

# PROLOGUE

“BEAM US UP SCOTTY!”



•  
•  
•

“HOW DO I DO THAT?”



•  
•  
•

“HERE’S THE CODE”



# The physicist's description

Alice has an ‘unknown’ qubit  $|\phi\rangle$  and wants to send it to Bob. They have the ability to communicate classical bits, and they share an entangled pair in the EPR-state, that is  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ , which Alice produced

by first applying a Hadamard-gate  $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  to the first qubit of a qubit pair in the ground state  $|00\rangle$ , and by then applying a CNOT-gate, that is

$$|00\rangle \mapsto |00\rangle \quad |01\rangle \mapsto |01\rangle \quad |10\rangle \mapsto |11\rangle \quad |11\rangle \mapsto |10\rangle,$$

then **she sends the first qubit of the pair to Bob.**

To teleport her qubit, Alice first performs a bipartite measurement on the unknown qubit and her half of the entangled pair in the Bell-base, that is

$$\left\{ |0x\rangle + (-1)^z |1(1-x)\rangle \mid x, z \in \{0, 1\} \right\},$$

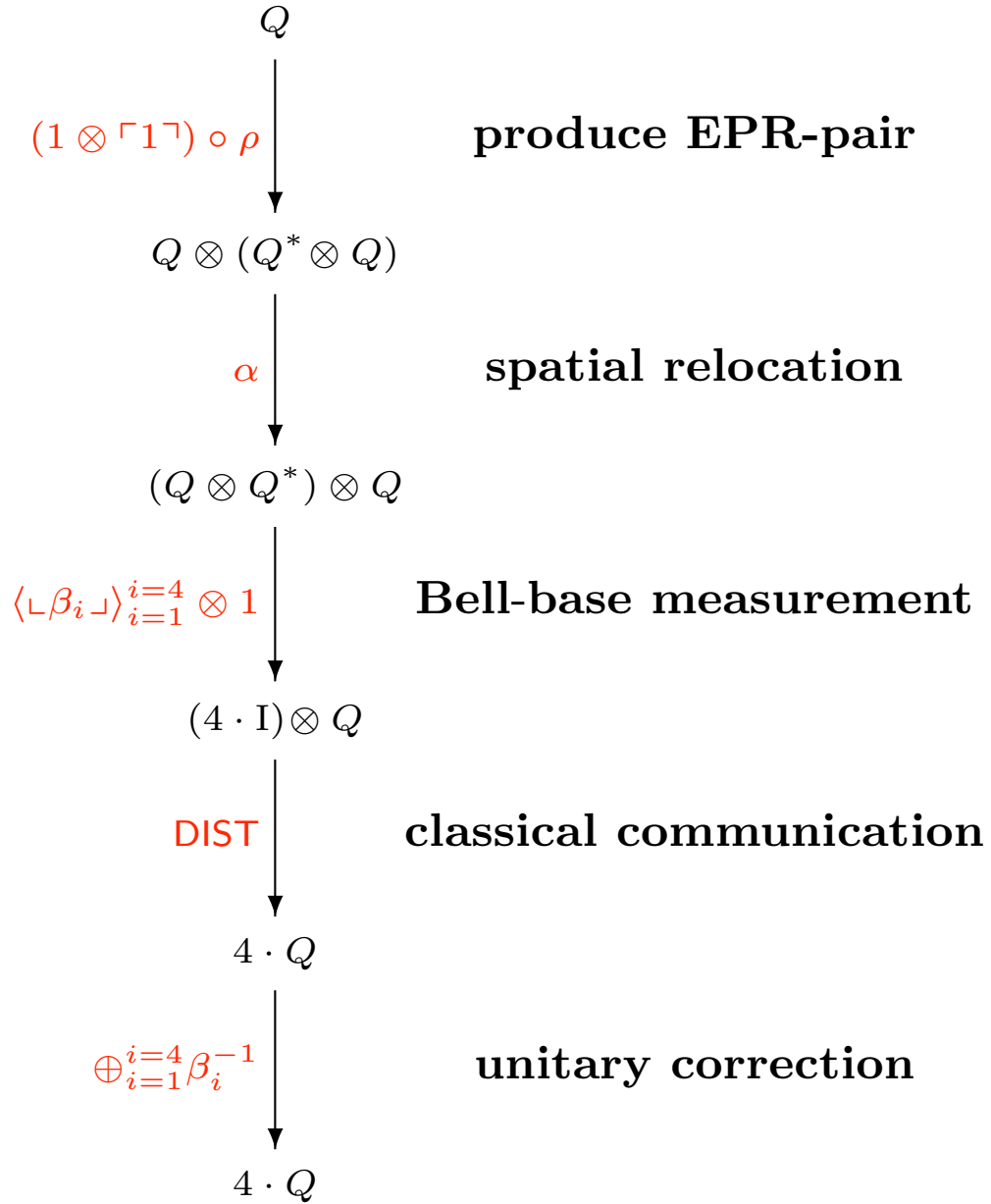
where we denote the four possible outcomes of the measurement by  $xz$ . Then **she sends the 2-bit outcome  $xz$  to Bob using the classical channel.**

