Towards a fully quantum complexity theory

John Bostanci
(Columbia University)

The (fully?) quantum future

Imagine a world where…

The (fully?) quantum future

Imagine a world where…

- Everyone has quantum computers

The (fully?) quantum future

Imagine a world where...

- Everyone has quantum computers
- People communicate over quantum networks

The (fully?) quantum future

Imagine a world where…

- Everyone has quantum computers
- People communicate over quantum networks
- People analyze quantum data

The (fully?) quantum future

Imagine a world where…

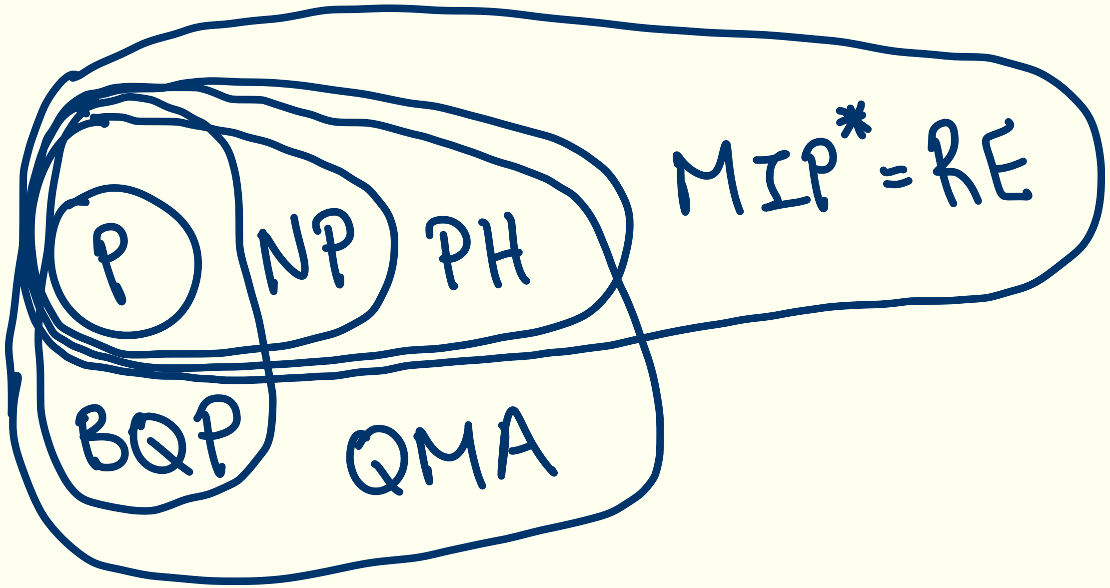
- Everyone has quantum computers
- People communicate over quantum networks
- People analyze quantum data

What are the problems those people will solve?

What can we say about the complexity of those problems?

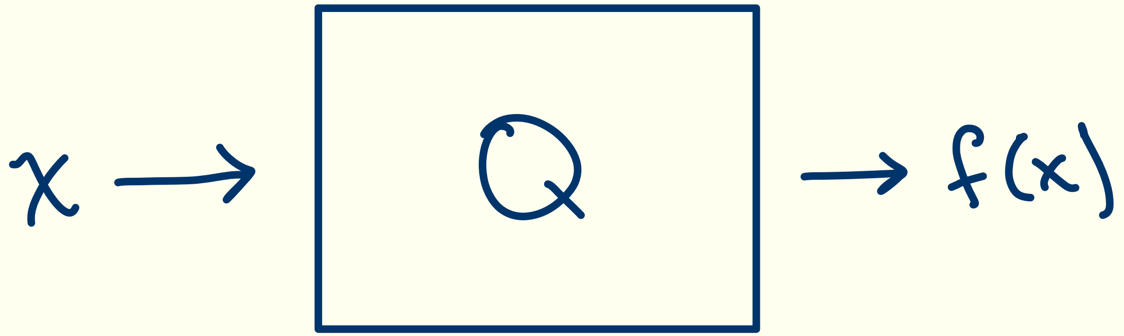
Complexity theory today

Complexity classes today (BQP, QMA, MIP*, etc.) have allowed us to study many quantum computational problems, and have led to many important insights about quantum advantage, condensed matter physics, C*-algebras, etc.



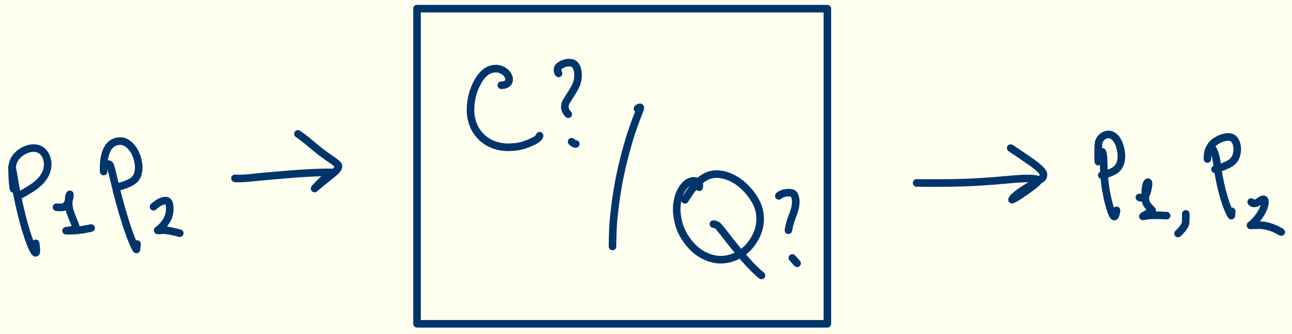
Complexity theory today

But they discuss problems that could also be solved on a classical computer, with classical input and classical output.



Complexity theory today

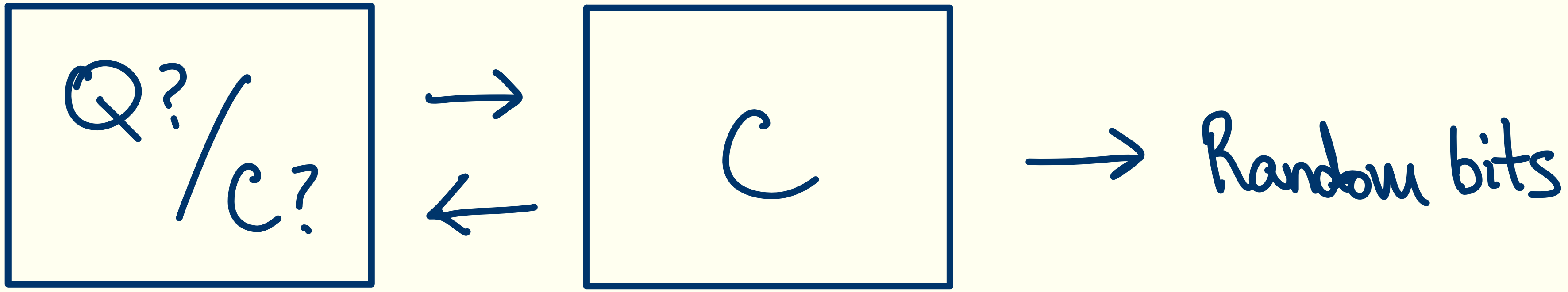
But they discuss problems that could also be solved on a classical computer, with classical input and classical output.



The point has been mostly to compare classical and quantum computers "apples-to-apples".

Complexity theory today

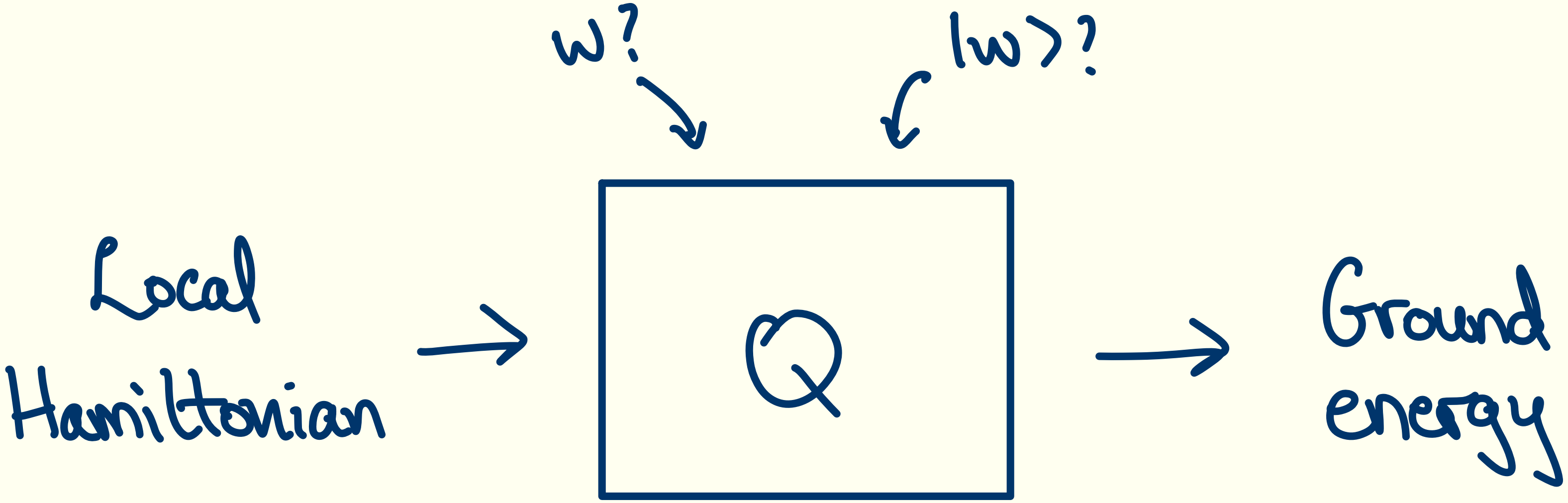
But they discuss problems that could also be solved on a classical computer, with classical input and classical output.



