO`
  **if** $\mathrm{tr}^2(g) \neq 1$ and $\left|\mathrm{tr}^2(g) - 1\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1})\right| < 1$ **then**
    return `NO`
  **if** $\mathrm{tr}^2(g) = 1$ and $\left|\mathrm{tr}(ghg^{-1}h^{-1})\right| \leq 1/2$ and $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 0$ **then**
    return `NO`
  **if** $\mathrm{tr}^2(g) = 1$ and $\left|\mathrm{tr}(ghg^{-1}h^{-1}) - 1\right| \leq 1/2$ and $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$ **then**
    return `NO`
  **if** $\mathrm{tr}(ghg^{-1}h^{-1}) \neq 1$ and $\left|\mathrm{tr}^2(g) - \mathrm{tr}(ghg^{-1}h^{-1})\right| + \left|\mathrm{tr}(ghg^{-1}h^{-1}) - 1\right| < 1$ **then**
    return `NO`
  **if** $\mathrm{tr}(ghg^{-1}h^{-1}) = 1$ and $\mathrm{tr}^2(g) \neq 1$ and $\left|\mathrm{tr}^2(g) - 1\right| \leq 1/2$ **then**
    return `NO`
return `IDK`


$\Gamma \subset \mathrm{SL}(2;\mathbb{C})$
IsElementary
IDK
NO
unclear
IsDiscrete
IDK
NO
unclear
IsLoxodromic
IDK
YES
unclear
$\langle\Gamma\rangle$ dense in $\mathrm{SL}(2;\mathbb{C})$


$\Gamma \subset \mathrm{gad}_1(\mathcal{S})$
IsElementary
IDK
NO
unclear
IsDiscrete
IDK
NO
unclear
IsLoxodromic
IDK
YES
unclear
classically intractable

# Instantaneous Quantum Polynomial



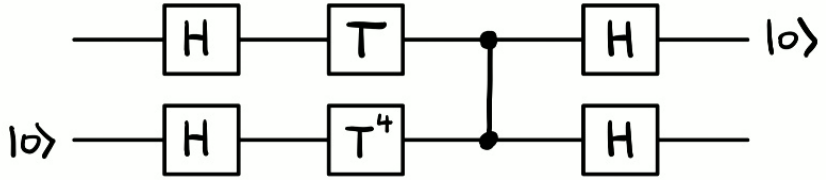

$$S_{IQP} = \{HTH,\ H \otimes H\ CZ\ H \otimes H\}$$

## Theorem (FkG, 2024):

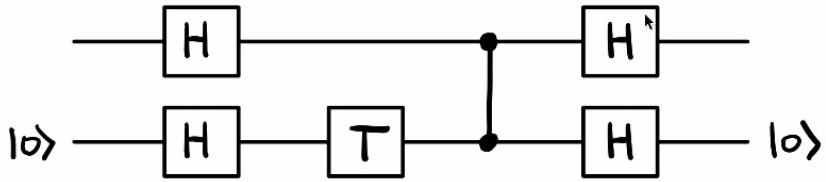
The following gadgets over $S_{IQP}$ generate a dense subgroup of $SL(2;\mathbb{C})$:

