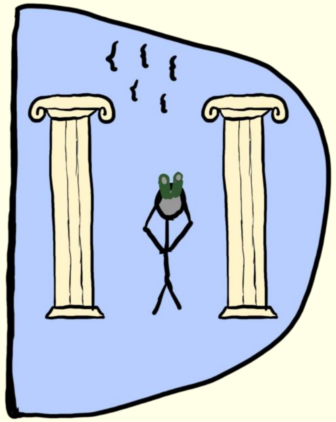
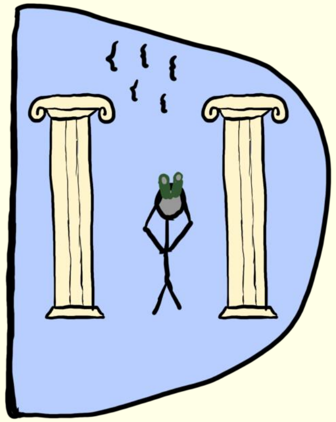
Translating Between the Common Haar State Model and the Unitary Model

Eli Goldin, Mark Zhandry

Oracle Separations

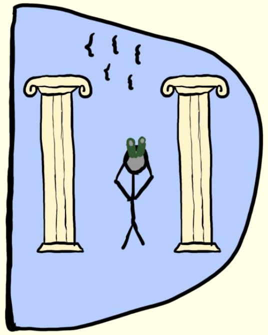
 - arbitrary inefficient function on strings

Oracle Separations

 - arbitrary inefficient function on strings

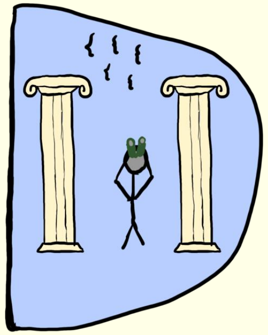
e.g. Random Oracle

Oracle Separations

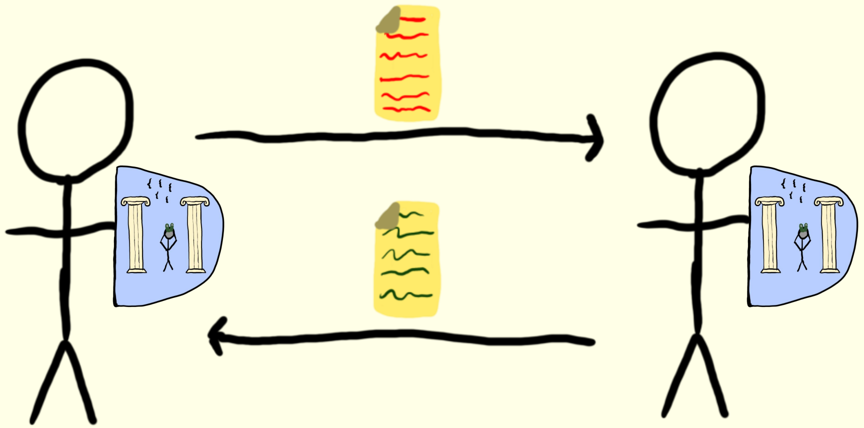
Primitive exists in 

Oracle Separations

Primitive exists in

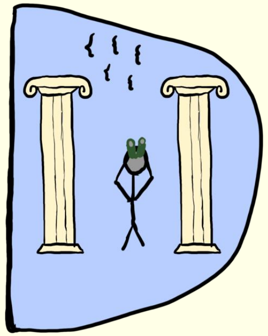


if you have

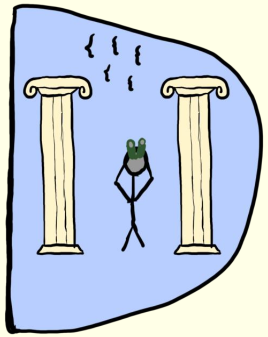


secure against

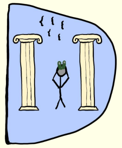
[IR89]

 = Random Oracle

[IR89]



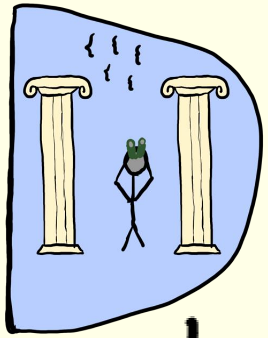
= Random Oracle



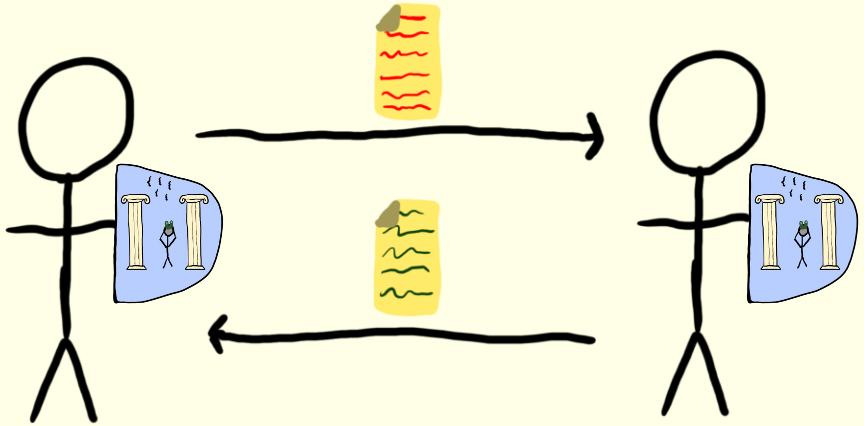
(x)

OWFs exist

[IR89]

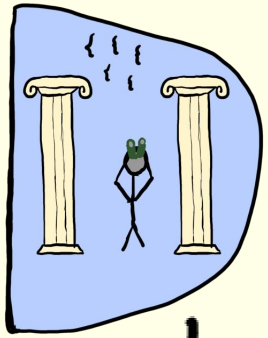
 = Random Oracle

OWFs exist

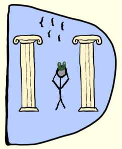


KE does not

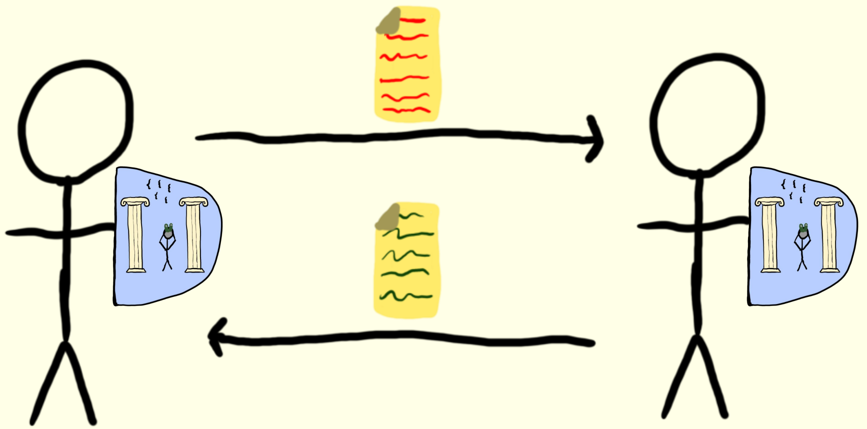
[IR89]



= Random Oracle



(x)

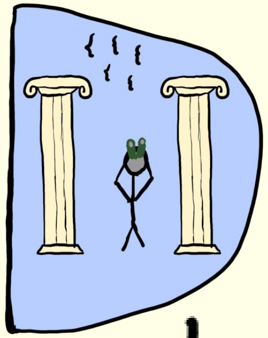


OWFs exist

KE does not

Cannot build KE from OWF in "black-box" way!

[IR89]



P_1 exists

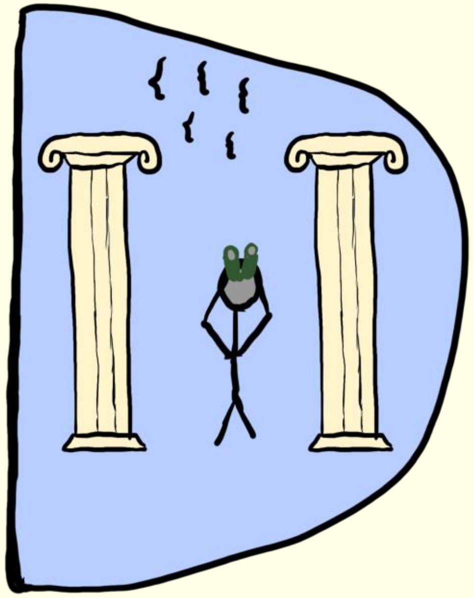
P_2 does not

Cannot build P_2 from P_1 in "black-box" way!

