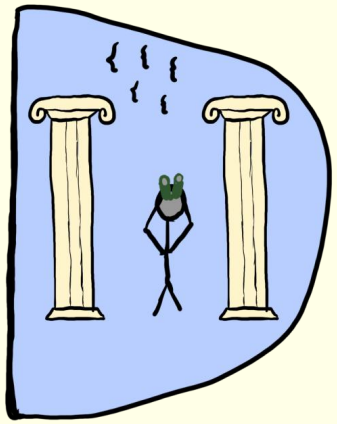
Translating Between the Common Haar State Model and the Unitary Model

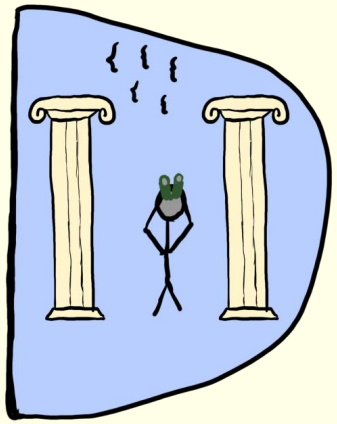
Eli Goldin, Mark Zhandry

Oracle Separations



– arbitrary deterministic function on strings

Oracle Separations



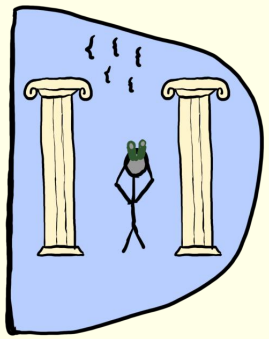
– arbitrary deterministic function on strings

can be distribution.

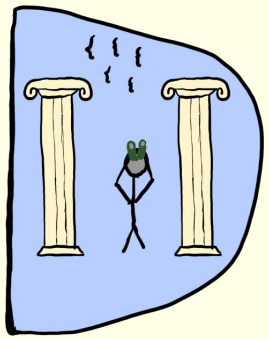
e.g. Random Oracle

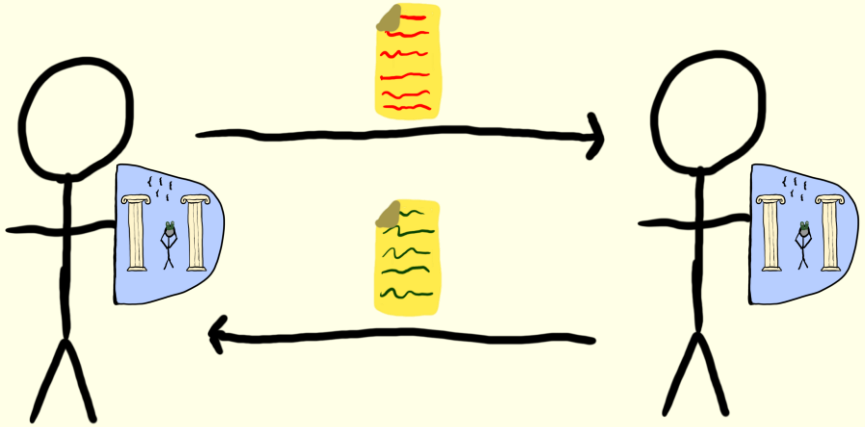
Oracle Separations

Primitive exists in



Oracle Separations

Primitive exists in  if you have



secure against

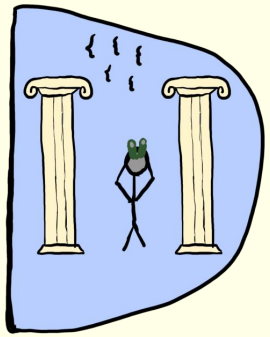


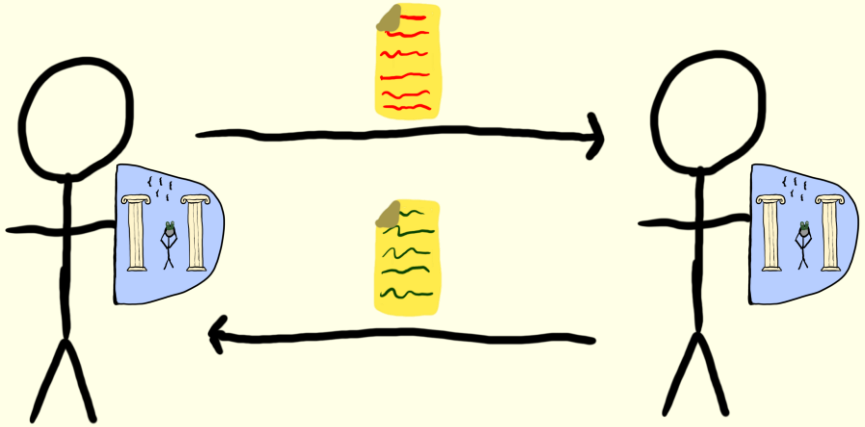
Oracle Separations

"efficient"

= poly calls

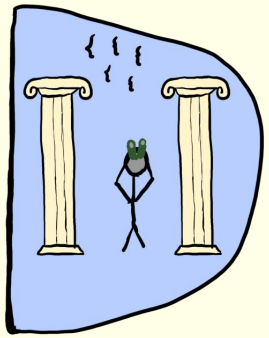
to





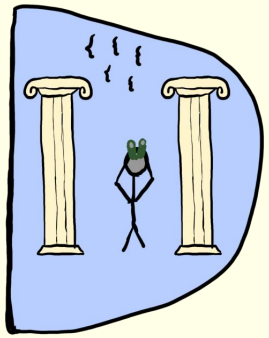


[IR89]



= Random Oracle

[IR89]



= Random Oracle

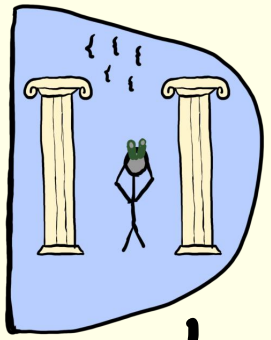




(x)

OWFs exist

[IR89]

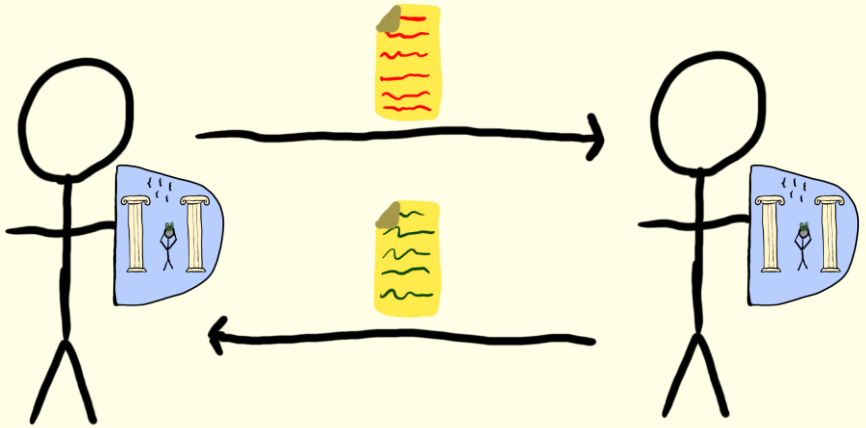


= Random Oracle





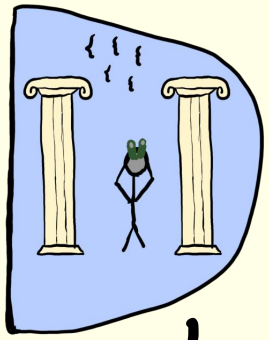
(x)



OWFs exist

KE does not

[IR89]

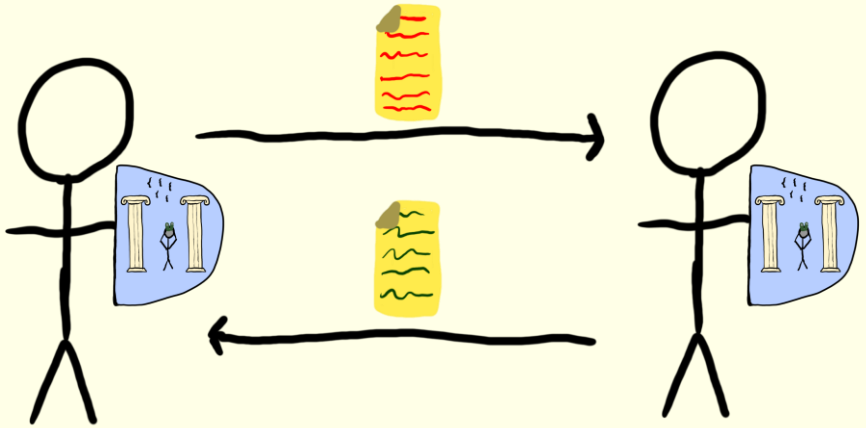


= Random Oracle





(x)