$\gamma_1 =$

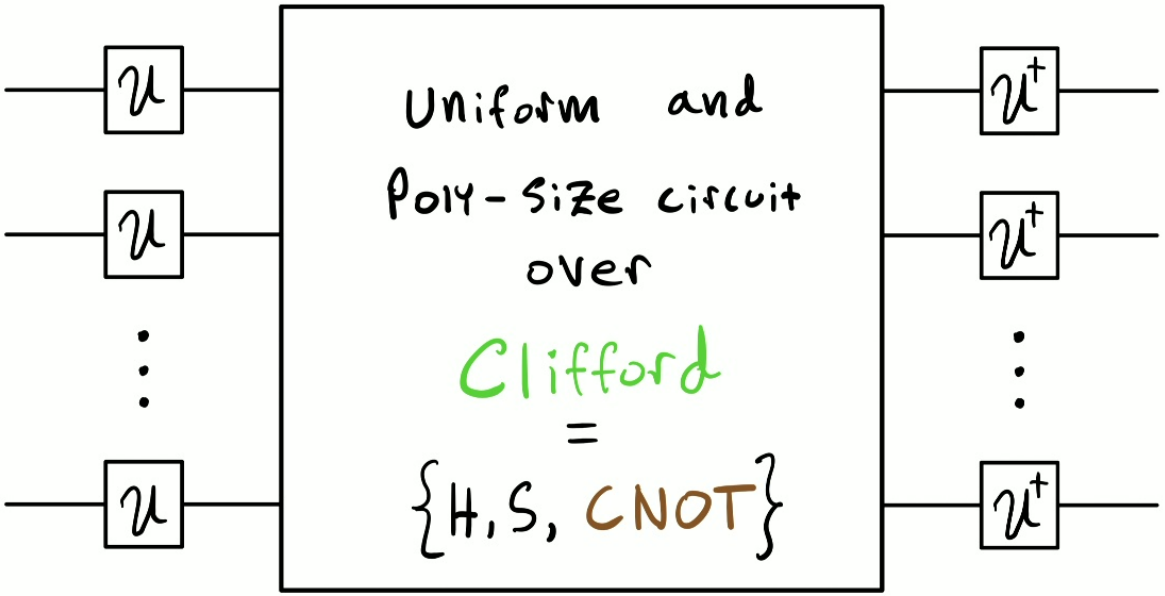

$\gamma_2 =$




$\gamma_3 =$



# Conjugated Clifford Circuits

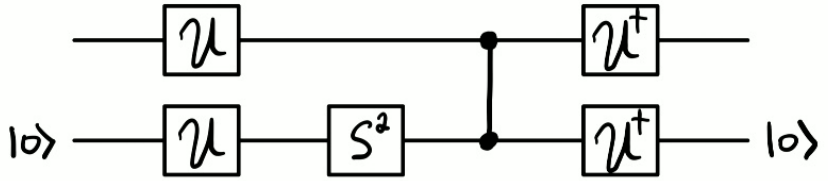



$$S_{ccc}(U) = \{UHU^\dagger,\ USU^\dagger,\ U\otimes U\ CNOT\ U^\dagger\otimes U^\dagger\}$$