Quantum Oracles

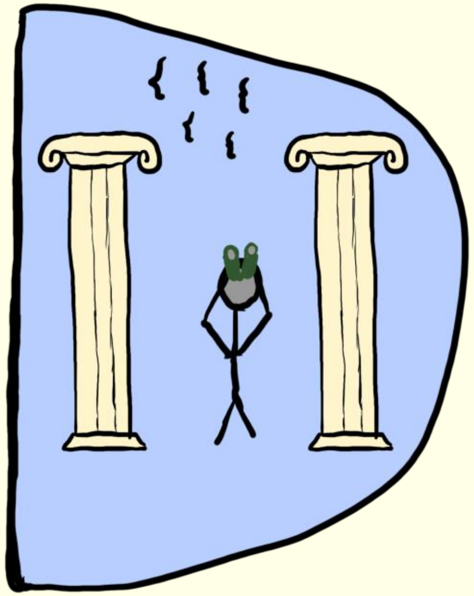
To separate quantum primitives, need quantum accessible oracles!

Quantum Oracles - Modeling



(quantum accessible) classical oracle

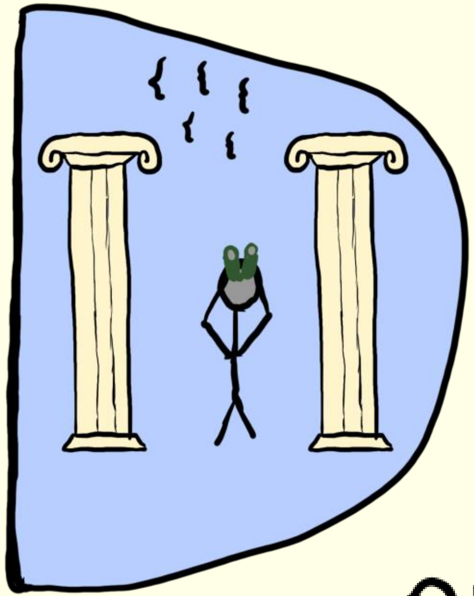
Quantum Oracles - Modeling



(quantum accessible) classical oracle

functionality: any function on strings

Quantum Oracles - Modeling

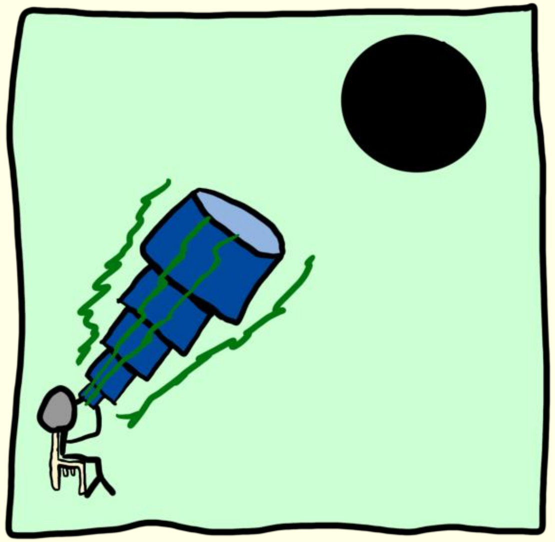


(quantum accessible) classical oracle

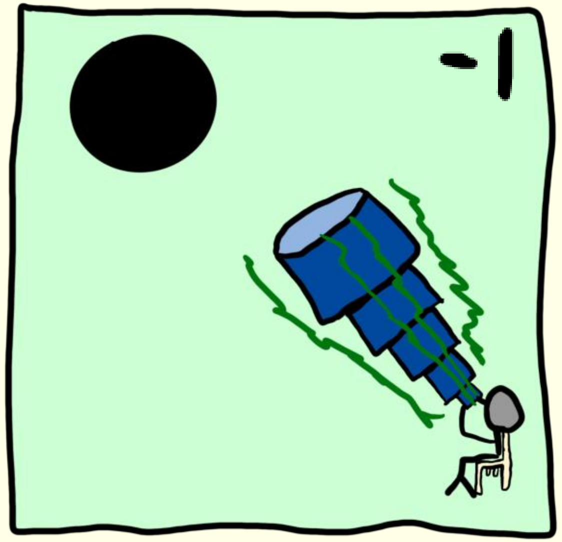
functionality: any function on strings

oracle separation rules out any quantum black-box constructions

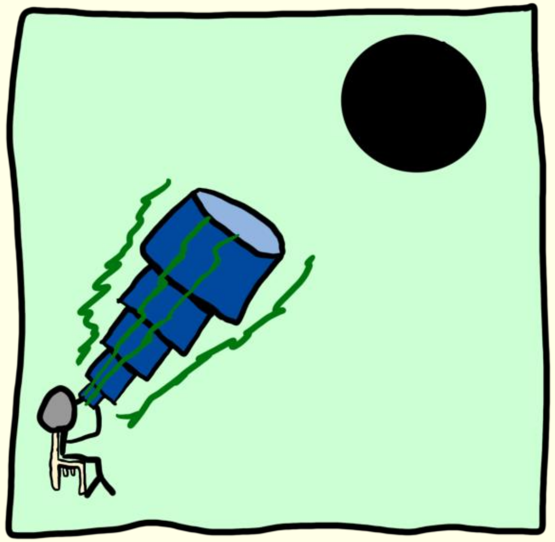
Quantum Oracles - Modeling



Unitary oracle

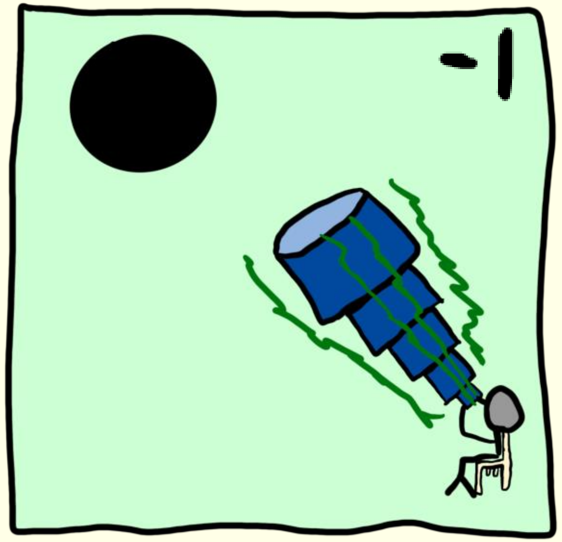


Quantum Oracles - Modeling

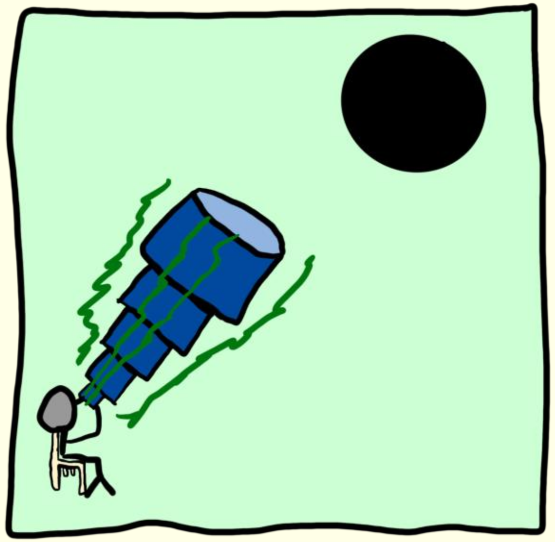


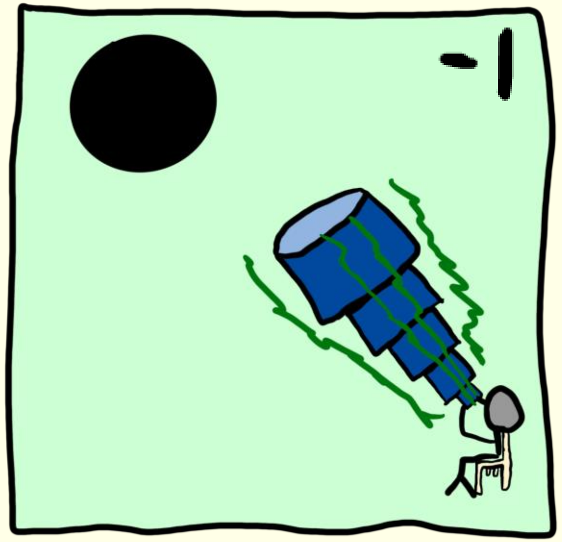
Unitary oracle

functionality: any unitary operation and its inverse



Quantum Oracles - Modeling



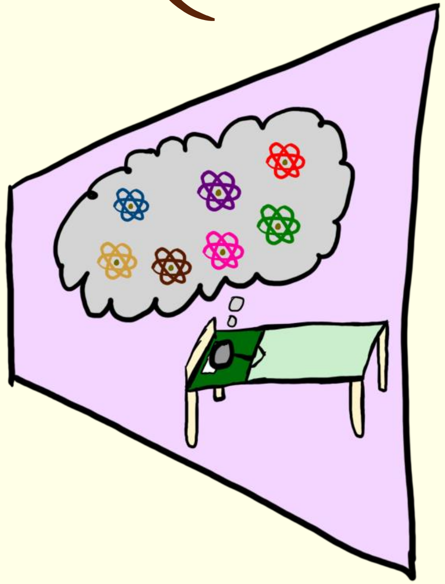


Unitary oracle

functionality: any unitary operation and its inverse

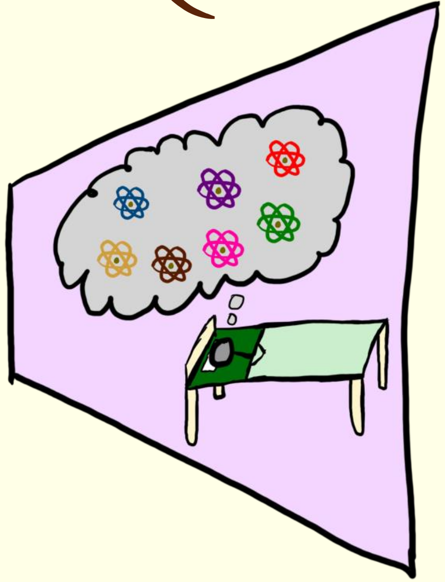
oracle separation rules out **most** black-box constructions

