Title: The Topology of Information Flow

Date: Sep 30, 2014 03:30 PM

URL: http://pirsa.org/14090076

Abstract: I will outline a new topological foundation for computation, and show how it gives rise to a unified treatment of classical encryption and quantum teleportation, and a strong classical model for many quantum phenomena. This work connects to some other interesting topics, including quantum field theory, classical combinatorics, thermodynamics, Morse theory and higher category theory, which I will introduce in an elementary way.

The Topology of Information Flow

Jamie Vicary
Department of Computer Science, University of Oxford

QMAC

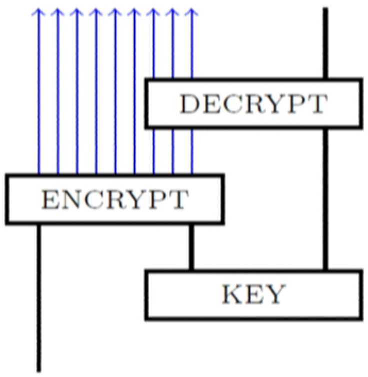
Quantum Foundations Seminar
Perimeter Institute, Waterloo, Canada
30 September 2014

Introduction

There is an analogy between classical encryption and quantum teleportation, extending to the foundations of computation.

Introduction

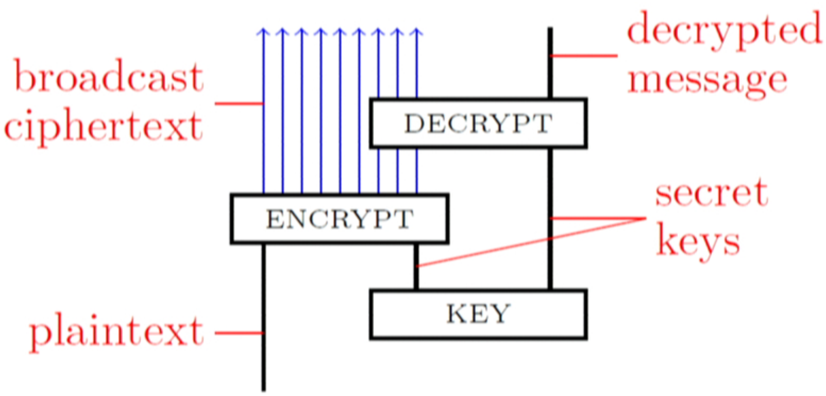
There is an analogy between classical encryption and quantum teleportation, extending to the foundations of computation.



Encrypted communication

Introduction

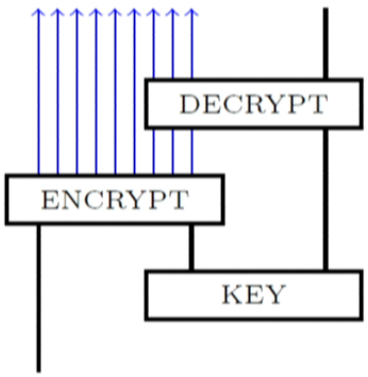
There is an analogy between classical encryption and quantum teleportation, extending to the foundations of computation.



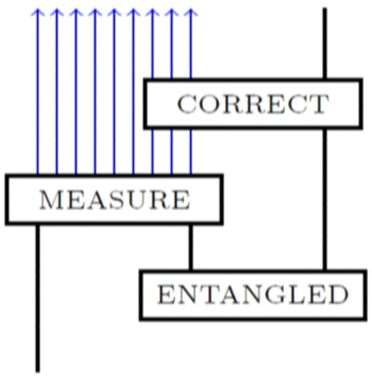
Encrypted communication

Introduction

There is an analogy between classical encryption and quantum teleportation, extending to the foundations of computation.



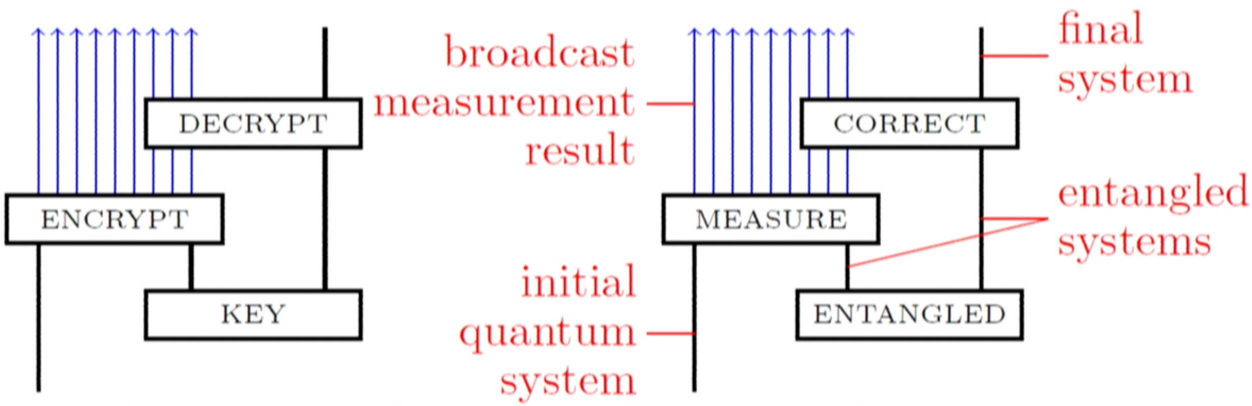
Encrypted communication



Quantum teleportation

Introduction

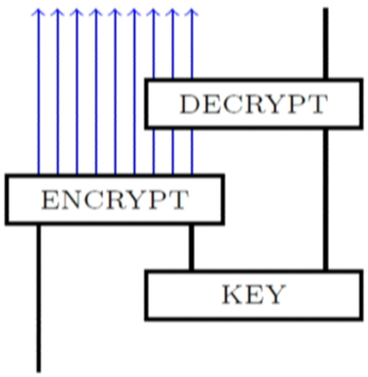
There is an analogy between classical encryption and quantum teleportation, extending to the foundations of computation.



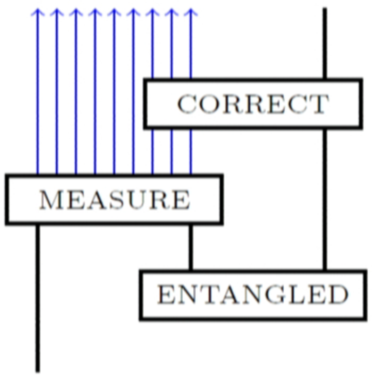
Encrypted communication Quantum teleportation

Introduction

There is an analogy between classical encryption and quantum teleportation, extending to the foundations of computation.



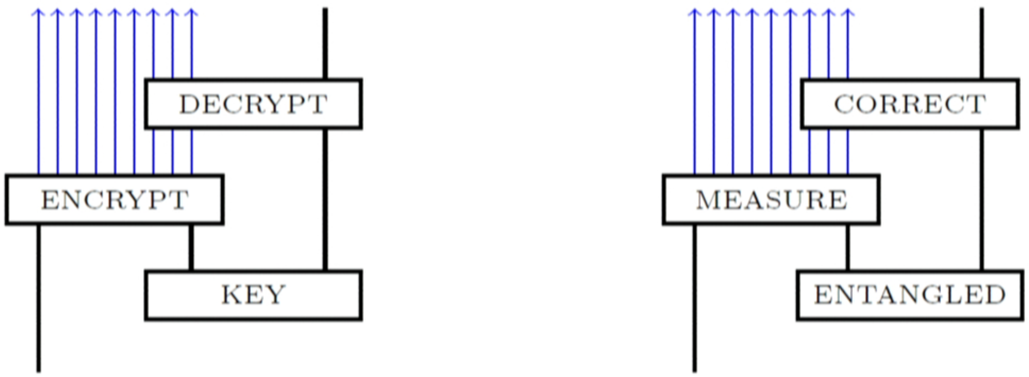
Encrypted communication



Quantum teleportation

Introduction

There is an analogy between classical encryption and quantum teleportation, extending to the foundations of computation.



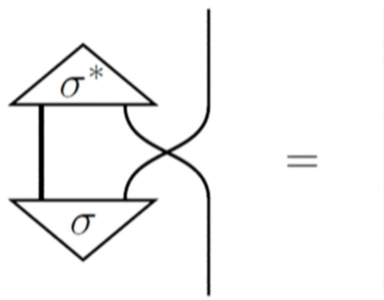
Encrypted communication

Quantum teleportation

New idea. We can make this precise using defects between topological field theories.

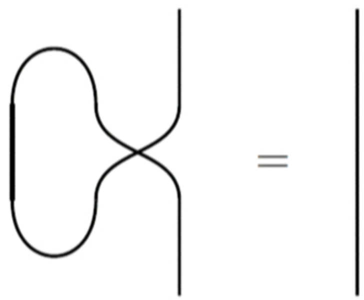
Strings and correlation

Consider the following equation, where σ is a joint state and σ^* is the corresponding joint measurement:



Strings and correlation

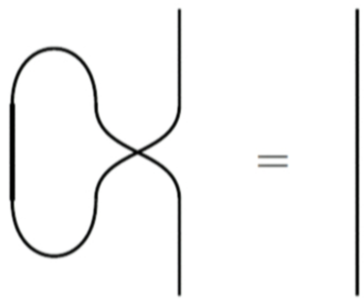
Consider the following equation, where σ is a joint state and σ^* is the corresponding joint measurement:



We change notation and use a **1d topological field theory**, where this is the first Reidemeister move.

Strings and correlation

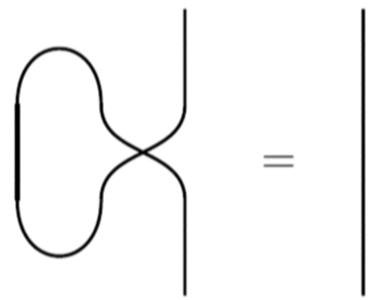
Consider the following equation, where σ is a joint state and σ^* is the corresponding joint measurement:



We change notation and use a **1d topological field theory**, where this is the first Reidemeister move.

Strings and correlation

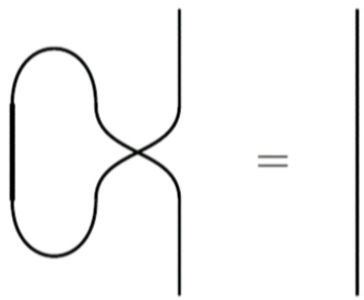
Consider the following equation, where σ is a joint state and σ^* is the corresponding joint measurement:



We change notation and use a **1d topological field theory**, where this is the first Reidemeister move.

Strings and correlation

Consider the following equation, where σ is a joint state and σ^* is the corresponding joint measurement:



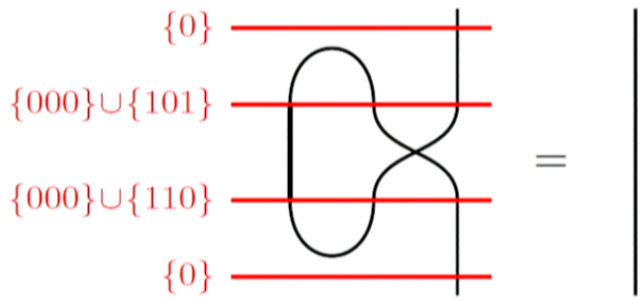
We change notation and use a **1d topological field theory**, where this is the first Reidemeister move.

We can investigate consequences of this equation in different settings.

- **Classical computation.**
  The state σ is *perfectly correlated*: $\sigma = \{00\} \cup \{11\}$.

Strings and correlation

Consider the following equation, where σ is a joint state and σ^* is the corresponding joint measurement:



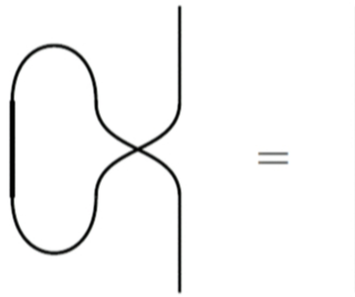
We change notation and use a **1d topological field theory**, where this is the first Reidemeister move.

We can investigate consequences of this equation in different settings.

- **Classical computation.**
  The state σ is *perfectly correlated*: $\sigma = \{00\} \cup \{11\}$.

Strings and correlation

Consider the following equation, where σ is a joint state and σ^* is the corresponding joint measurement:



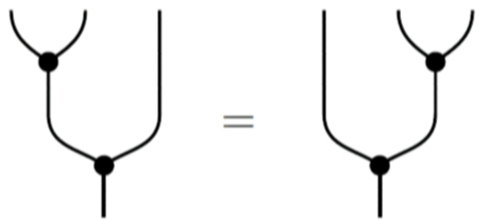
We change notation and use a **1d topological field theory**, where this is the first Reidemeister move.

We can investigate consequences of this equation in different settings.

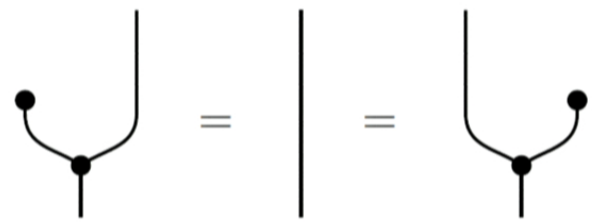
- **Classical computation.**
  The state σ is *perfectly correlated*: $\sigma = \{00\} \cup \{11\}$.
- **Quantum theory.**
  The state σ is *maximally entangled*: $|\sigma\rangle = |00\rangle + |11\rangle$

Surfaces and logic

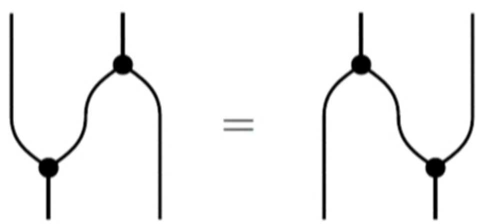
We now think about basic properties of copying, comparing and deleting classical information:



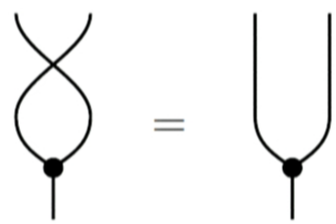
Associativity



Unit



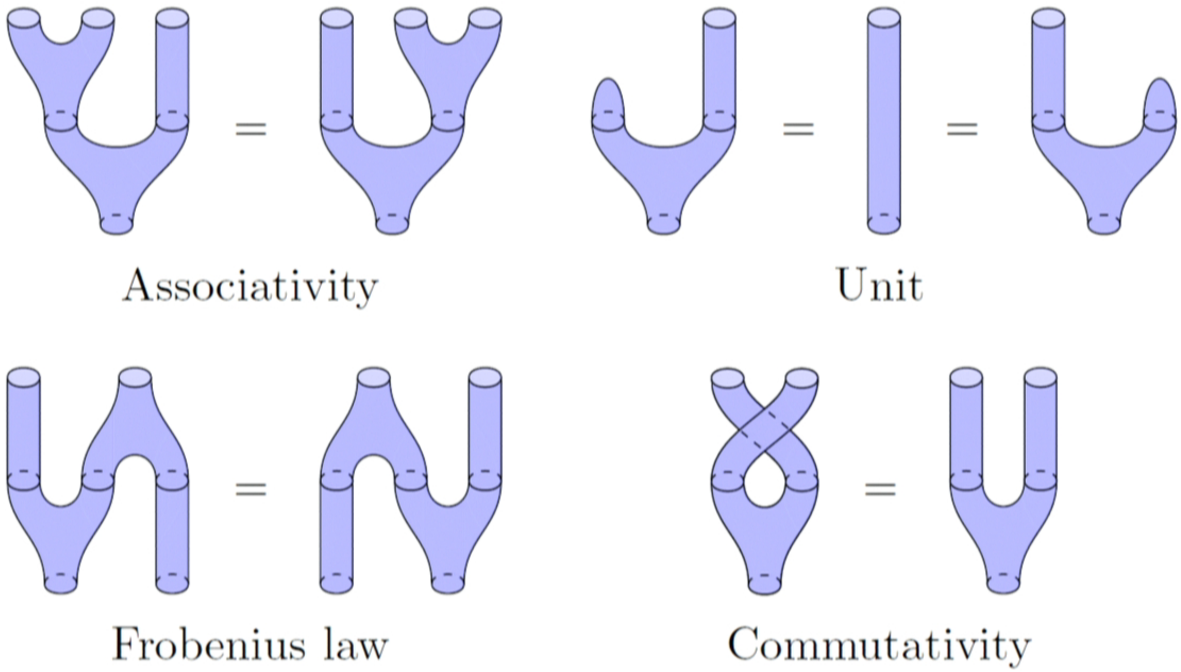
Frobenius law



Commutativity

Surfaces and logic

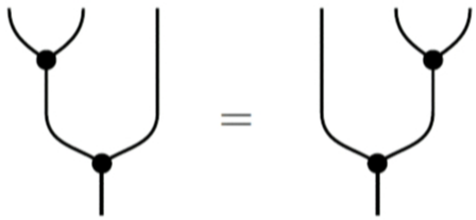
We now think about basic properties of copying, comparing and deleting classical information:



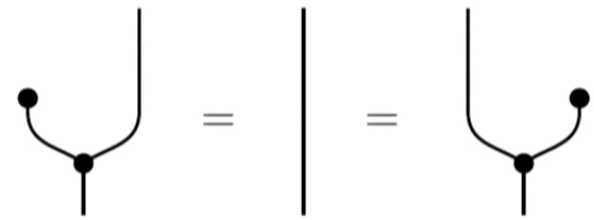
These are the laws obeyed by surfaces up to deformation!
So we change notation and use a **2d topological field theory**.