OWFs exist

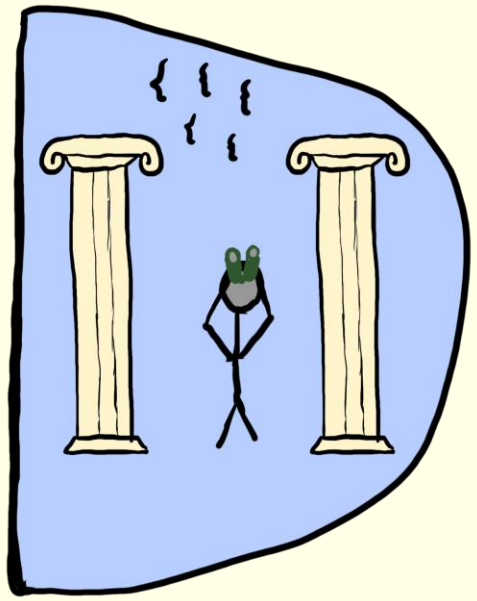
KE does not

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

Quantum Oracles

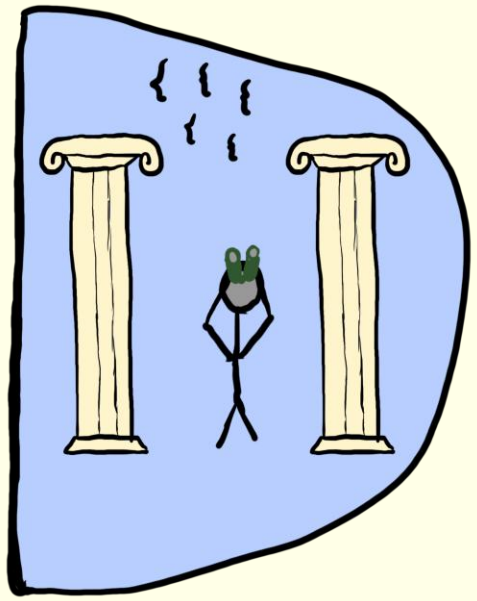
To separate quantum primitives, need quantum accessible oracles!

