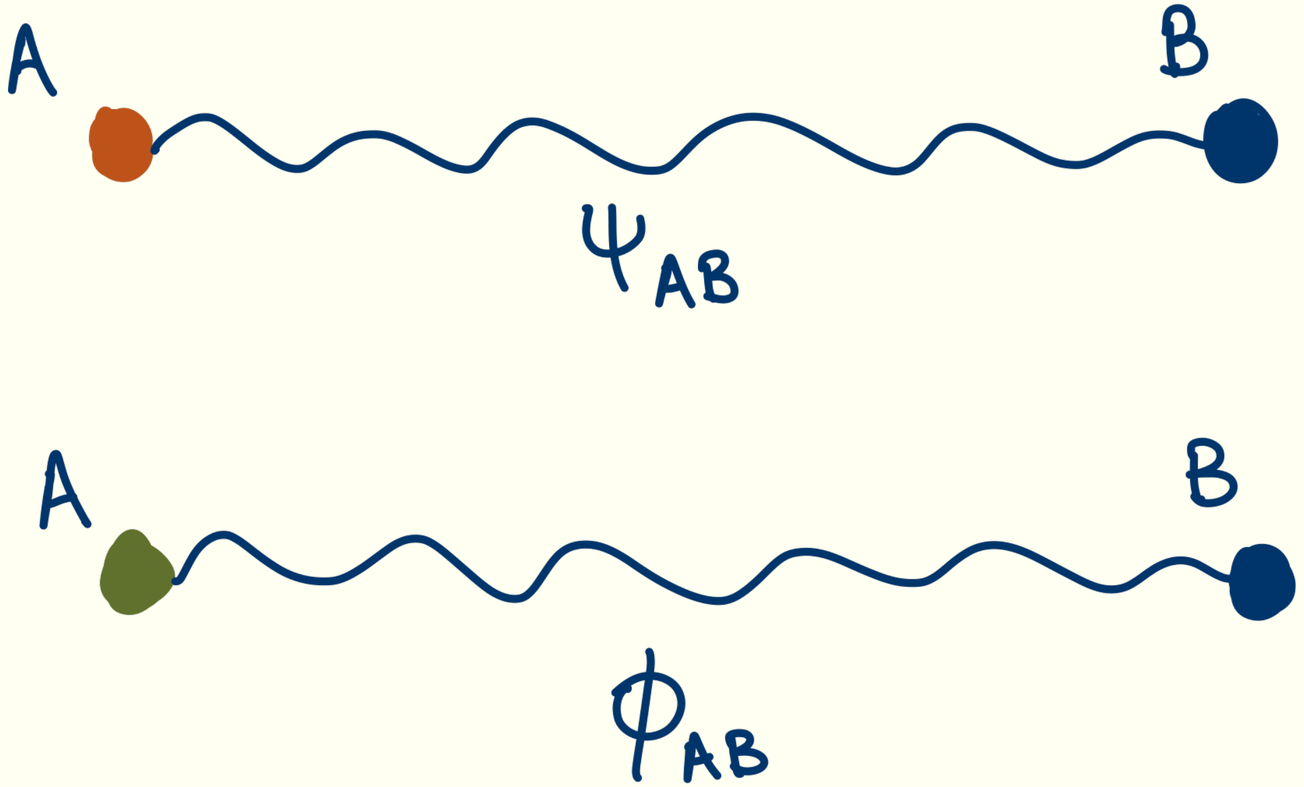
Unitary complexity theory and the Uhlmann transformation problem

John Bostanci, Yuval Efron, Tony Metger,
Alex Poremba, Luowen Qian, and Henry Yuen