Then, if  $x = 1$ , Bob performs the unitary operation  $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  on its half of the shared entangled pair, and he also performs a unitary operation  $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  on it if  $z = 1$ . Now **Bob's half of the initially entangled pair is in state  $|\phi\rangle$ .**

# Ours

$$\rho_Q; \mathbf{1} \otimes \lceil \mathbf{1} \rceil; \alpha; \langle \lfloor \beta_i \rfloor \rangle_{i=1}^{i=4} \otimes \mathbf{1}; \text{DIST}; \bigoplus_{i=1}^{i=4} \beta_i^{-1}$$

I.e.



# The physicist's proof

In the case that the measurement outcome of the Bell-base measurement is  $xz$ , for

$$\mathbf{P}_{xz} := \langle 0x + (-1)^z 1(1-x) | - \rangle \langle 0x + (-1)^z 1(1-x) |$$

we have to apply  $\mathbf{P}_{xz} \otimes \text{id}$  to the input state

$$|\phi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Setting  $|\phi\rangle := \phi_0|0\rangle + \phi_1|1\rangle$  we rewrite the input as

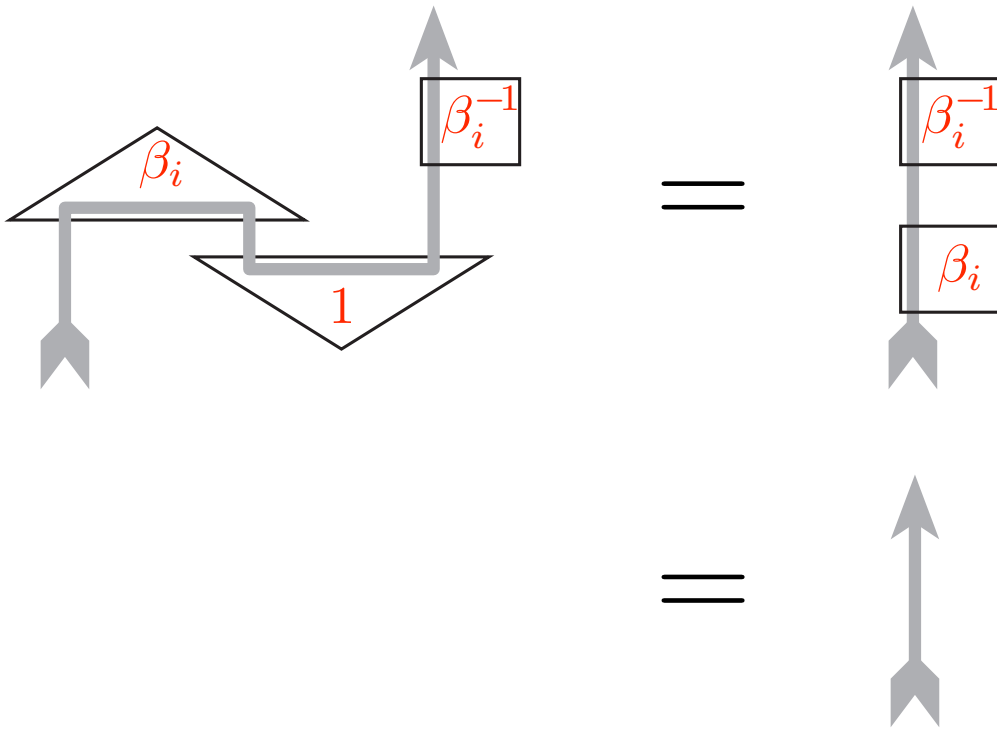
$$\begin{aligned} & \frac{1}{\sqrt{2}}(\phi_0|000\rangle + \phi_0|011\rangle + \phi_1|100\rangle + \phi_1|111\rangle) \\ &= \frac{1}{\sqrt{2}}\left(\phi_0 \sum_{x=0,1} |0xx\rangle + \phi_1 \sum_{x=0,1} |1(1-x)(1-x)\rangle\right) \end{aligned}$$

and application of  $\mathbf{P}_{xz} \otimes \text{id}$  then yields

$$\frac{1}{\sqrt{2}}|0x + (-1)^z 1(1-x)\rangle \otimes (\phi_0|x\rangle + (-1)^z \phi_1|1-x\rangle).$$

There are four cases concerning the unitary corrections  $U_{xz}$  which have to be applied. For  $x = z = 0$  the third qubit is  $\phi_0|0\rangle + \phi_1|1\rangle = |\phi\rangle$ . If  $x = 0$  and  $z = 1$  it is  $\phi_0|0\rangle - \phi_1|1\rangle$  which after applying  $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  becomes  $|\phi\rangle$ . If  $x = 1$  it is  $\phi_0|1\rangle + (-1)^z \phi_1|0\rangle$  which after applying  $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  brings us back to the previous two cases. Hence the result follows.