Quantum Oracles - Modeling



(quantum accessible) classical oracle

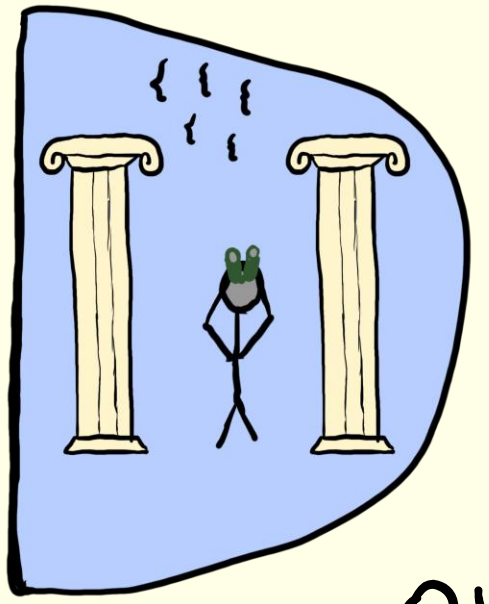
Quantum Oracles - Modeling



(quantum accessible) classical oracle

functionality: any function on strings

Quantum Oracles - Modeling

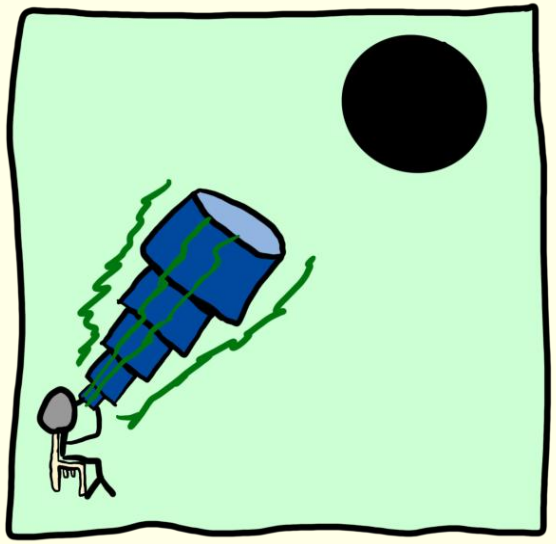


(quantum accessible) classical oracle

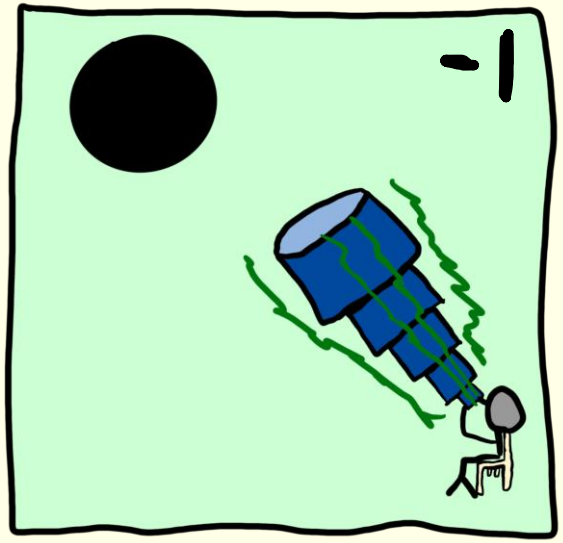
functionality: any function on strings

oracle separation rules out any black-box construction

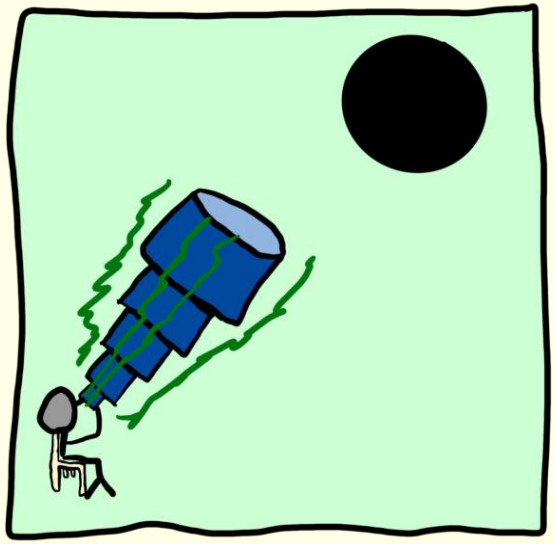
Quantum Oracles - Modeling



Unitary oracle

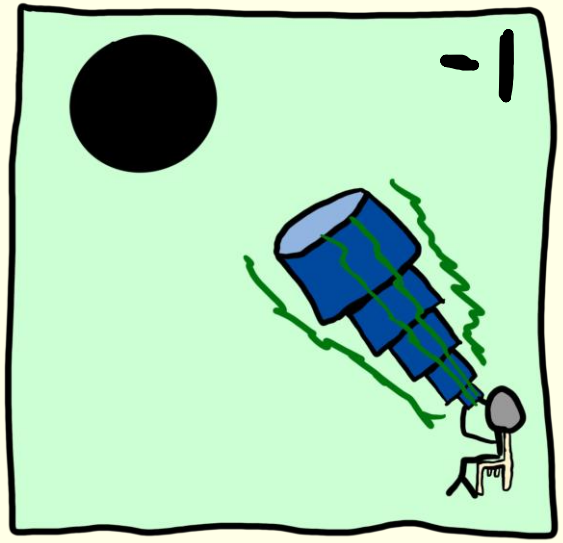


Quantum Oracles - Modeling

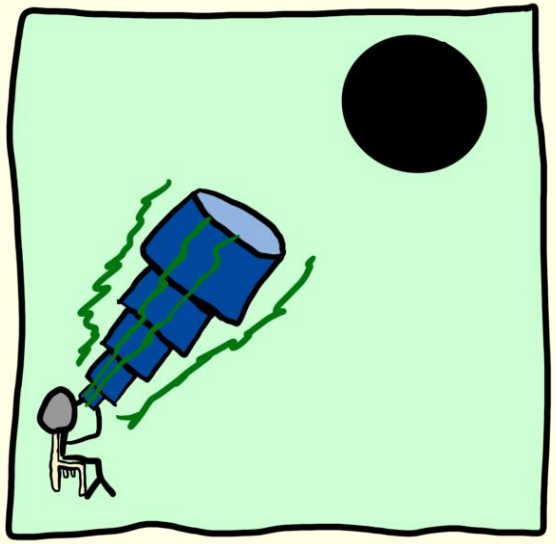


Unitary oracle

functionality: any unitary operation and its inverse

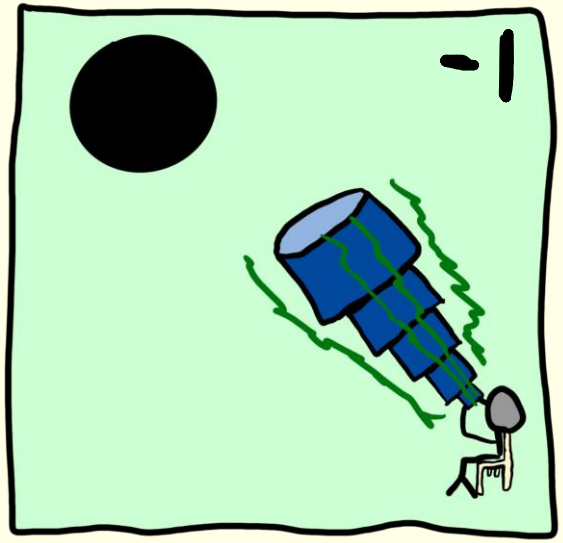


Quantum Oracles - Modeling



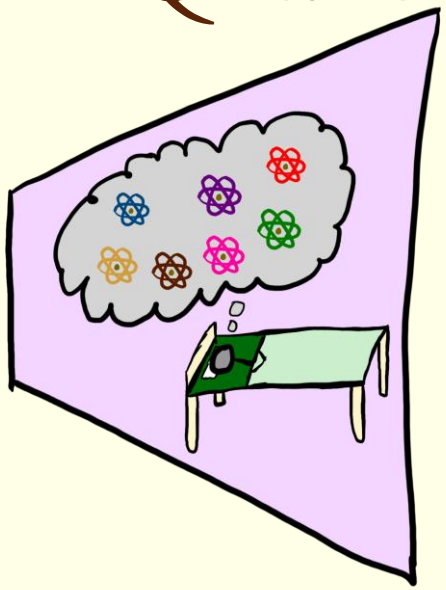
Unitary oracle

functionality: any unitary operation and its inverse



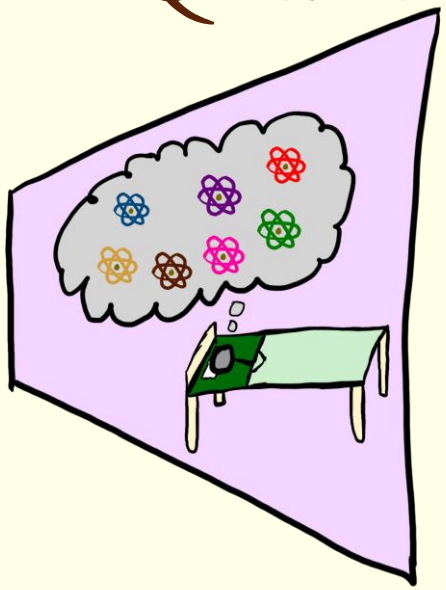
oracle separation rules out most black-box constructions

Quantum Oracles - Modeling



Isometry oracle

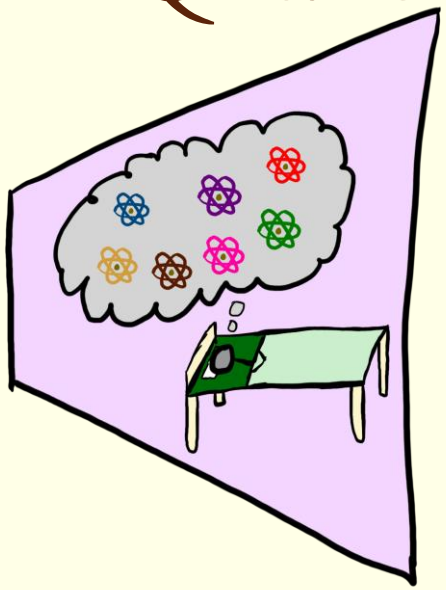
Quantum Oracles - Modeling



Isometry oracle

functionality: any isometry
(irreversible quantum operation)

Quantum Oracles - Modeling

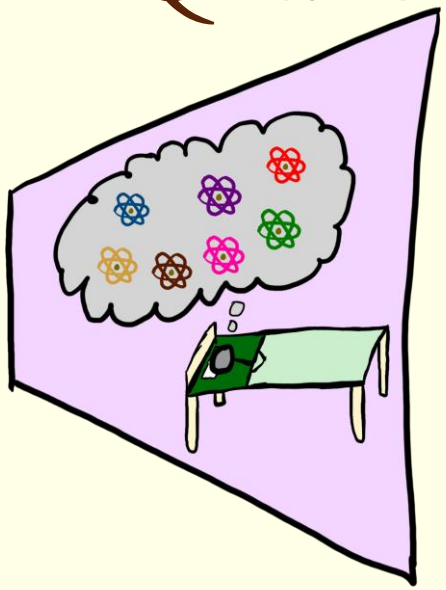


Isometry oracle

functionality: any isometry
(irreversible quantum operation)

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

Quantum Oracles - Modeling

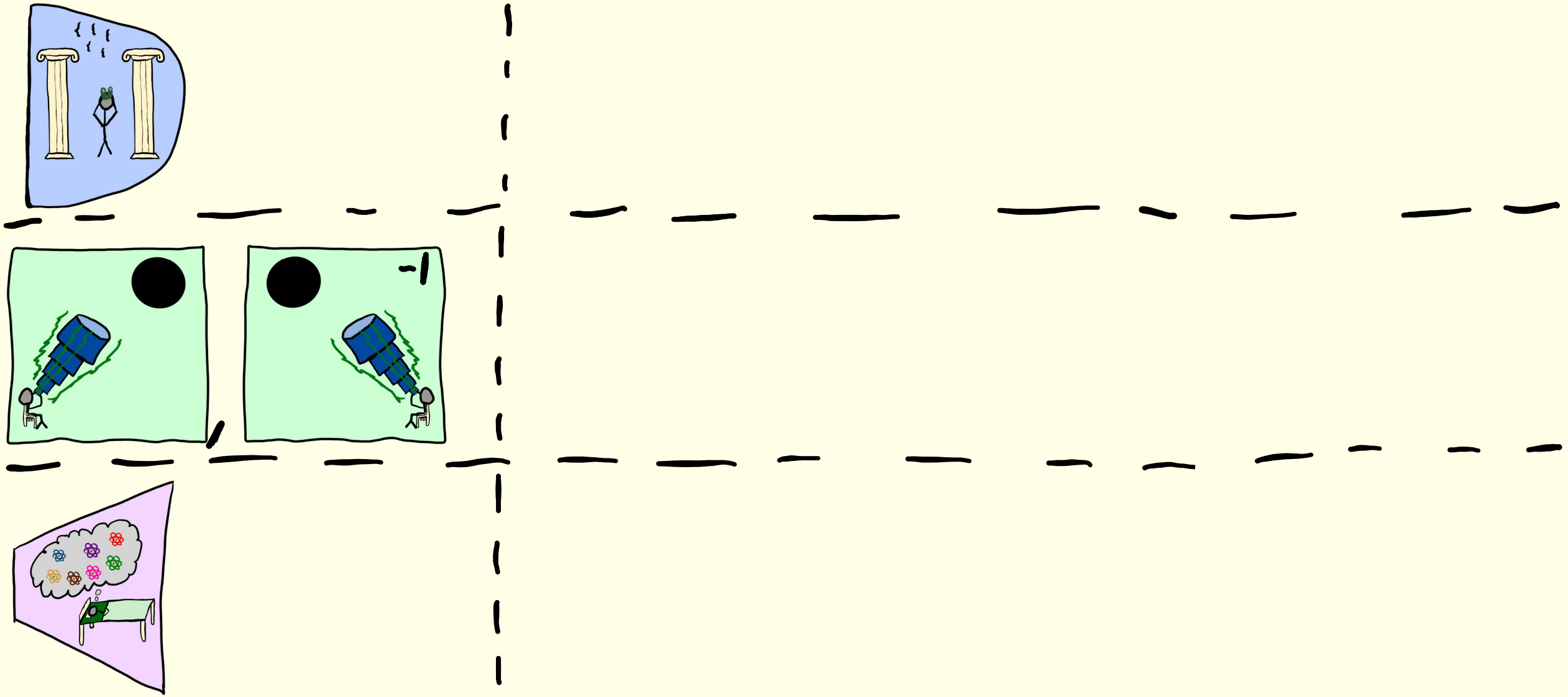


Isometry oracle

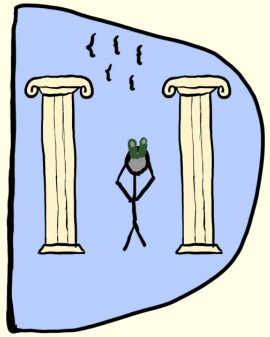
functionality: any isometry
(irreversible quantum operation)