The point has been mostly to compare classical and quantum computers “apples-to-apples”.

Complexity theory today

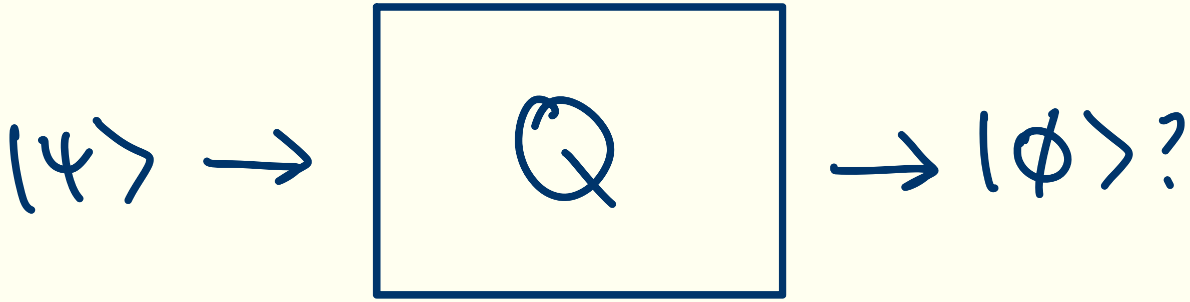
But they discuss problems that could also be solved on a classical computer, with classical input and classical output.



The point has been mostly to compare classical and quantum computers “apples-to-apples”.

Complexity theory today

But they discuss problems that could also be solved on a classical computer, with classical input and classical output.



What about problems with quantum inputs and outputs?

Classical versus quantum complexity

Quantum data is inherently different than classical data.

Classical versus quantum complexity

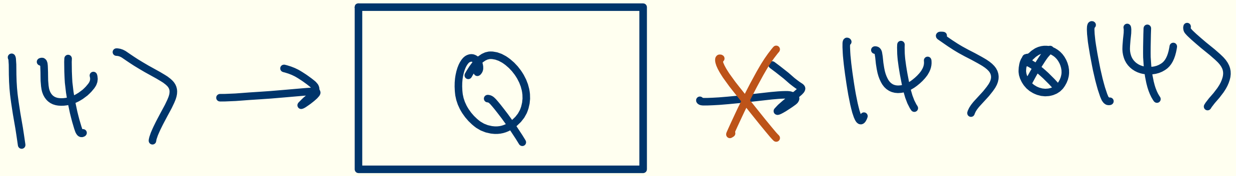
Quantum data is inherently different than classical data.

- No cloning: $|\psi\rangle \rightarrow \boxed{Q} \not\rightarrow |\psi\rangle \otimes |\psi\rangle$

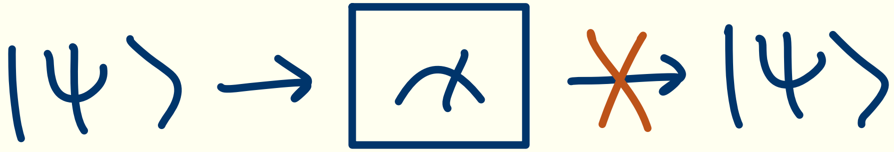
Classical versus quantum complexity

Quantum data is inherently different than classical data.

- No cloning:

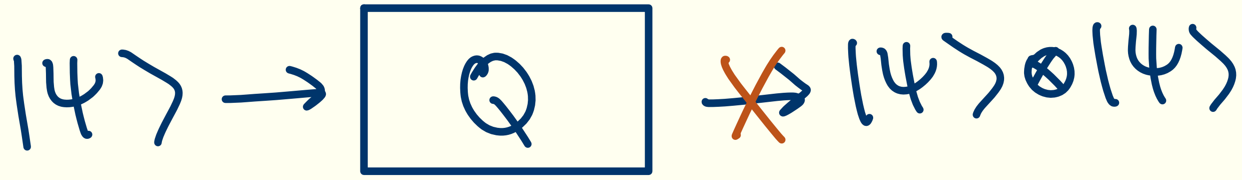
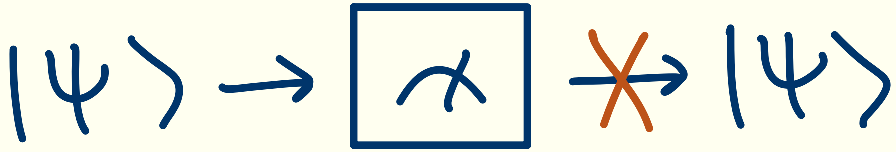
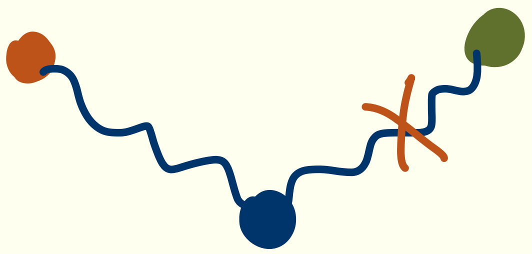


- Information/disturbance trade-off:



Classical versus quantum complexity

Quantum data is inherently different than classical data.

- No cloning: 
- Information/disturbance trade-off: 
- Monogamy of entanglement: 

Classical versus quantum complexity

Lots of more formal evidence proving quantum complexity must be inherently different:

Classical versus quantum complexity

Lots of more formal evidence proving quantum complexity must be inherently different:

- Fully quantum cryptography exists even if P=NP [Kretschmer, Qian, Sinha, Tal ‘23].

Classical versus quantum complexity

Lots of more formal evidence proving quantum complexity must be inherently different:

- Fully quantum cryptography exists even if P=NP [Kretschmer, Qian, Sinha, Tal ‘23].
- There are unitaries that do not have efficient implementations, even given infinite classical computational time [Lombardi, Ma, Wright ‘23].

Classical versus quantum complexity

Lots of more formal evidence proving quantum complexity must be inherently different:

- Fully quantum cryptography exists even if P=NP [Kretschmer, Qian, Sinha, Tal ‘23].
- There are unitaries that do not have efficient implementations, even given infinite classical computational time [Lombardi, Ma, Wright ‘23].
- Being able to determines a Hamiltonian’s ground energy does not let you make a copy of it’s ground state [Irani, Rao, Natarajan, Nirkhe, Yuen ‘21].

Summary so far

- In the future, we hope to be solving problems that involve accepting quantum inputs and returning quantum outputs.

Summary so far

- In the future, we hope to be solving problems that involve accepting quantum inputs and returning quantum outputs.
- Traditional complexity theory is geared towards comparing classical and quantum computers, instead of discussing the relative hardness of these problems.

Summary so far

- In the future, we hope to be solving problems that involve accepting quantum inputs and returning quantum outputs.
- Traditional complexity theory is geared towards comparing classical and quantum computers, instead of discussing the relative hardness of these problems.
- Evidence suggests that these problems are actually inherently different than traditional problems, and need a new, "fully-quantum" theory.

Unitary complexity theory

and the Uhlmann transformation problem.

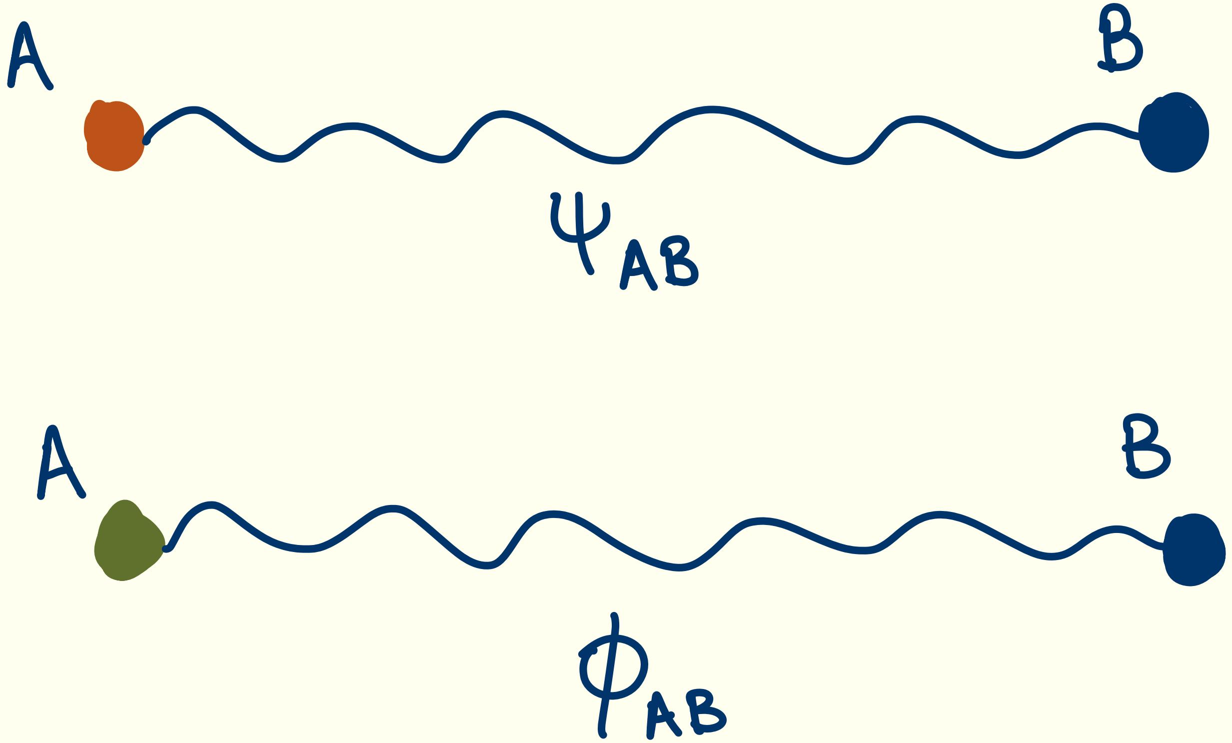
Based on joint work with Yuval Efron, Tony Metger, Luowen Qian, Alex Poremba, and Henry Yuen.