Ours



Quantum formalism := von Neumann [1932]

“I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more.”

von Neumann [1935]

$$\frac{\text{???}}{\text{von Neumann QM}} \simeq \frac{\text{high-level language}}{\text{low-level language}}$$

Defects of von Neumann’s quantum formalism for **Quantum Informatics**:

- **Types** do not reflect kinds,
- **Classical data-flow** isn’t addressed,
- **Quantum data-flow** i.e. the feature which enables teleportation, is hidden.

# OUTLINE

## **Qubits and quantum information flow.**

B. Coecke. “The logic of entanglement”. OUCL-PRG-RR-03-12 <http://web.comlab.ox.ac.uk/oucl/publications/tr/rr-03-12.html>

## **From von Neumann quantum mechanics to high-level quantum mechanics.**

S. Abramsky and B. Coecke. “A categorical semantics of quantum protocols”. 19th IEEE Conference on Logic in Computer Science (LiCS'04) [www.arXiv.org/quant-ph/0402130](http://www.arXiv.org/quant-ph/0402130)

## **On transdisciplinary opportunities and methodological contributions of computer science to the other sciences.**

A **bit** admits

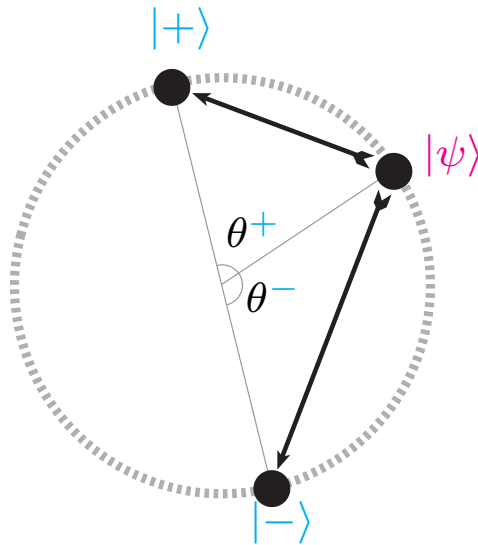
- two values 0, 1,
- it is freely readable,
- it admits arbitrary transformations.

A **qubit** admits

- a sphere of values spanned by  $|0\rangle, |1\rangle$ ,



- a measurement of it
  - has two outcomes  $|-\rangle, |+\rangle$ ,
  - changes the value  $|\psi\rangle$ ,
- it admits unitary transformations i.e. opposites and angles are preserved.



$$\mathbf{P}_+ : |\psi\rangle \mapsto |+\rangle \qquad \mathbf{P}_- : |\psi\rangle \mapsto |-\rangle$$

have chance  $\text{prob}(\theta^\#)$  for  $\# \in \{+, -\}$ . On the sphere  $Q$  we obtain **partial constant maps**

$$\mathbf{P}_\# : Q \rightarrow Q :: |\psi\rangle \mapsto | \# \rangle.$$

We know the value after a measurement, but not what it was before it.

- Bad: measurements destroy data.
- Good: measurements act on data.

Quantum computing and quantum protocols: acrobatics between “the good” and “the bad”.