Surfaces and logic

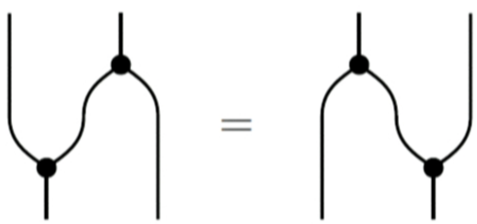
We now think about basic properties of copying, comparing and deleting classical information:



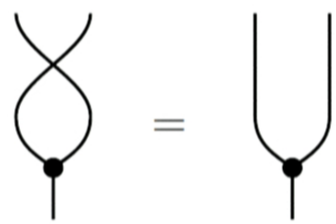
Associativity



Unit



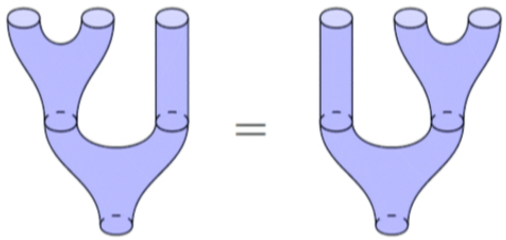
Frobenius law



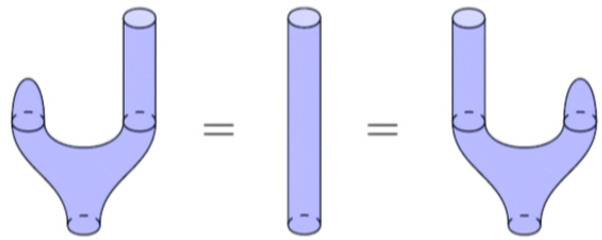
Commutativity

Surfaces and logic

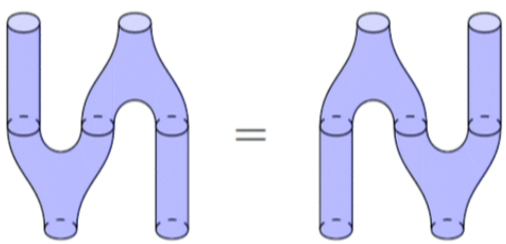
We now think about basic properties of copying, comparing and deleting classical information:



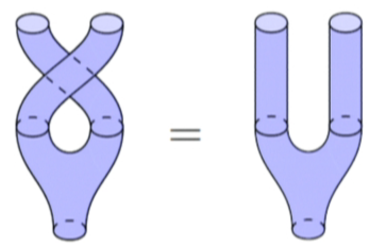
Associativity



Unit



Frobenius law

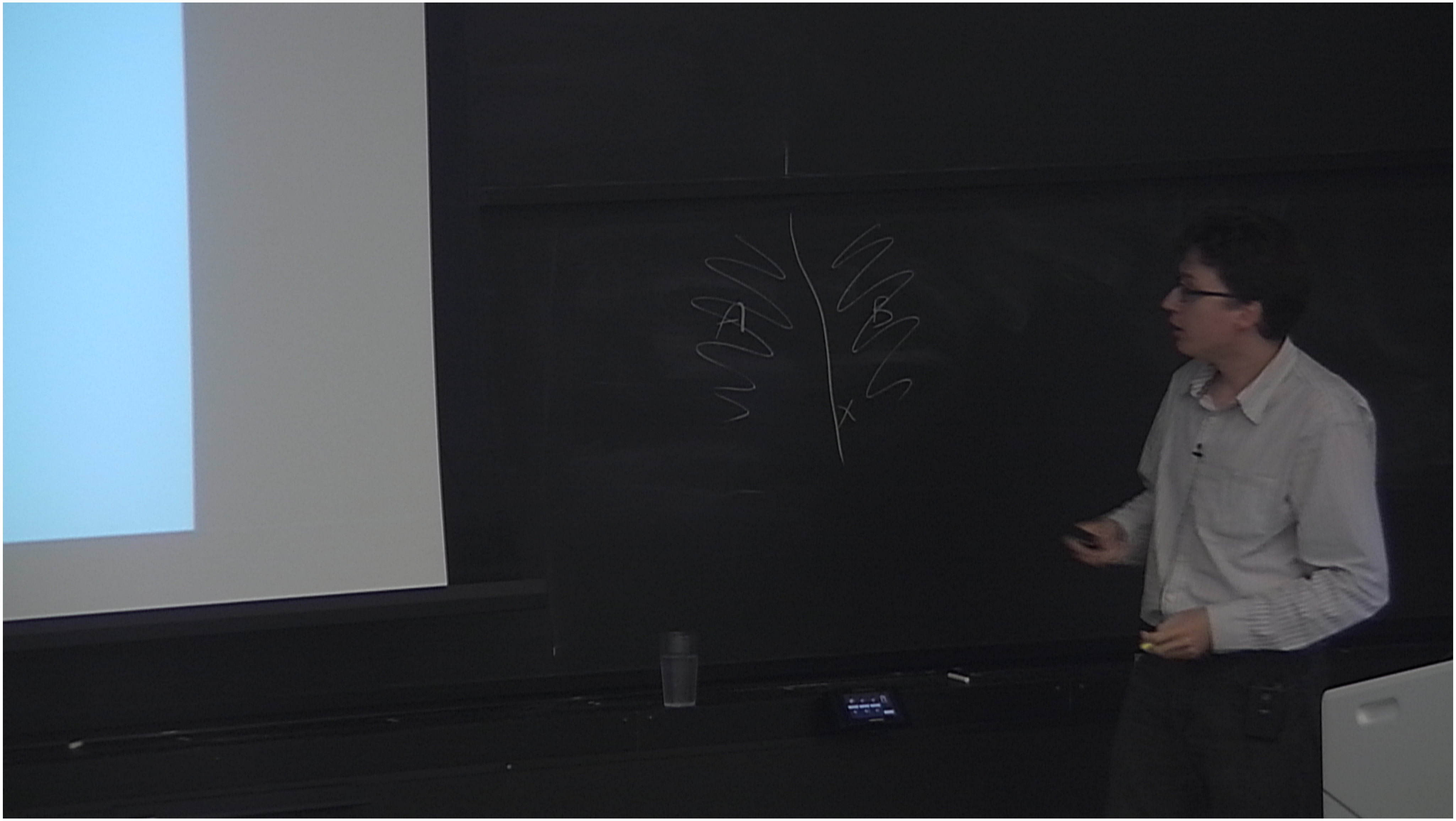


Commutativity

These are the laws obeyed by surfaces up to deformation!
So we change notation and use a **2d topological field theory**.

Interactions

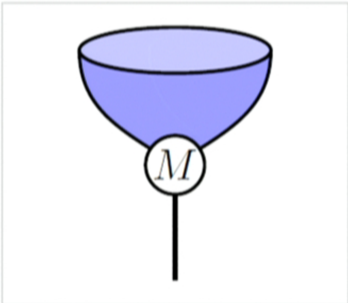
We now consider 'interactions' between our lines and surfaces.


A
B

Interactions

We now consider 'interactions' between our lines and surfaces.

We focus on 3 basic interaction types:

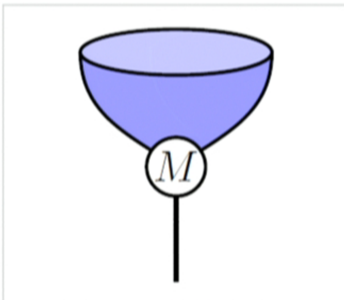


Measurement

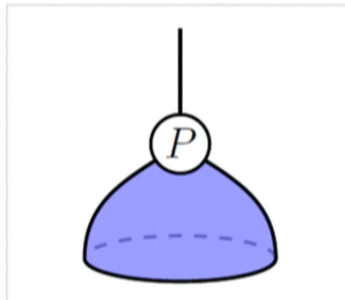
Interactions

We now consider 'interactions' between our lines and surfaces.

We focus on 3 basic interaction types:



Measurement

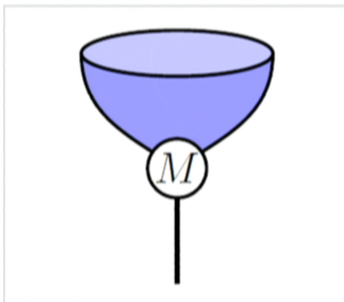


Preparation

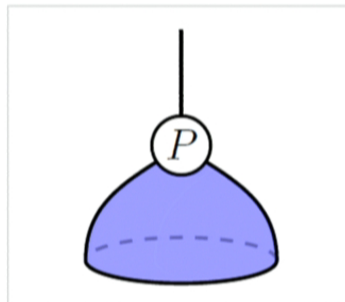
Interactions

We now consider 'interactions' between our lines and surfaces.

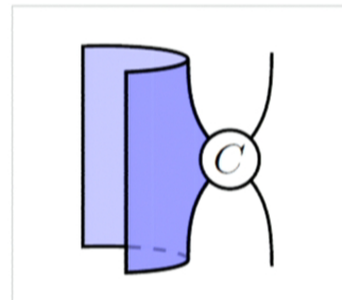
We focus on 3 basic interaction types:



Measurement



Preparation

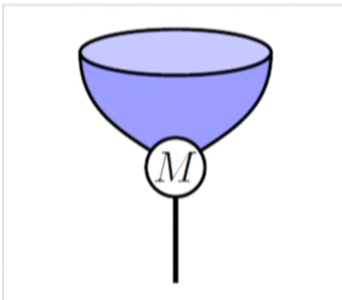


Controlled operation

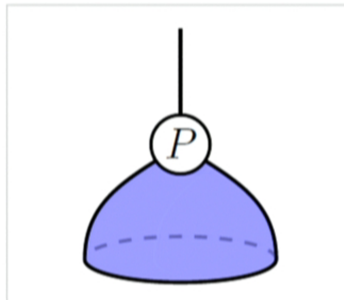
Interactions

We now consider 'interactions' between our lines and surfaces.

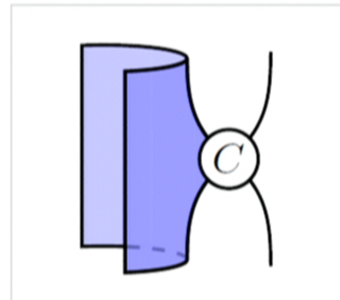
We focus on 3 basic interaction types:



Measurement



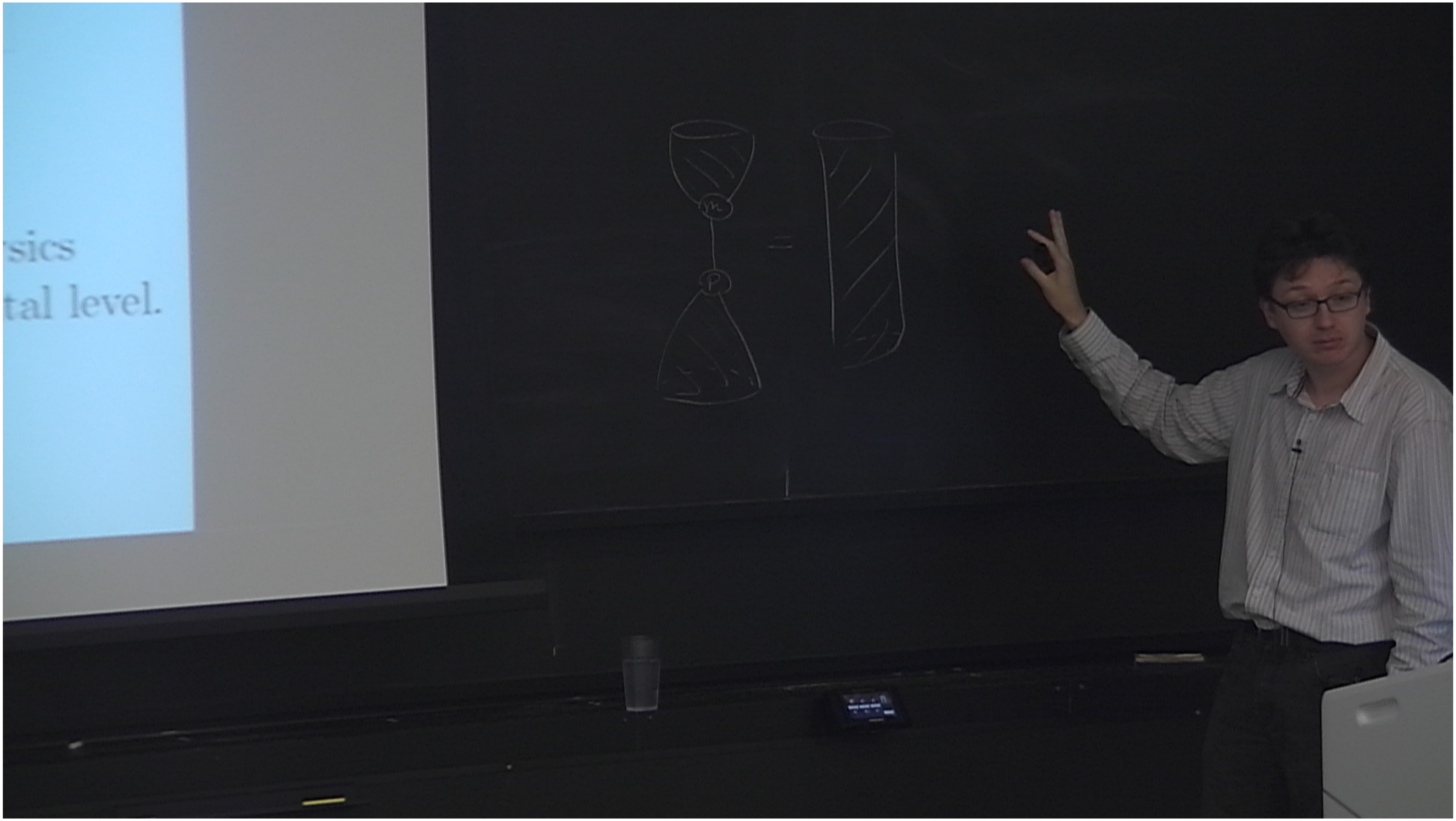
Preparation

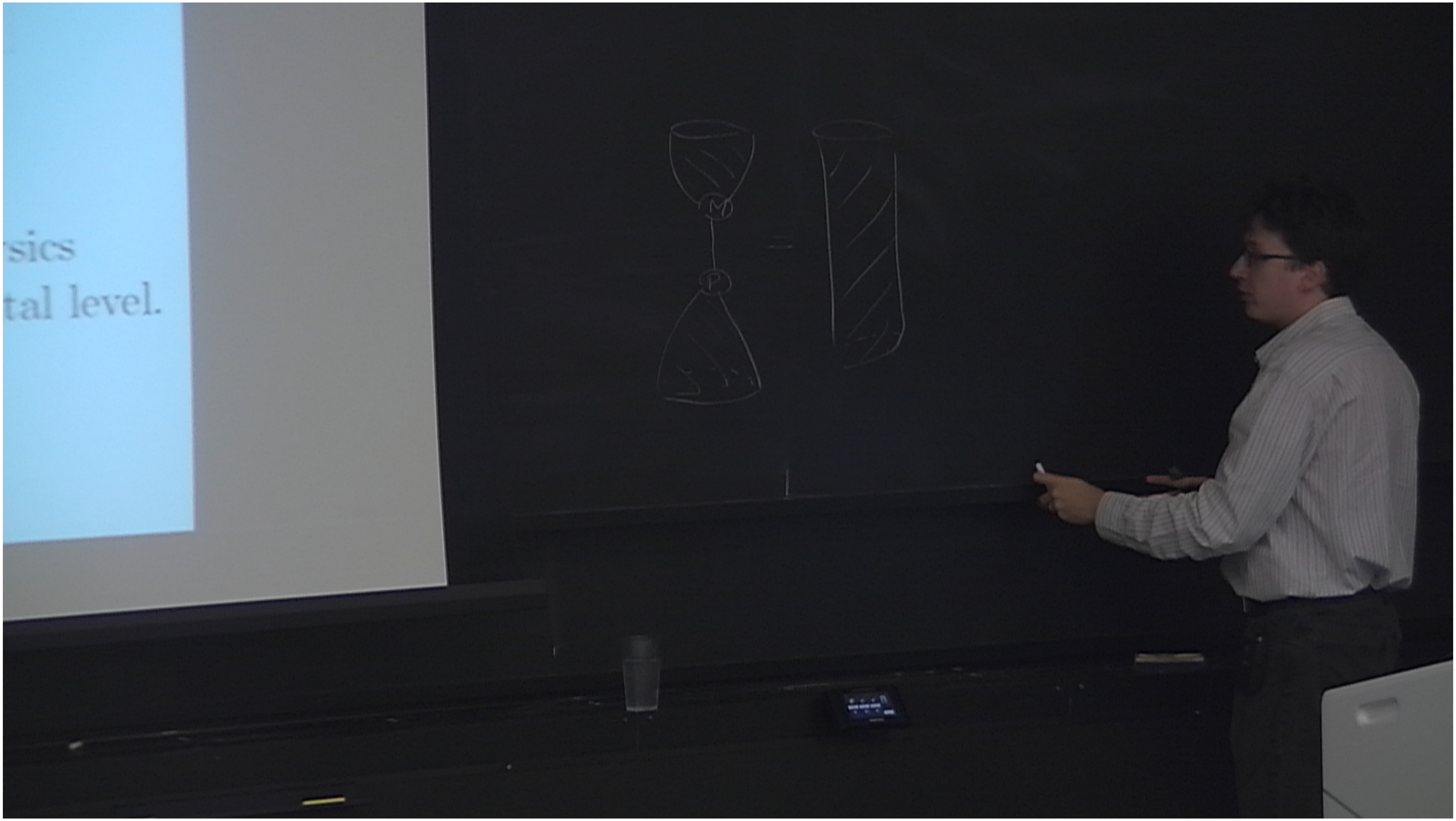


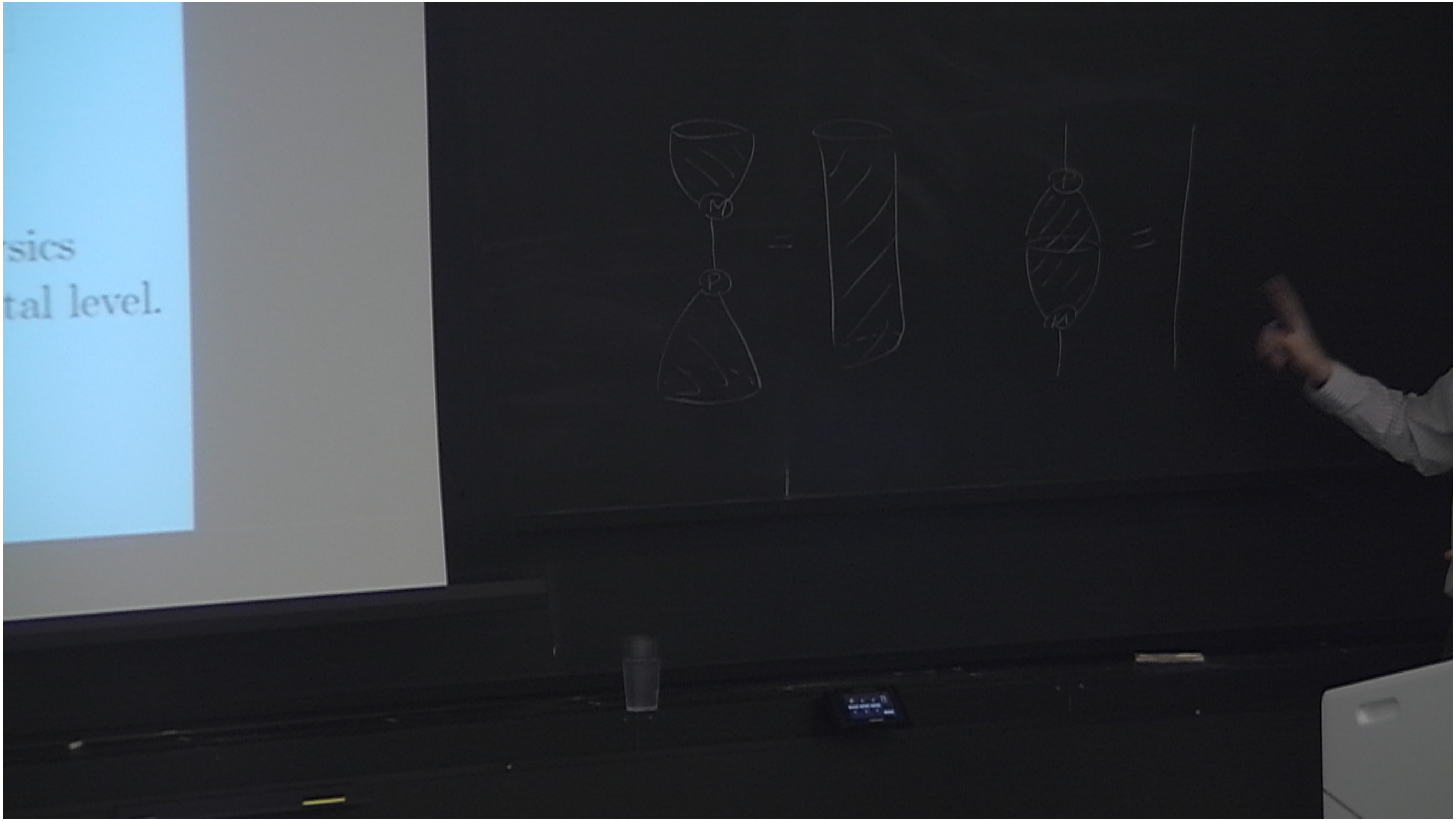
Controlled operation

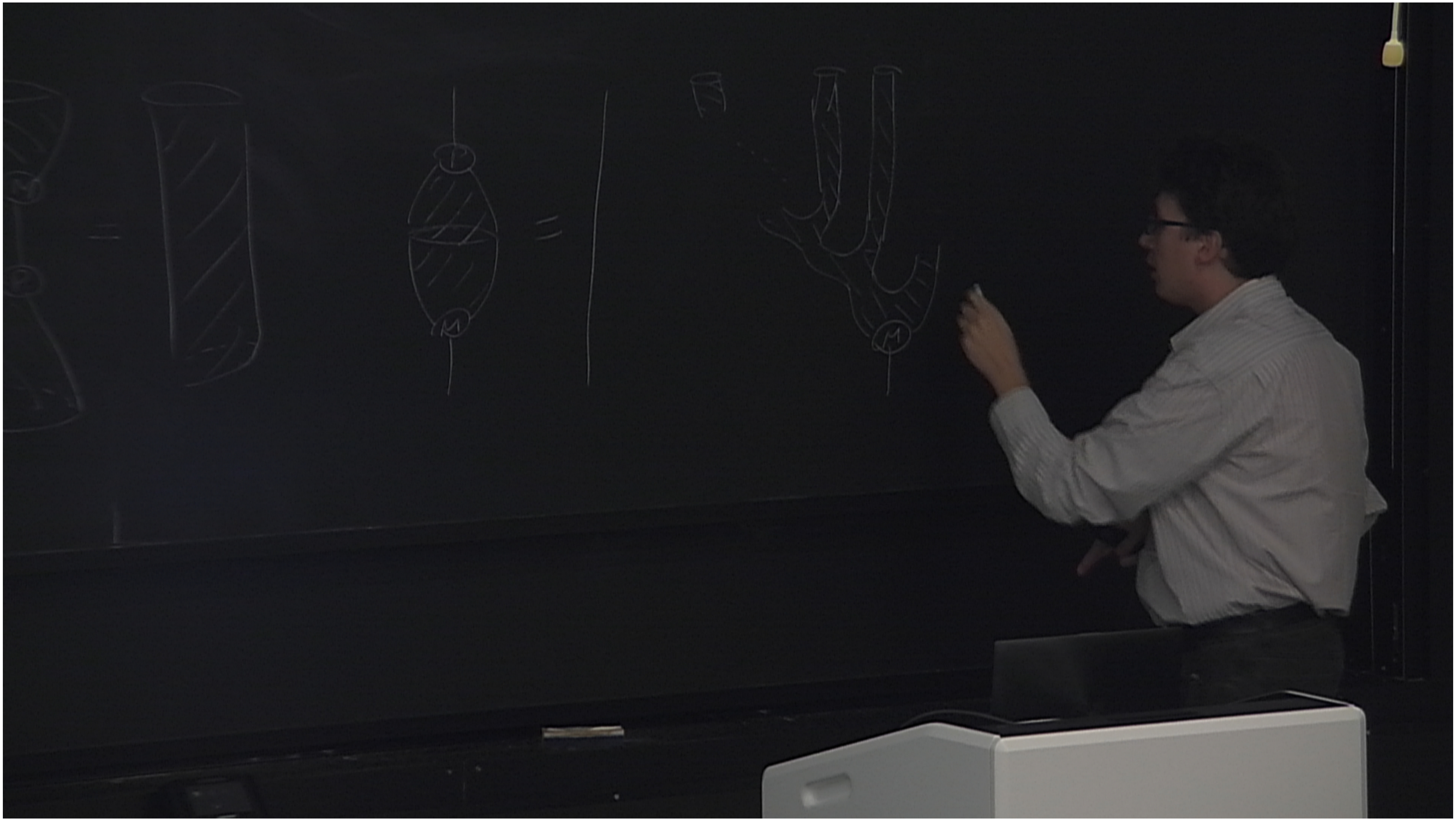
We require these to be invertible, because *all* processes in physics and computer science are (arguably) reversible at a fundamental level.