Quantum information basics

- A "register" in this talk is a Hilbert space (i.e. vector space with an inner product). "n-qubits" means the dimension is 2^n.
- A "ket" is a normalized vector: $|\psi\rangle \in$ R, $\sqrt{\langle\psi|\psi\rangle} = 1$.
- A "unitary" is a linear operation on a register that is norm preserving (i.e. maps unit vectors to unit vectors).
- Two quantum registers compose via the tensor product, so vectors in register AB are a linear combination of the tensor products of a vector in A and a tensor product in B.

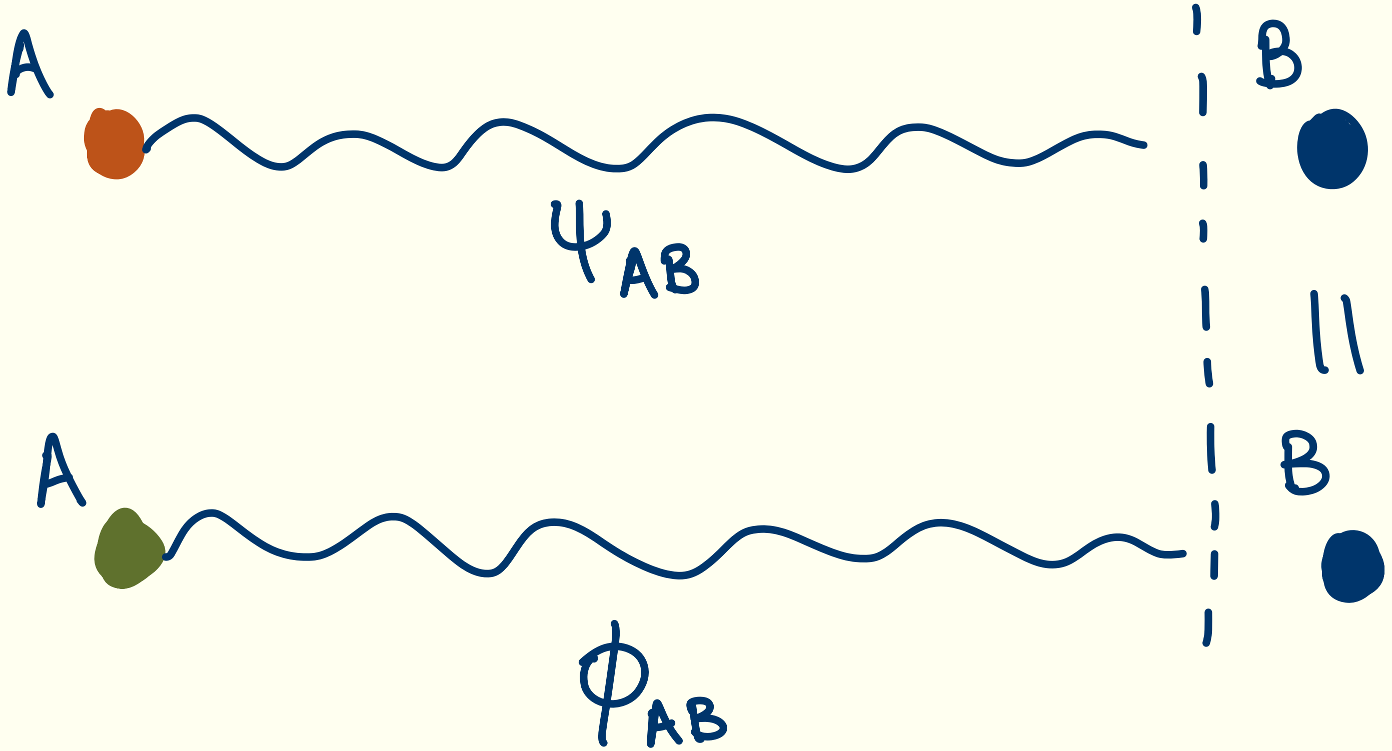
Motivating example: Uhlmann's theorem

Say that we know about two bipartite states, $|\psi\rangle$ and $|\phi\rangle$, such that their reduced states on register B is the same.



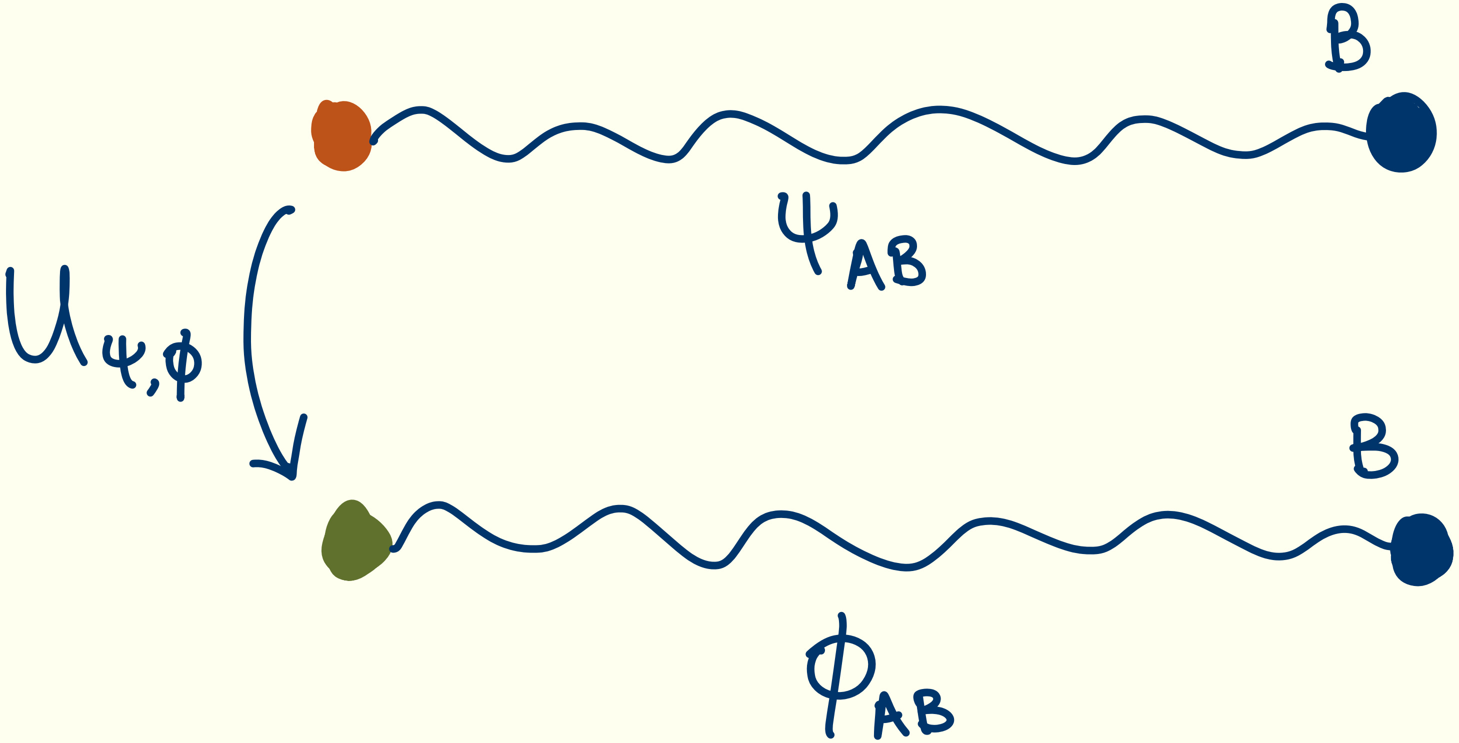
Motivating example: Uhlmann's theorem

Say that we know about two bipartite states, $|\psi\rangle$ and $|\phi\rangle$, such that their reduced states on register B is the same.