# Q.M. in a nutshell

**Systems** are described by vectors (up to a scalar) of an inner-product space over  $\mathbb{C}$ .

**Compoundness** is described by  $- \otimes -$ .

**Operations** is described by unitaries.

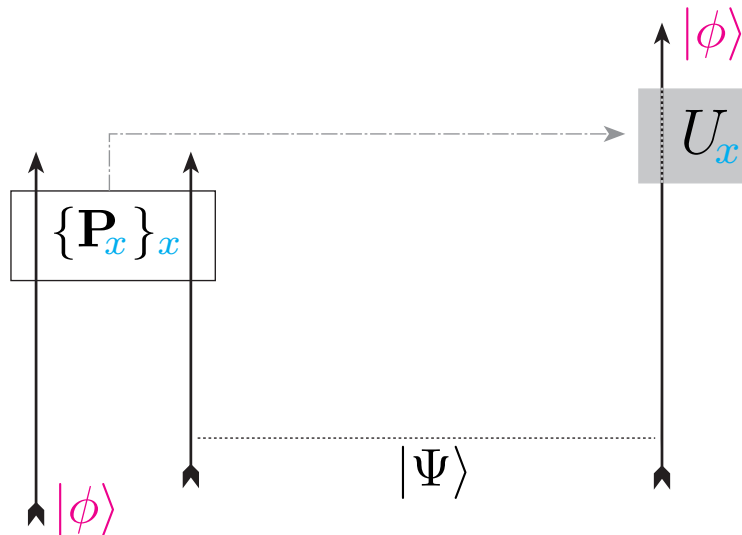
**Measurements** “are described” by self-adjoint operators  $H : \mathcal{H} \rightarrow \mathcal{H}$  i.e.

$$H = a_1 \cdot \mathbf{P}_1 + \dots + a_n \cdot \mathbf{P}_n .$$

The measurement process constitutes:

- One  $\mathbf{P}_i$  in  $(\mathbf{P}_1, \dots, \mathbf{P}_n)$  happens.
- The observer **receives** the token  $a_i$ .
- The probability of this is  $|\mathbf{P}_i(\psi)|^2$ .

## Quantum teleportation [Bennett et al. 1993]



Continuous data transmission through 2 bits?

So what causes the magic?

A pair of qubits isn't described by a pair

$$|\psi_1, \psi_2\rangle \in Q_1 \times Q_2$$

but by a function

$$|f : Q_1 \rightarrow Q_2\rangle \in Q_1 \otimes Q_2$$

Indeed, the tensor product  $\mathcal{H}_1 \otimes \mathcal{H}_2$  of Hilbert spaces  $\mathcal{H}_1, \mathcal{H}_2$  is the Hilbert space spanned by

$$\begin{array}{ccc} |11\rangle & \cdots & |1n\rangle \\ \vdots & \ddots & \vdots \\ |k1\rangle & \cdots & |kn\rangle \end{array}$$

hence,

$$\begin{aligned} \sum_{ij} m_{ij} |ij\rangle &\xleftrightarrow{\cong} \begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{k1} & \cdots & m_{kn} \end{pmatrix} \\ &\xleftrightarrow{\cong} |i\rangle \mapsto \sum_j m_{ij} |j\rangle \end{aligned}$$

e.g. for  $k = n$ ,

$$|11\rangle + \dots + |nn\rangle \xleftrightarrow{\cong} |i\rangle \mapsto |i\rangle$$

Pairs  $|\psi_1, \psi_2\rangle$  are a special case in  $\mathcal{H}_1 \otimes \mathcal{H}_2$  — reducing to  $|ij\rangle$  in a well-chosen base.

The identity

$$|\text{id} : Q \rightarrow Q\rangle \in Q \otimes Q$$

is the **Einstein-Podolsky-Rosen** state.

A measurement of  $Q \otimes Q$  has four outcomes

$$|f_1\rangle, |f_2\rangle, |f_3\rangle, |f_4\rangle$$

cf.

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

and corresponding

$$\mathbf{P}_f : Q \otimes Q \rightarrow Q \otimes Q :: |g\rangle \mapsto |f\rangle$$

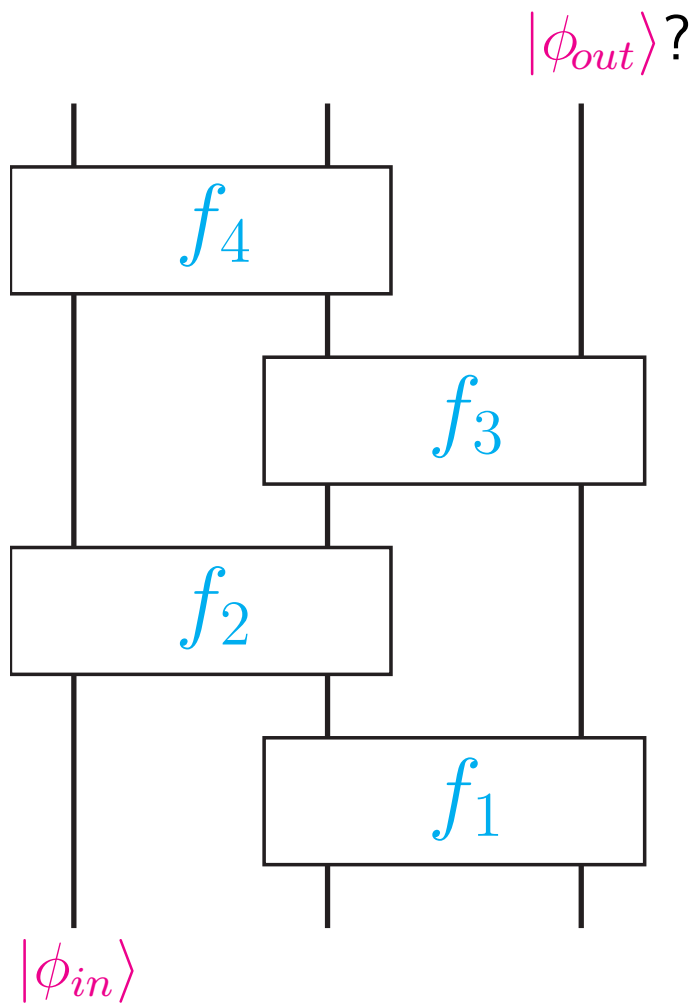
e.g.