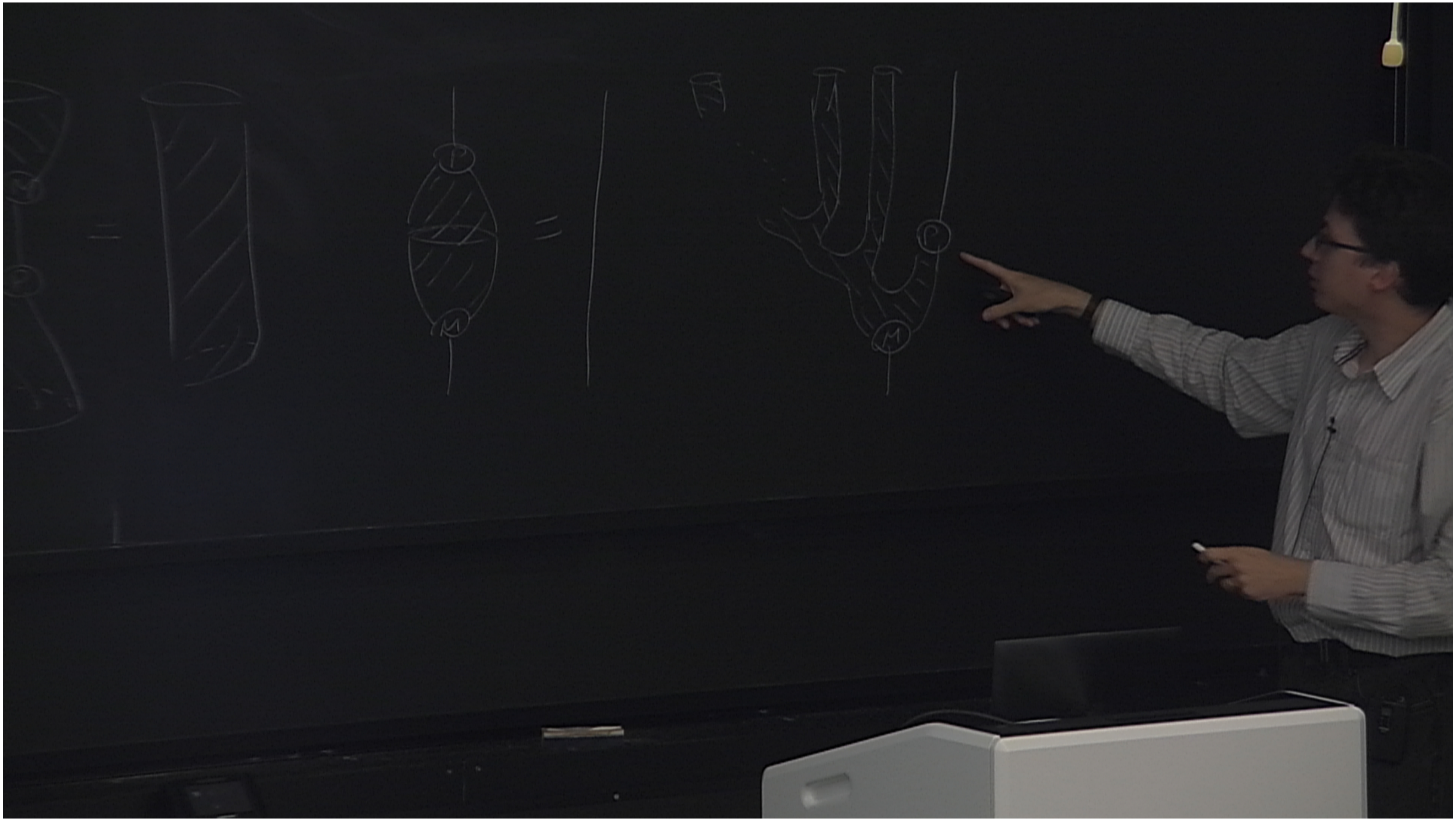
Also, M and P are inverse.

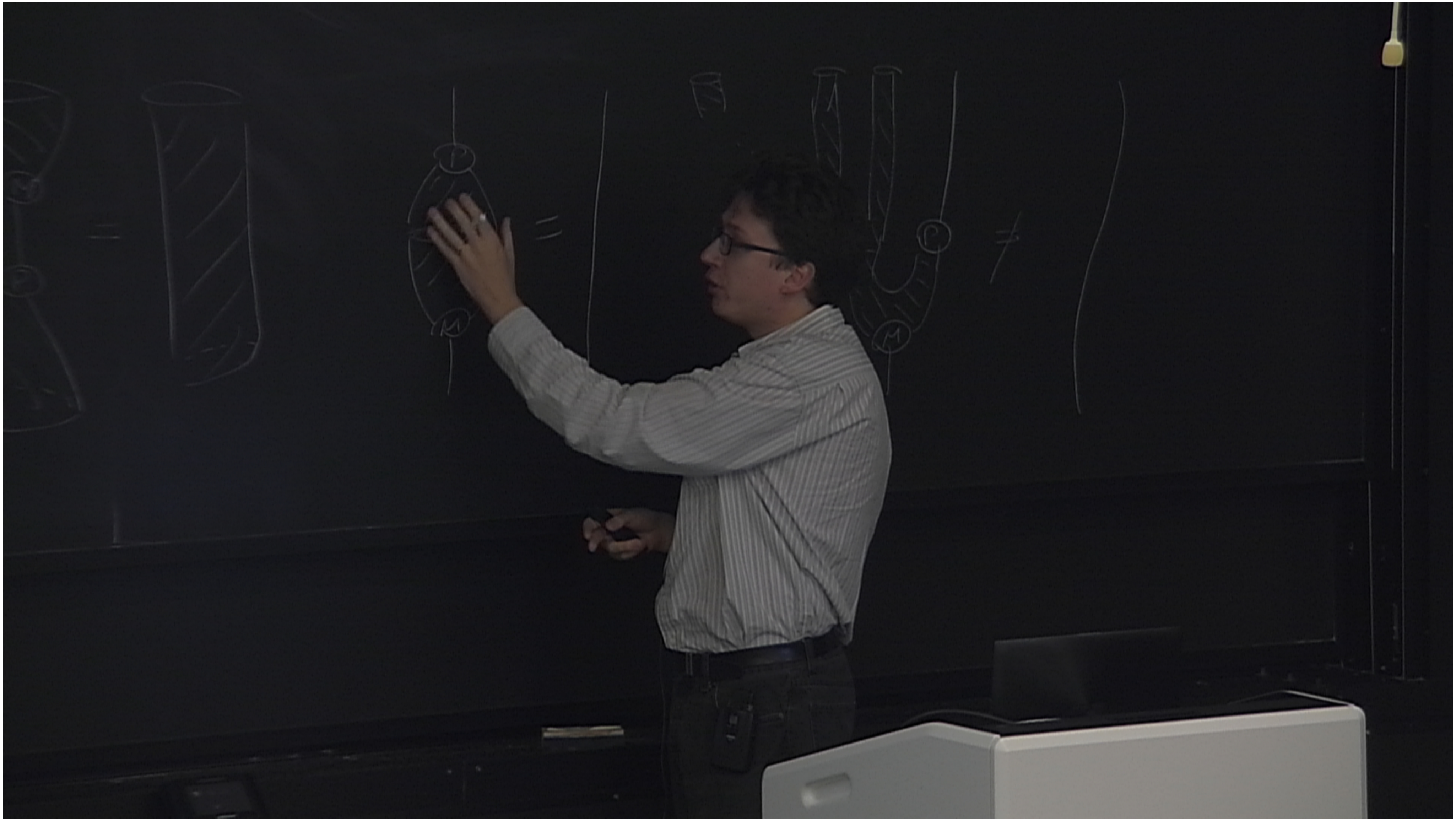


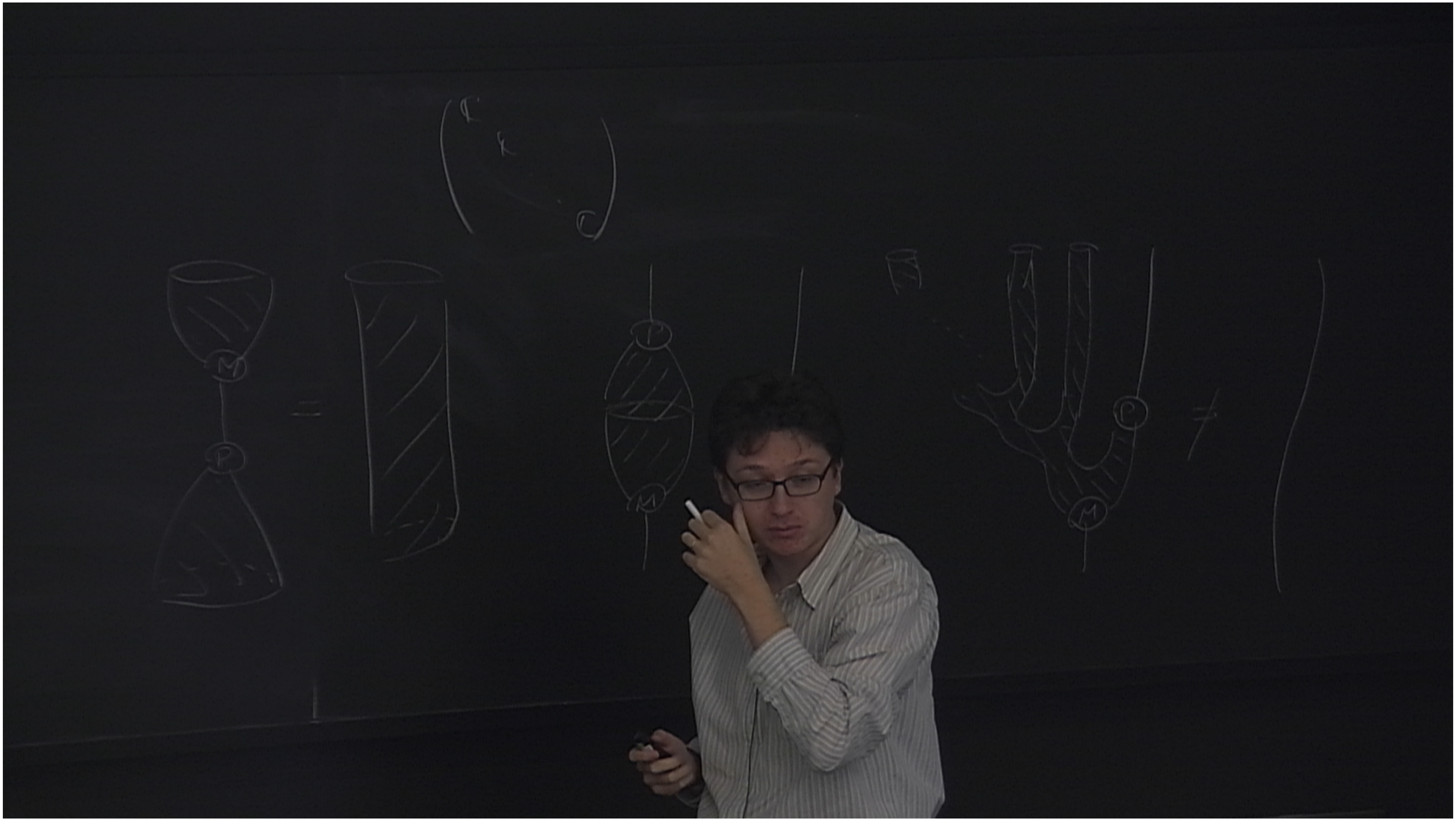

sics
tal level.


sics
tal level.





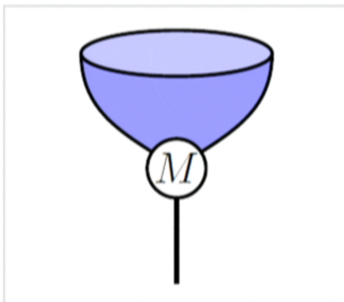




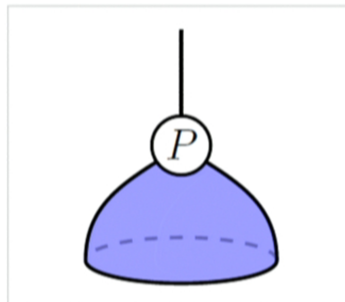
Interactions

We now consider 'interactions' between our lines and surfaces.

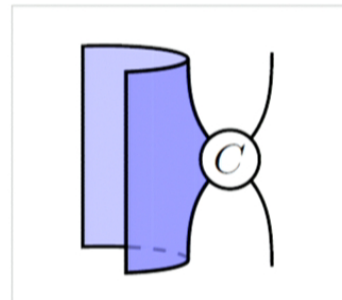
We focus on 3 basic interaction types:



Measurement



Preparation



Controlled operation

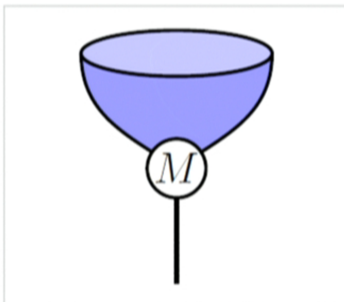
We require these to be invertible, because *all* processes in physics and computer science are (arguably) reversible at a fundamental level.

Also, M and P are inverse.

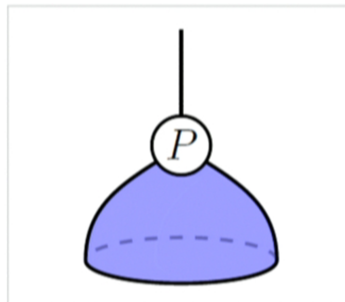
Interactions

We now consider ‘interactions’ between our lines and surfaces.

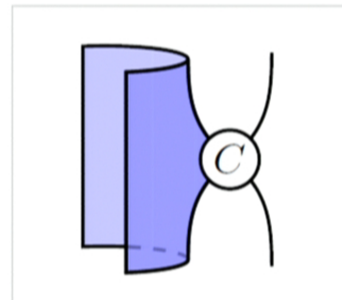
We focus on 3 basic interaction types:



Measurement



Preparation



Controlled operation

We require these to be invertible, because *all* processes in physics and computer science are (arguably) reversible at a fundamental level.

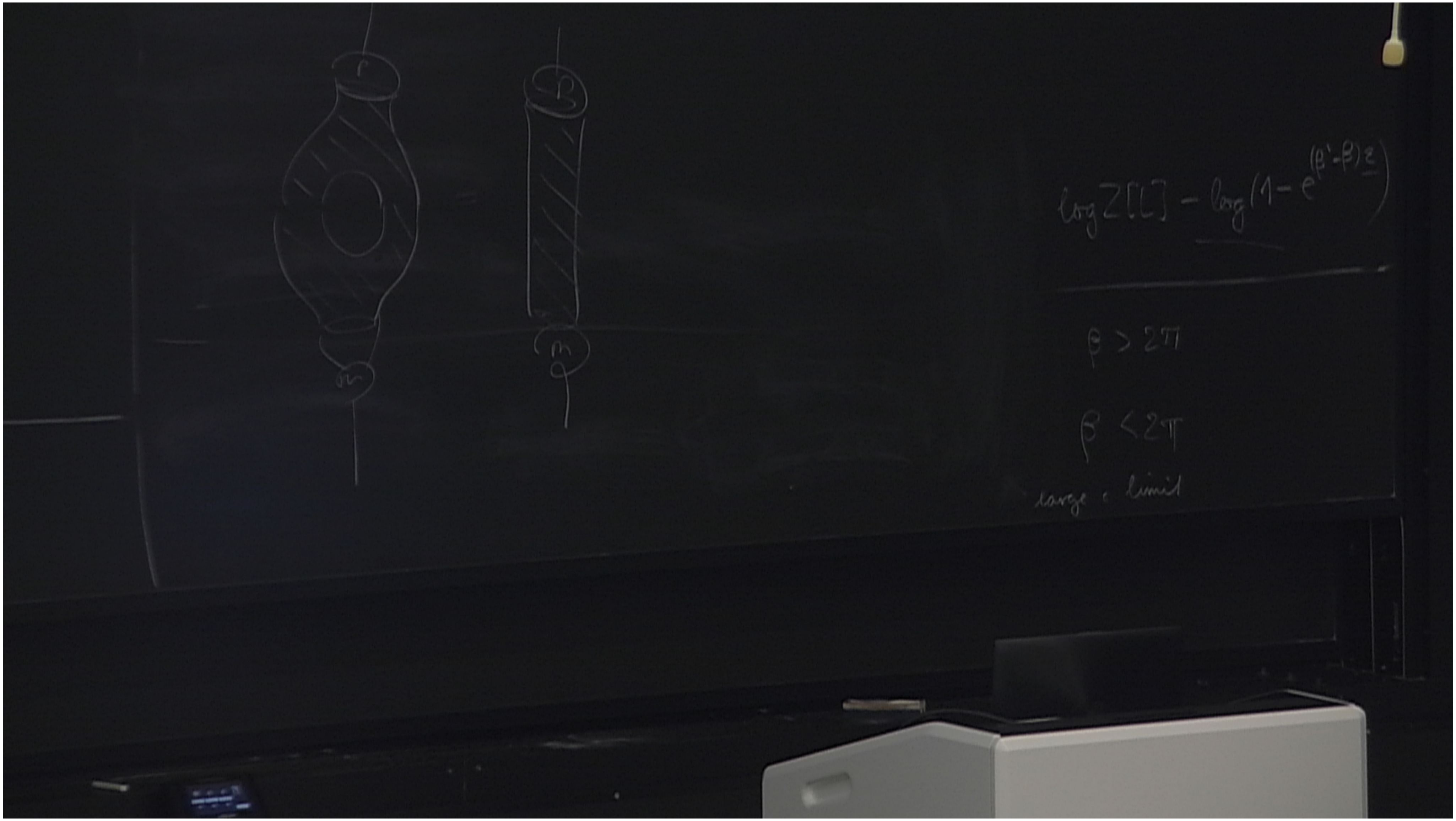
Also, M and P are inverse.