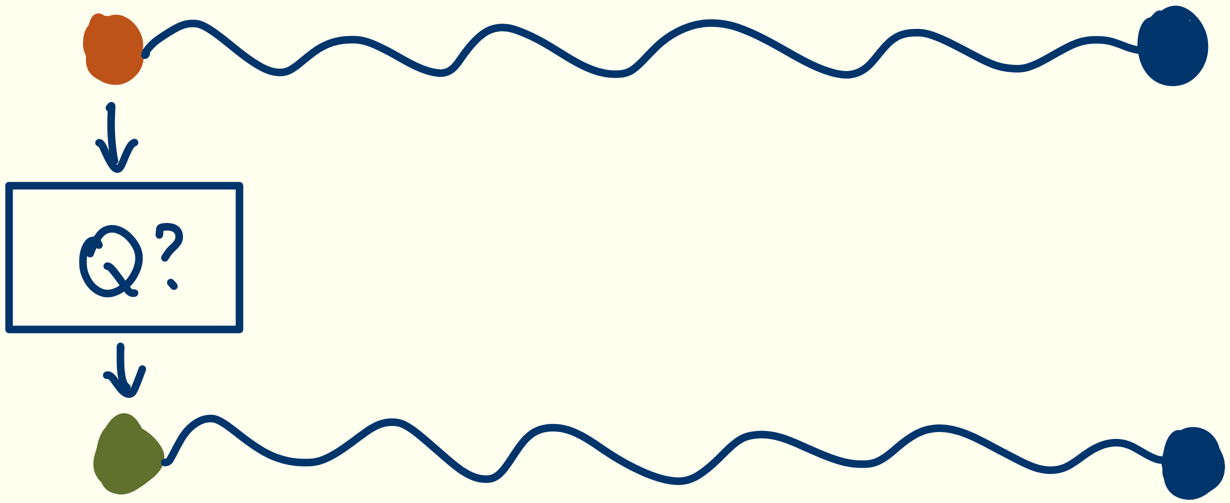
Motivating example: Uhlmann's theorem

Uhlmann's theorem says that there exists a unitary, $U_{\psi,\phi}$ that transforms $|\psi\rangle$ to $|\phi\rangle$ while only touching the A register.



Motivating example: Uhlmann's theorem

Uhlmann's theorem says that there exists a unitary, $U_{\psi,\phi}$ that transforms $|\psi\rangle$ to $|\phi\rangle$ while only touching the A register.



But how hard is it to actually implement that unitary?

Implementing Uhlmann's theorem

In the previous setup, Alice has:

Implementing Uhlmann's theorem

In the previous setup, Alice has:

- The A register of $|\psi\rangle_{AB}$.

Implementing Uhlmann's theorem

In the previous setup, Alice has:

- The A register of $|\psi\rangle_{AB}$.
- Knowledge of what $|\psi\rangle$ and $|\phi\rangle$ are.

Implementing Uhlmann's theorem

In the previous setup, Alice has:

- The A register of $|\psi\rangle_{\mathrm{AB}}$.
- Knowledge of what $|\psi\rangle$ and $|\phi\rangle$ are.
- A precision ϵ that they must approximate the unitary to.

Implementing Uhlmann's theorem

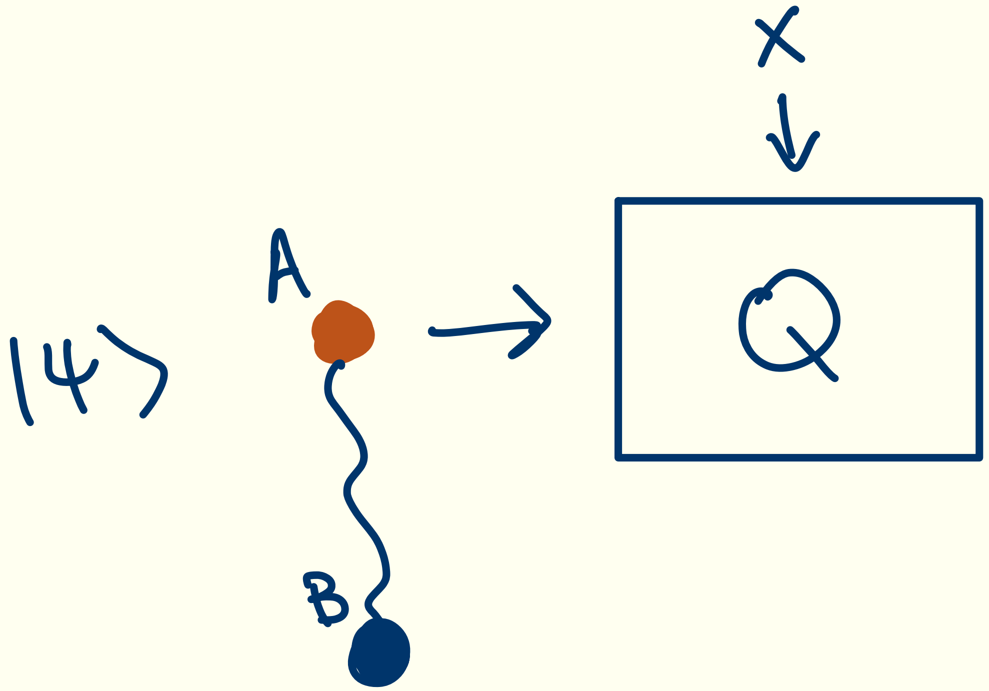
In the previous setup, Alice has:

- The A register of $|\psi\rangle_{\mathrm{AB}}$.
- Knowledge of what $|\psi\rangle$ and $|\phi\rangle$ are.
- A precision ϵ that they must approximate the unitary to.

They should output a quantum register A such that, when paired with the original register B, should be close to $|\phi\rangle$.

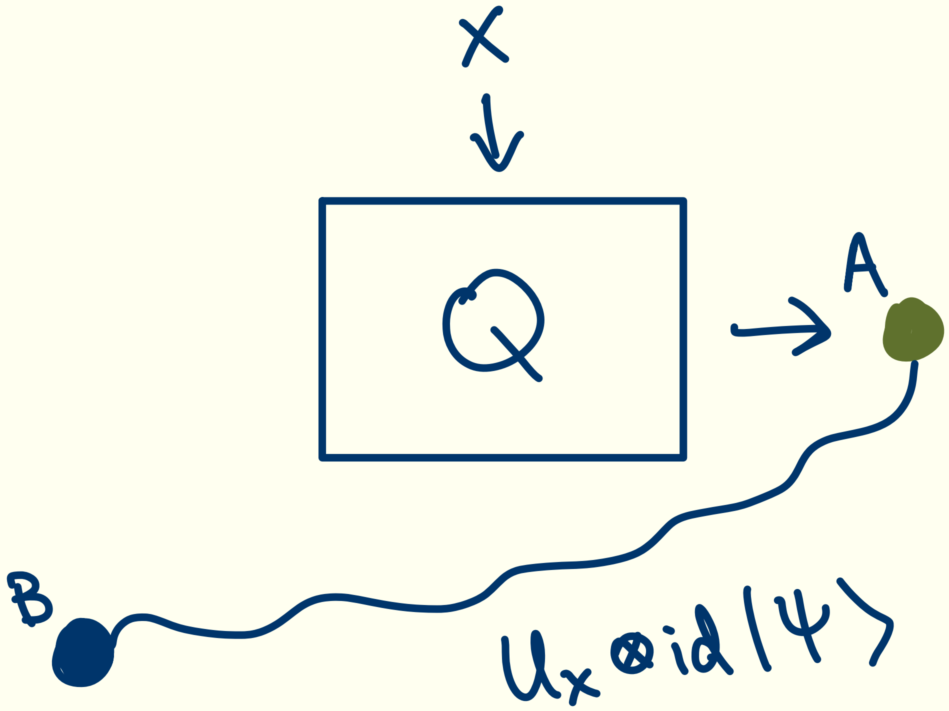
Unitary synthesis problems

A unitary synthesis problem is a family of unitary transformations indexed by a classical instance x: $\mathcal{U} = (U_x)_{x \in \{0,1\}^*}$.



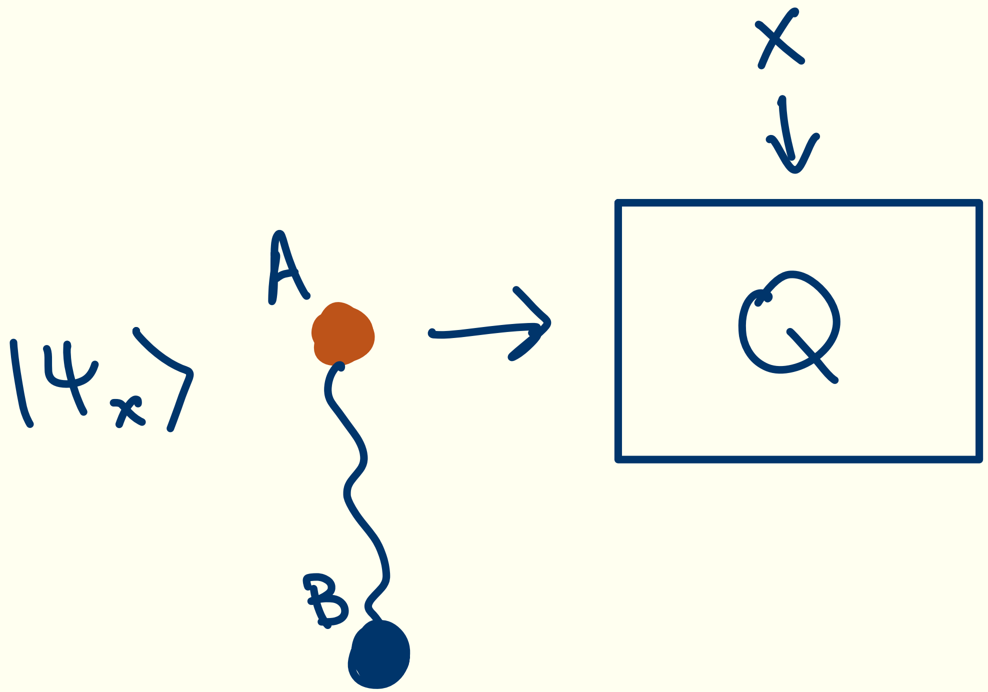
Unitary synthesis problems

A quantum model of computation implements $\mathcal{U}$ if given x and any (potentially entangled) quantum input $|\psi\rangle$, the model outputs $U_x \otimes \mathrm{id}\,|\psi\rangle$.