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

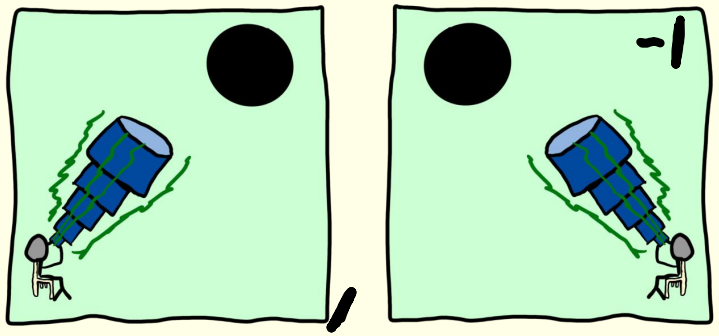
Quantum Oracle Separations - Ranked

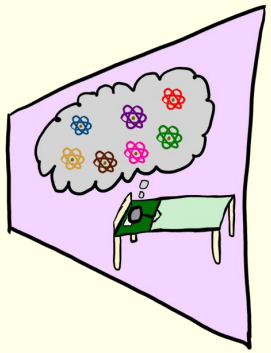


Quantum Oracle Separations - Ranked

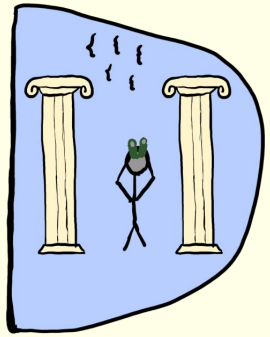


best we can hope for

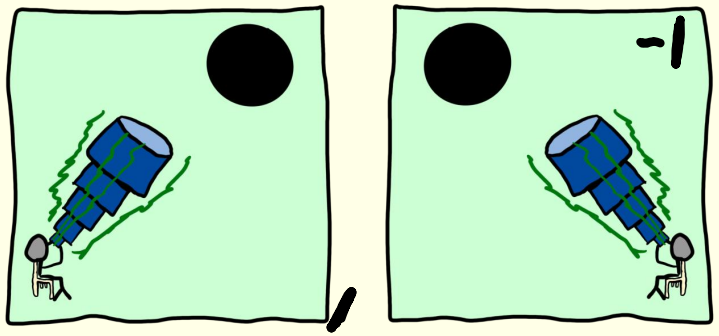




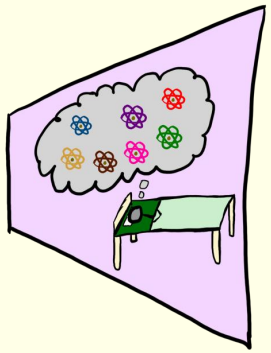
Quantum Oracle Separations - Ranked



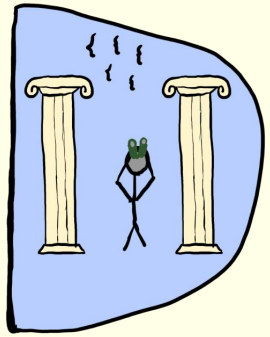
best we can hope for



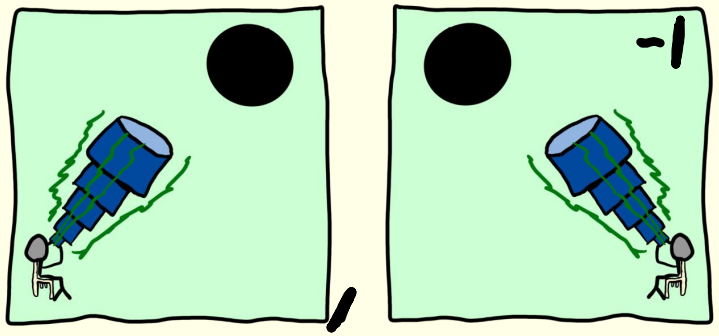
good enough



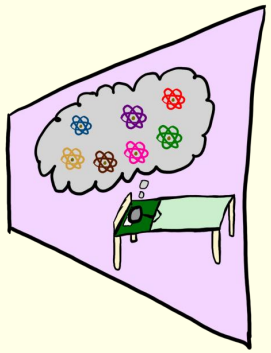
Quantum Oracle Separations - Ranked



best we can hope for



good enough



preliminary result

Common Haar Random State Model

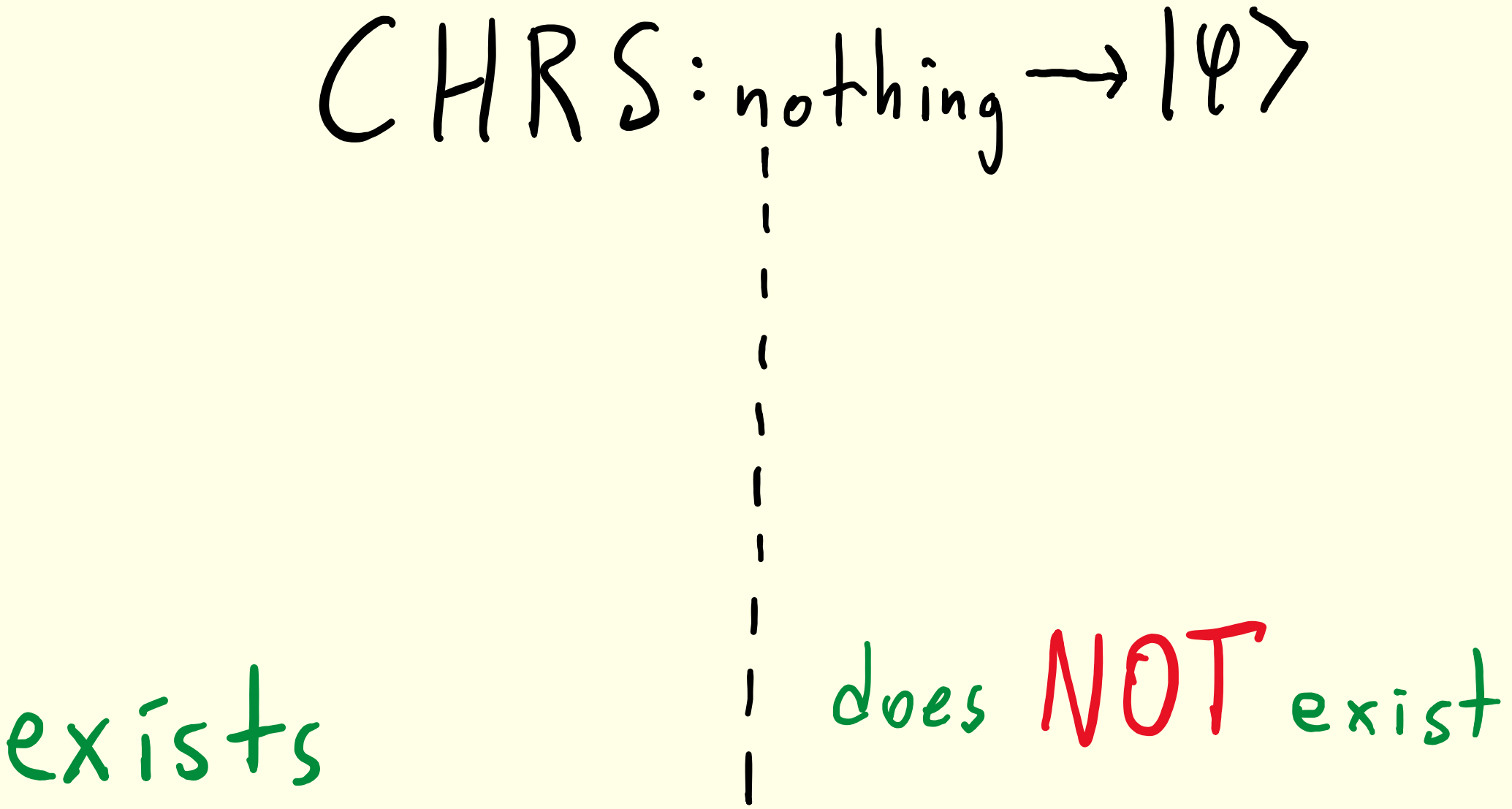
$\mathsf{CHRS}: \text{nothing} \to |\varphi\rangle$

Common Haar Random State Model

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

fixed Haar random state

Common Haar Random State Model



Common Haar Random State Model

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

poly-copy pseudorandom states

exists

does NOT exist

Common Haar Random State Model

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

poly-copy pseudorandom states

classical communication (QCCC)

cryptography

exists

does NOT exist

Common Haar Random State Model

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

poly-copy pseudorandom states

classical communication (QCCC)

cryptography

...

exists

does NOT exist

Common Haar Random State Model

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

1-copy pseudorandom states

poly-copy pseudorandom states

classical communication (QCCC)

cryptography

...

exists

does NOT exist

Common Haar Random State Model

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

1-copy pseudorandom states

quantum commitments

exists

poly-copy pseudorandom states

classical communication (QCCC)

cryptography

...