Quantum Oracles - Modeling



State oracle

Quantum Oracles - Modeling



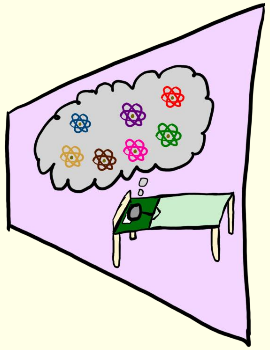
State oracle

functionality: takes in no input, outputs some fixed state

Common Haar Random State Model

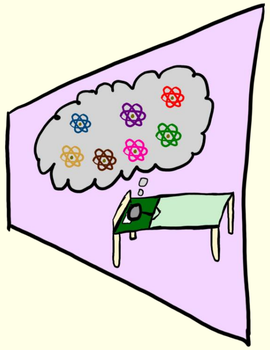
CHRS: nothing $\rightarrow |\varphi\rangle$

fixed random state



Common Haar Random State Model

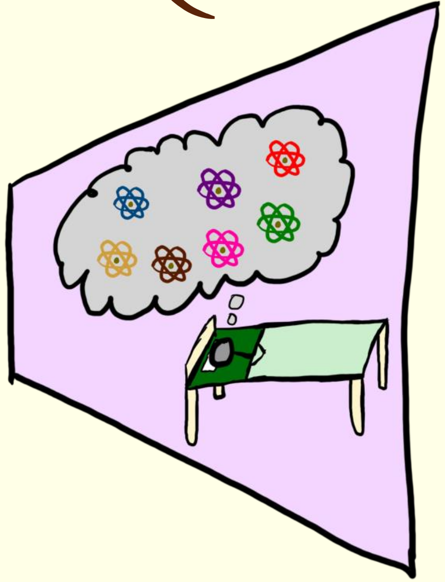
CHRS: nothing $\rightarrow |\varphi\rangle$



- NOT reversible

fixed random state

Quantum Oracles - Modeling

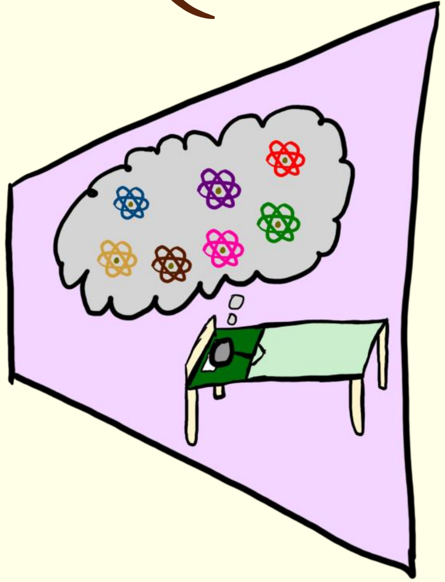


State oracle

functionality: takes in no input, outputs some fixed state

Oracle separation rules out black-box constructions which do not "run the primitive in reverse"

Quantum Oracles - Modeling

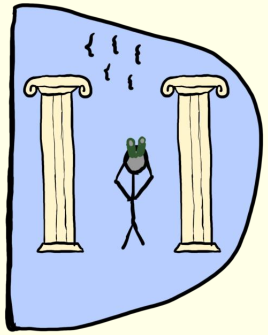


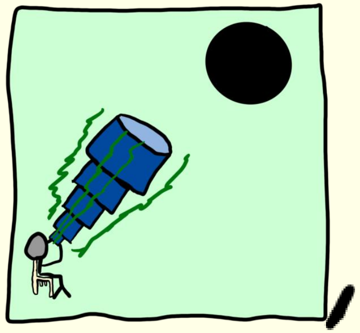
State oracle

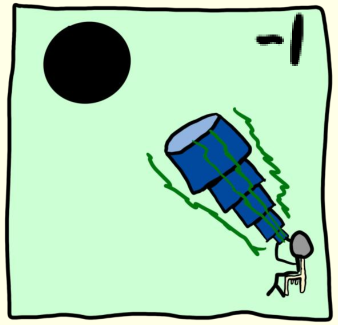
functionality: takes in no input, outputs some fixed state

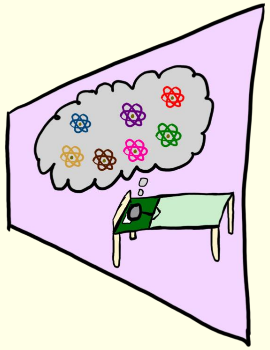
Oracle separation rules out black-box constructions which do not "run the primitive in reverse" - fairly common