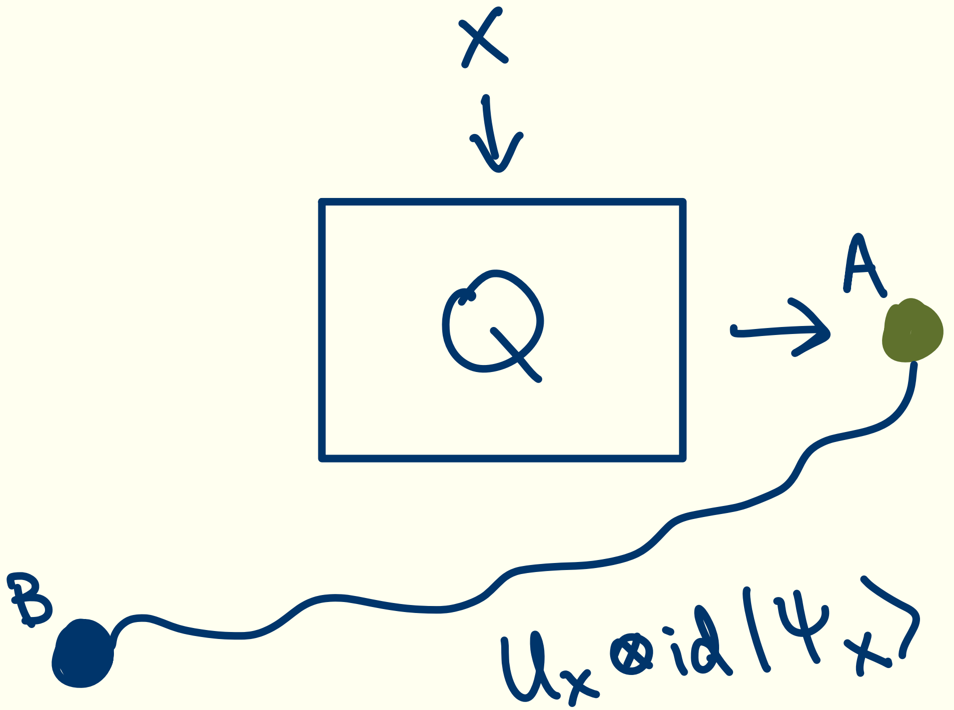
Distributional unitary synthesis problems

A distributional unitary synthesis problem is a family of unitary transformations and a family of states indexed by the same x, $(\mathcal{U} = (U_x)_{x\in\{0,1\}^*}, \Psi = (|\psi\rangle_x)_{x\in\{0,1\}^*})$.



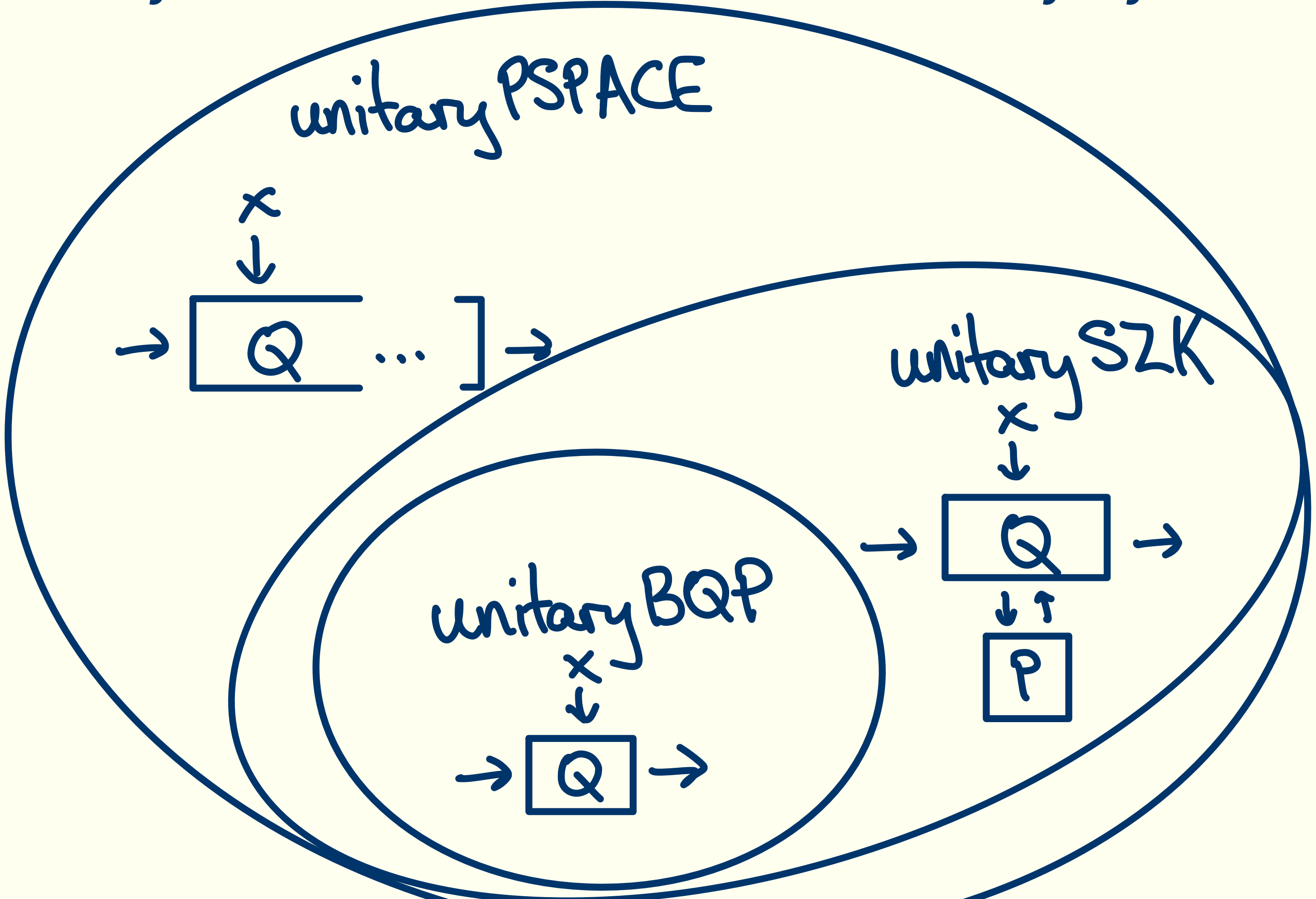
Distributional unitary synthesis problems

A quantum model of computation implements $(\mathcal{U}, \Psi)$ if given x and a copy of $|\psi_x\rangle$, the model outputs $U_x \otimes \mathrm{id}\,|\psi_x\rangle$.



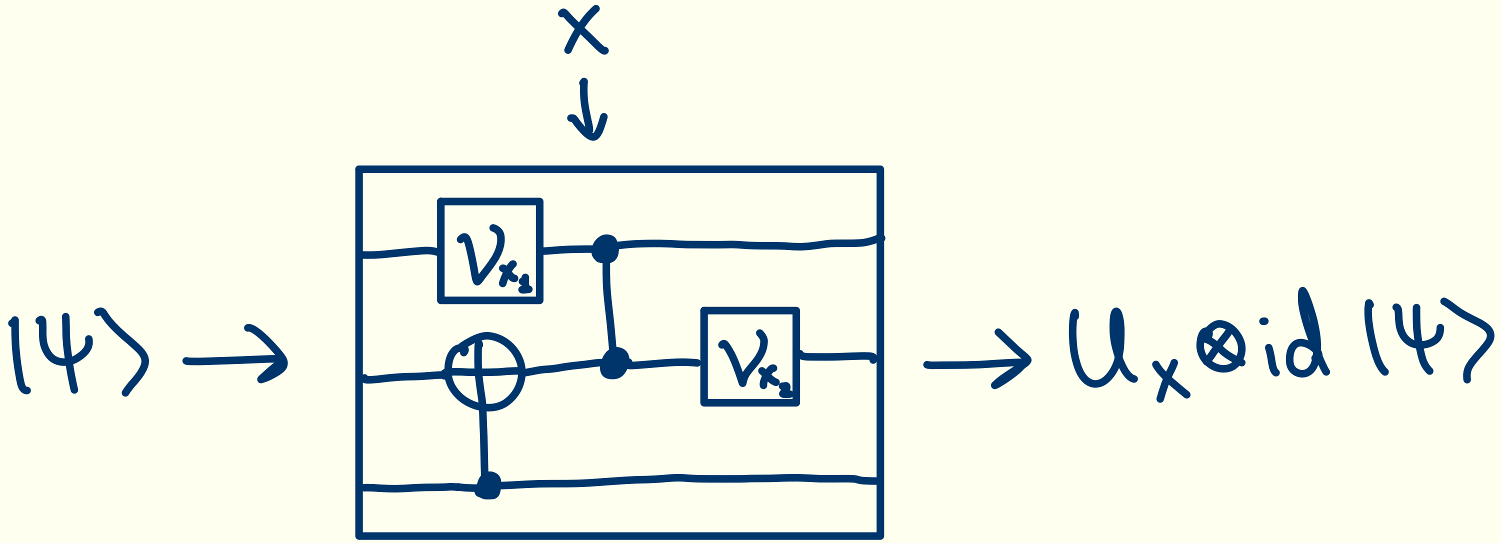
Unitary complexity classes

A unitary complexity class is a collection of unitary synthesis problems.