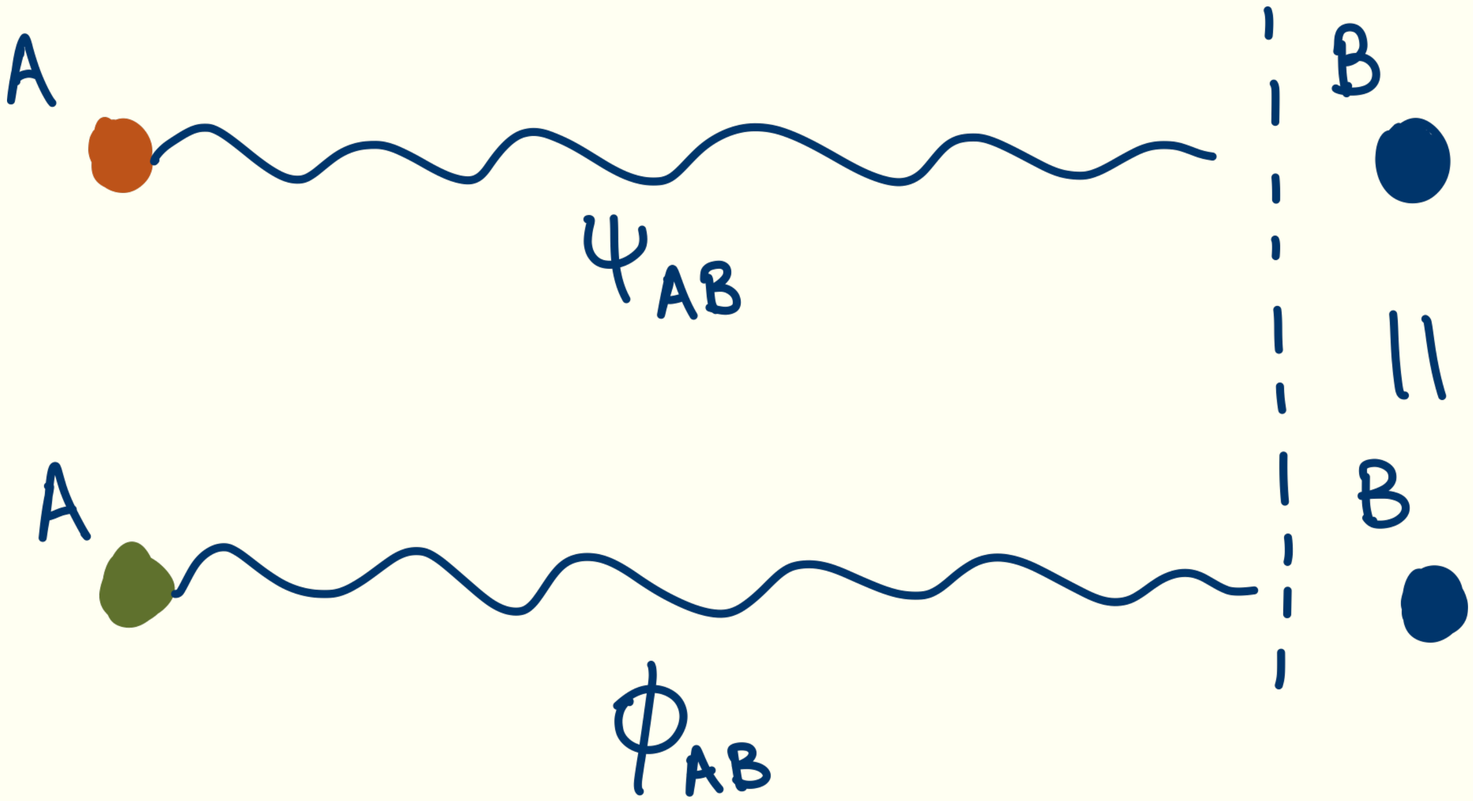
Uhlmann's theorem

Say we know two states, $|C\rangle_{AB}$ and $|D\rangle_{AB}$ that have the same reduced states on the B register,