$$\mathbf{P}_{\text{id}} : Q \otimes Q \rightarrow Q \otimes Q :: |g\rangle \mapsto |\text{id}\rangle$$

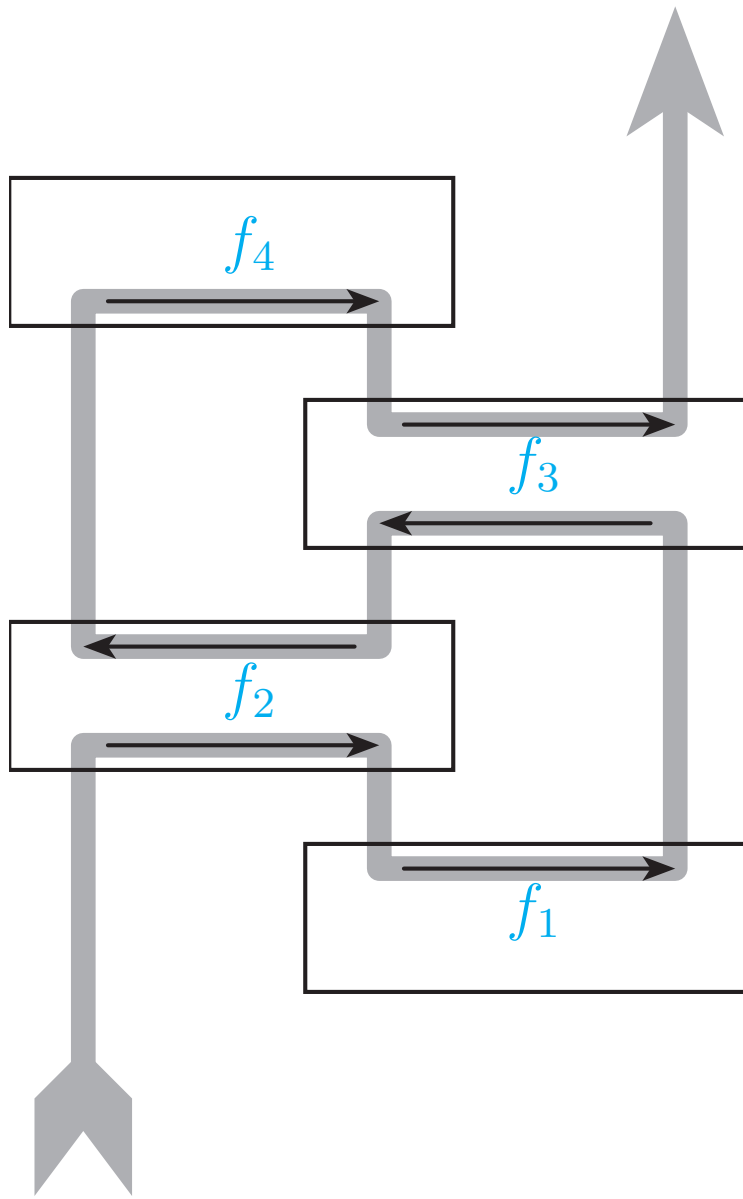
produces the **EPR** state.

Do  $Q \otimes Q$ -functions **compose** (in some way)?