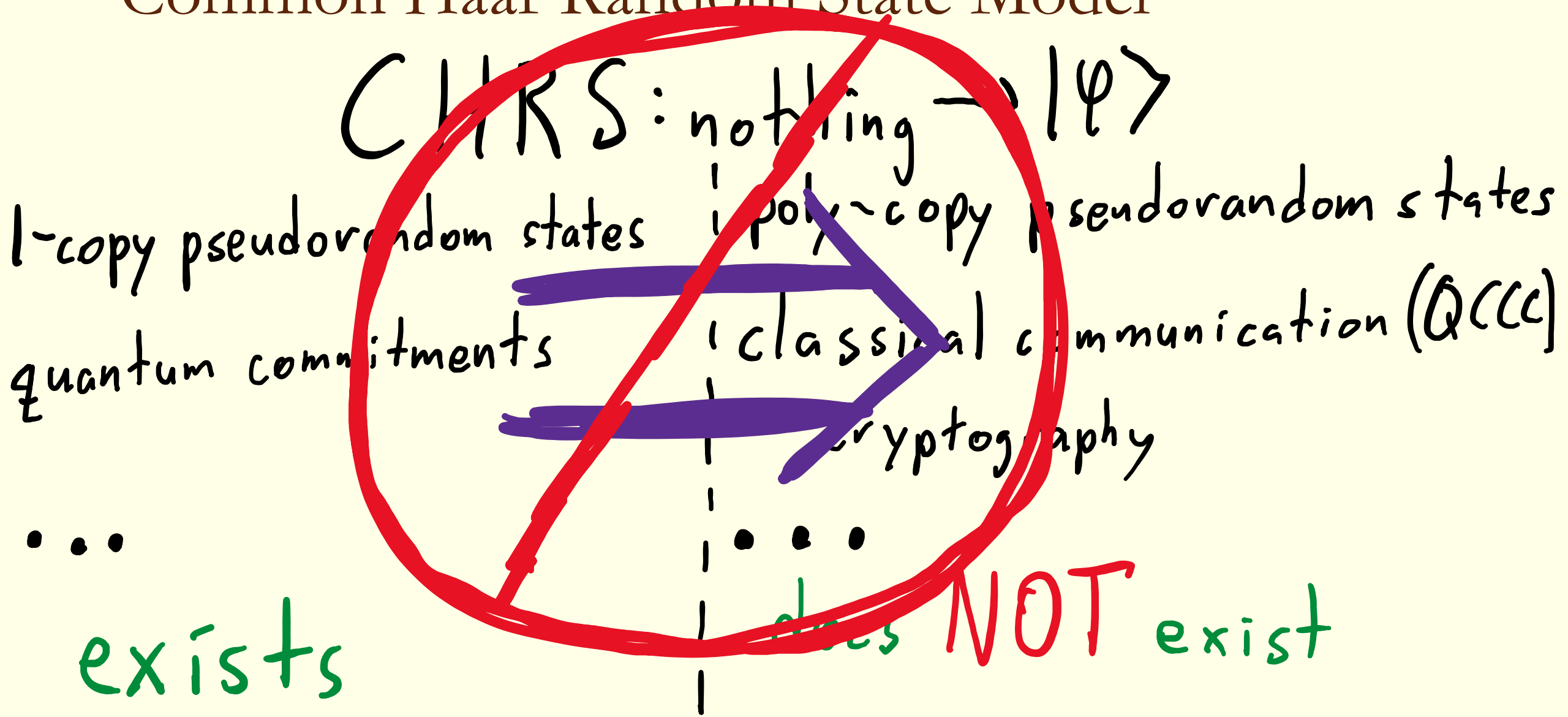
does NOT exist

Common Haar Random State Model

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

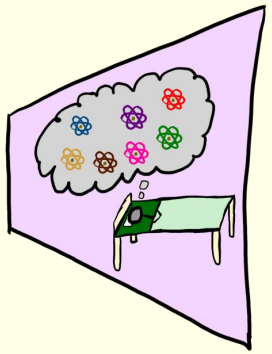
1-copy pseudorandom states	poly-copy pseudorandom states
quantum commitments	classical communication (QCCC)
	cryptography
...	...
exists	does NOT exist

Common Haar Random State Model



Common Haar Random State Model

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

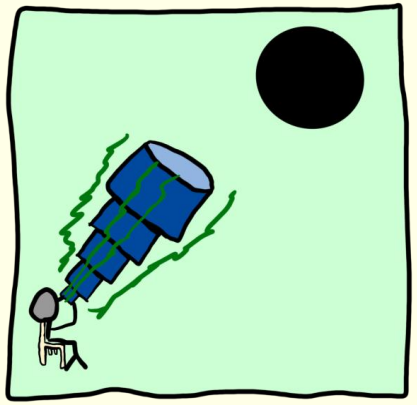


- NOT reversible isometry oracle

Common Haar Random State Model

Big Question: Can we make these separations unitary?

Common Haar Random State Model

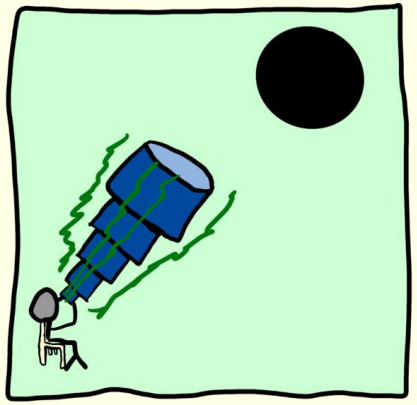


[CCS25]

[BCN25]

[BMM+25]

Common Haar Random State Model



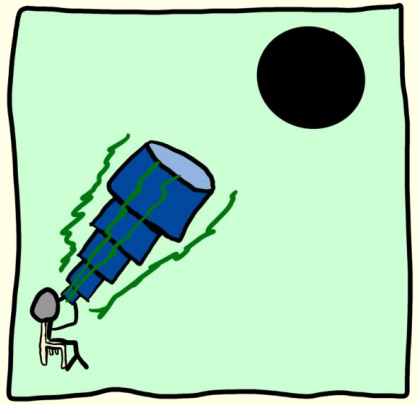
[CCS25]

[BCN25]

[BMM+25]

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

Common Haar Random State Model



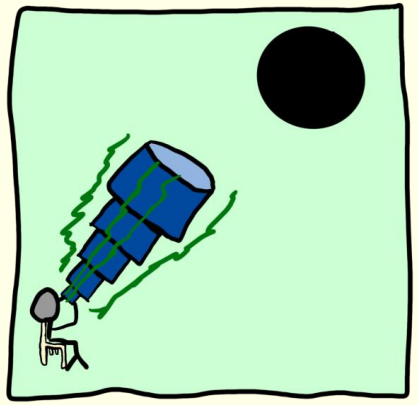
[CCS25] SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$

[BCN25]

[BMM+25] subset swap oracle

Common Haar Random State Model

proof breaks down :(

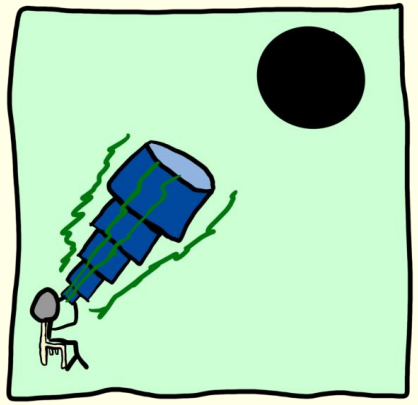


[CCS25] [BCN25] SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$

[BMM+25] subset swap oracle

Common Haar Random State Model

proof breaks down :(



[CCS25] SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$

[BCN25]

[BMM+25] subset swap oracle ✓

Conjecture

CHRS: nothing $\to |\psi\rangle$ 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-.

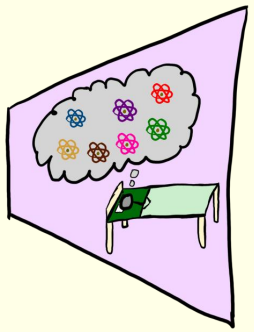
Our Results

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

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

similar, most proofs work!

Unitary separation template

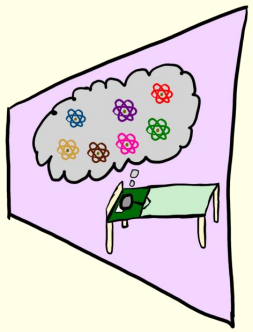


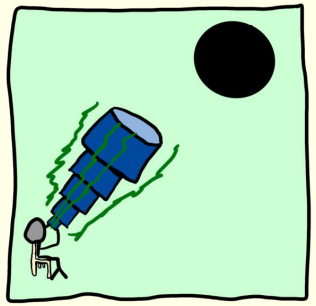
CHRS

P_1 exists

P_2 does NOT exist

Unitary separation template





CHRS

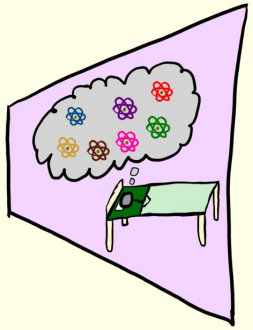
SWAP

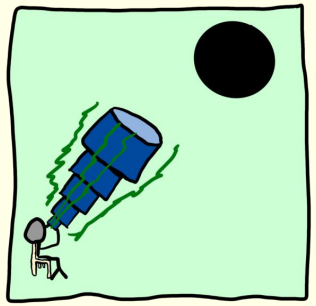
P_1 P_2 P_1

exists does NOT exist exists

FREE

Unitary separation template





CHRS

P_1 exists

P_2 does NOT exist

FREE

P_1 exists

SWAP

P_2 does NOT exist

adapt proof

CHRS- Model

For $|\varphi\rangle$ any state,

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

CHRS- Model

For $|\varphi\rangle$ any state,

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

$CHRS-: \text{nothing} \to |\varphi-\rangle$

CHRS- Model

For $|\varphi\rangle$ any state,

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

$\mathcal{C}_{HRS-}$: nothing $\to |\varphi_-\rangle$

└ fixed Haar random $|\varphi\rangle$

Computing SWAP with CRSH-

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

Computing SWAP with CRSH-

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

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

Computing SWAP with CRSH-

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

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

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

Computing SWAP with CRSH-

SWAP: $|0\rangle \leftrightarrow |\varphi\rangle$ CRSH-: nothing $\rightarrow |\varphi^-\rangle$

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

SWAP is reflection around $|\varphi^-\rangle$.

Computing SWAP with CRSH-

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

SWAP: $|0\rangle \leftrightarrow |\psi\rangle$ CRSH-: 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 $|\psi^-\rangle$. DONE

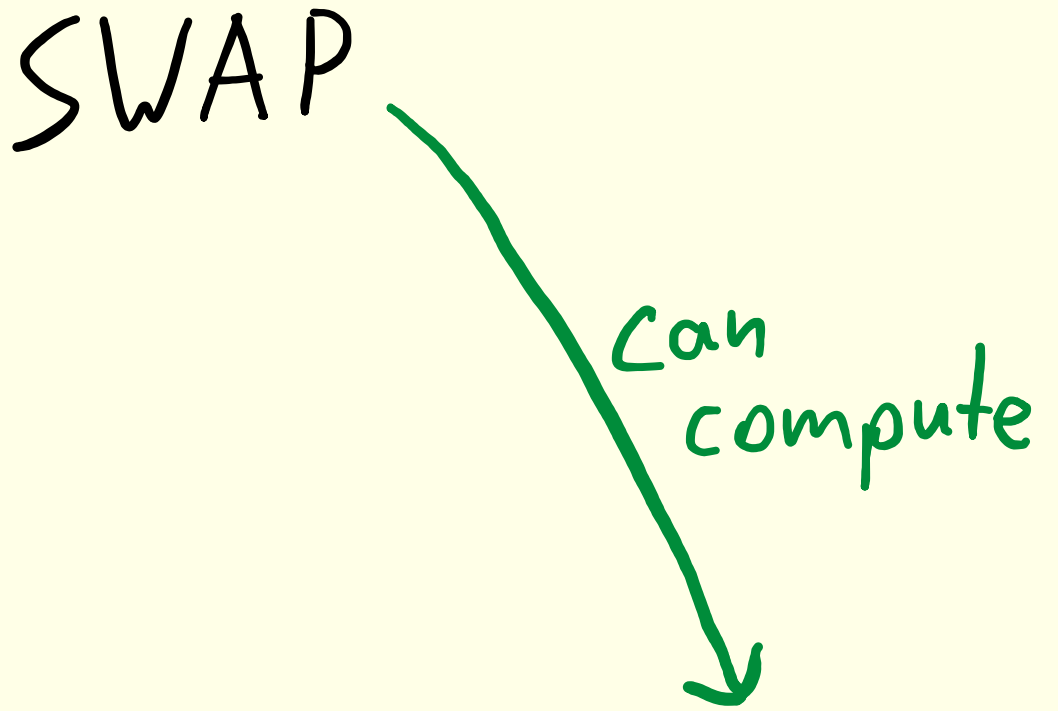
Why?