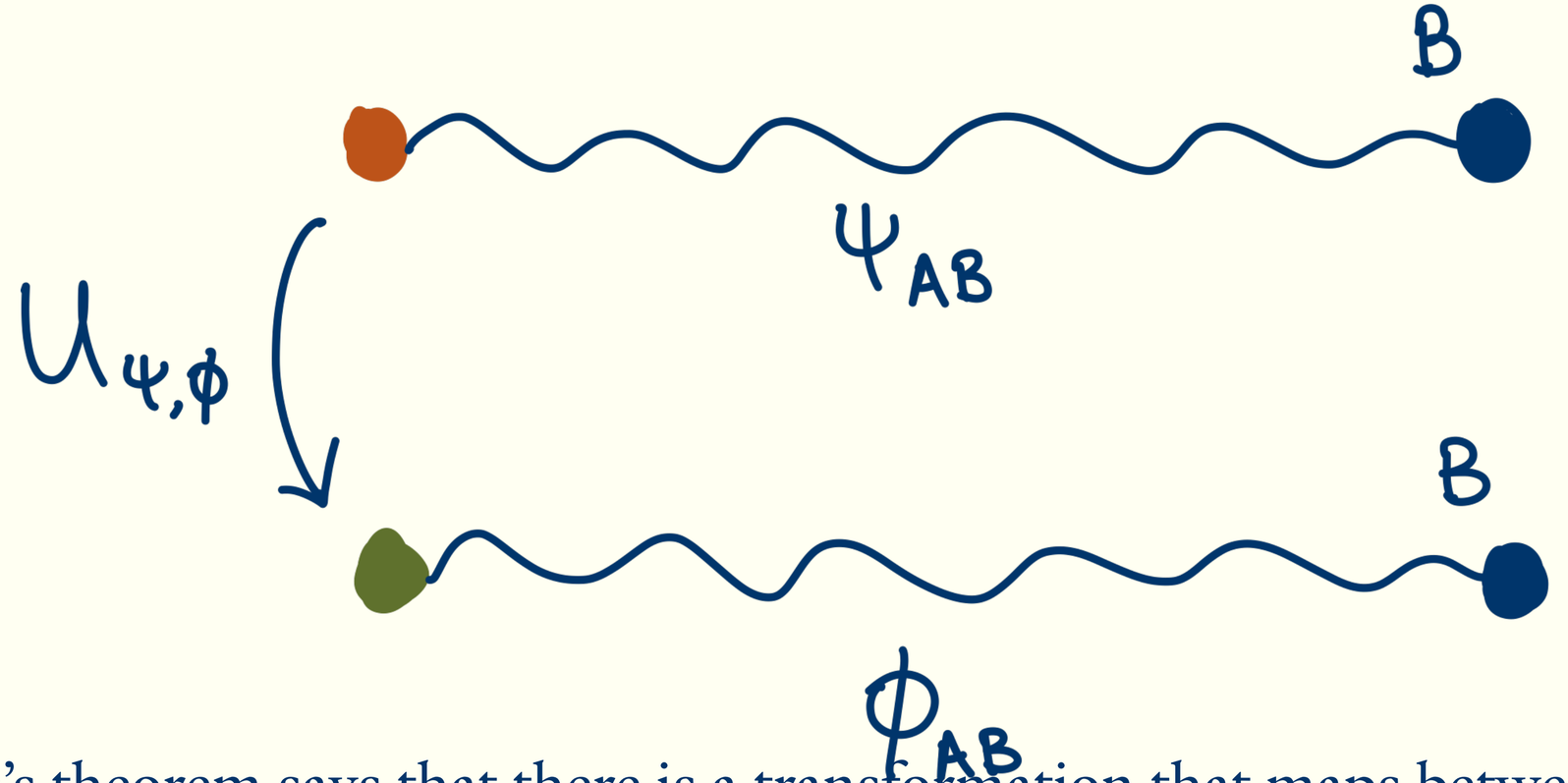
Uhlmann's theorem

Say we know two states, $|C\rangle_{AB}$ and $|D\rangle_{AB}$ that have the same reduced states on the B register,



Uhlmann's theorem

Say we know two states, $|C\rangle_{AB}$ and $|D\rangle_{AB}$ that have the same reduced states on the B register,



Uhlmann's theorem says that there is a transformation that maps between the two states while only touching the A register!