**They do!**

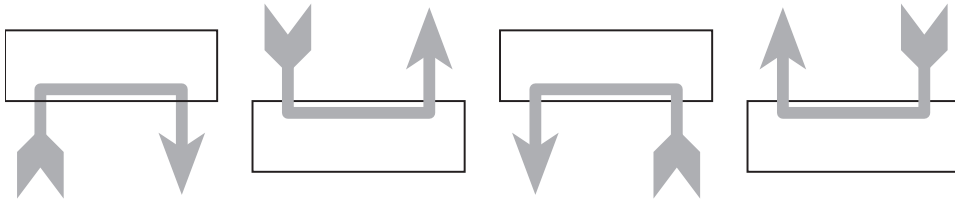


$$\phi_{out} = (f_2 ; f_1 ; f_3^\dagger ; f_2^\dagger ; f_4 ; f_3)(\phi_{in})$$

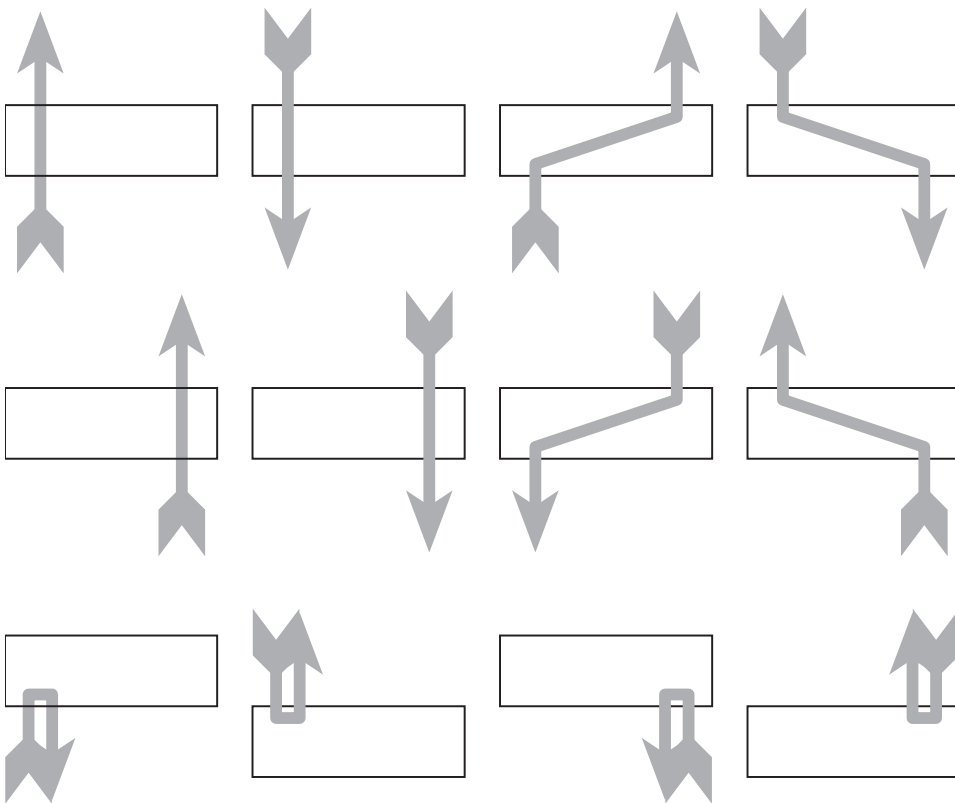


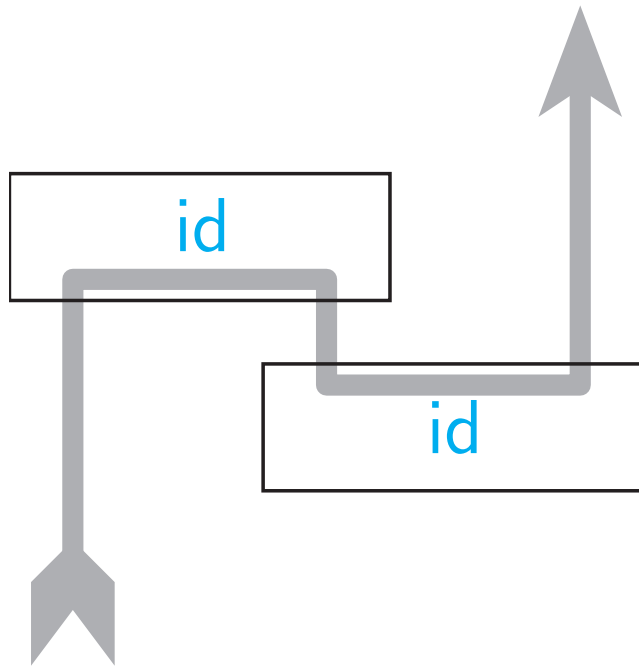
$f_2 ; f_1 ; f_3^\dagger ; f_2^\dagger ; f_4 ; f_3$