Quantum Oracle Separations - Ranked

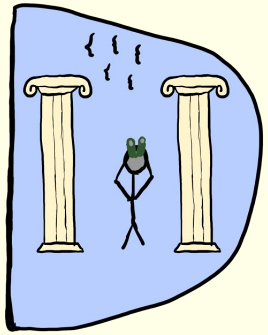




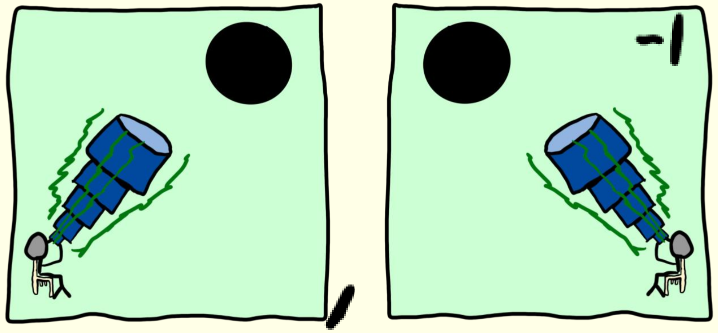


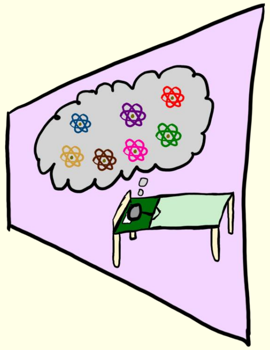


Quantum Oracle Separations - Ranked

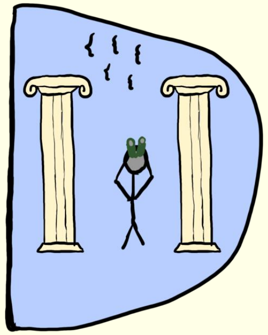


best we can hope for

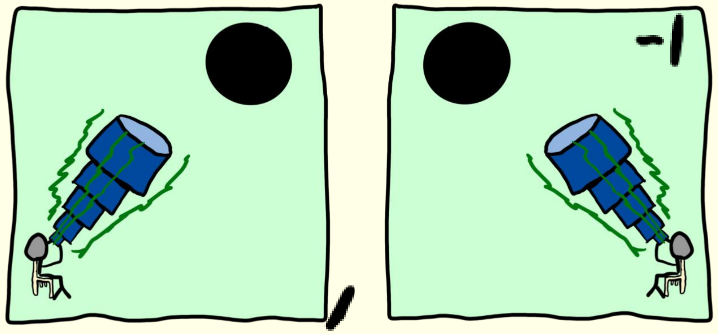




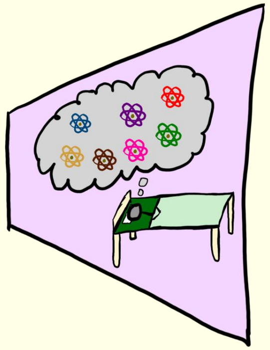
Quantum Oracle Separations - Ranked



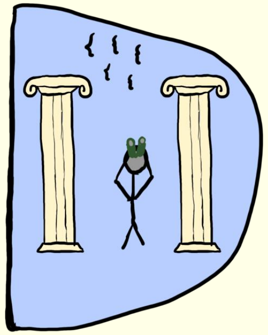
best we can hope for



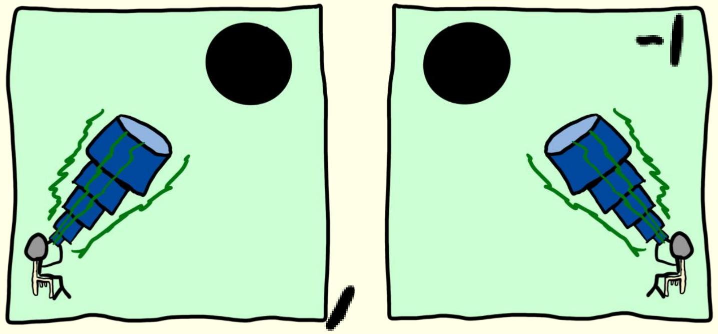
good enough



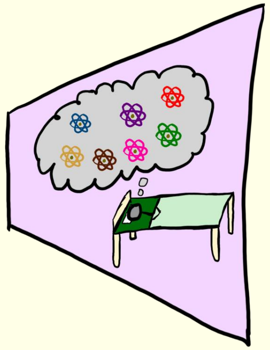
Quantum Oracle Separations - Ranked



best we can hope for



good enough



preliminary result

Common Haar Random State Model

$\text{CHRS}: \text{nothing} \rightarrow |\varphi\rangle$

exists

does NOT exist

Common Haar Random State Model

CHRS: nothing $\rightarrow |\varphi\rangle$

1-copy pseudorandom states	
exists	does NOT exist

Common Haar Random State Model

CHRS: nothing $\rightarrow |\varphi\rangle$

1-copy pseudorandom states

quantum commitments

exists

does NOT exist

Common Haar Random State Model

CHRS: nothing $\rightarrow |\varphi\rangle$

1-copy pseudorandom states

quantum commitments

...

exists

does NOT exist

Common Haar Random State Model

CHRS: nothing $\rightarrow |\varphi\rangle$

1-copy pseudorandom states	poly-copy pseudorandom states
quantum commitments	
...	
exists	does NOT exist

Common Haar Random State Model

CHRS: nothing $\to |\varphi\rangle$

1-copy pseudorandom states

quantum commitments

...

exists

poly-copy pseudorandom states

classical communication (QCCC) cryptography

does NOT exist

Common Haar Random State Model

CHRS: nothing $\to |\varphi\rangle$

1-copy pseudorandom states	poly-copy pseudorandom states
quantum commitments	classical communication (QCCC) cryptography
...	...
exists	does NOT exist

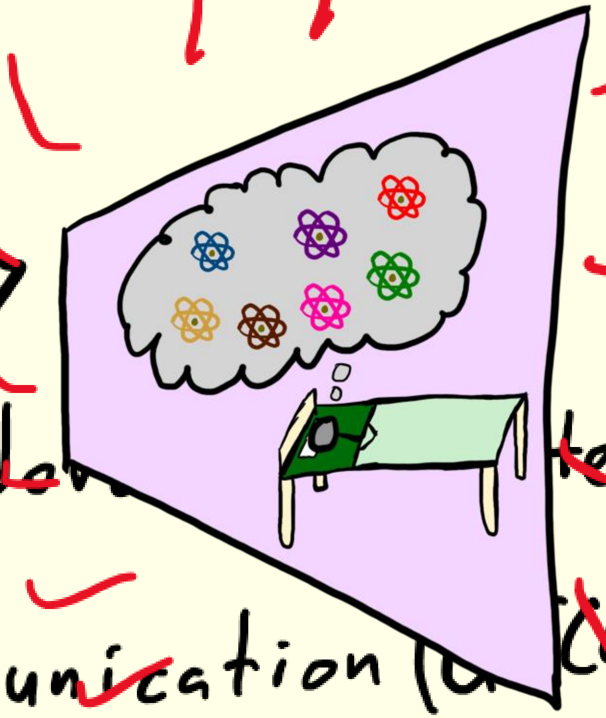
Common Haar Random State Model

CHRS: nothing $\rightarrow |\varphi\rangle$

1-copy pseudorandom states	$\not\Rightarrow$	poly-copy pseudorandom states
quantum commitments		classical communication (QCCC) cryptography
...		...
exists		does NOT exist

Common Haar Random State Model

CHRS: nothing $\rightarrow |\varphi\rangle$

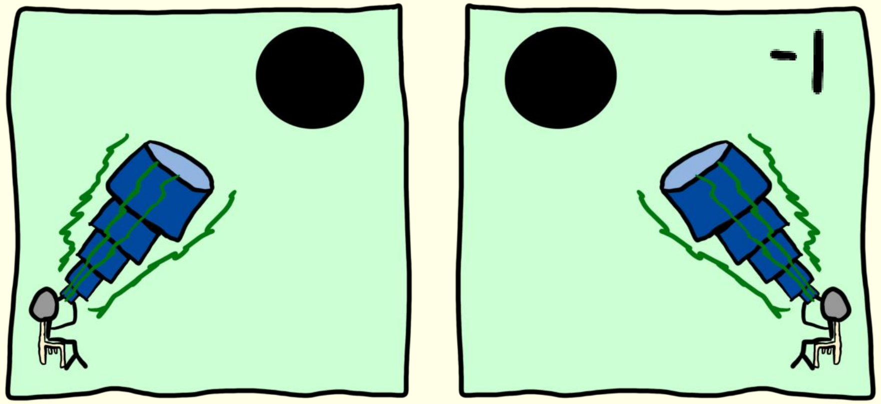


1-copy pseudorandom states	$\not\Rightarrow$	poly-copy pseudorandom states
quantum commitments		classical communication cryptography
...		...
exists		does NOT exist

Common Haar Random State Model

Big Question: Can we make these separations unitary?