Uhlmann's transformations

Uhlmann transformations appear all over the place!

Uhlmann's transformations

Uhlmann transformations appear all over the place!

- Algorithms for quantum Shannon theory: Entanglement distillation, state merging, noisy channel decoding, compressing quantum information, etc.

Uhlmann's transformations

Uhlmann transformations appear all over the place!

- Algorithms for quantum Shannon theory: Entanglement distillation, state merging, noisy channel decoding, compressing quantum information, etc.
- Breaking quantum cryptography: binding of quantum bit commitments, cloning one-way state generators, etc.

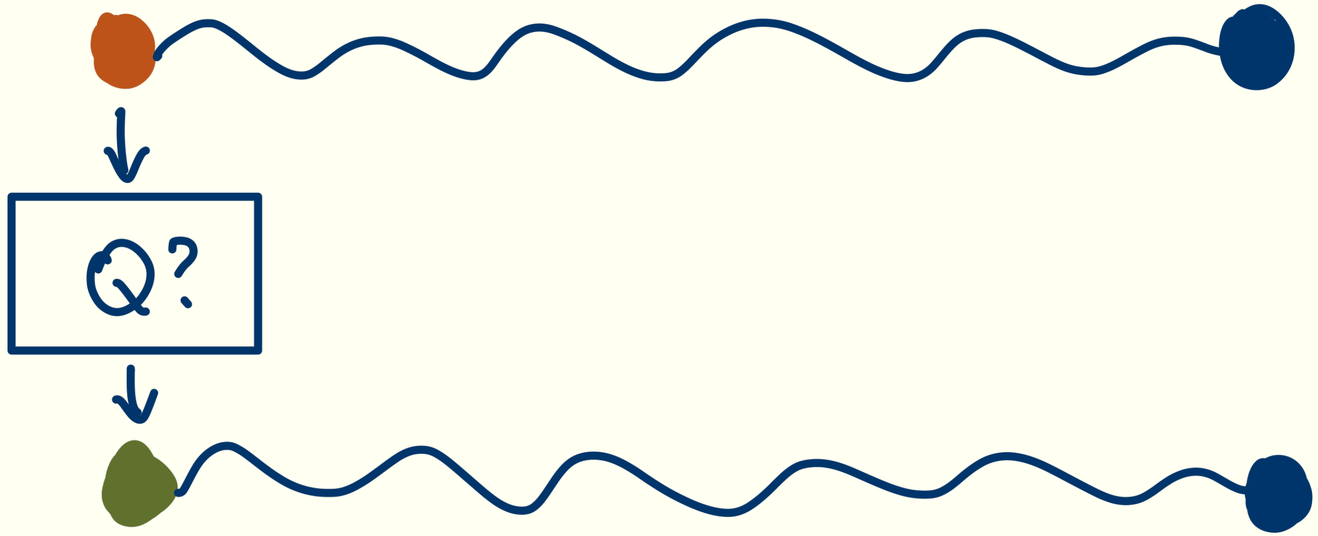
Uhlmann's transformations

Uhlmann transformations appear all over the place!

- Algorithms for quantum Shannon theory: Entanglement distillation, state merging, noisy channel decoding, compressing quantum information, etc.
- Breaking quantum cryptography: binding of quantum bit commitments, cloning one-way state generators, etc.
- High energy physics: Decoding black hole radiation.