# Permitted



# Forbidden

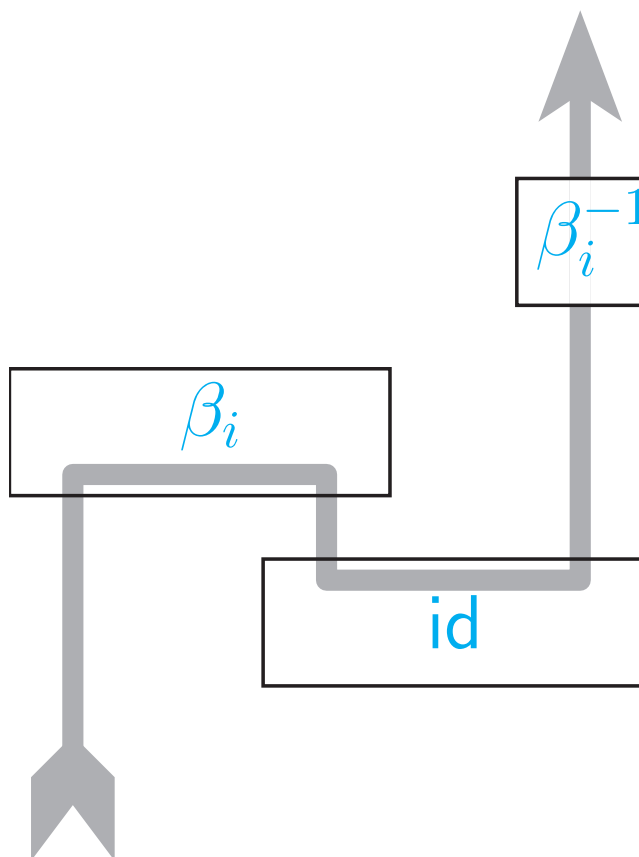




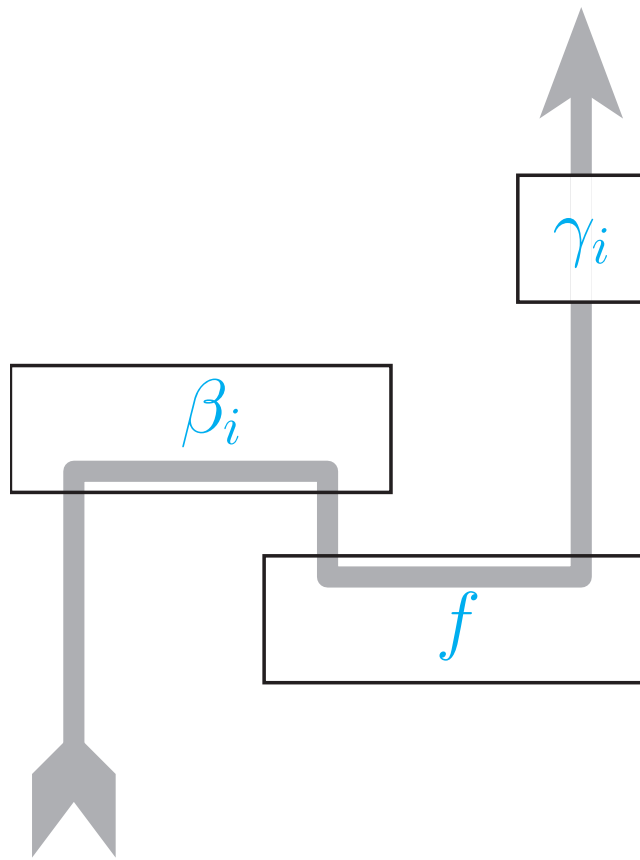
$$\text{id} ; \text{id} = \text{id}$$

**$\Rightarrow$  Teleportation**

$$1 \leq i \leq 4$$

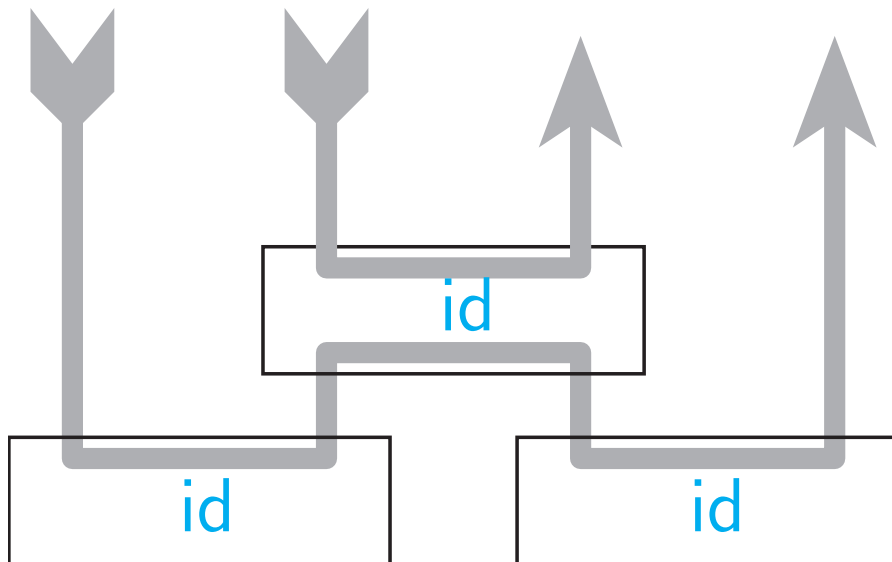


$$\beta_i ; \text{id} ; \beta_i^{-1} = \text{id}$$



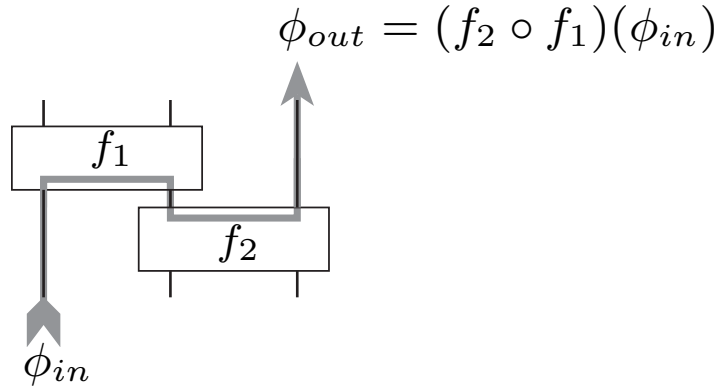
$$\beta_i ; f ; \gamma_i = f$$

$\Rightarrow$  Logic-gate teleportation



$$\text{id} ; \text{id} ; \text{id} = \text{id}$$

⇒ Entanglement swapping



$$\begin{aligned} & \left( (\mathbf{P}_{f_1} \otimes 1) \circ (1 \otimes \mathbf{P}_{f_2}) \right) (\phi_{in} \otimes \dots) \\ & = \dots \otimes (f_2 \circ f_1)(\phi_{in}) \end{aligned}$$

Hilbert space	$\rightsquigarrow$	<b>set</b>
linear function	$\rightsquigarrow$	<b>relation</b>
tensor product	$\rightsquigarrow$	<b>product</b>

$$\begin{aligned} \mathbf{P}_R & := R \times R \\ & = \{((x_1, y_1), (x_2, y_2)) \mid x_1 R y_1, x_2 R y_2\} \end{aligned}$$

$$\begin{aligned} & (s_{in}, \cdot, \cdot) \left( (\mathbf{P}_{R_1} \otimes 1) \circ (1 \otimes \mathbf{P}_{R_2}) \right) (\cdot, \cdot, s_{out}) \\ & \Rightarrow s_{in} (R_2 \circ R_1) s_{out} \end{aligned}$$

## High-level quantum mechanics

A category  $\underline{\mathbf{C}}$  has **objects**  $A, B, C, \dots$  and for each two objects  $A, B$  a set of **morphisms**  $\underline{\mathbf{C}}(A, B)$ . It also has  $\text{id}_A \in \underline{\mathbf{C}}(A, A)$  and composition  $g \circ f$  when types match.