Common Haar Random State Model

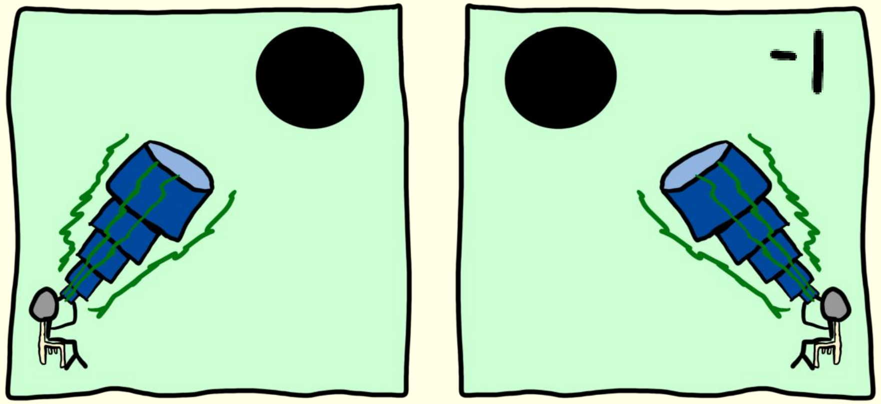


[CCS25]

[BCN25]

[BMM+25]

Common Haar Random State Model



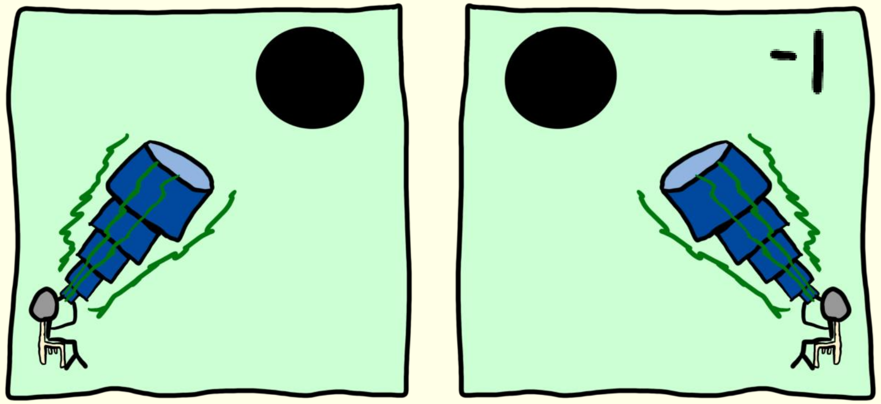
[CCS25]

[BCN25]

SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$

[BMM+25]

Common Haar Random State Model



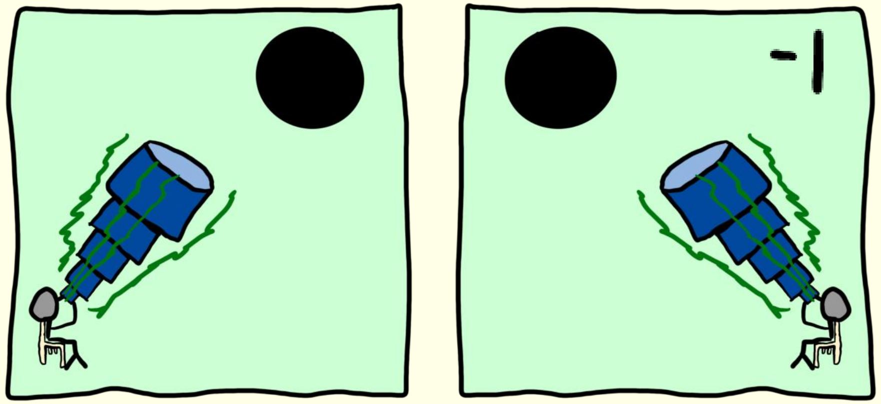
[CCS25]
[BCN25]

SWAP: $|0\rangle \longleftrightarrow |\varphi\rangle$

[BMM+25]

subset swap oracle

Common Haar Random State Model



proof breaks down

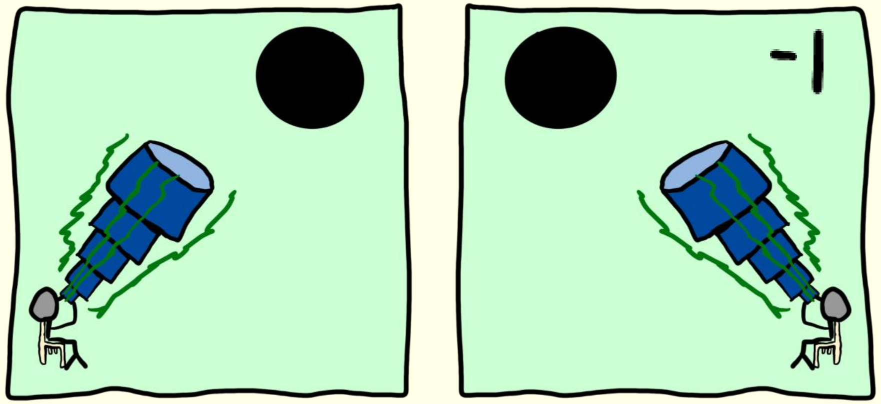
~~[CCS25]~~
~~[BCN25]~~

~~SWAP:~~ $\cancel{|0\rangle \longleftrightarrow |\varphi\rangle}$

[BMM+25]

subset swap oracle

Common Haar Random State Model



proof breaks down :(

~~[CCS25]~~
~~[BCN25]~~ ~~SWAP: $|0\rangle \leftrightarrow |\psi\rangle$~~

[BMM+25] subset swap oracle ✓

Conjecture

CHRS: nothing $\rightarrow |\psi\rangle$

SWAP: $|0\rangle \leftrightarrow |\psi\rangle$

Conjecture: all oracle separations in CHRS also hold in SWAP.

i.e. P exists in CHRS

$\iff$ P exists in SWAP

Our Results

Thm*: P exists in CHRS

$\Rightarrow$ P exists in SWAP.

Our Results

Thm*: P exists in CHRS

$\Rightarrow$ P exists in SWAP.

Thm*: P exists in SWAP

$\Rightarrow$ P exists in CHRS−.

Our Results

Thm*: P exists in CHRS

$\Rightarrow$ P exists in SWAP.

Thm*: P exists in SWAP

$\Rightarrow$ P exists in CHRS-.

similar; most proofs work!

Our Results

Thm*: P exists in CHRS

$\Rightarrow$ P exists in SWAP.

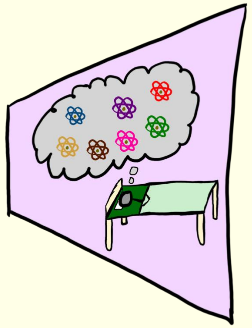
generalizes to all state oracles!

Thm*: P exists in SWAP

$\Rightarrow$ P exists in CHRS−.

similar, most proofs work!

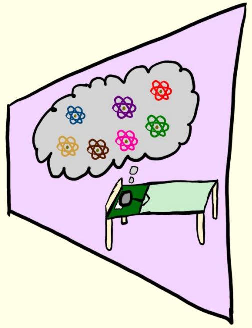
Unitary separation template

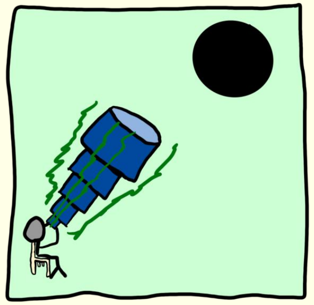


CHRS

P_1	P_2
exists	does NOT exist

Unitary separation template





CHRS

P_1 exists

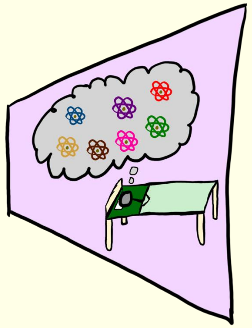
P_2 does NOT exist

SWAP

P_1 exists

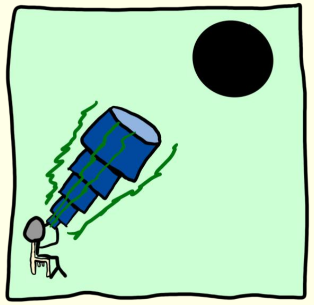
FREE

Unitary separation template



CHRS

P_1 exists | P_2 does NOT exist



SWAP

P_1 exists | P_2 does NOT exist

FREE

adapt proof

CHRS- Model

For $|\psi\rangle$ any state,

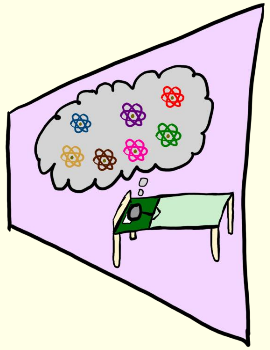
define $|\psi_-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |\psi\rangle\right)$.