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

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

similar, most proofs work!

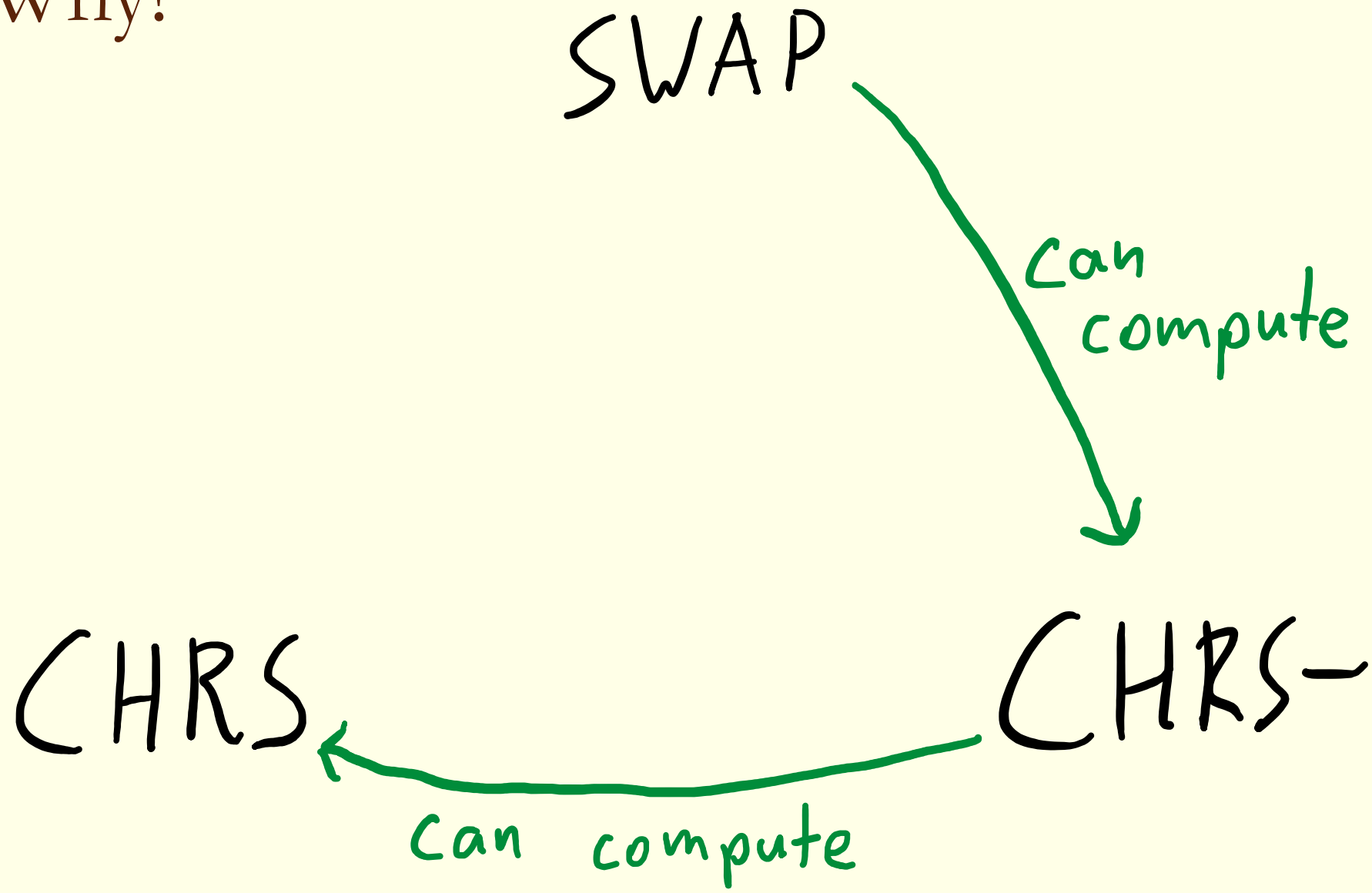
Why?