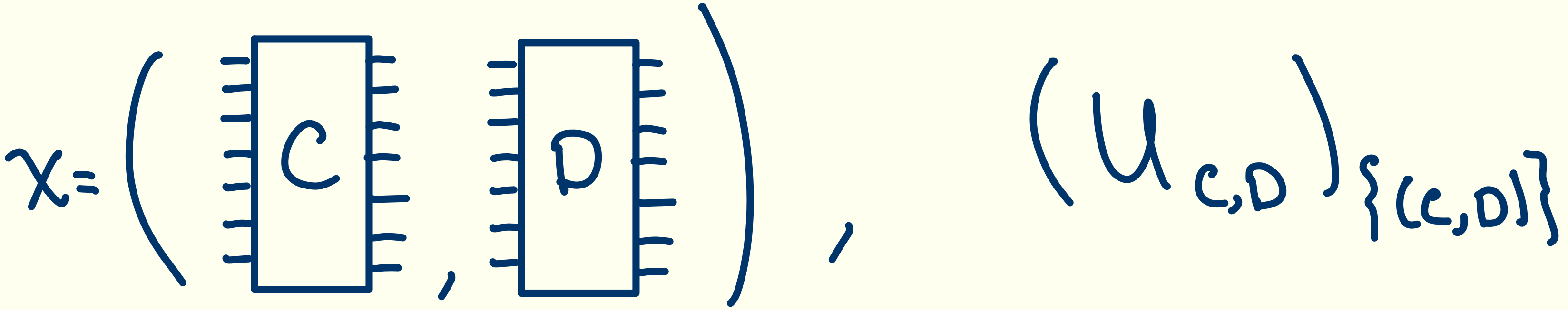
Reductions

A unitary synthesis problem $\mathcal{U}$ reduces to another unitary synthesis problem $\mathcal{V}$ if there is a polynomial-time algorithm with query access to $\mathcal{V}$ that implements $\mathcal{U}$.



The Uhlmann transformation problem

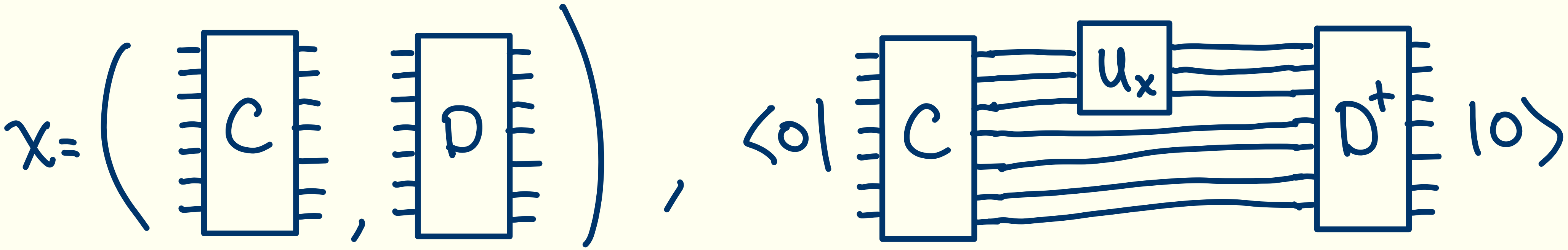
Uhlmann = $(U_x)_{x \in \{0,1\}^*}$ such that $x = (C, D)$ is a pair of polynomial sized circuits such that $|\psi\rangle = C|0\rangle$ and $|\phi\rangle = D|0\rangle$, and U_x is the unitary that maps between the two.



The Uhlmann transformation problem

Uhlmann = $(U_x)_{x\in\{0,1\}^*}$ such that $x = (C, D)$ is a pair of polynomial sized circuits such that $|\psi\rangle = C|0\rangle$ and $|\phi\rangle = D|0\rangle$, and U_x is the unitary that maps between the two.

The input is all of the C states: $\Psi_{\text{Uhlmann}} = (C|0\rangle)_{x=(C,D)\in\{0,1\}^*}$.



The complexity of Uhlmann

avgUnitarySZK (informal): The unitary complexity class of all unitary synthesis problems that can be implemented by a polynomial-time verifier interacting with a prover, such that the interaction with the honest prover can be simulated.

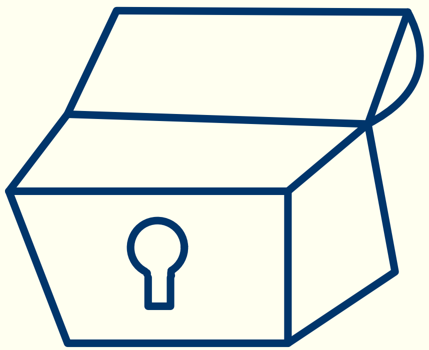
A somewhat natural extension of QSZK to unitary synthesis problems.

The complexity of Uhlmann

Theorem (informal): Uhlmann is complete for the distributional unitary complexity class avgUnitarySZK.

Uhlmann and cryptography

Bit commitments are the cryptographic equivalent of sending a message in a sealed envelope to a receiver.



Uhlmann and cryptography

Bit commitments are the cryptographic equivalent of sending a message in a sealed envelope to a receiver.

A bit commitment has two phases, a commit phase and a reveal phase.

Sender

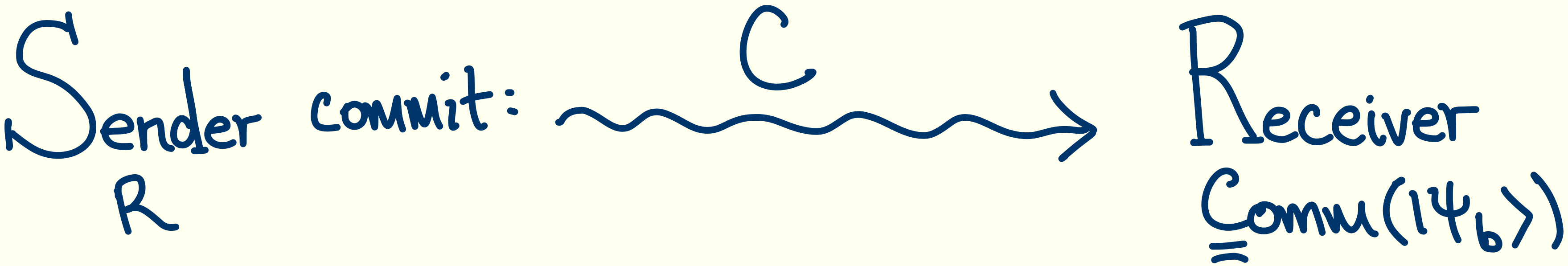
$|\psi_b\rangle\langle\psi_b|_{RC}$

Receiver

Uhlmann and cryptography

Bit commitments are the cryptographic equivalent of sending a message in a sealed envelope to a receiver.

A bit commitment has two phases, a commit phase and a reveal phase.



Uhlmann and cryptography

Bit commitments are the cryptographic equivalent of sending a message in a sealed envelope to a receiver.

A bit commitment has two phases, a commit phase and a reveal phase.

Sender

R

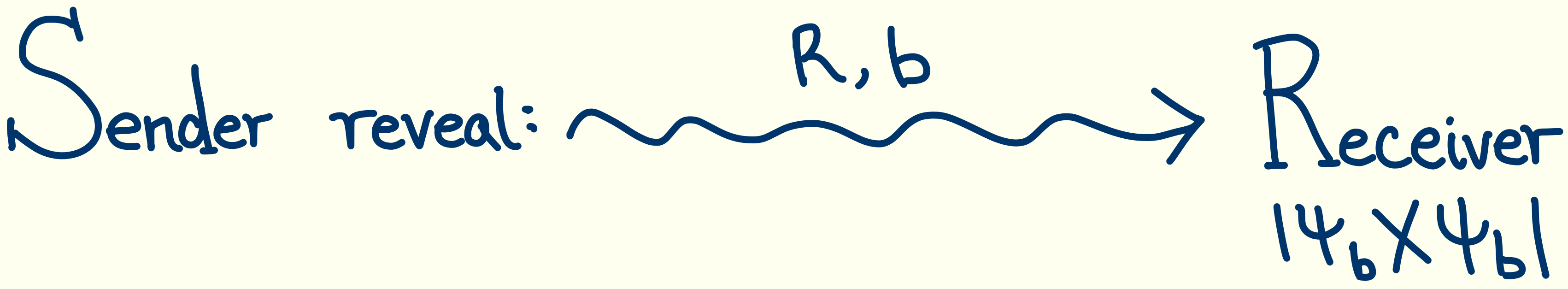
Receiver

$\mathrm{Comm}(|\psi_b\rangle)$

Uhlmann and cryptography

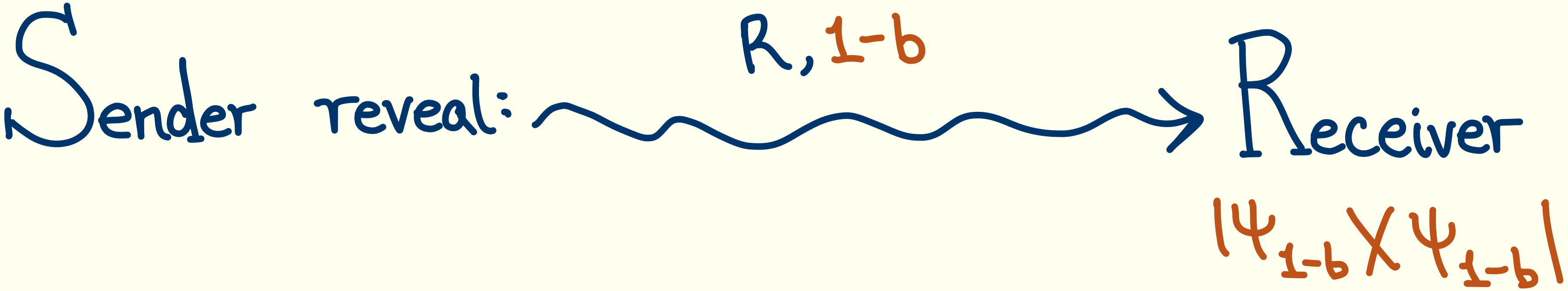
Bit commitments are the cryptographic equivalent of sending a message in a sealed envelope to a receiver.