CHRS- Model

For $|\varphi\rangle$ any state,
define $|\varphi_-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |\varphi\rangle\right)$.

CHRS-: nothing $\rightarrow |\varphi_-\rangle$

fixed Haar random $|\varphi\rangle$

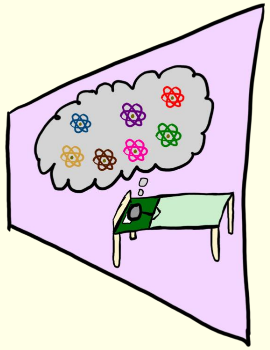


CHRS- Model

For $|\varphi\rangle$ any state,
define $|\varphi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |\varphi\rangle)$.

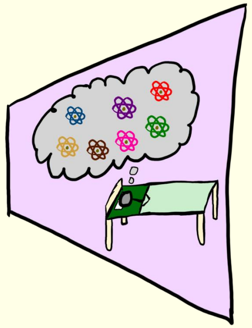
CHRS-: nothing $\rightarrow |\varphi_-\rangle$

fixed Haar random $|\varphi\rangle$



STATE ORACLE!

Unitary separation template

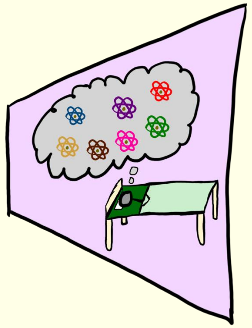


CHRS

P_2

does NOT exist

Unitary separation template

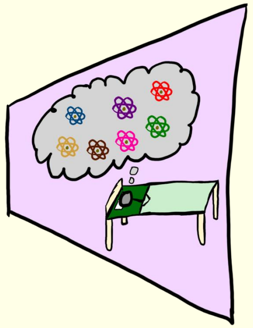


CHRS

P_2

does NOT exist

adapt proof

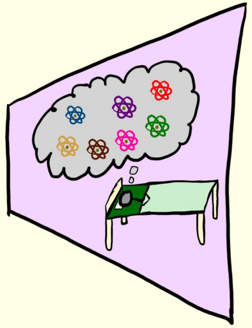


CHRS-

P_2

does NOT exist

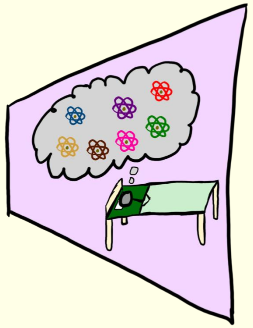
Unitary separation template



CHRS

P_2

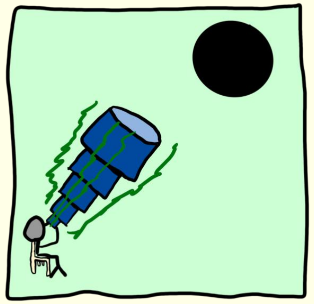
does NOT exist



CHRS-

P_2

does NOT exist



SWAP

P_2

does NOT exist

adapt proof

FREE

Computing SWAP with CHRS-

SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$ CHRS-: nothing $\rightarrow |\varphi_-\rangle$

Computing SWAP with CHRS-

$\mathrm{SWAP}: |0\rangle \leftrightarrow |\varphi\rangle$ $\quad$ CHRS-: nothing $\rightarrow |\varphi_-\rangle$

$$\mathrm{SWAP}|\varphi_-\rangle = \mathrm{SWAP}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|\varphi\rangle\right)$$

Computing SWAP with CHRS-

SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$ CHRS-: nothing $\rightarrow |\varphi_-\rangle$

$$\text{SWAP}|\varphi_-\rangle = \text{SWAP}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|\varphi\rangle\right)$$

$$= \frac{1}{\sqrt{2}}|\varphi\rangle - \frac{1}{\sqrt{2}}|0\rangle$$

Computing SWAP with CHRS-

SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$ CHRS-: nothing $\rightarrow |\varphi_-\rangle$

$$\text{SWAP}|\varphi_-\rangle = \text{SWAP}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|\varphi\rangle\right)$$

$$= \frac{1}{\sqrt{2}}|\varphi\rangle - \frac{1}{\sqrt{2}}|0\rangle = (-1)\cdot|\varphi_-\rangle$$

Computing SWAP with CHRS-

SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$ CHRS-: nothing $\rightarrow |\varphi_-\rangle$

SWAP: $|\varphi_-\rangle \leftrightarrow (-1)\cdot|\varphi_-\rangle$

SWAP is reflection around $|\varphi_-\rangle$.

Computing SWAP with CHRS-

SWAP: $|0\rangle \leftrightarrow |\psi\rangle$ CHRS-: nothing $\rightarrow |\psi_-\rangle$

SWAP: $|\psi_-\rangle \leftrightarrow (-1)\cdot|\psi_-\rangle$

SWAP is reflection around $|\psi_-\rangle$.

[JLS 18, BMM+25]: Given $|\psi_-\rangle|\psi_-\rangle\cdots|\psi_-\rangle$, can compute reflection around $|\psi_-\rangle$.

Computing SWAP with CHRS-

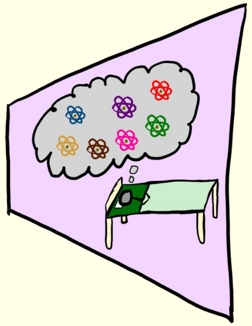
SWAP: $|0\rangle \leftrightarrow |\psi\rangle$ CHRS-: nothing $\to |\psi_-\rangle$

SWAP: $|\psi_-\rangle \leftrightarrow (-1)\cdot|\psi_-\rangle$

SWAP is reflection around $|\psi_-\rangle$.

[JLS 18, BMM+25]: Given $|\psi_-\rangle|\psi_-\rangle\cdots|\psi_-\rangle$, can compute reflection around $|\psi_-\rangle$. DONE

Our Results



CHRS: nothing $\to |\varphi\rangle$

1-copy pseudorandom states

quantum commitments

...

exists

poly-copy pseudorandom states

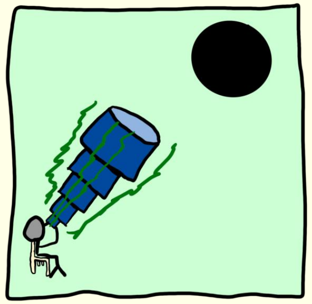
classical communication (QCCC)

cryptography

...

does NOT exist

Our Results



$$\text{SWAP}: |0\rangle \longleftrightarrow |\varphi\rangle$$

1-copy pseudorandom states

quantum commitments

...

exists

poly-copy pseudorandom states

classical communication (QCCC) cryptography

...

does NOT exist

Open questions

Thm*: P exists in CHRS
$\Rightarrow$ P exists in SWAP.

Thm*: P exists in SWAP
$\Rightarrow$ P exists in CHRS$^-$.

Open questions

Thm*: P exists in CHRS

$\Rightarrow$ P exists in SWAP.

Thm*: P exists in SWAP ?

$\Rightarrow$ P exists in CHRS ✗.

Open Questions

P^{CHRS-} secure in CHRS-

$\overset{?}{\Longrightarrow} \exists\, \tilde{P}^{CHRS}$ secure in CHRS?

Open Questions

$P^{CHRS\text{-}}$ secure in CHRS-

$\overset{?}{\Longrightarrow} \exists\, \tilde{P}^{CHRS}$ secure in CHRS?

No candidate!

Open Questions

$P^{\text{CHRS-}}$ secure in CHRS-

$\overset{?}{\Longrightarrow} \exists\, \tilde{P}^{\text{CHRS}}$ secure in CHRS?

Relationships between other quantum oracles?

Open Questions

$P^{\text{CHRS-}}$ secure in CHRS-

$\overset{?}{\Longrightarrow} \exists\, \tilde{P}^{\text{CHRS}}$ secure in CHRS?