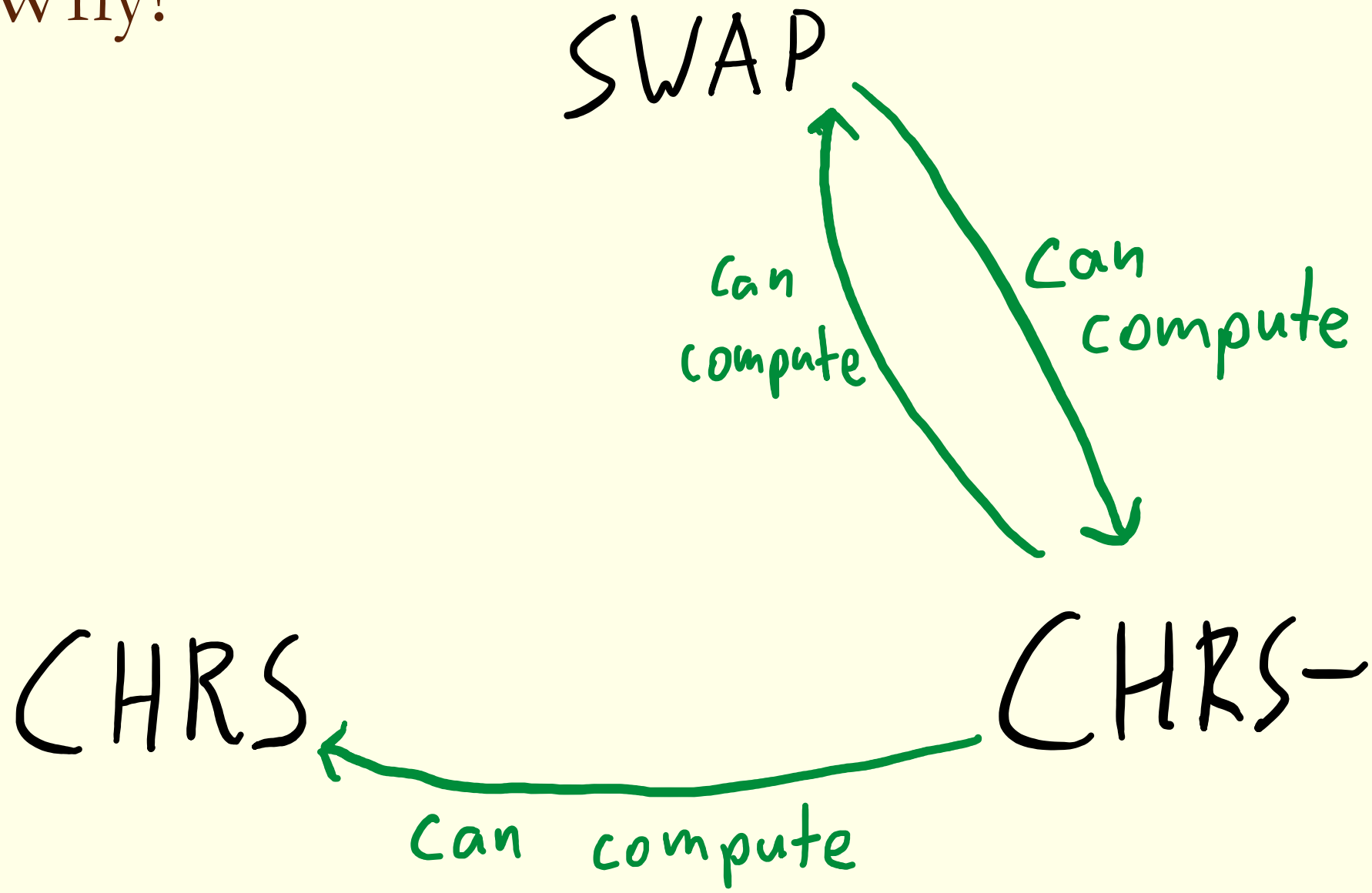
CHRS

CHRS-

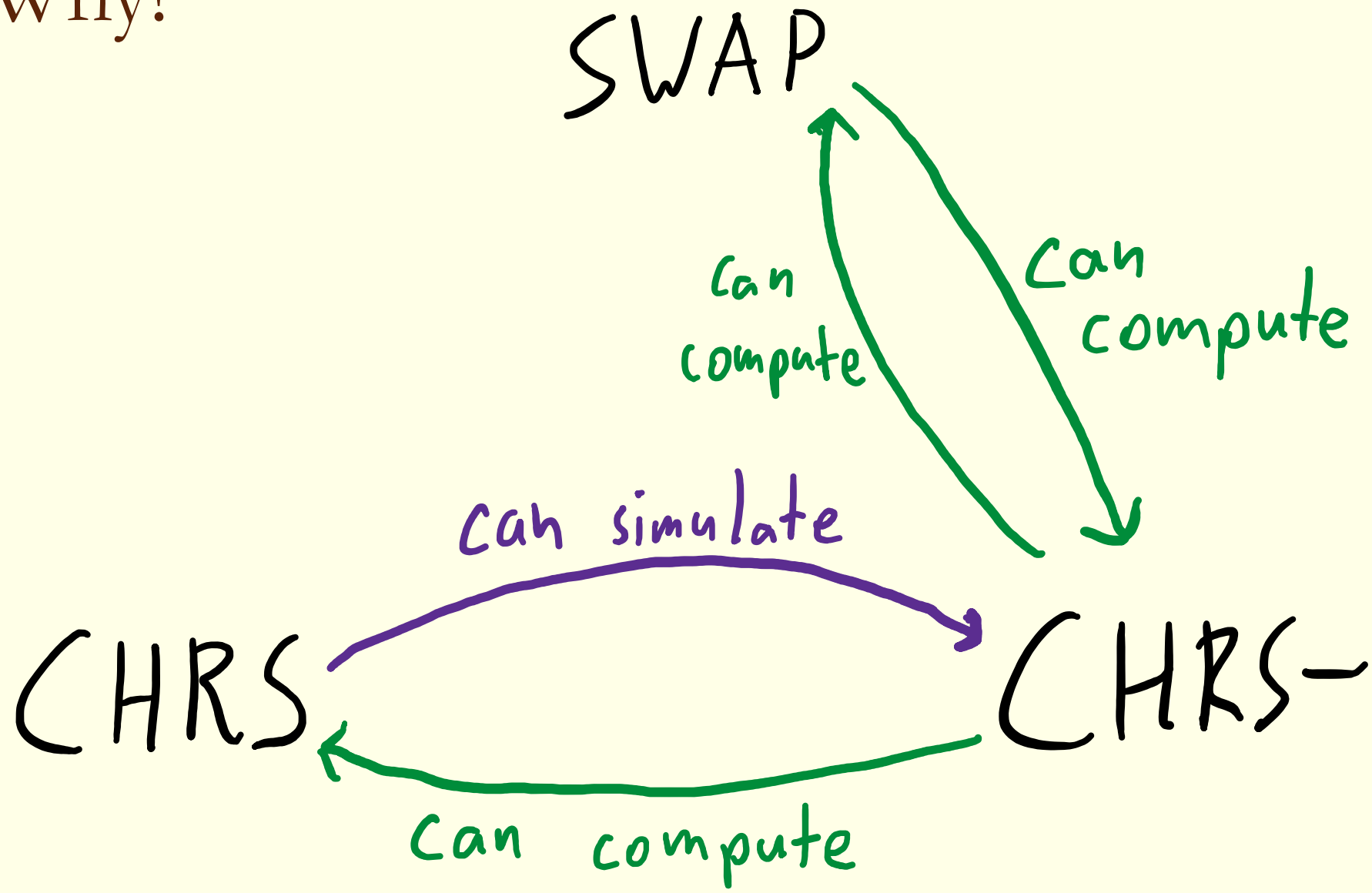
Why?



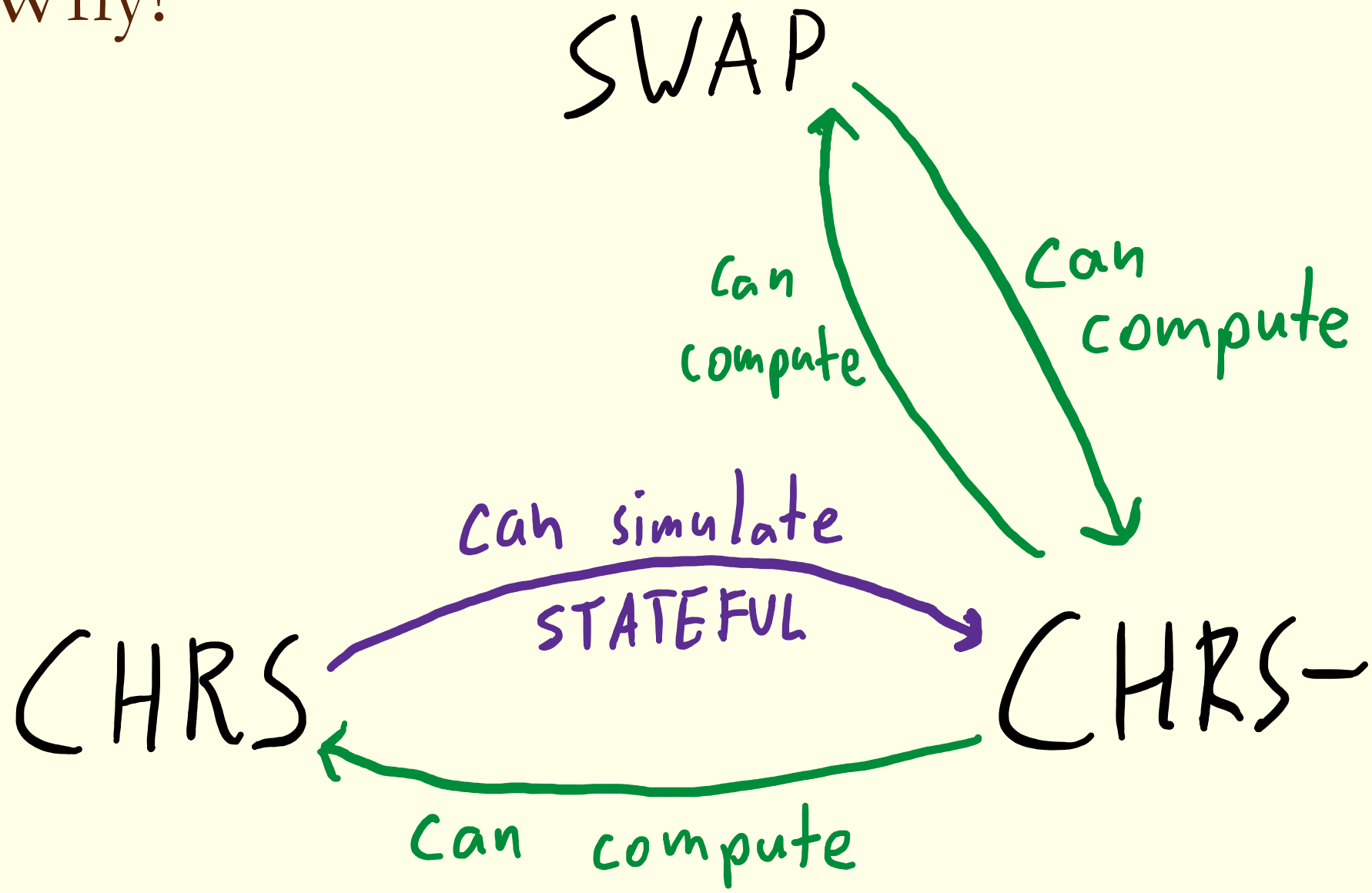
Why?



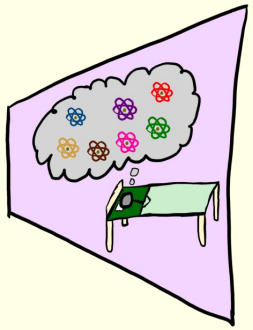
Why?


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

Why?


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

Our Results



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

1-copy pseudorandom states

quantum commitments

...

exists

poly-copy pseudorandom states

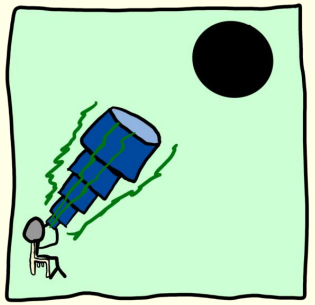
classical communication (QCCC)

cryptography

...

does NOT exist

Our Results



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

1-copy pseudorandom states

quantum commitments

...