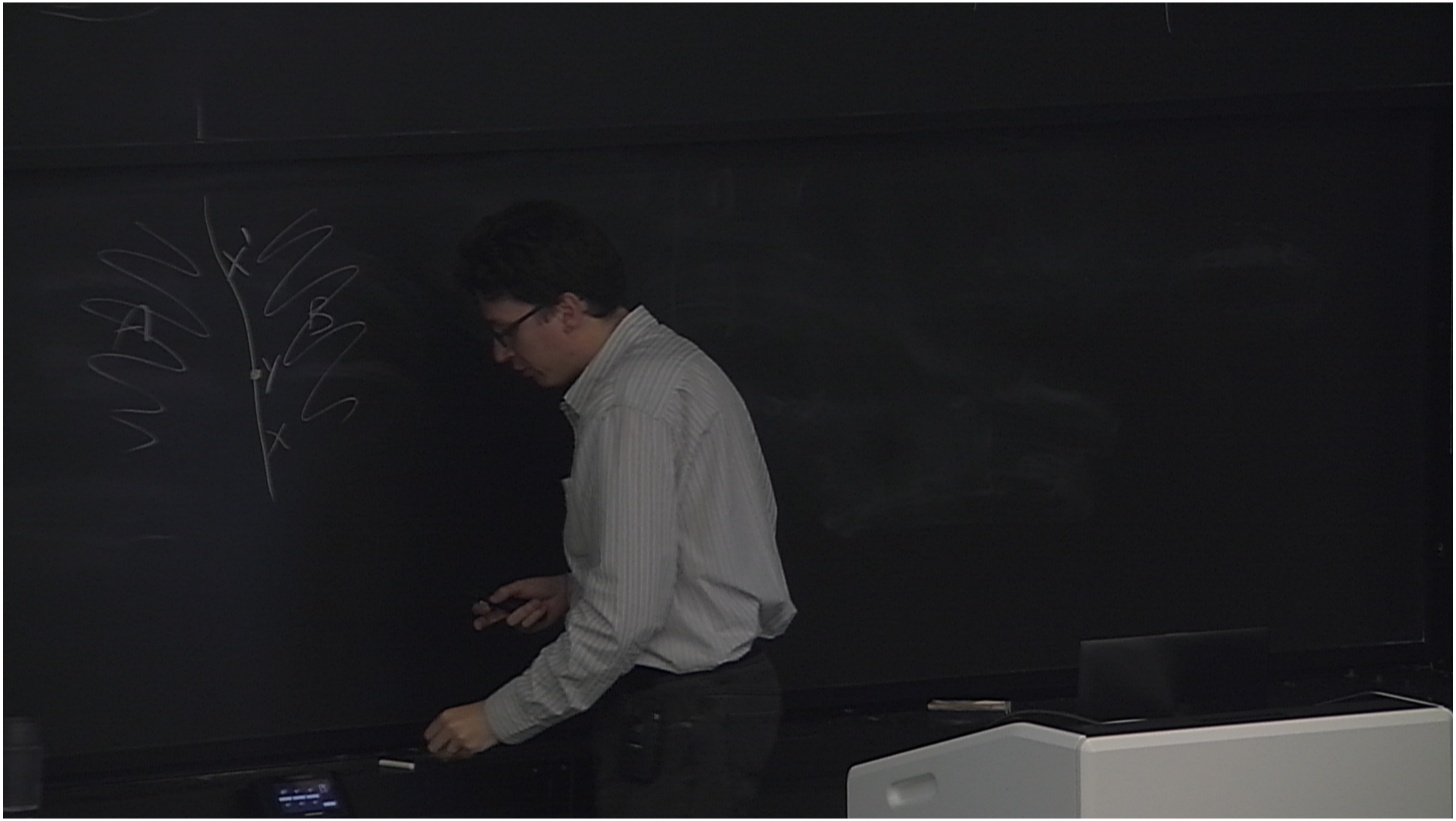
This is a **0-1-2 topological field theory with defects**.

log Z[L] − log(1 − e^{(β'−β)ε})
θ > 2π
2π


Z[L] − log(1− e(β'−β)ε)
2π


log Z[L] − log(1 − e^(β'−β)ε)
β > 2π
β < 2π
large c limit

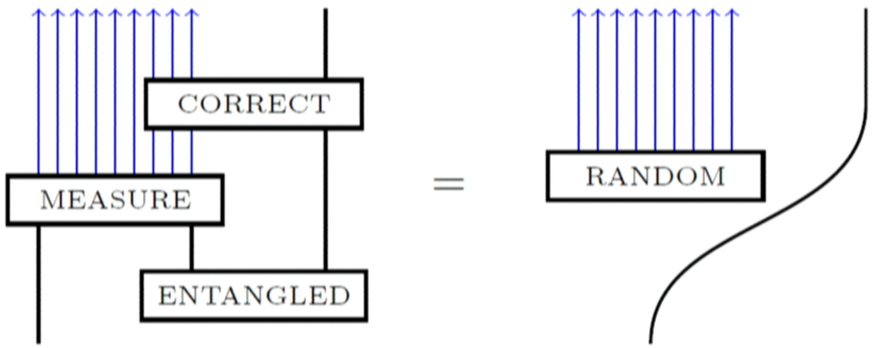

log Z[L] − log(1 − e^(β'−β)ε)
β > 2π
β < 2π
large c limit



A
B
x'
y
x

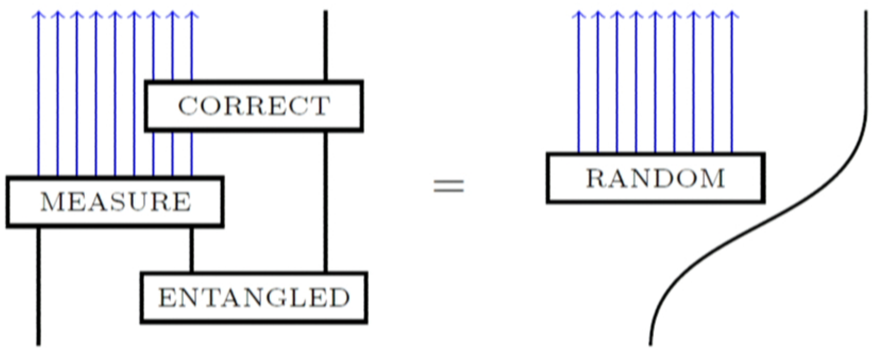
Topological structure

Here is the heuristic quantum teleportation diagram:



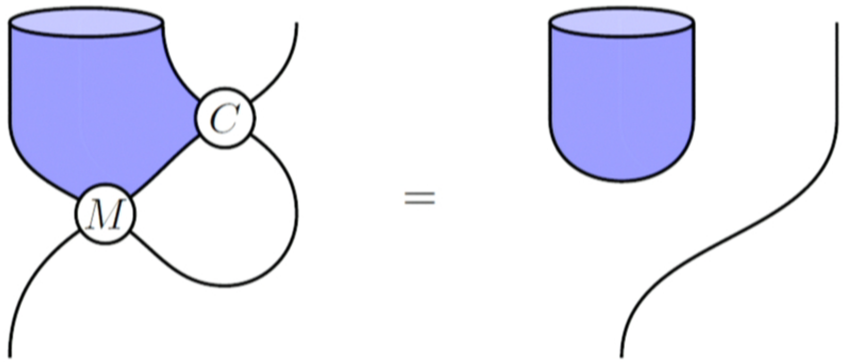
Topological structure

Here is the heuristic quantum teleportation diagram:



Topological structure

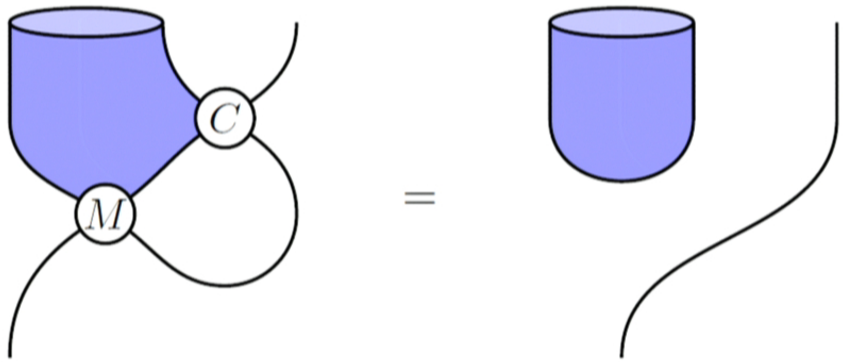
Here is the heuristic quantum teleportation diagram:



We make it rigorous with this equation between topological defects.

Topological structure

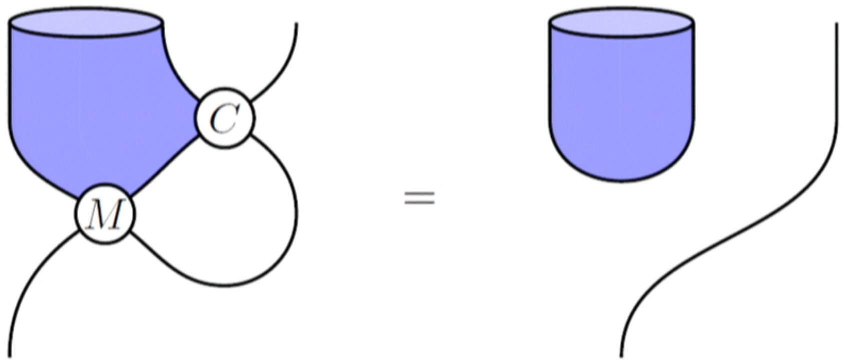
Here is the heuristic quantum teleportation diagram:



We make it rigorous with this equation between topological defects.

Topological structure

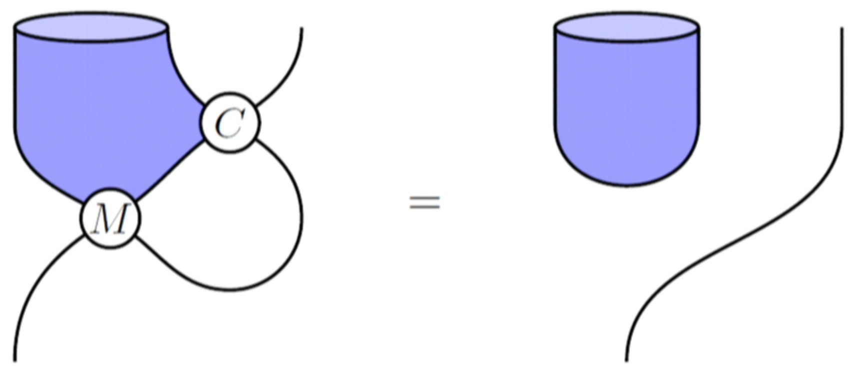
Here is the heuristic quantum teleportation diagram:



We make it rigorous with this equation between topological defects.

Topological structure

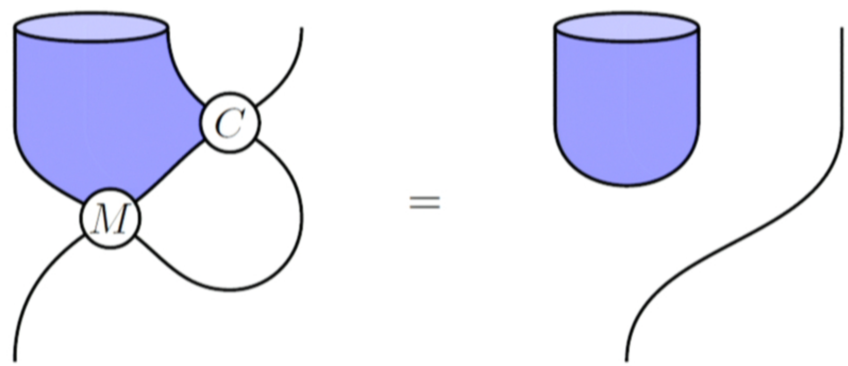
Here is the heuristic quantum teleportation diagram:



We make it rigorous with this equation between topological defects.

Topological structure

Here is the heuristic quantum teleportation diagram:



We make it rigorous with this equation between topological defects.

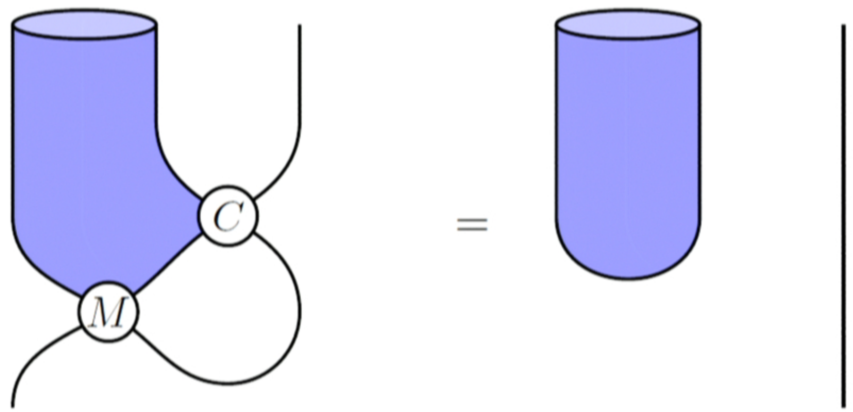
Topological reasoning

We can use the topological formalism to prove interesting things.

Topological reasoning

We can use the topological formalism to prove interesting things.

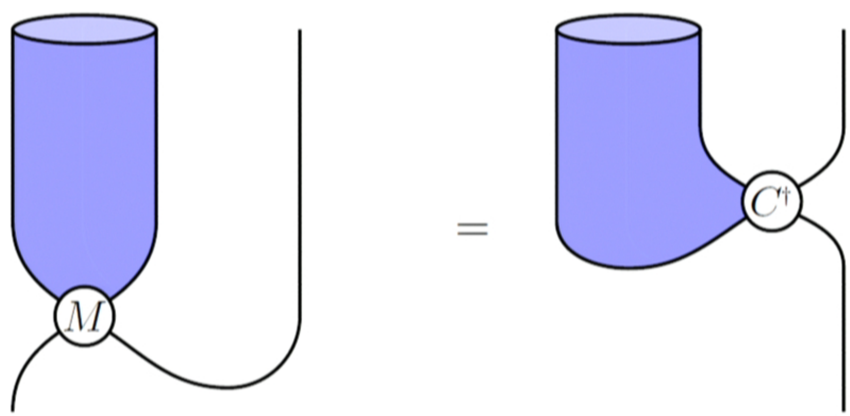
We begin with the definition of quantum teleportation:



Topological reasoning

We can use the topological formalism to prove interesting things.

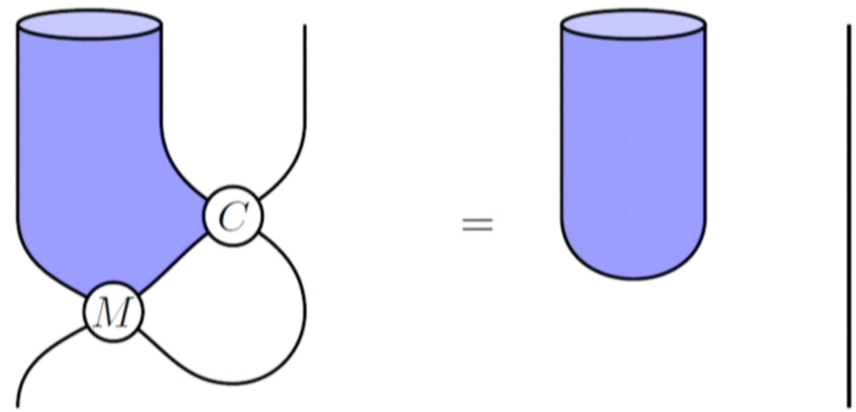
Apply $C^\dagger$:



Topological reasoning

We can use the topological formalism to prove interesting things.

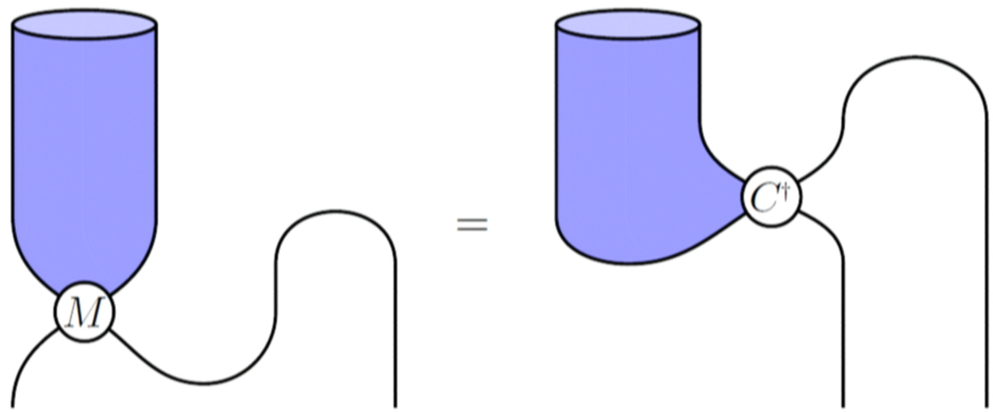
We begin with the definition of quantum teleportation:



Topological reasoning

We can use the topological formalism to prove interesting things.

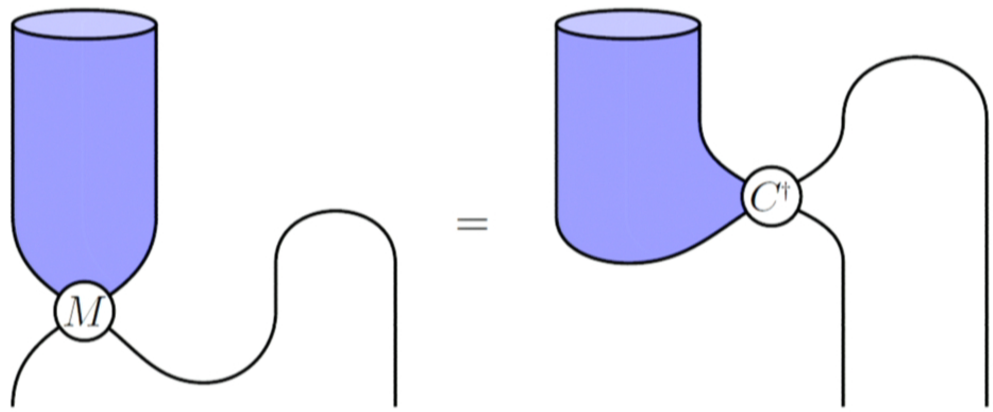
Bend down a wire:



Topological reasoning

We can use the topological formalism to prove interesting things.

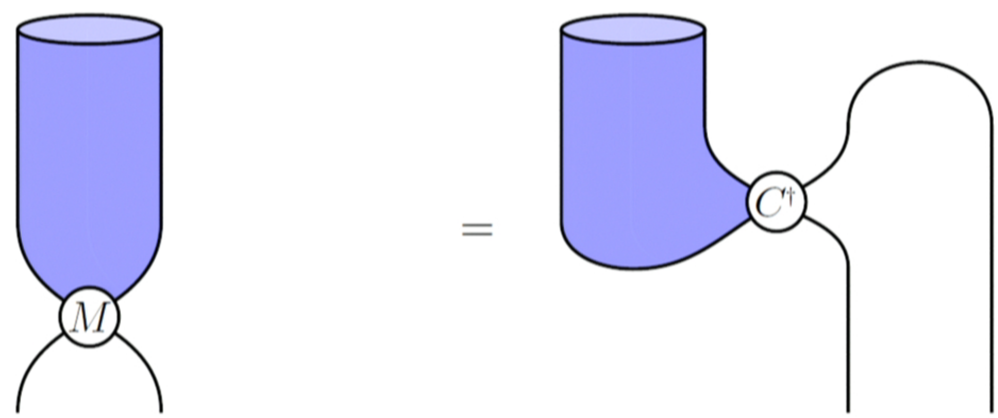
Bend down a wire:



Topological reasoning

We can use the topological formalism to prove interesting things.

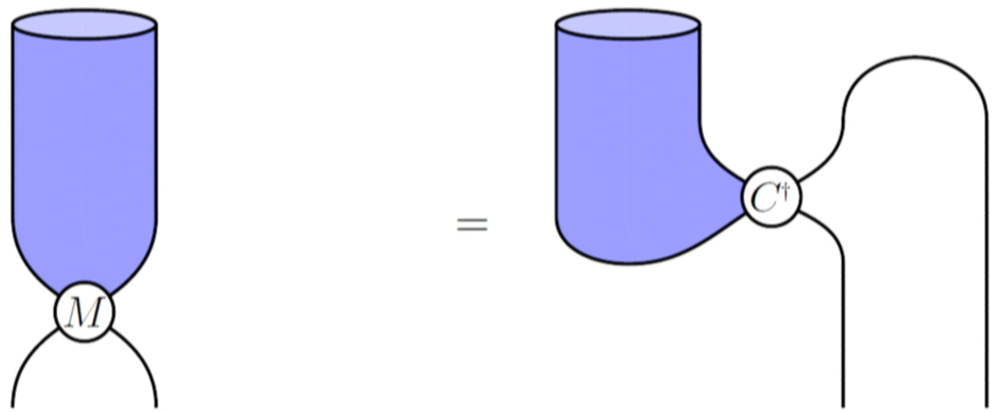
Bend down a wire:



Topological reasoning

We can use the topological formalism to prove interesting things.