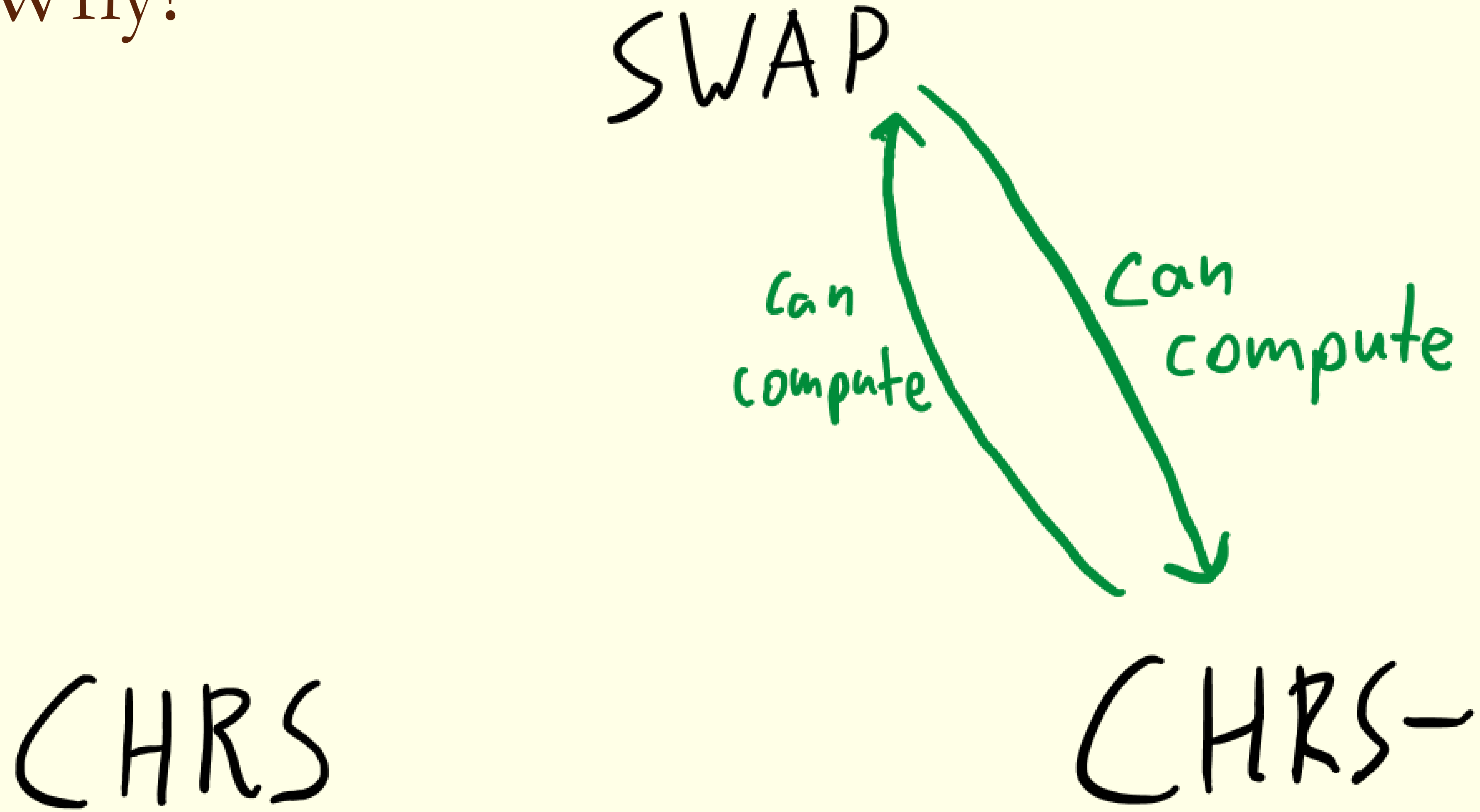
Relationships between other quantum oracles? Haar unitary, QROM, ...

Thank you!

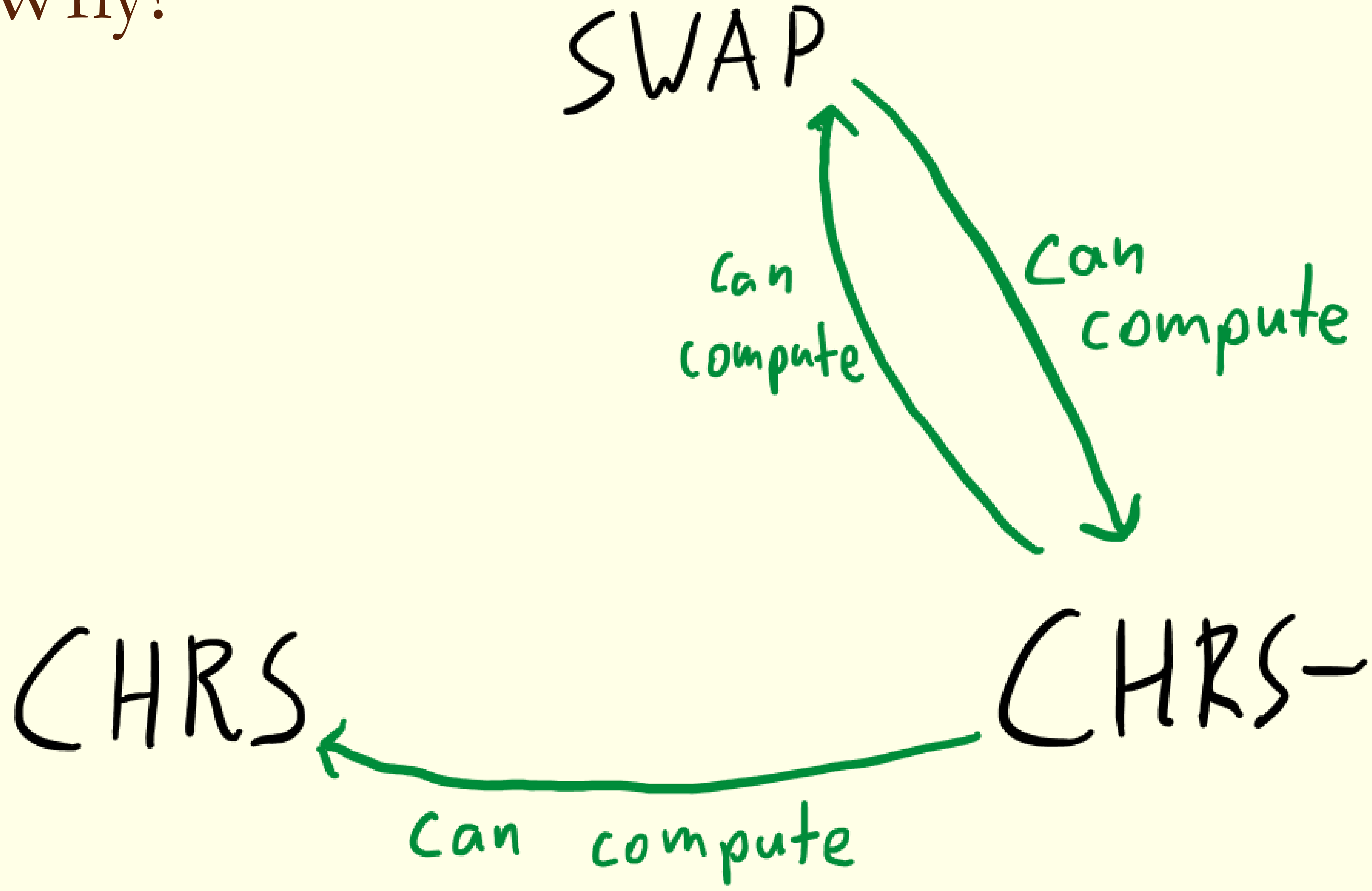
Why?

$$\begin{tikzcd} & \mathrm{SWAP} \arrow[dr, "\text{can compute}"] & \\ \mathrm{CHRS} & & \mathrm{CHRS}^{-} \end{tikzcd}$$