exists

poly-copy pseudorandom states

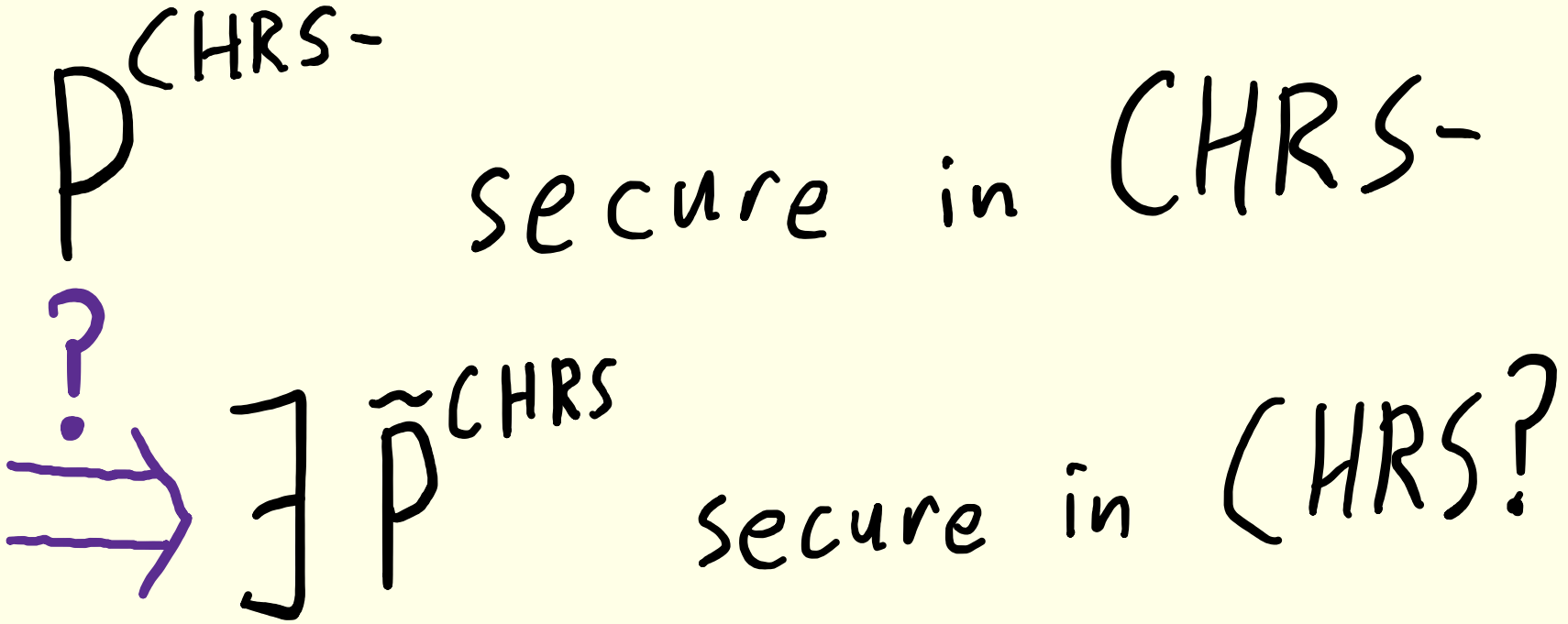
classical communication (QCCC)

cryptography

...

does NOT exist

Open Questions



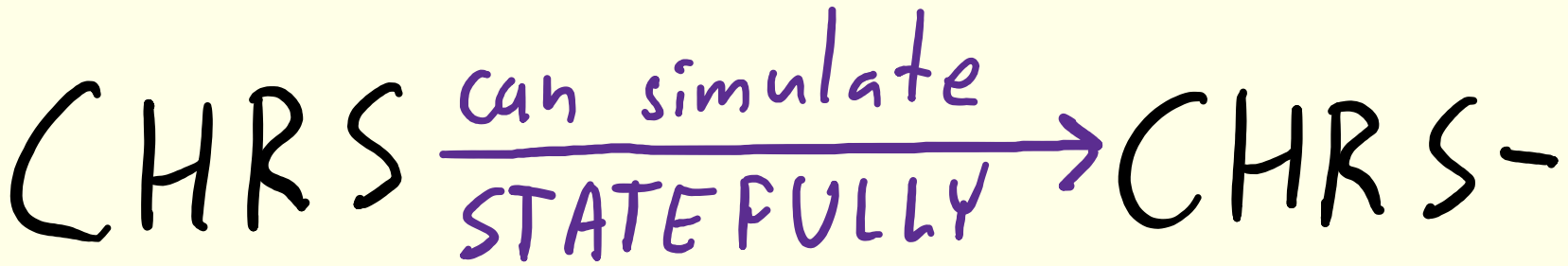
Open Questions

P^{CHRS-} secure in CHRS-

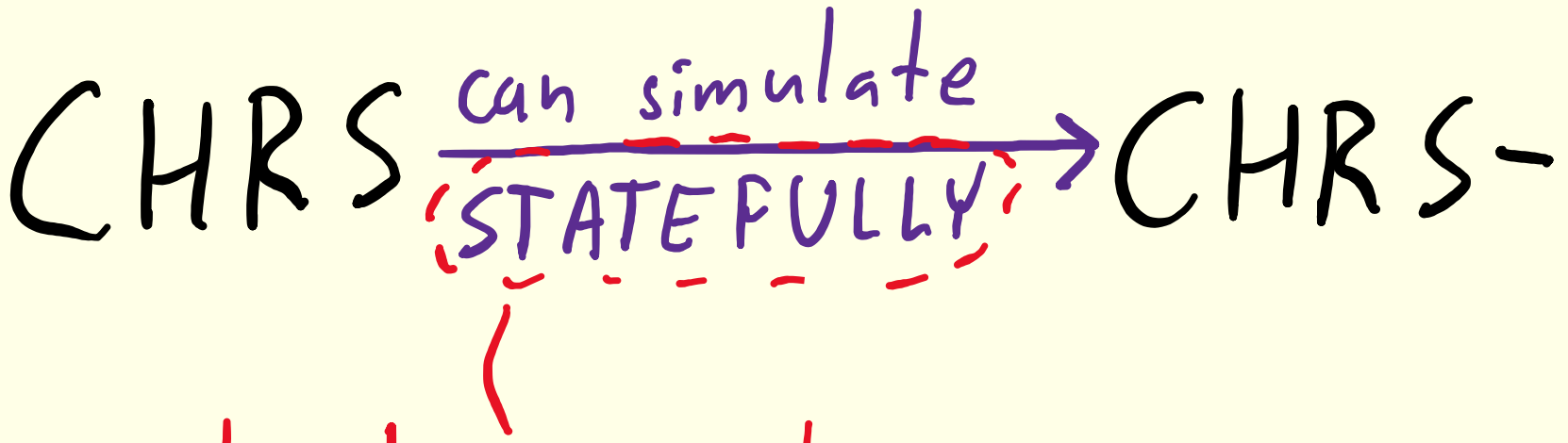
$\overset{?}{\Longrightarrow}$ $\exists\, \tilde{P}^{CHRS}$ secure in CHRS?

No candidate!

Open Questions

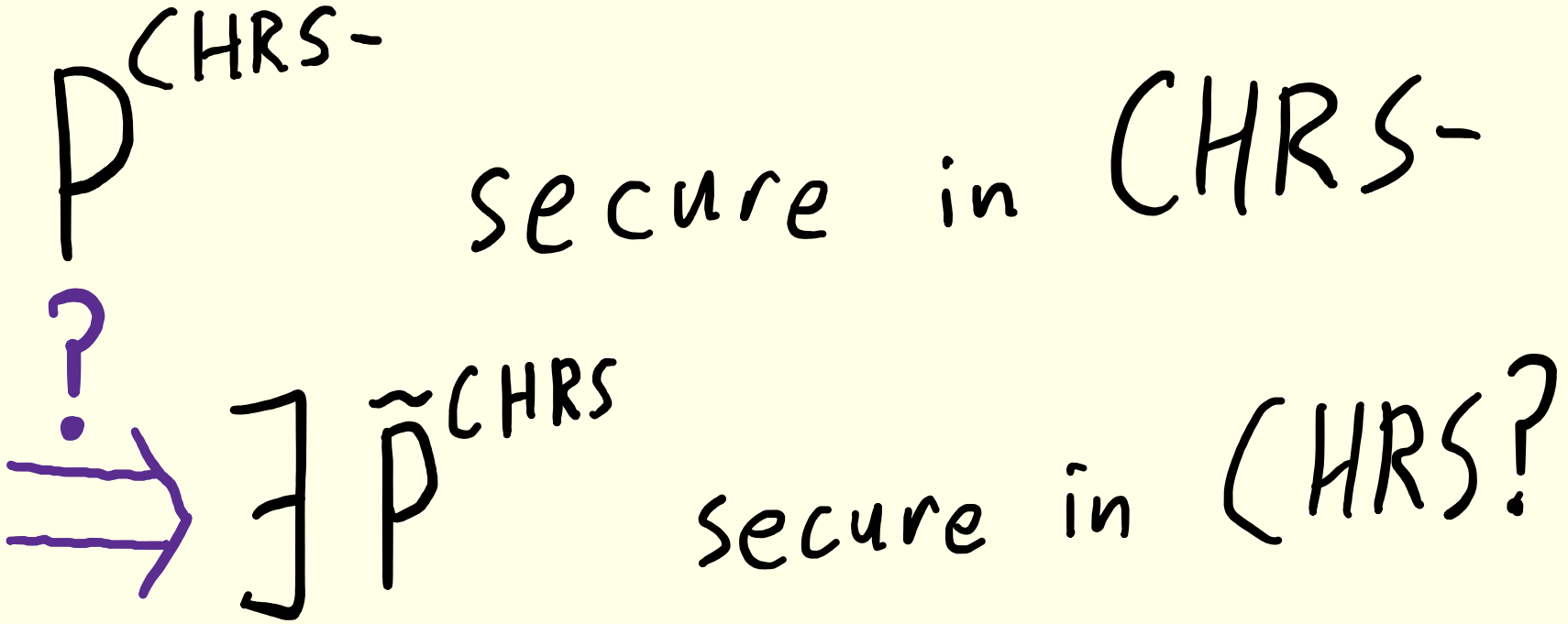


Open Questions



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

Open Questions



Open Questions

P^{CHRS-} secure in CHRS-

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

Relationships between other quantum oracles?

Open Questions

P^{CHRS-} secure in CHRS-

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

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