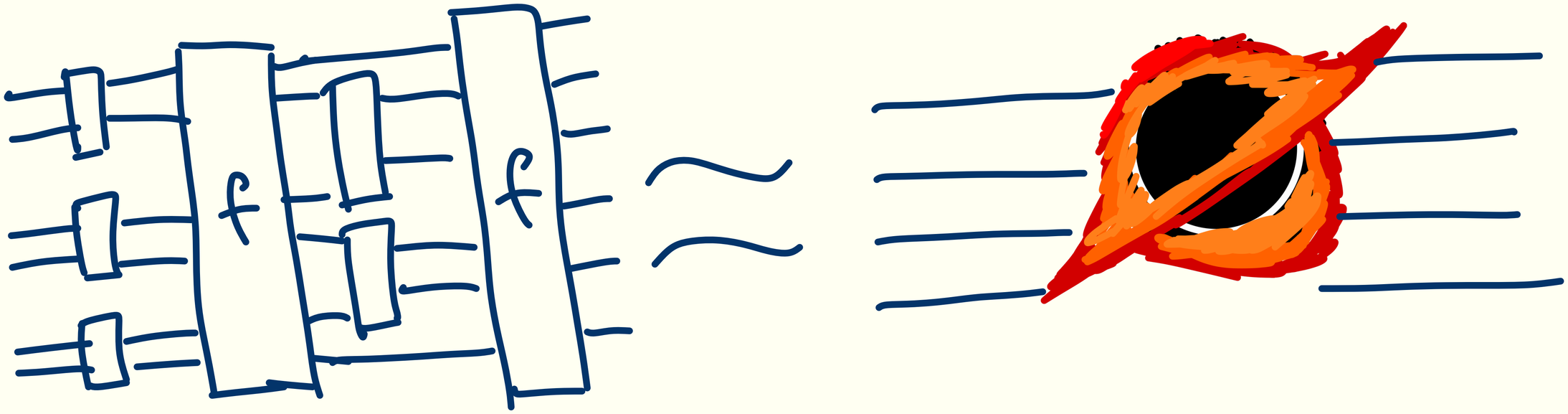
Uhlmann's transformations

How hard is it to do an Uhlmann transformation, given circuits for $|C\rangle$ and $|D\rangle$?



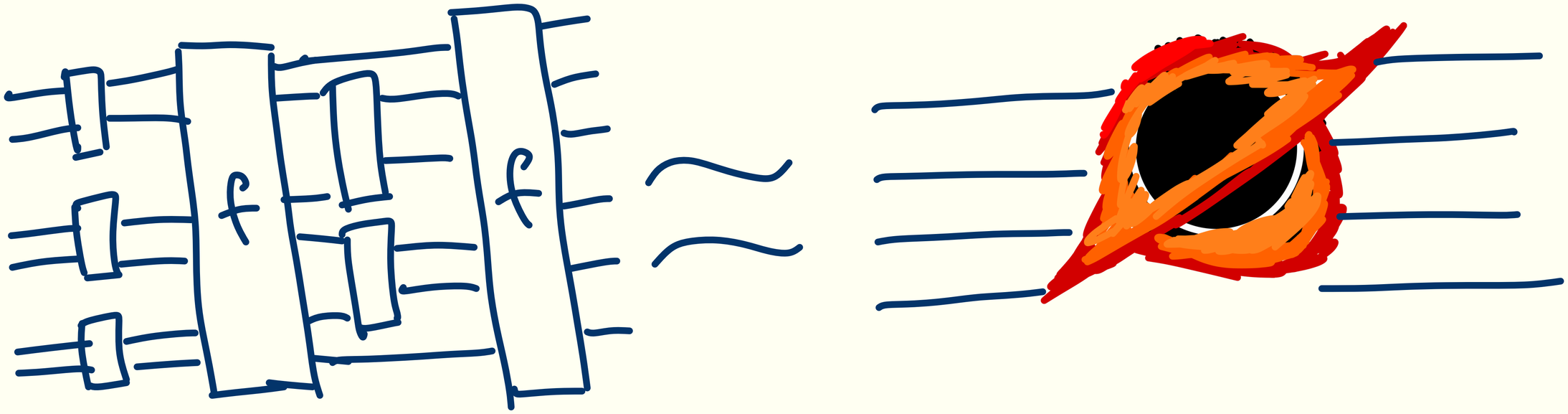
Unitary complexity theory

The unitary synthesis problem is a long standing open question in quantum complexity theory. It asks about the relation between fully quantum and classical problems.