A bit commitment has two phases, a commit phase and a reveal phase.



Uhlmann and cryptography

A commitment is binding if the sender can not change their message after they give the sender their commitment.



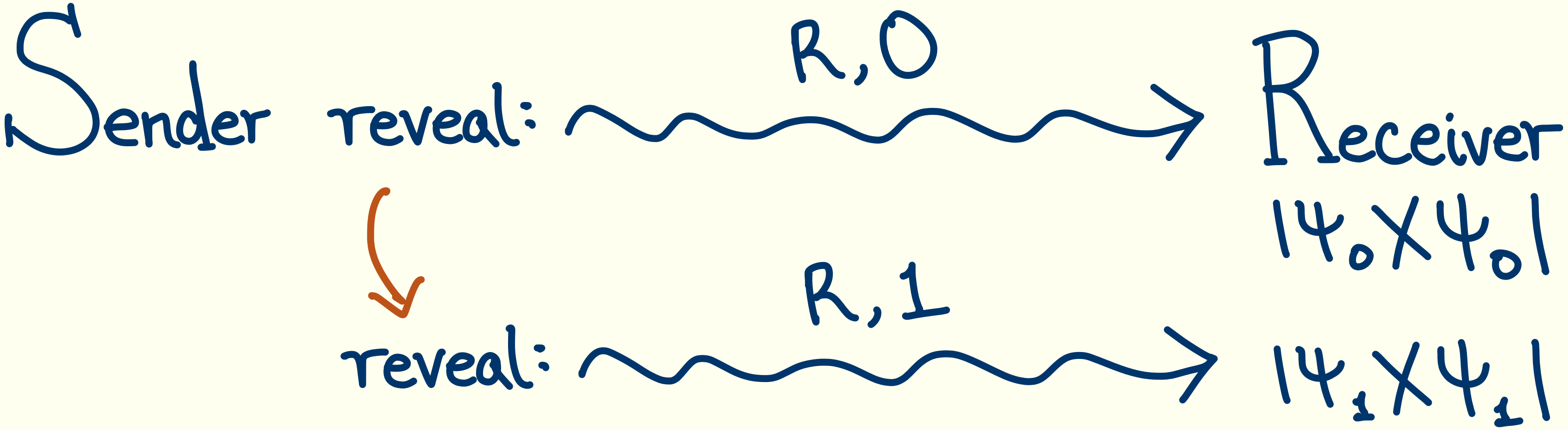
Uhlmann and cryptography

Theorem (informal): Uhlmann is equivalent to the problem of breaking the binding property of (statistically hiding) quantum commitments.

Uhlmann and cryptography

Theorem (informal): Uhlmann is equivalent to the problem of breaking the binding property of (statistically hiding) quantum commitments.

Idea: The commitments to 0 and 1 for statistically hiding commitments are valid Uhlmann instances.



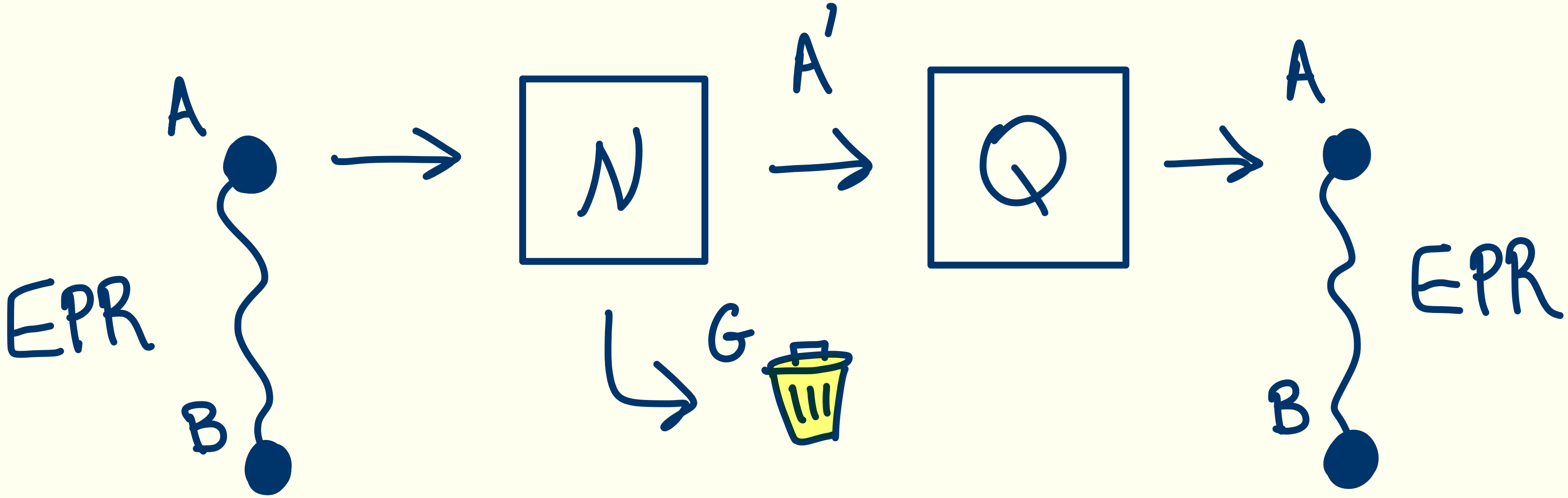
Uhlmann and cryptography

Theorem (informal): Uhlmann is equivalent to the problem of breaking the binding property of (statistically hiding) quantum commitments.

Corollary (informal): Combined with BQSY'23, Uhlmann is not in avgUnitaryBQP if and only if (infinitely often) secure commitments exist.

Uhlmann and Shannon theory

Informally, the decodable channel problem is the following: Say that I have a channel $\mathcal{N}$, and I put half of a maximally entangled state into it. Recover the maximally entangled state with only the output of the channel.



Uhlmann and Shannon theory

More formally, $\mathcal{U}_{\text{DecodableChannel}} = (U_{\mathcal{N}})_{\mathcal{N} \text{ quantum channel}}$, $\Psi_{\text{DecodableChannel}} = (|\text{EPR}_n\rangle)_{\mathcal{N}}$, where n is the input length of $\mathcal{N}$.

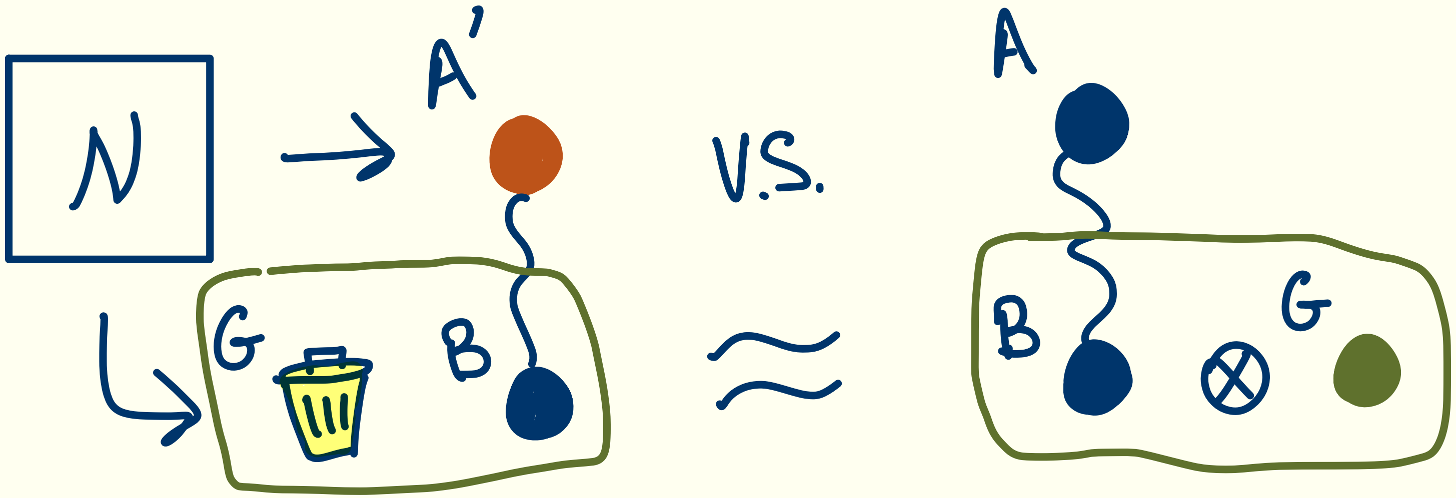
Uhlmann and Shannon theory

Theorem (informal): The decodable channel problem is equivalent to the Uhlmann transformation problem.