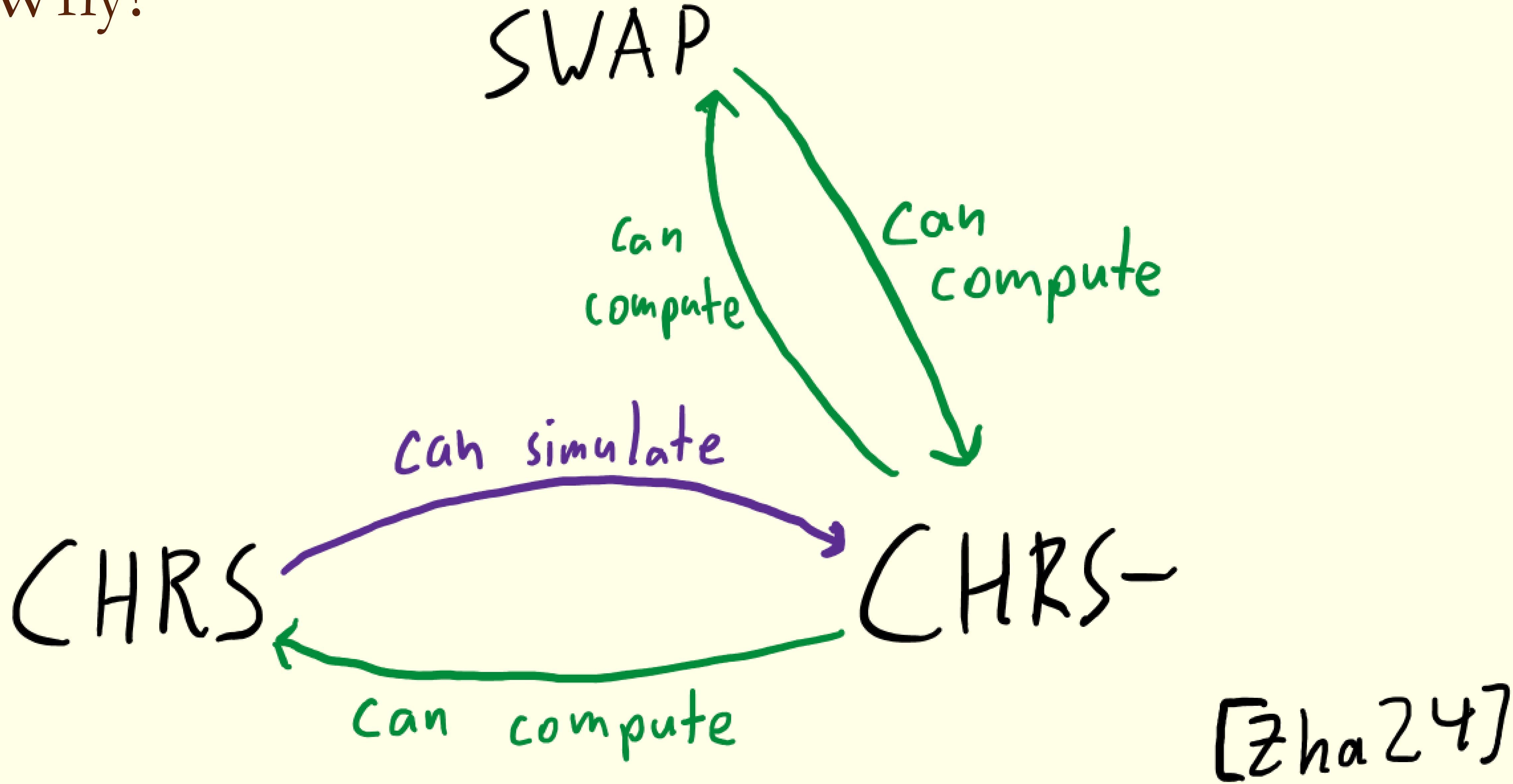
Why?



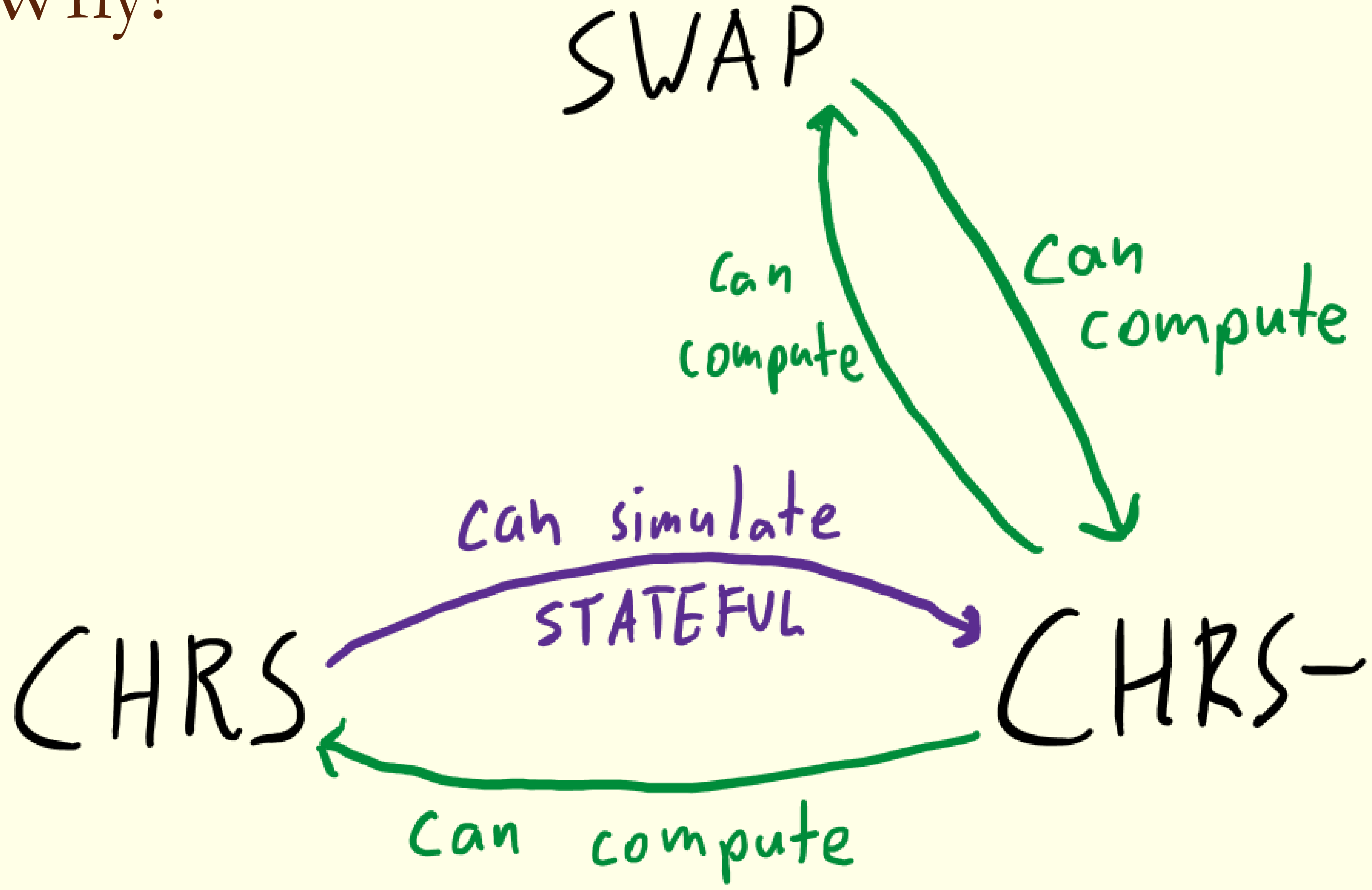
Why?



Why?


SWAP
can compute
can compute
can simulate
CHRS
CHRS-
can compute
[Zha24]

Why?



SWAP
can compute
can compute
can simulate
STATEFUL
CHRS
CHRS-
can compute

[Zha24]

Open Questions

P^{CHRS-} secure in CHRS-

$\overset{?}{\Longrightarrow} \exists\, \tilde{P}^{CHRS}$ secure in CHRS?

Open Questions

$$\mathrm{CHRS} \xrightarrow[\text{STATEFULLY}]{\text{can simulate}} \mathrm{CHRS}^{-}$$

Open Questions

$$\text{CHRS} \xrightarrow[\text{STATEFULLY}]{\text{can simulate}} \text{CHRS-}$$

$$\tilde{P}^{\text{CHRS}} = P^{\text{Sim}^{\text{CHRS}}} \quad ?$$

Open Questions

CHRS $\xrightarrow[\text{STATEFULLY}]{\text{can simulate}}$ CHRS-

can't be used in stateless/deterministic/pure primitives...