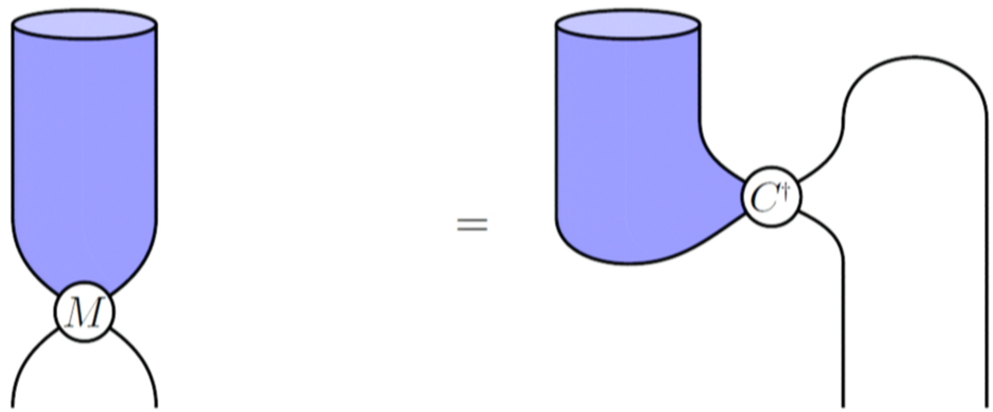
Bend down a wire:



Topological reasoning

We can use the topological formalism to prove interesting things.

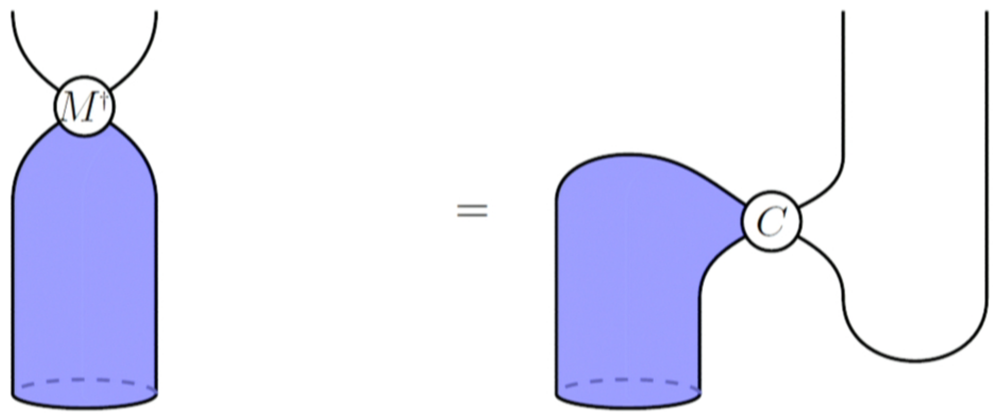
Bend down a wire:



Topological reasoning

We can use the topological formalism to prove interesting things.

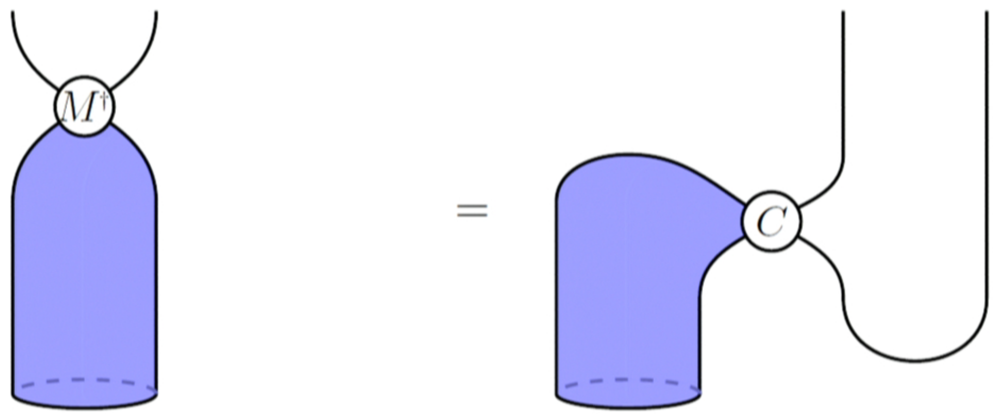
Take adjoints:



Topological reasoning

We can use the topological formalism to prove interesting things.

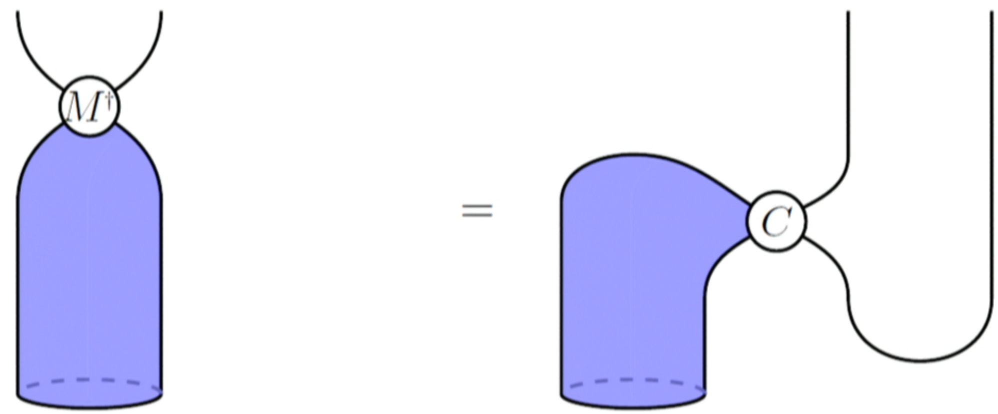
Take adjoints:



Topological reasoning

We can use the topological formalism to prove interesting things.

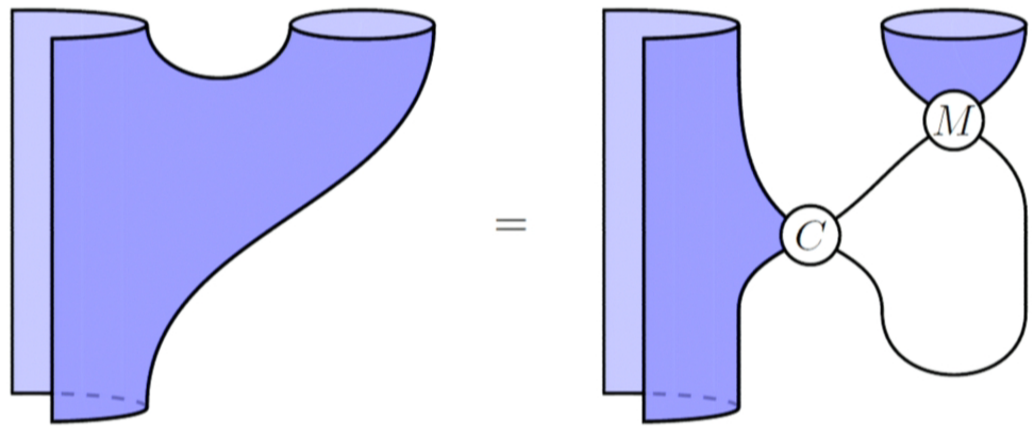
Take adjoints:



Topological reasoning

We can use the topological formalism to prove interesting things.

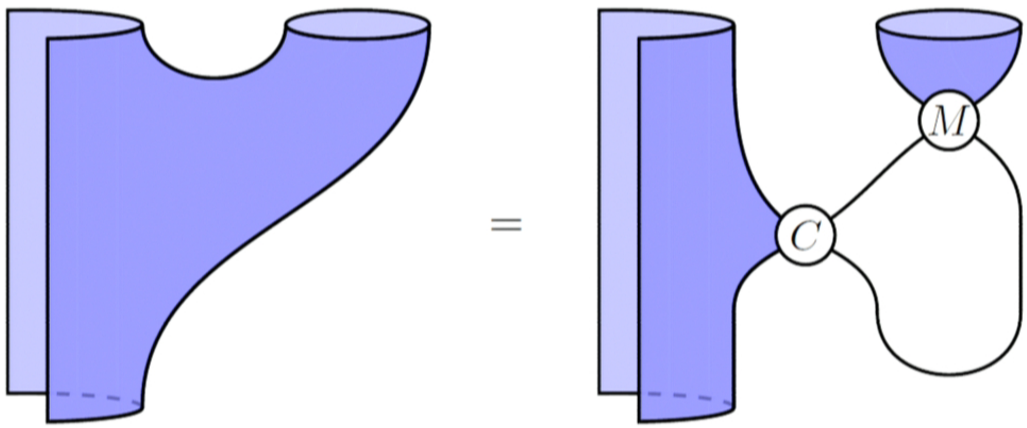
Bend up the surface:

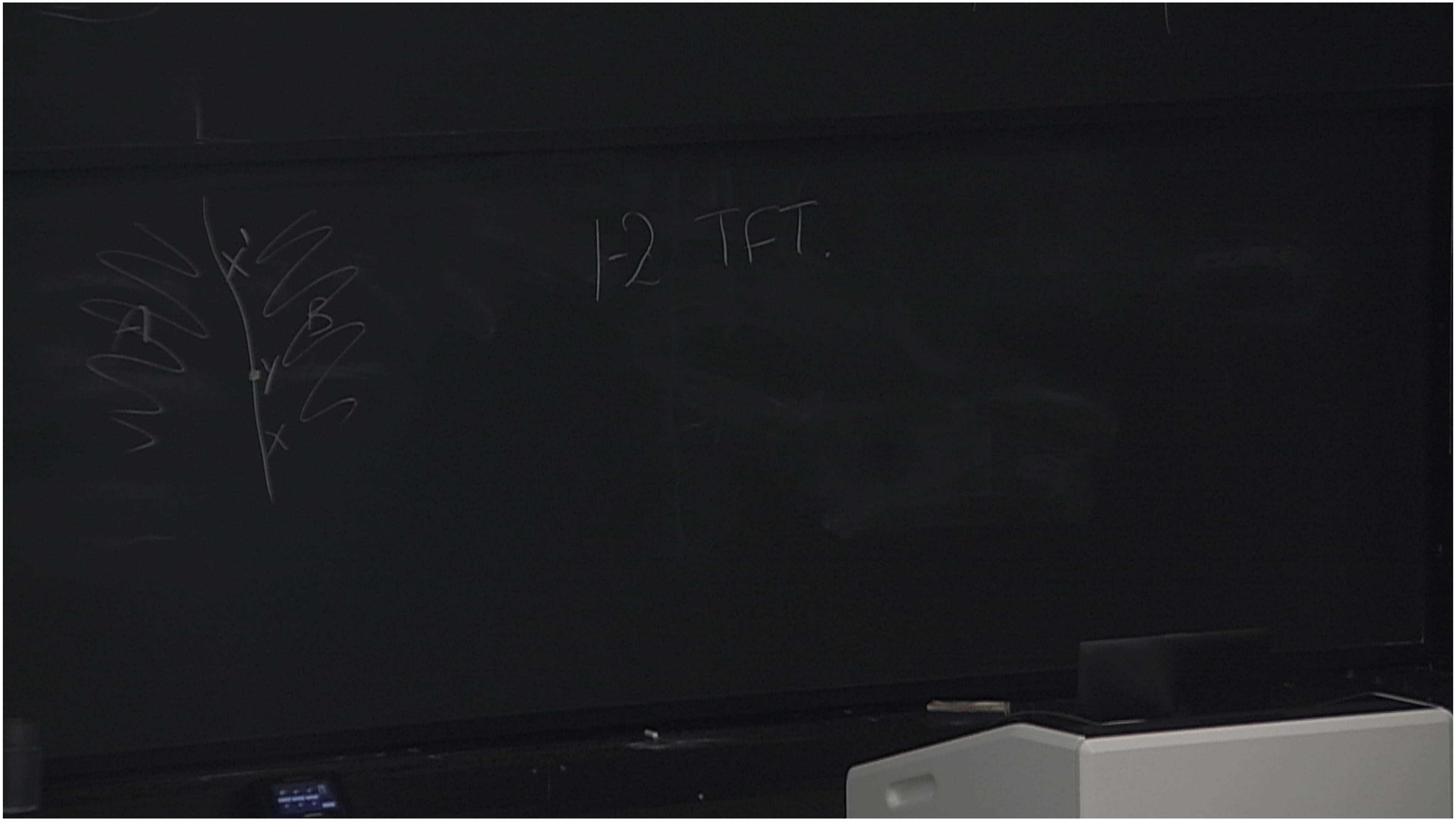


Topological reasoning

We can use the topological formalism to prove interesting things.

Bend up the surface:

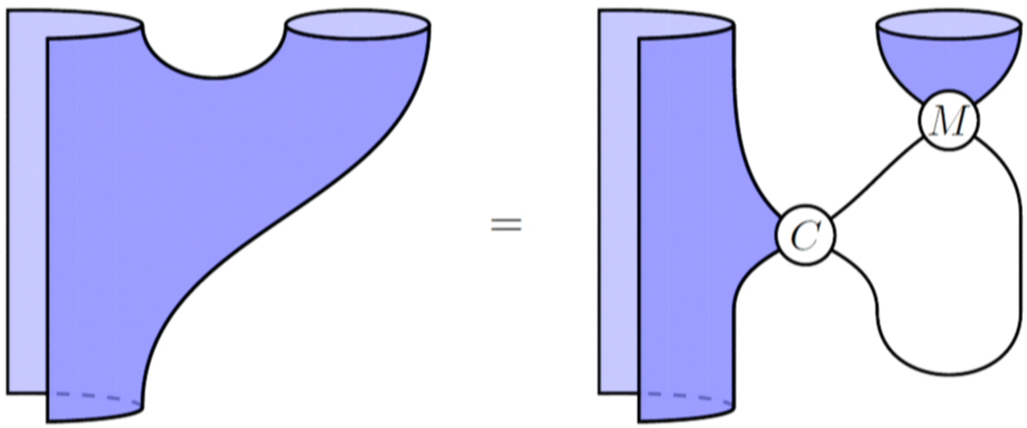



1-2 TFT.
A
B
x'
y
x

Topological reasoning

We can use the topological formalism to prove interesting things.

Bend up the surface:



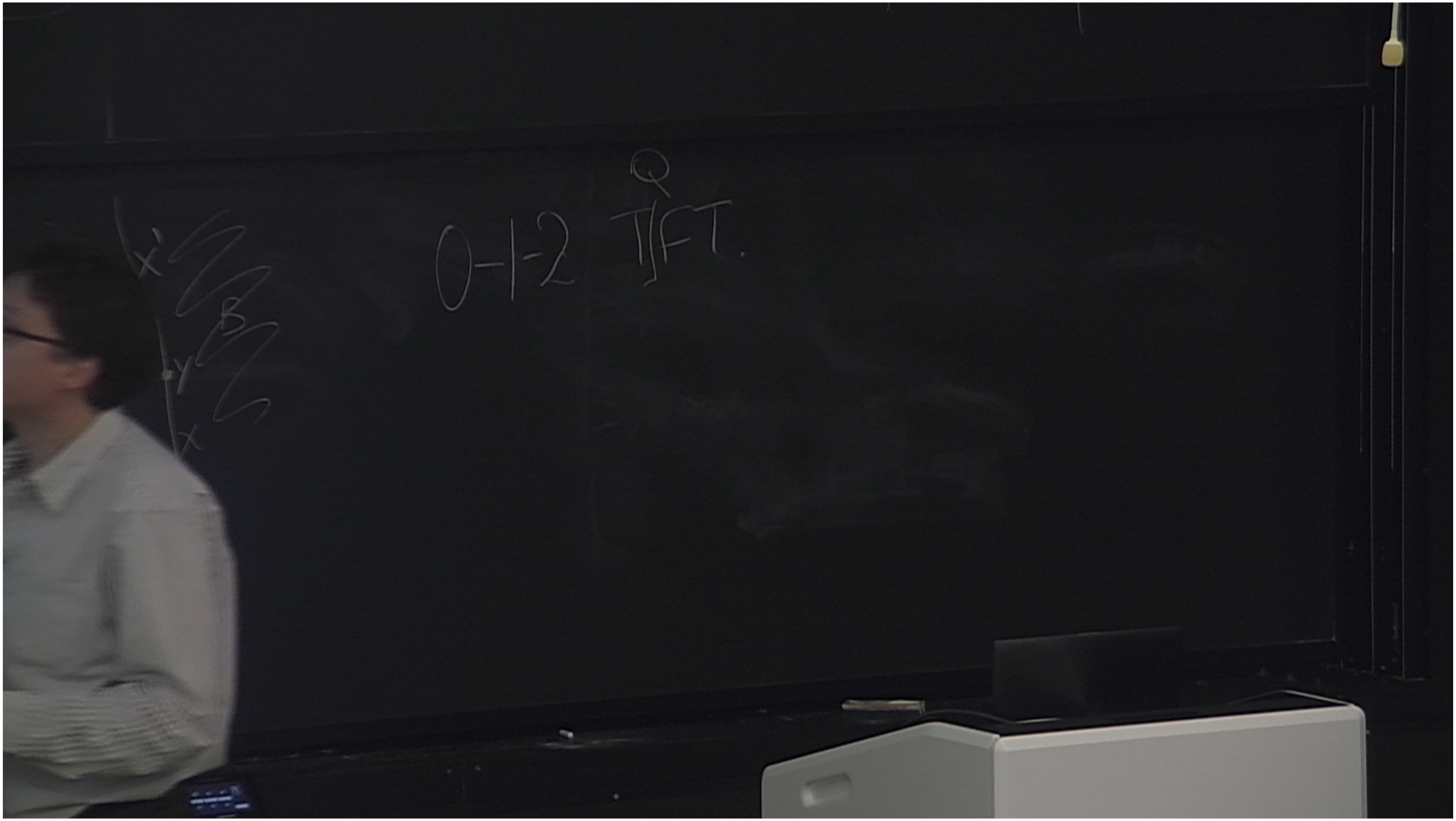
This is dense coding!

So we have a *topological* proof of equivalence with teleportation, independent of the Hilbert space formalism.

Models of computation

What do these pictures have to do with computation?

- We can look for 0-1-2 TFTs with defects in any *symmetric monoidal 2-category.*


0-1-2 TQFT.

Models of computation

What do these pictures have to do with computation?

- We can look for 0-1-2 TFTs with defects in any *symmetric monoidal 2-category*.
- The choice of 2-category represents the 'theory of physics', or 'model of computation', in which we choose to work.
- For *quantum* computation, we choose the 2-category **2Hilb** of 2–Hilbert spaces.

Models of computation

What do these pictures have to do with computation?

- We can look for 0-1-2 TFTs with defects in any *symmetric monoidal 2-category*.
- The choice of 2-category represents the 'theory of physics', or 'model of computation', in which we choose to work.
- For *quantum* computation, we choose the 2-category **2Hilb** of 2–Hilbert spaces.
- For *classical* computation, we choose the 2-category **2Gpd** of groupoids, actions on sets, and spans.

Models of computation

What do these pictures have to do with computation?

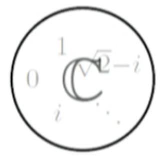
- We can look for 0-1-2 TFTs with defects in any *symmetric monoidal 2-category*.
- The choice of 2-category represents the ‘theory of physics’, or ‘model of computation’, in which we choose to work.
- For *quantum* computation, we choose the 2-category **2Hilb** of 2–Hilbert spaces.
- For *classical* computation, we choose the 2-category **2Gpd** of groupoids, actions on sets, and spans.

In this way, we obtain strong classical ‘toy models’ of quantum phenomena, with some resemblance to Rob Spekkens’ toy theory.