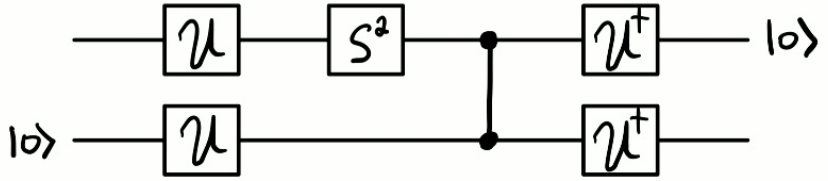
**Theorem (FkG, 2024):**

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

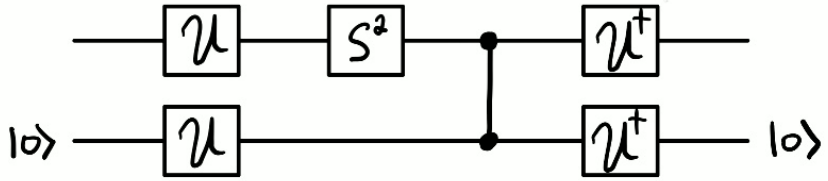
$\gamma_1 =$



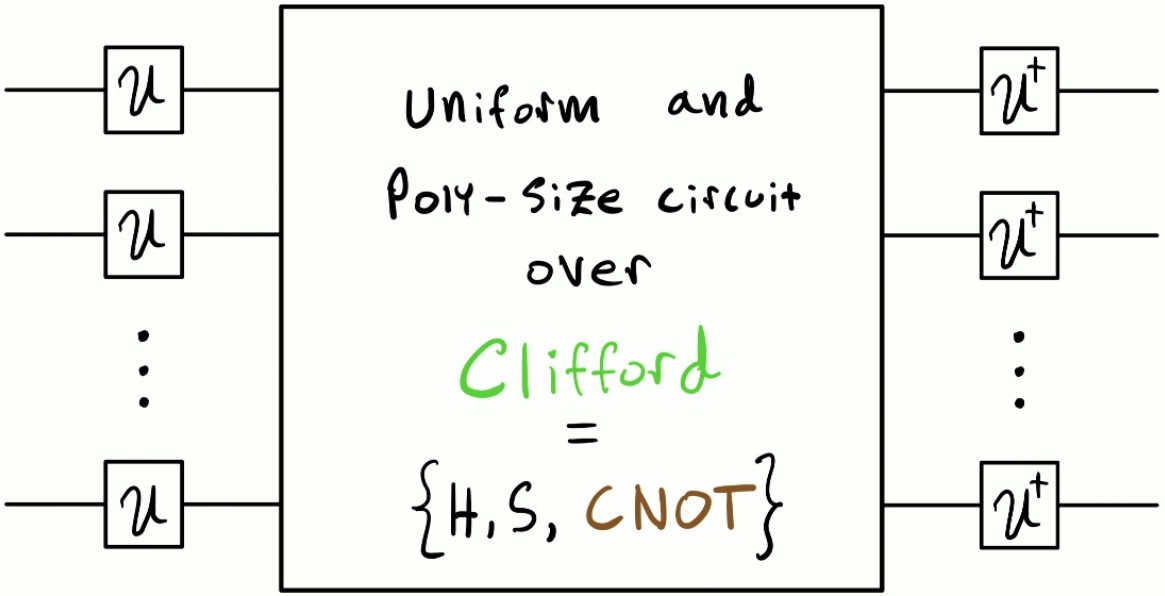

$\gamma_2 =$



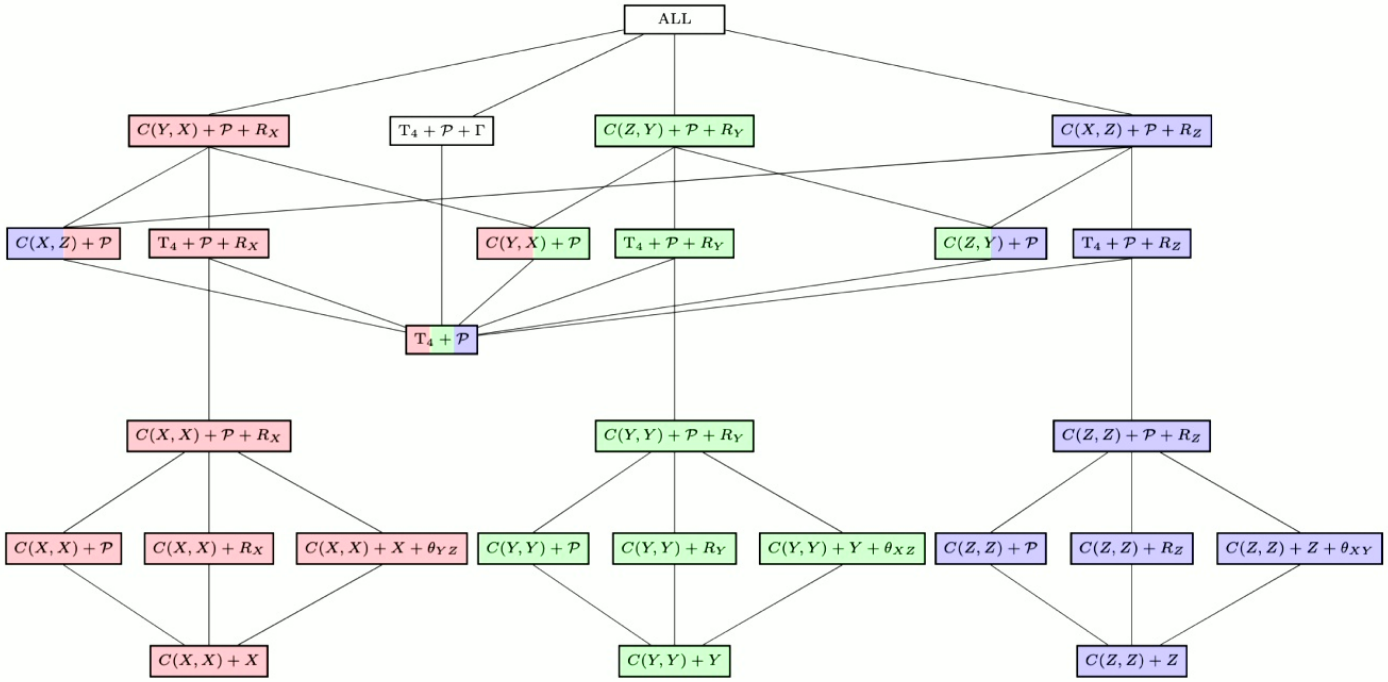

$\gamma_3 =$



# Conjugated Clifford Circuits




$$S_{ccc}(U) = \{UHU^\dagger,\ USU^\dagger,\ U\otimes U\ CNOT\ U^\dagger\otimes U^\dagger\}$$