Unitary complexity theory

The unitary synthesis problem is a long standing open question in quantum complexity theory. It asks about the relation between fully quantum and classical problems.



Given that we can’t resolve this question, can we still characterize the complexity of quantum tasks using a “fully-quantum” complexity theory?

Unitary complexity theory

Goals for unitary complexity theory:

Unitary complexity theory

Goals for unitary complexity theory:

- Can capture interesting problems in many different areas of quantum computer science.

Unitary complexity theory

Goals for unitary complexity theory:

- Can capture interesting problems in many different areas of quantum computer science.
- Has complete problems and interesting complexity classes.

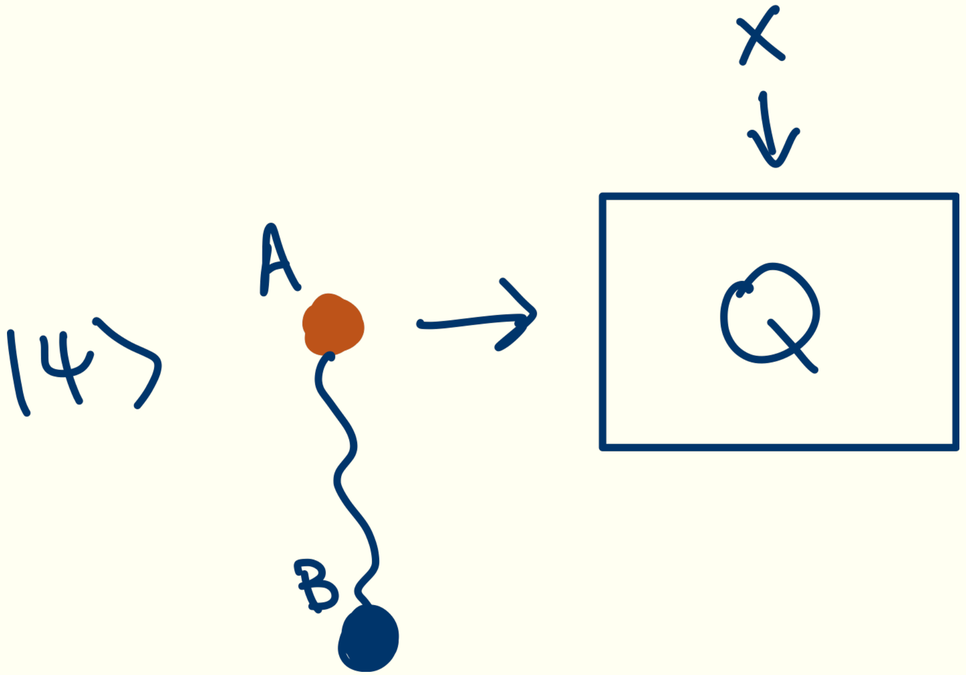
Unitary complexity theory

Goals for unitary complexity theory:

- Can capture interesting problems in many different areas of quantum computer science.
- Has complete problems and interesting complexity classes.
- Has a robust notion of reduction that we can use to relate different complexity classes.