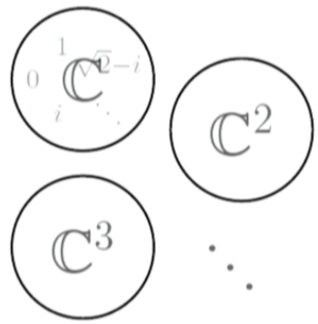
2–Hilbert spaces

$$\begin{matrix} & 1 & \sqrt{2}-i \\ 0 & & \\ & i & \ddots \end{matrix}$$

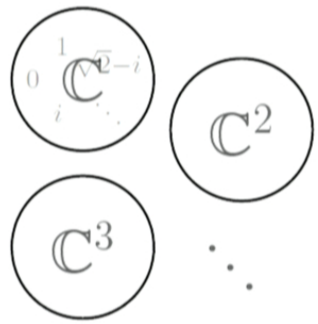
2–Hilbert spaces



2–Hilbert spaces



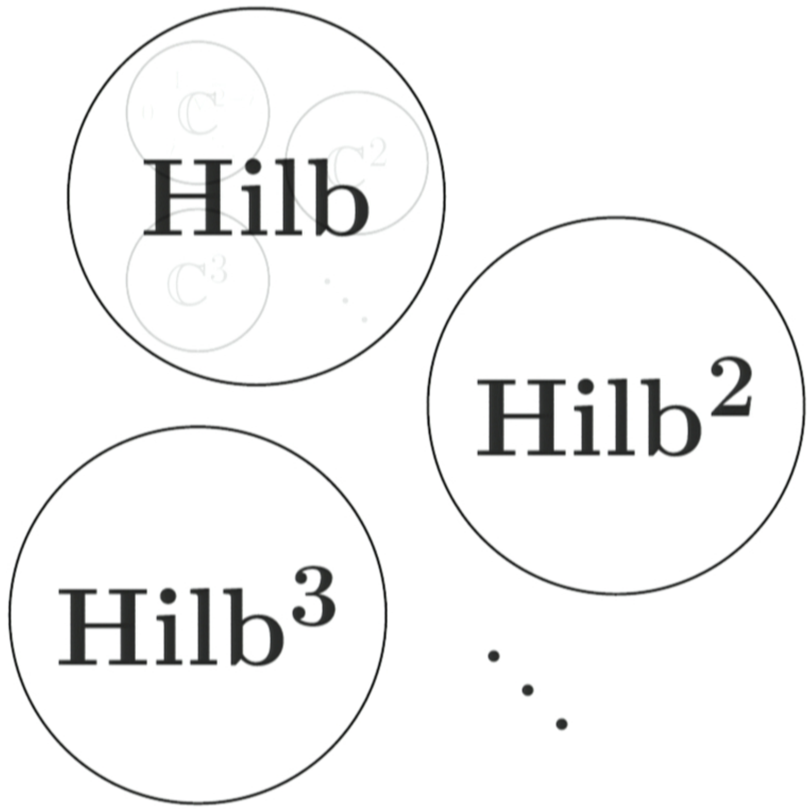
2–Hilbert spaces



2–Hilbert spaces

2–Hilbert spaces

2–Hilbert spaces



2–Hilbert spaces

2–Hilbert spaces

2–Hilbert spaces

Definition. The symmetric monoidal 2-category **2Hilb** is built from the following structures:

- 0-cells are finite-dimensional 2–Hilbert spaces
- 1-cells are linear functors, meaning $F(f+g) = F(f) + F(g)$
- 2-cells are natural transformations

2–Hilbert spaces

Definition. The symmetric monoidal 2-category **2Hilb** is built from the following structures:

- 0-cells are finite-dimensional 2–Hilbert spaces
- 1-cells are linear functors, meaning $F(f+g) = F(f) + F(g)$
- 2-cells are natural transformations

2–Hilbert spaces

Definition. The symmetric monoidal 2-category **2Hilb** is built from the following structures:

- 0-cells are finite-dimensional 2–Hilbert spaces
- 1-cells are linear functors, meaning $F(f+g) = F(f) + F(g)$
- 2-cells are natural transformations

This is a standard structure in higher representation theory.

2–Hilbert spaces

Definition. The symmetric monoidal 2-category **2Hilb** is built from the following structures:

- 0-cells are categories $\mathbf{Hilb}^n$
- 1-cells are linear functors, meaning $F(f+g) = F(f) + F(g)$
- 2-cells are natural transformations

This is a standard structure in higher representation theory.

2–Hilbert spaces

Definition. The symmetric monoidal 2-category **2Hilb** is built from the following structures:

- 0-cells are natural numbers
- 1-cells are matrices of Hilbert spaces
- 2-cells are natural transformations

This is a standard structure in higher representation theory.

There is a matrix calculus, just as for ordinary Hilbert spaces.

2–Hilbert spaces

Definition. The symmetric monoidal 2-category **2Hilb** is built from the following structures:

- 0-cells are natural numbers
- 1-cells are matrices of Hilbert spaces
- 2-cells are matrices of linear maps

This is a standard structure in higher representation theory.

There is a matrix calculus, just as for ordinary Hilbert spaces.

2–Hilbert spaces

Definition. The symmetric monoidal 2-category **2Hilb** is built from the following structures:

- 0-cells are natural numbers
- 1-cells are matrices of Hilbert spaces
- 2-cells are matrices of linear maps

This is a standard structure in higher representation theory.

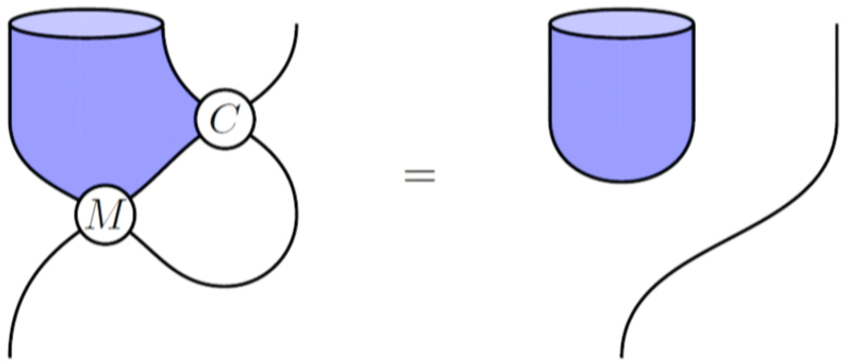
There is a matrix calculus, just as for ordinary Hilbert spaces.

A quote from Schrödinger:

> "I knew of [matrix mechanics], but I felt discouraged by the methods ... which appeared difficult to me"

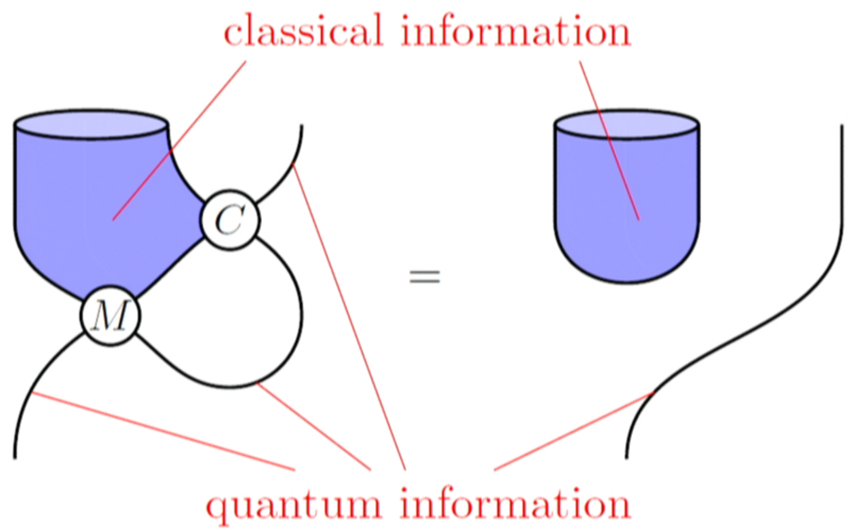
Quantum teleportation

Theorem. Solutions to the teleportation equation in **2Hilb** correspond exactly to quantum teleportation schemes.



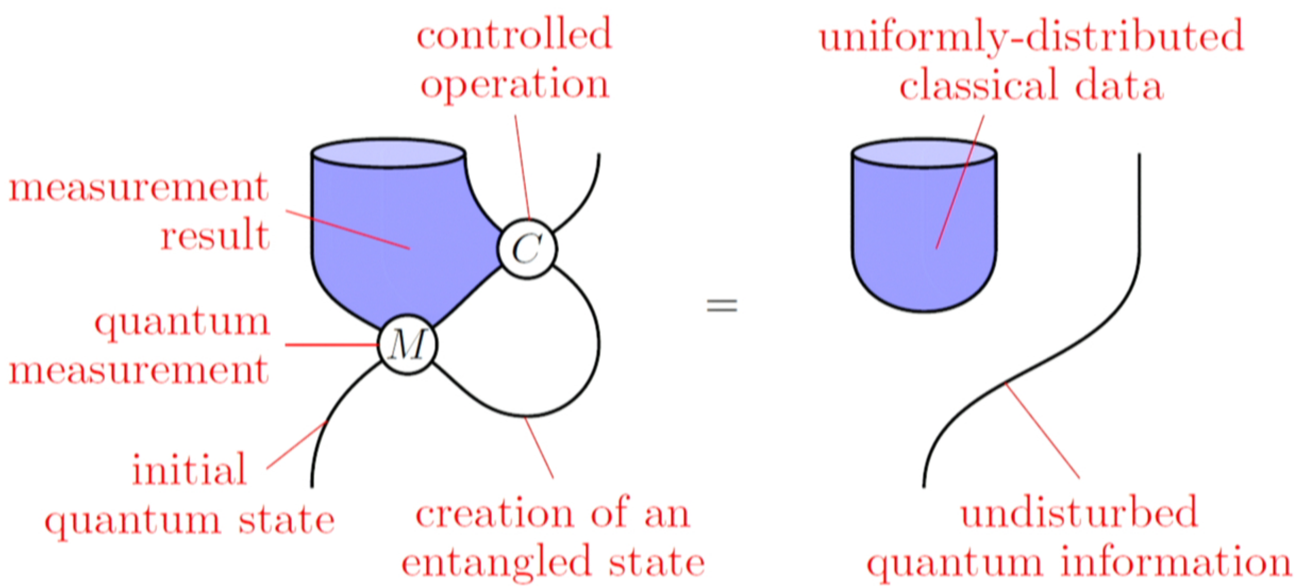
Quantum teleportation

Theorem. Solutions to the teleportation equation in **2Hilb** correspond exactly to quantum teleportation schemes.



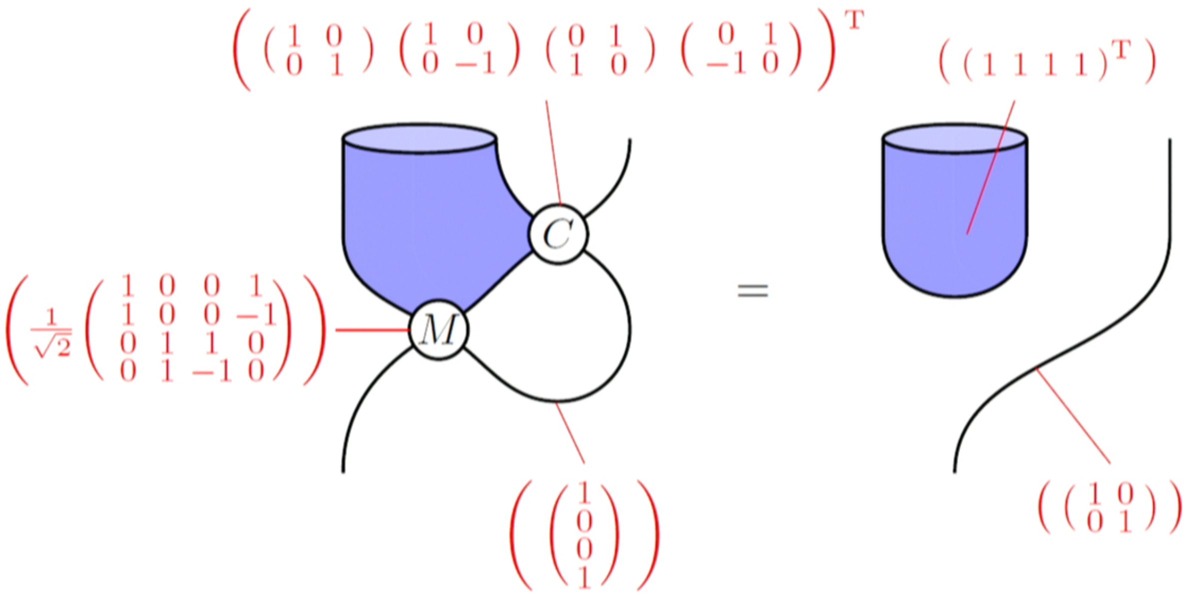
Quantum teleportation

Theorem. Solutions to the teleportation equation in **2Hilb** correspond exactly to quantum teleportation schemes.



Quantum teleportation

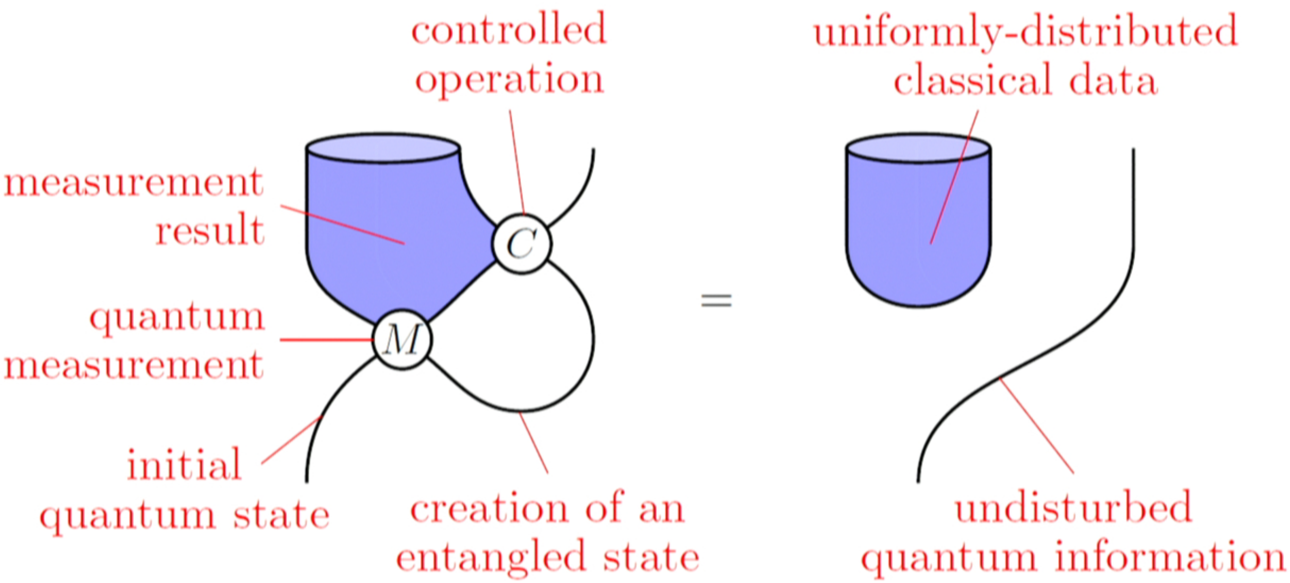
Theorem. Solutions to the teleportation equation in **2Hilb** correspond exactly to quantum teleportation schemes.



This is exactly the data that would appear in a quantum information textbook.

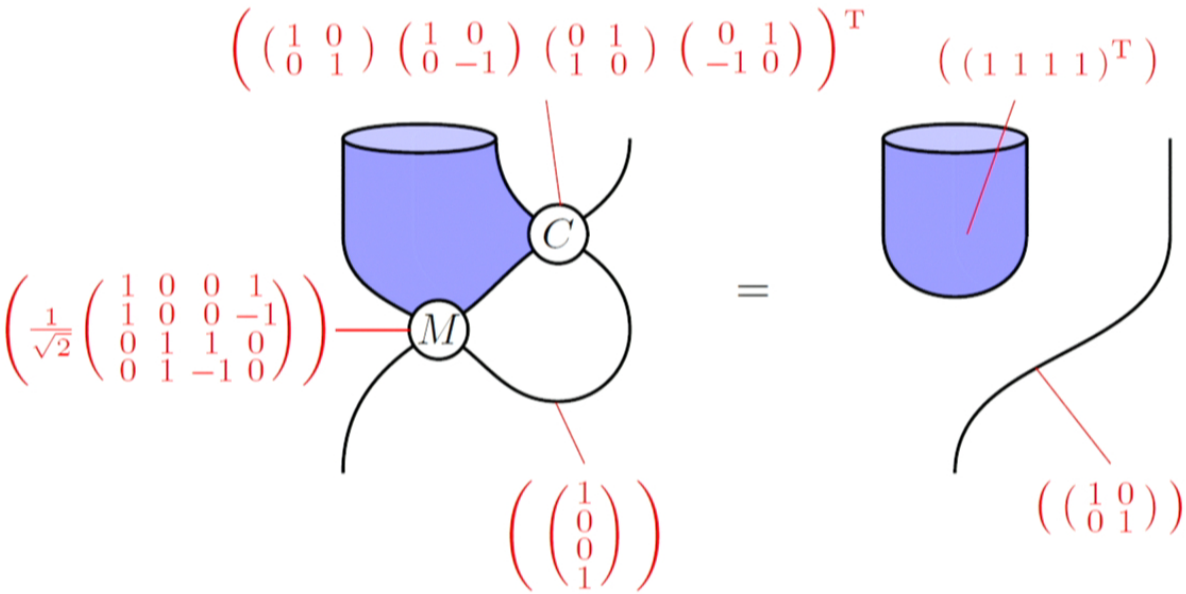
Quantum teleportation

Theorem. Solutions to the teleportation equation in **2Hilb** correspond exactly to quantum teleportation schemes.



Quantum teleportation

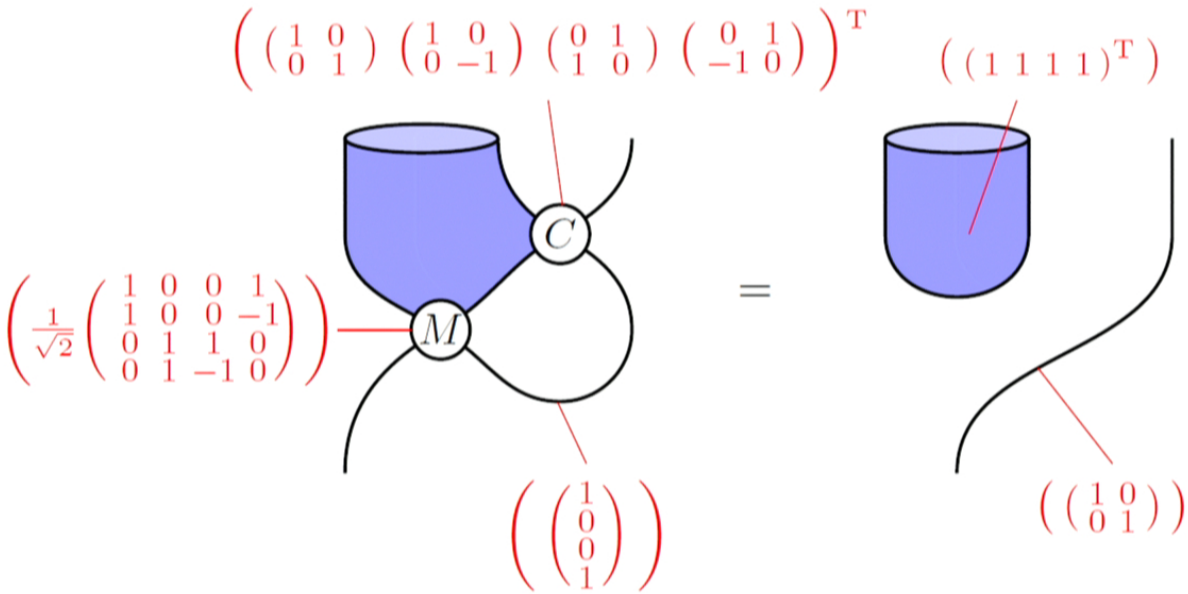
Theorem. Solutions to the teleportation equation in **2Hilb** correspond exactly to quantum teleportation schemes.



This is exactly the data that would appear in a quantum information textbook.

Quantum teleportation

Theorem. Solutions to the teleportation equation in **2Hilb** correspond exactly to quantum teleportation schemes.



This is exactly the data that would appear in a quantum information textbook.