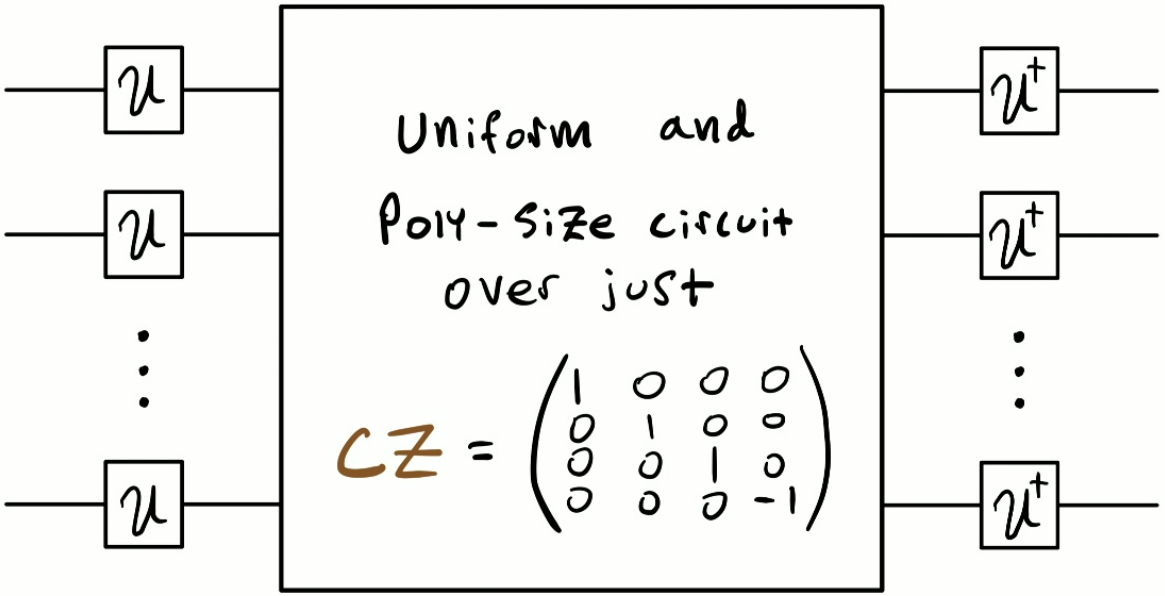



(GS, 2022)

**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 $S_{CZ}(\mathcal{U})$ afford a weak $(\sqrt{2}-1)$-quantum advantage

$\Longleftrightarrow$

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

where

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

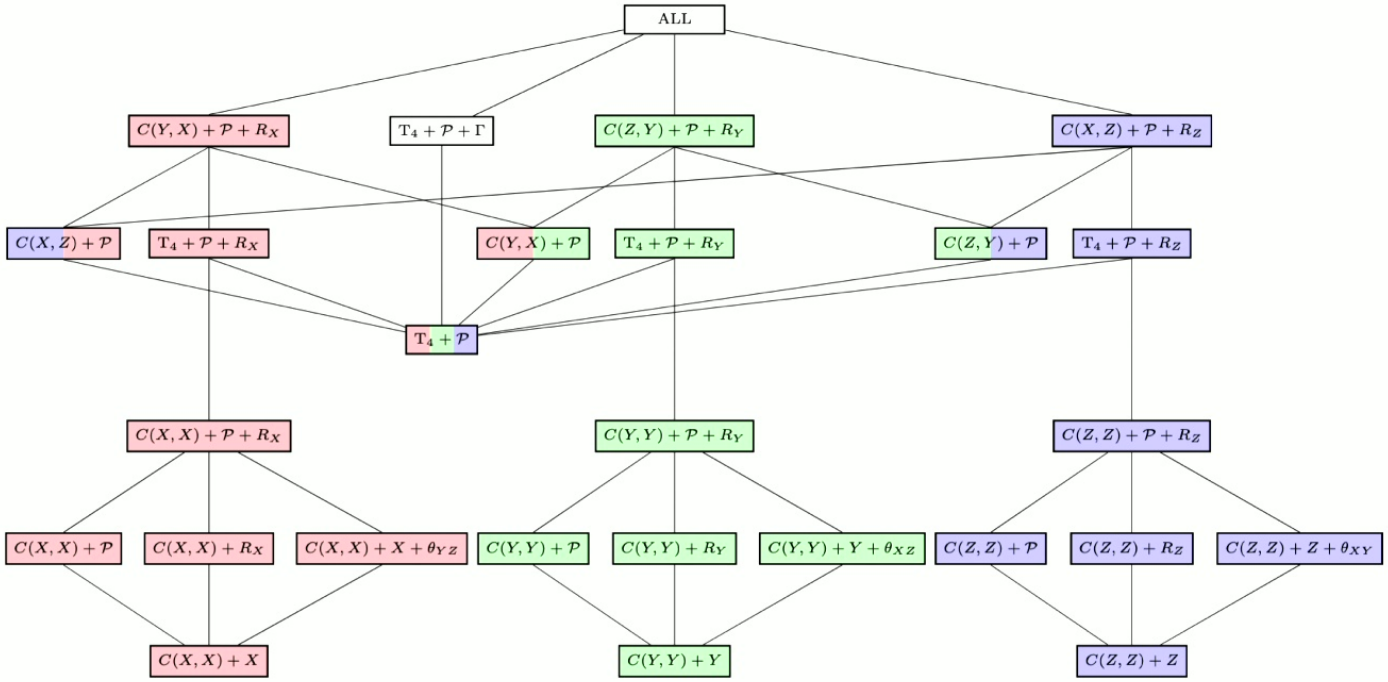
# Some Open Questions

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

Thank You!

Paper ⇝

Slides ⇝




(GS, 2022)

**Theorem (FKG, 2024):**

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