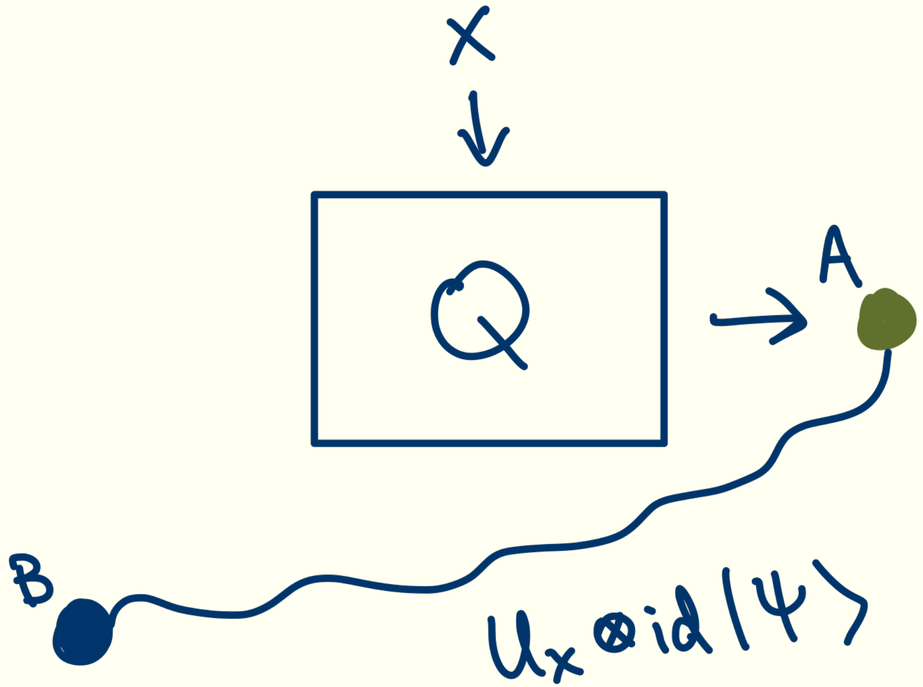
Unitary synthesis problems

A unitary synthesis problem, $\mathcal{U}$, is a family of unitaries, $(U_x)_{x\in\{0,1\}^*}$, one for every "instance" x.



Unitary synthesis problems

A unitary synthesis problem, $\mathcal{U}$, is a family of unitaries, $(U_x)_{x\in\{0,1\}^*}$, one for every "instance" x.



Unitary synthesis problems

A unitary synthesis problem, $\mathscr{U}$, is a family of unitaries, $(U_x)_{x\in\{0,1\}^*}$, one for every "instance" x.

A circuit is an implementation of the unitary synthesis problem if for all x, r,

$$\|C_{x,r} - U_x\|_\diamond \leq \frac{1}{r}\,.$$

Distributional unitary synthesis problems

A distributional unitary synthesis problem, $\mathcal{U}$, is a family of unitaries, $(U_x)_{x\in\{0,1\}^*}$, and states $\Psi = (|\psi_x\rangle)_{x\in\{0,1\}^*}$.

A circuit is an implementation of a distributional unitary synthesis problem if for all x, r,

$$\mathrm{td}\left(C_{x,r}(|\psi_x\rangle\langle\psi_x|), U_x(|\psi_x\rangle\langle\psi_x|)\right) \leq \frac{1}{r}.$$

Interactive protocols

A distributional unitary synthesis problem is in $\mathsf{avgUnitaryQIP}_{c,s}$ if there is a polynomial time quantum verifier such that:

Interactive protocols

A distributional unitary synthesis problem is in $\mathsf{avgUnitaryQIP}_{c,s}$ if there is a polynomial time quantum verifier such that:

- (Completeness): There is an honest prover P^* such that

$$\Pr[V_{x,r}(|\psi_{x,r}\rangle) \leftrightarrows P^* \text{ accepts}] \geq c(|x|).$$

Interactive protocols

A distributional unitary synthesis problem is in $\mathsf{avgUnitaryQIP}_{c,s}$ if there is a polynomial time quantum verifier such that:

- (Completeness): There is an honest prover P^* such that

$$\Pr[V_{x,r}(|\psi_{x,r}\rangle) \leftrightarrows P^* \text{ accepts}] \geq c(|x|).$$

- (Soundness): For all provers, P, there exists a channel completion Φ_x of U_x such that

$$\text{If } \Pr[V_{x,r}(|\psi_{x,r}\rangle) \leftrightarrows P \text{ accepts}] \geq s, \text{ then } \mathrm{td}(\sigma_{x,r}, \Phi_x \otimes \mathrm{id}(|\psi_{x,r}\rangle\langle\psi_{x,r}|)) \leq \frac{1}{r},$$

where $\sigma_{x,r}$ is the state that the verifier outputs at the end of the protocol.