Encrypted communication

Theorem. Solutions to the teleportation equation in **2Gpd** correspond to perfectly secure classical encryption schemes.

Perfectly secure encryption schemes are exactly *Latin squares*:

secret key \ plaintext				
	1	2	3	4
	2	4	1	3
	3	1	4	2
	4	3	2	1

Encrypted communication

Theorem. Solutions to the teleportation equation in **2Gpd** correspond to perfectly secure classical encryption schemes.

Perfectly secure encryption schemes are exactly *Latin squares*:

secret key \ plaintext				
	1	2	3	4
	2	4	1	3
	3	1	4	2
	4	3	2	1

Encrypted communication

Theorem. Solutions to the teleportation equation in **2Gpd** correspond to perfectly secure classical encryption schemes.

Perfectly secure encryption schemes are exactly *Latin squares*:

	plaintext			
secret key	1	2	3	4
	2	4	1	3
	3	1	4	2
	4	3	2	1

They are axiomatized by *quasigroups*, which are sets equipped binary operators $\{*, /, \backslash\}$ such that the following hold for all x, y:

$$y = x * (x \backslash y) = x \backslash (x * y) = (y / x) * x = (y * x) / x$$

Encrypted communication

Theorem. Solutions to the teleportation equation in **2Gpd** correspond to perfectly secure classical encryption schemes.

Perfectly secure encryption schemes are exactly *Latin squares*:

plaintext

secret key

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

They are axiomatized by *quasigroups*, which are sets equipped binary operators $\{*, /, \backslash\}$ such that the following hold for all x, y:

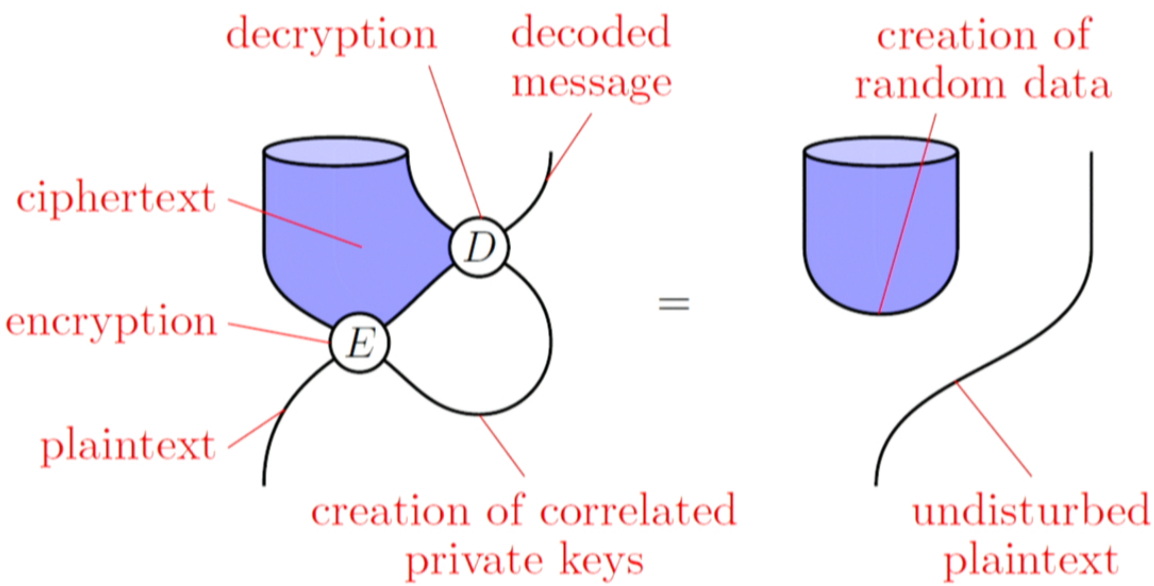
$$y = x * (x \backslash y) = x \backslash (x * y) = (y / x) * x = (y * x) / x$$

Using key k, encryption is $(-) * k$, and decryption is $(-) / k$.

Encrypted communication

Theorem. Solutions to the geometrical equation in **2Gpd** correspond to perfectly secure encryption schemes.

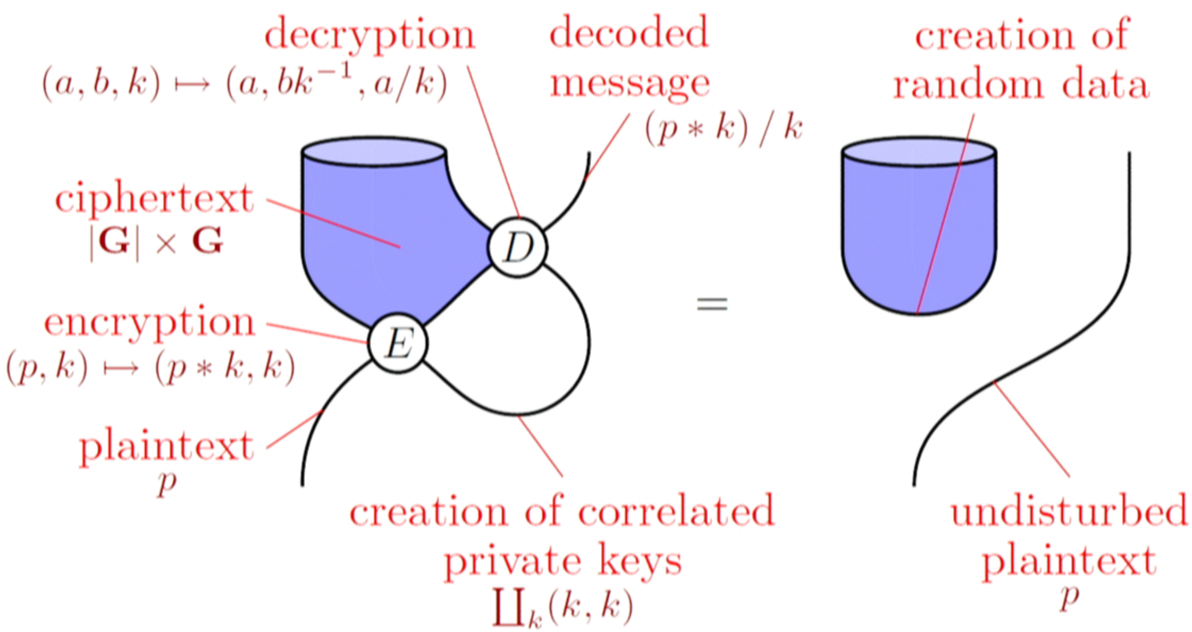
We can use a quasigroup to build such a solution as follows:



Encrypted communication

Theorem. Solutions to the geometrical equation in **2Gpd** correspond to perfectly secure encryption schemes.

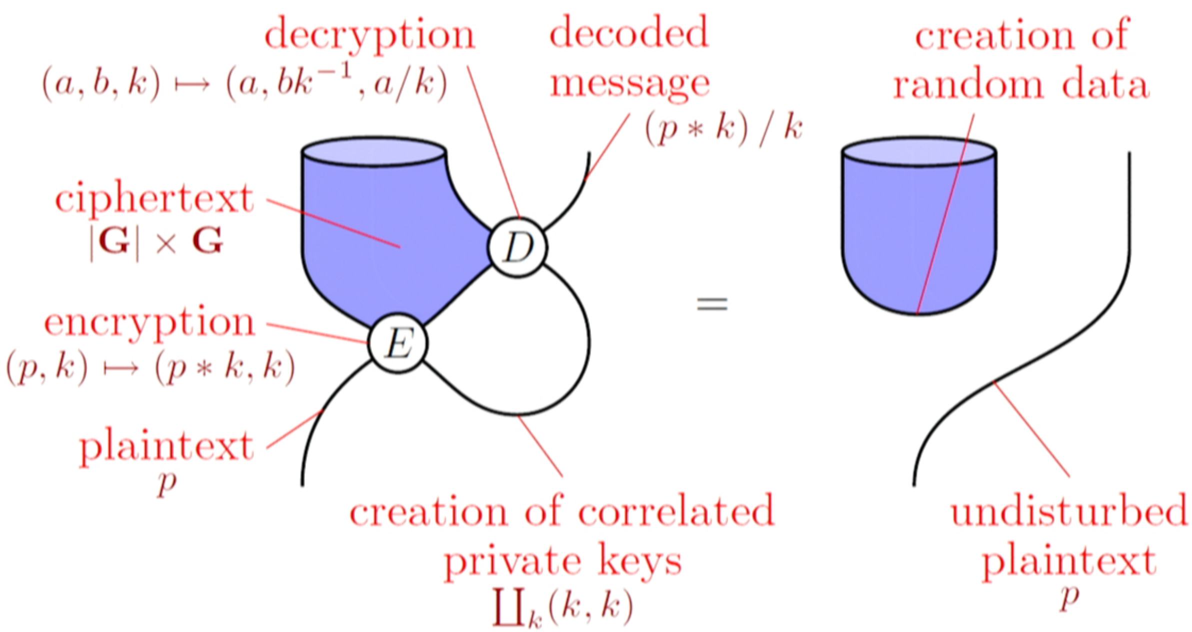
We can use a quasigroup to build such a solution as follows:



Encrypted communication

Theorem. Solutions to the geometrical equation in **2Gpd** correspond to perfectly secure encryption schemes.

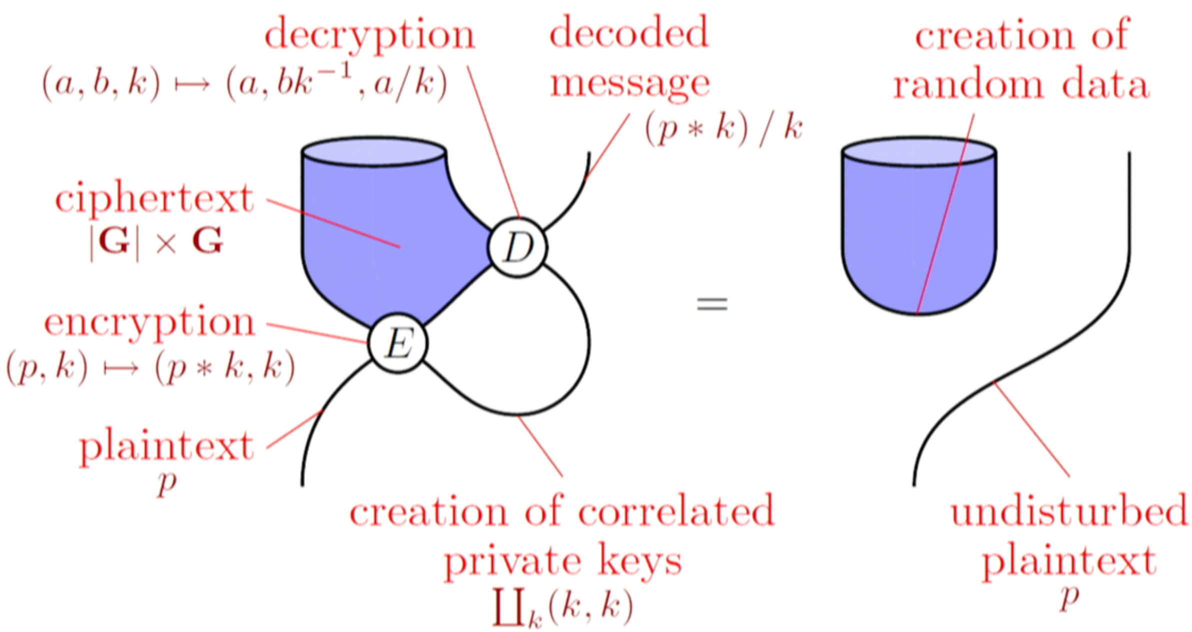
We can use a quasigroup to build such a solution as follows:



Encrypted communication

Theorem. Solutions to the geometrical equation in **2Gpd** correspond to perfectly secure encryption schemes.

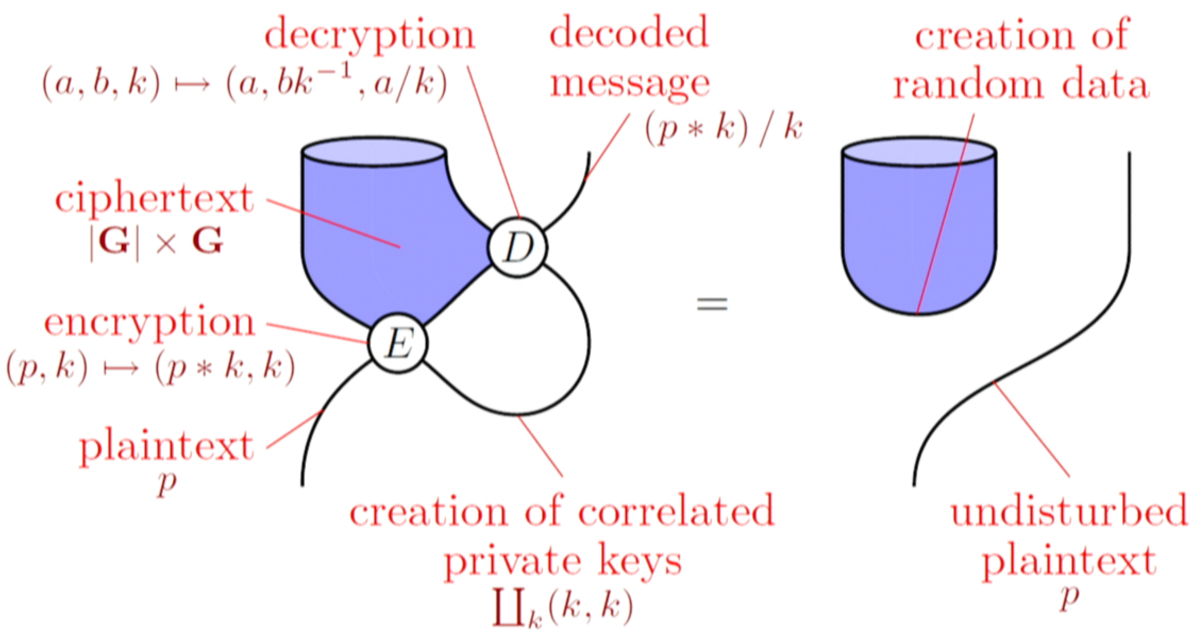
We can use a quasigroup to build such a solution as follows:



Encrypted communication

Theorem. Solutions to the geometrical equation in **2Gpd** correspond to perfectly secure encryption schemes.

We can use a quasigroup to build such a solution as follows:



Encryption is *invertible*. Consistent with foundations of computation.
A successful attacker must access the *entire system*.

The Big Picture

theory of teleportation $\mathbf{T}$

The Big Picture

theory of teleportation **T**

2Hilb quantum theory

(*Baez, Voevodsky, Khovanov*)

The Big Picture

theory of teleportation $\mathbf{T} \xrightarrow[\text{quantum teleportation}]{S} \mathbf{2Hilb}$ quantum theory

quantum teleportation

(*Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters*)

Theorem. Structure-preserving maps $\mathbf{T} \to \mathbf{2Hilb}$ correspond to implementations of quantum teleportation.

The Big Picture

theory of 0,1,2-dimensional
topological manifolds
(*Baez, Dolan, Lurie, Hopkins*)

$\mathbf{Bord_{012}}$

theory of teleportation $\quad \mathbf{T} \xrightarrow[\text{quantum teleportation}]{S} \mathbf{2Hilb} \quad$ quantum theory

The Big Picture

theory of 0,1,2-dimensional
topological manifolds
(*Baez, Dolan, Lurie, Hopkins*)

topological
quantum
field theory
(*Atiyah, Segal*)

$$\begin{tikzcd} & \mathbf{Bord_{012}} \arrow[dr, bend left, "Z"] & \\ \mathbf{T} \arrow[rr, "S", "\text{quantum teleportation}"'] & & \mathbf{2Hilb} \end{tikzcd}$$

theory of
teleportation

quantum
theory

The Big Picture

theory of 0,1,2-dimensional
topological manifolds
(*Baez, Dolan, Lurie, Hopkins*)

topological
quantum
field theory
(*Atiyah, Segal*)

$$\begin{tikzcd}
 & \mathbf{Bord_{012}} \arrow[dl, hook, bend right] \arrow[dr, bend left, "Z"] & \\
\mathbf{T} \arrow[rr, "S"] & & \mathbf{2Hilb}
\end{tikzcd}$$

theory of
teleportation

quantum teleportation

quantum
theory

Theorem. Every implementation of quantum teleportation gives rise to a 2d topological quantum field theory.

The Big Picture

$$\begin{tikzcd} & \mathbf{Bord}_{\mathbf{012}} \arrow[dl, hook, bend right] \arrow[dr, bend left, "Z"] & \\ \mathbf{T} \arrow[rr, "S"] & & \mathbf{2Hilb} \end{tikzcd}$$

theory of teleportation

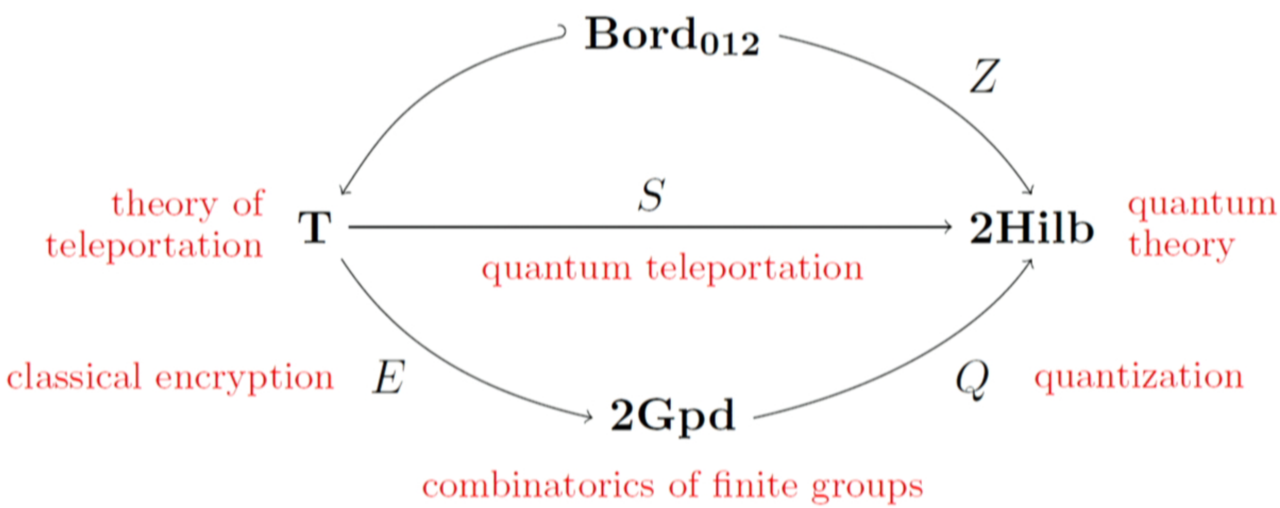
quantum teleportation

quantum theory

2Gpd

combinatorics of finite groups

The Big Picture



Theorem. The map Q transports encrypted communication into quantum teleportation.

The Big Picture

theory of teleportation

classical encryption

$$
\begin{tikzcd}
 & \mathbf{Bord_{012}} \arrow[dl, hook', bend right] \arrow[dr, bend left, "Z"] & \\
\mathbf{T} \arrow[rr, "S"] \arrow[dr, bend right, "E"'] & & \mathbf{2Hilb} \\
 & \mathbf{2Gpd} \arrow[ur, bend right, "Q"'] &
\end{tikzcd}
$$

Theorem. The map Q transports encrypted communication into quantum teleportation. Related to Werner's combinatorial construction.