Uhlmann and Shannon theory

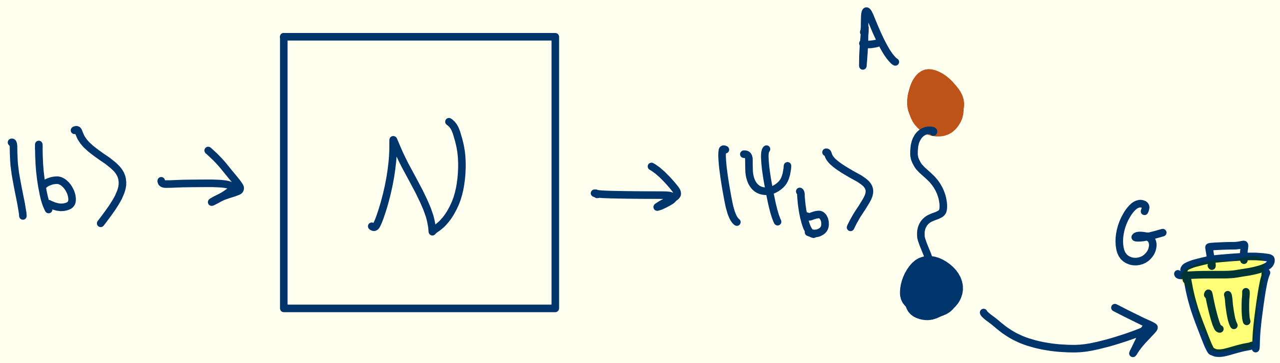
Theorem (informal): The decodable channel problem is equivalent to the Uhlmann transformation problem.

Idea: In one direction, the state before and after the (purification of the) channel are a valid Uhlmann instance.



Uhlmann and Shannon theory

Idea: In the other direction, given a input-output pair for Uhlmann, have the channel map 0 and 1 to the input and output respectively, and trace out the B register.

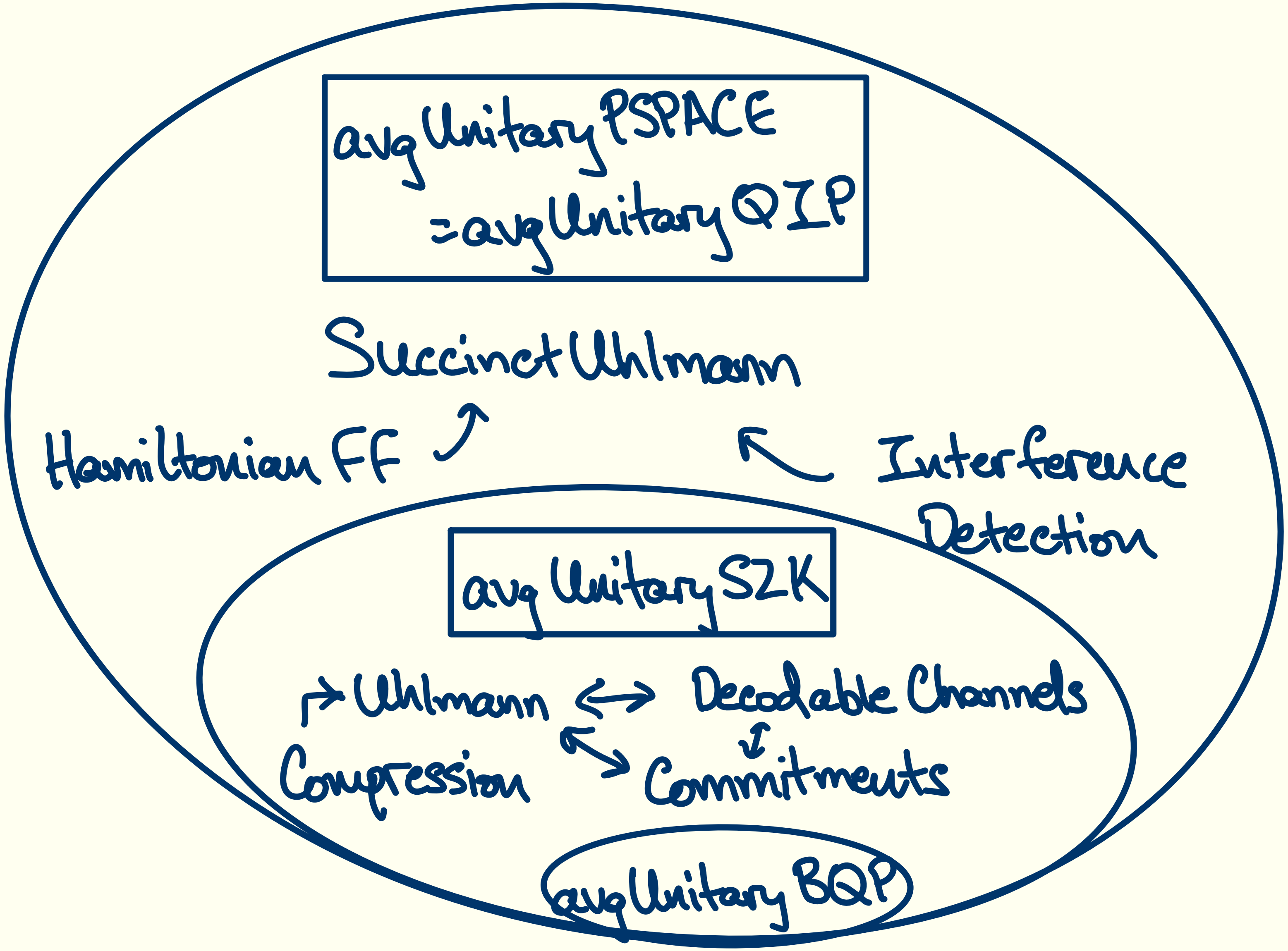


Solving the decodable channel problem on this instance can be used to implement the Uhlmann transformation.

Succinct Uhlmann and PSPACE

If we instead allow the instance to be “succinct”, we get a problem that turns out to be complete for both avgUnitaryPSPACE and avgUnitaryQIP, thus showing that these two classes are equal!

The unitary synthesis landscape today



The future of unitary synthesis

Populating the zoo: UnitaryQMA?

The first direction I want to pitch is studying more unitary complexity classes and finding complete problems for them.

Populating the zoo: UnitaryQMA?

The first direction I want to pitch is studying more unitary complexity classes and finding complete problems for them.

I think a natural one is an equivalent of QMA, but it's not so easy to define it in a reasonable way!

Unitaries with quantum witnesses?

Here's a first attempt:

Say that a family of unitaries $\mathcal{U} = (U_x)_{x \in \{0,1\}^*}$ is in unitaryQMA if there a quantum polynomial-time verifier that can implement $\mathcal{U}$ with an additional quantum witness.

Unitaries with quantum witnesses?

Completeness: There is some subspace of witnesses that cause the verifier to implement the correct unitary.

Soundness: If the verifier correctly implements the unitary, the state must come from the "good witness" subspace.

Unitaries with quantum witnesses?

The definition is quite subtle, as we also need the verifier to "correctly" implement no instances of a QMA problem: Our verifier should do something for every input.

Imagine a unitary synthesis problem that is identity if the instance is in a language, and a sign flip it is not, why is this unitary synthesis problem in this version of unitaryQMA?

Unitaries with quantum witnesses?

I have some ideas for complete problems, but I haven't figured out how to show that they are complete.

I also have no idea for how to relate this class to other sub-fields of quantum computer science!

Efficiently verifiable unitaries?

Maybe another way to define unitaryQMA is that a unitary is in unitaryQMA if there is a quantum polynomial-time verifier that gets a pair of states in tensor product, $|\psi\rangle \otimes |\phi\rangle$, and should accept if and only if $|\phi\rangle = U_x|\psi\rangle$.

Efficiently verifiable unitaries?

This definition seems more natural for some cryptography applications, like one-way state generators.

High level: For a one-way state generator, it should be hard to $|\psi_k\rangle$ to a key k that is accepted by a verifier that takes a copy of the state and the proposed key. The verifier will play the role of the unitaryQMA verifier.

Efficiently verifiable unitaries?

However, I do not know of a “good” complete problem for this class (i.e. something that is not complete by definition).

Motivating quantum complexity

Another big open problem is: Can you find a pair of unitary complexity classes (or a problem and complexity class) that have a "different" relationship than their classical counterparts?

Motivating quantum complexity

One approach: In some restricted cases, commuting Hamiltonians have been shown to be classical (i.e. a NP verifier can check the ground energy), but the proofs are non-constructive (i.e. the witness can not be used to construct the ground state).

Motivating quantum complexity

Can you show that the ground states of commuting Hamiltonians are stateQMA complete?

Can you show that mapping between ground-spaces of commuting Hamiltonians (for some reasonable definition of this) is unitaryQMA complete?

This would imply solving the decision version of some problems can remove the quantum-ness from the problem!

Thanks for listening!