Reductions between unitary synthesis problems

A unitary synthesis problem $\mathscr{U}$ reduces to $\mathscr{V}$ in polynomial time if there's a family of uniform polynomial sized circuit making calls to "$\mathscr{V}$-gates" that implements $\mathscr{U}$,

"If $\mathscr{V}$ was efficient to implement, then $\mathscr{U}$ would be too"

The Uhlmann transformation problem

We can define two "unitary synthesis problems" related to Uhlmann transformations:

- Uhlmann: For a string $x = (C, D)$, an explicit description of two circuits, U_x is the Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

The Uhlmann transformation problem

We can define two "unitary synthesis problems" related to Uhlmann transformations:

- Uhlmann: For a string $x = (C, D)$, an explicit description of two circuits, U_x is the Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

- SuccinctUhlmann: For a string $x = (\tilde{C}, \tilde{D})$, a succinct description of two circuits, U_x is the Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

The Uhlmann transformation problem

We can define two "unitary synthesis problems" related to Uhlmann transformations:

- Uhlmann: For a string $x = (C, D)$, an explicit description of two circuits, U_x is the Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

Complete for avgUnitaryHVPZK!

- SuccinctUhlmann: For a string $x = (\tilde{C}, \tilde{D})$, a succinct description of two circuits, U_x is the Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

The Uhlmann transformation problem

We can define two "unitary synthesis problems" related to Uhlmann transformations:

- Uhlmann: For a string $x = (C, D)$, an explicit description of two circuits, U_x is the Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

Complete for avgUnitaryHVPZK!

- SuccinctUhlmann: For a string $x = (\tilde{C}, \tilde{D})$, a succinct description of two circuits, U_x is the Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

Complete for avgUnitaryPSPACE and avgUnitaryQIP → avgUnitaryPSPACE = avgUnitaryQIP

The Uhlmann transformation problem

We can relate a lot of problems in quantum computer science to complexity now!

The Uhlmann transformation problem

We can relate a lot of problems in quantum computer science to complexity now!

- Quantum bit commitments can are broken if avgUnitaryHVSZK = avgUnitaryBQP, and they imply that DistUhlmann is hard for avgUnitaryBQP.

The Uhlmann transformation problem

We can relate a lot of problems in quantum computer science to complexity now!

- Quantum bit commitments can are broken if avgUnitaryHVSZK = avgUnitaryBQP, and they imply that DistUhlmann is hard for avgUnitaryBQP.
- If avgUnitaryPSPACE = avgUnitaryBQP, all falsifiable assumptions are broken.

The Uhlmann transformation problem

We can relate a lot of problems in quantum computer science to complexity now!

- Quantum bit commitments can are broken if avgUnitaryHVSZK = avgUnitaryBQP, and they imply that DistUhlmann is hard for avgUnitaryBQP.
- If avgUnitaryPSPACE = avgUnitaryBQP, all falsifiable assumptions are broken.
- Optimal noisy channel decoding and compression are easy if avgUnitarySZK = avgUnitaryBQP.

Next steps

- Populating the zoo: We defined the complexity classes avgUnitaryBQP, avgUnitaryPZK, avgUnitarySZK, avgUnitaryQIP, avgUnitaryPSPACE, but there are so many more models of computation one can consider.

- Characterizing more tasks: The complexity of many other tasks in quantum information theory, like state merging, FQSW, entanglement distillation, is unknown. Similarly, the complexity of breaking PRS, quantum money, PRU, etc. remains unknown. Can we characterize these tasks in unitary complexity theory?

- The unitary synthesis problem: Can we prove that certain quantum tasks can not be solved with unbounded classical resources (in polynomial time)? For certain complexity classes like avgUnitarySZK, can we rule out implementing those unitaries in small classical complexity classes?

Thanks for listening!