The Big Picture

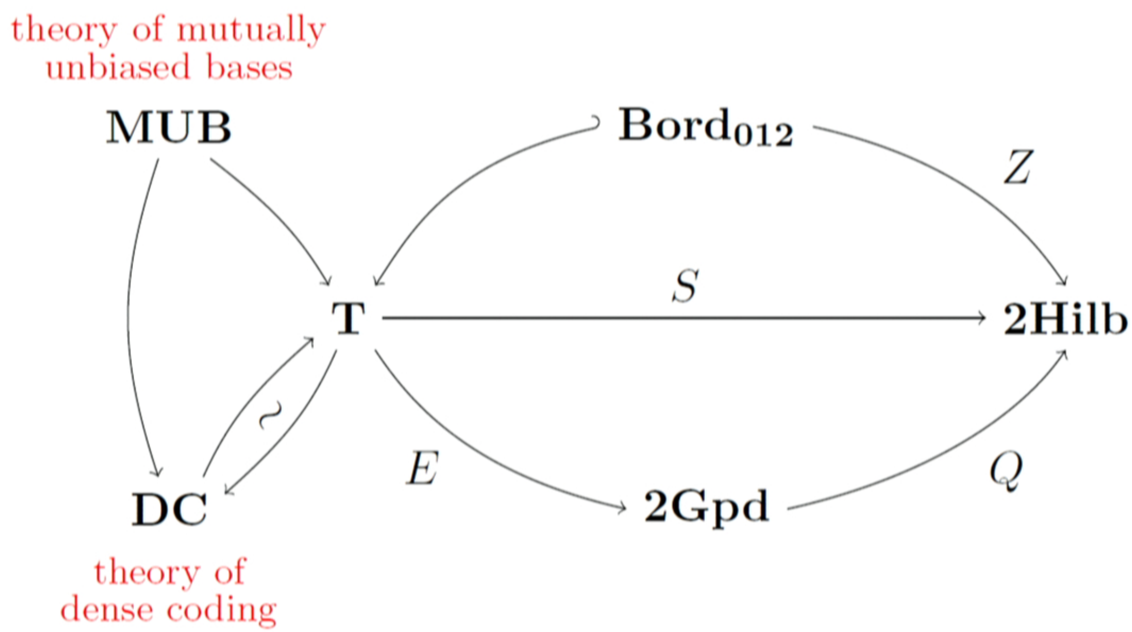
$$
\begin{tikzcd}
 & & \mathbf{Bord_{012}} \arrow[dl, hook', bend right] \arrow[dr, bend left, "Z"] & \\
 & \mathbf{T} \arrow[rr, "S"] \arrow[dr, bend right, "E"'] \arrow[dl, bend left] & & \mathbf{2Hilb} \\
\mathbf{DC} \arrow[ur, bend left, "\simeq"'] & & \mathbf{2Gpd} \arrow[ur, bend right, "Q"'] &
\end{tikzcd}
$$

equivalence
(*Werner*)

theory of
dense coding

Theorem. Teleportation and dense coding are syntactically equivalent.

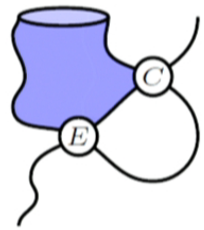
The Big Picture



Theorem. Syntactic construction of teleportation and dense coding from mutually-unbiased bases.

Future directions

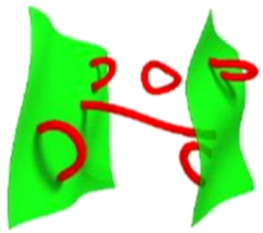
- Try to extend results to *geometrical* field theories



- Treatment of mixed states and completely-positive maps

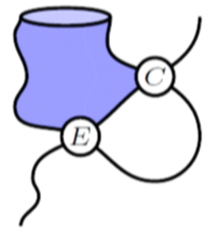
- Combinatorial models for other phenomena — classical information-theoretic key distribution?

- Information processing with topological branes — can you teleport a topological quantum string?

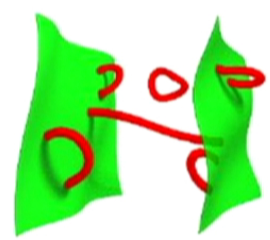


Future directions

- Try to extend results to *geometrical* field theories

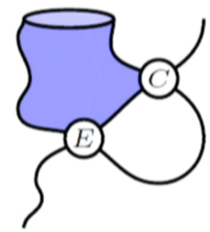


- Treatment of mixed states and completely-positive maps
- Combinatorial models for other phenomena — classical information-theoretic key distribution?
- Information processing with topological branes — can you teleport a topological quantum string?



Future directions

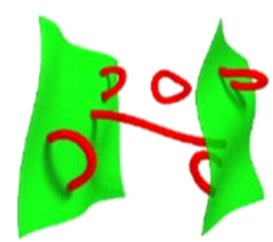
- Try to extend results to *geometrical* field theories



- Treatment of mixed states and completely-positive maps

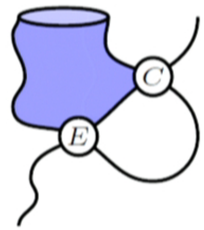
- Combinatorial models for other phenomena — classical information-theoretic key distribution?

- Information processing with topological branes — can you teleport a topological quantum string?



Future directions

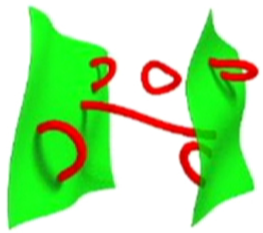
- Try to extend results to *geometrical* field theories



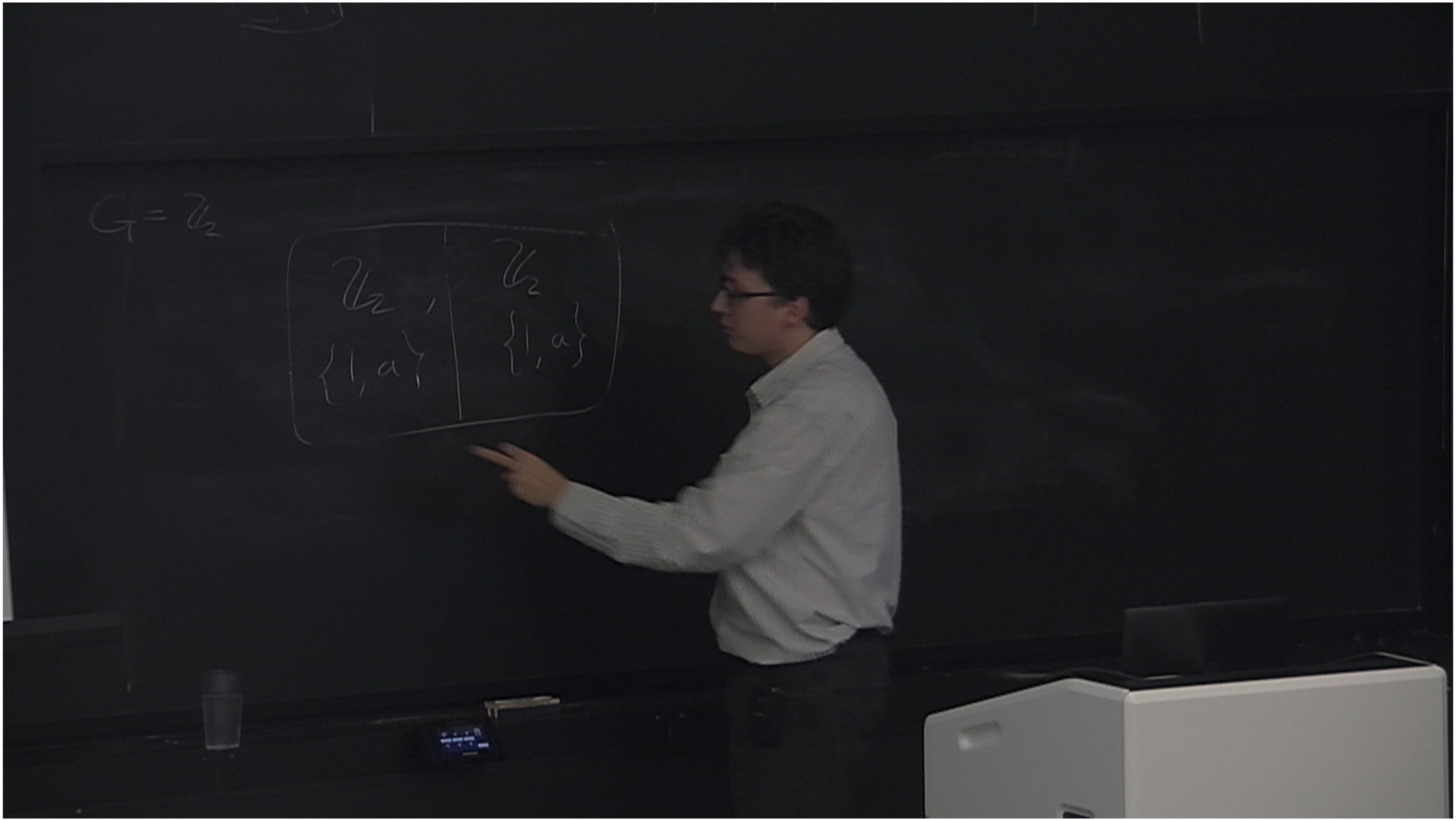
- Treatment of mixed states and completely-positive maps

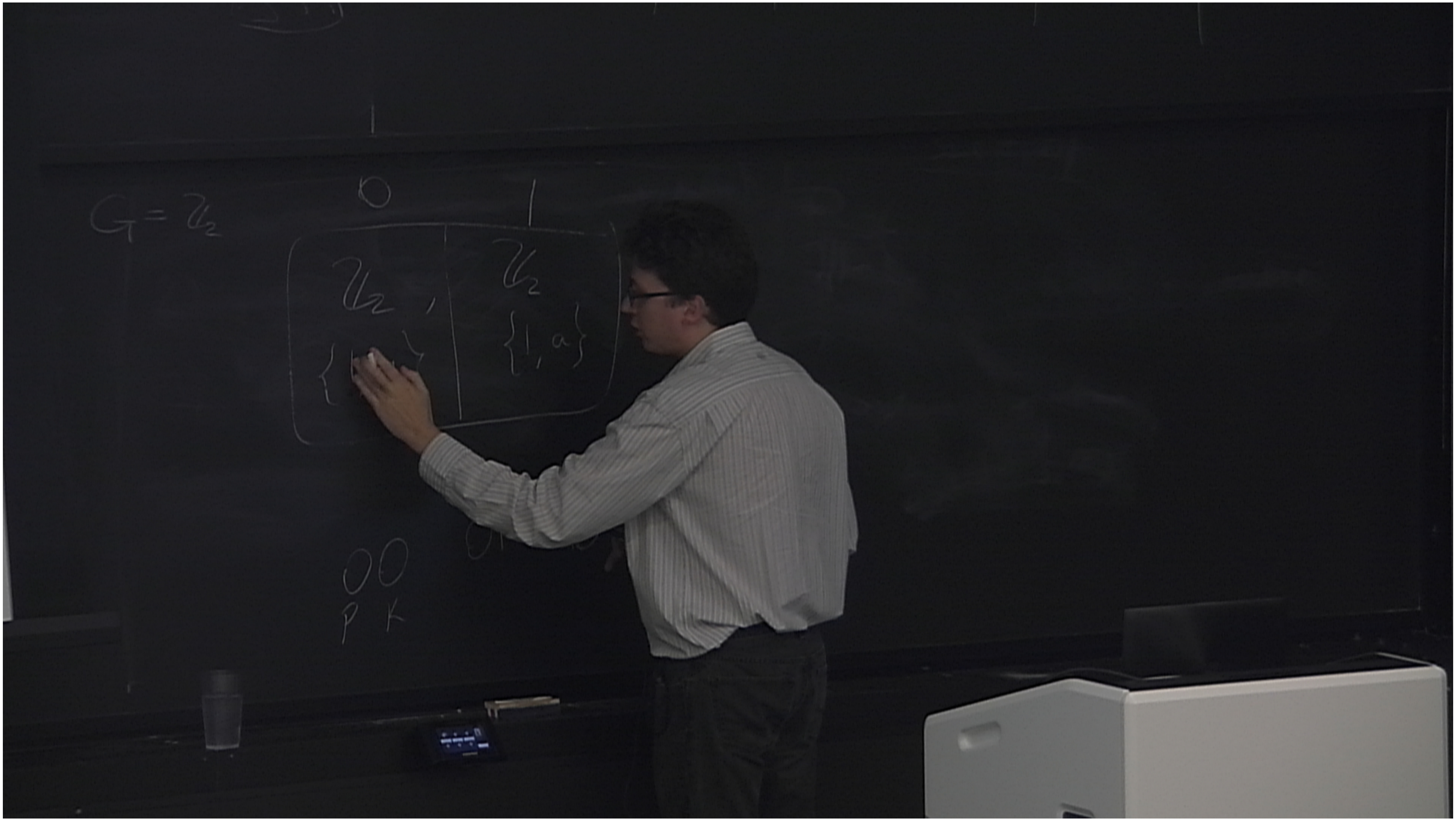
- Combinatorial models for other phenomena — classical information-theoretic key distribution?

- Information processing with topological branes — can you teleport a topological quantum string?

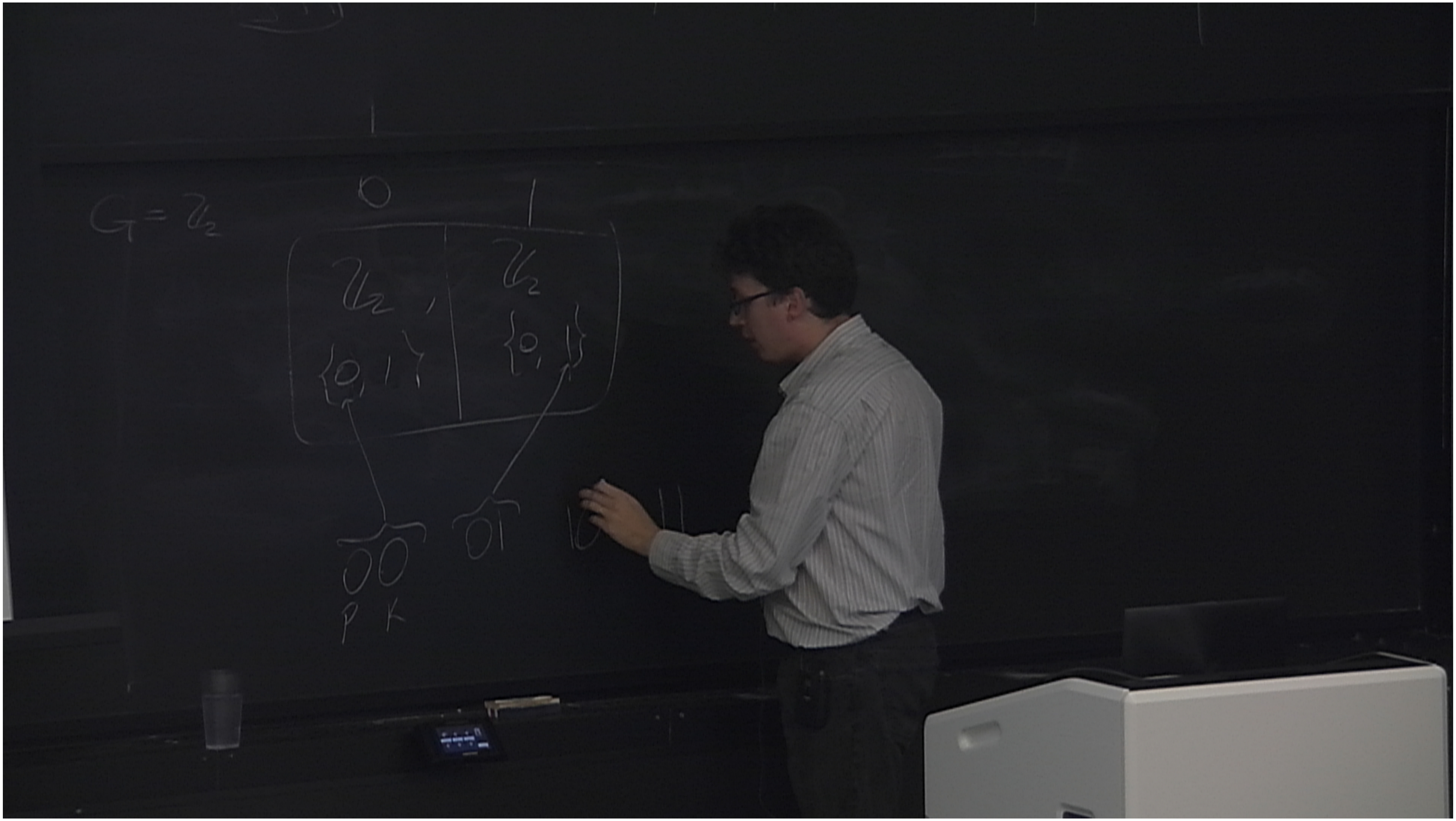


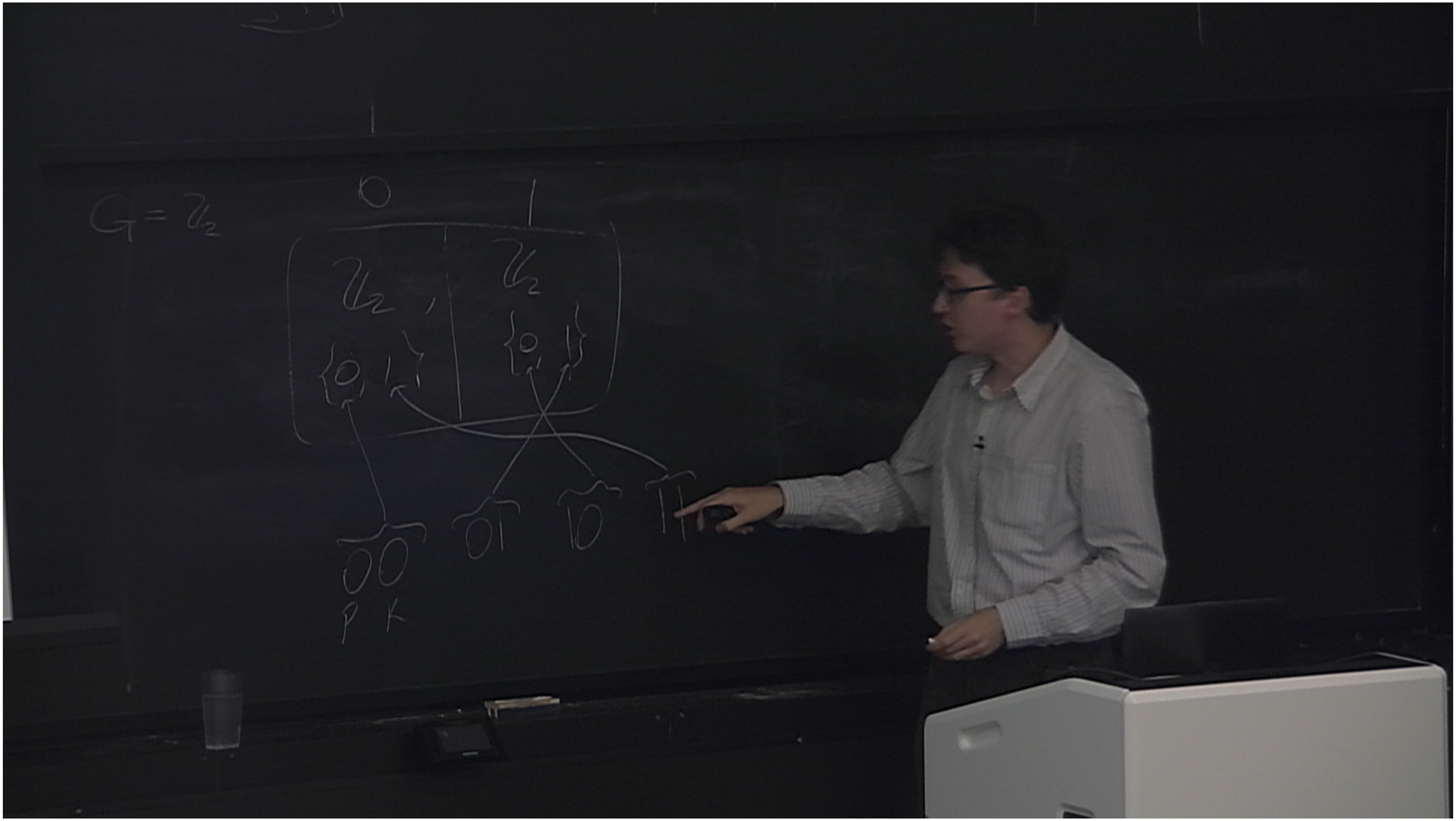
Thank you!


$G = \mathbb{Z}_2$
$\mathbb{Z}_2$,
$\{1, a\}$
$\mathbb{Z}_2$
$\{1, a\}$



G = Z_2
0
1
Z_2 ,
Z_2
{1, a}
P K


G = Z2
0
1
Z2 , Z2
{0, 1}
{0, 1}
00
01
10
11
P K



G = Z₂
0
1
Z₂ , Z₂
{0, 1} {0, 1}
00 01 10 11
p k