Why categories? Since they allow to deal explicitly with processes e.g.

<b>Logic</b>	<b>Programming</b>
Propositions	I/O-Types
Proofs	Programs

Variables (e.g. qubits  $Q$ )  $\sim$  objects

Processes (e.g. measurements)  $\sim$  morphisms

Compoundness (e.g.  $Q \otimes Q$ )  $\sim$  morphism sets

We also want an associative connective  $\otimes$  which encodes compound systems as objects.

A **symmetric monoidal category** is a category in which we can “plug *things* together”, *things* being both objects and morphisms:

$$A \otimes B \quad f_1 \otimes f_2 : A_1 \otimes A_2 \rightarrow B_1 \otimes B_2$$

There exist natural operations e.g. swapping,

$$\sigma_{A,B} : A \otimes B \rightarrow B \otimes A,$$

which satisfy obvious behavioral rules e.g.

$$\begin{array}{ccc}
 A_1 \otimes A_2 & \xrightarrow{f_1 \otimes f_2} & B_1 \otimes B_2 \\
 \sigma_{A_1, A_2} \downarrow & & \downarrow \sigma_{B_1, B_2} \\
 A_2 \otimes A_1 & \xrightarrow{f_2 \otimes f_1} & B_2 \otimes B_1
 \end{array}$$

There is some **locality** for components

$$\begin{array}{ccc}
 A_1 \otimes A_2 & \xrightarrow{f_1 \otimes \text{id}} & B_1 \otimes A_2 \\
 \text{id} \otimes f_2 \downarrow & & \downarrow \text{id} \otimes f_2 \\
 A_1 \otimes B_2 & \xrightarrow{f_1 \otimes \text{id}} & B_1 \otimes B_2
 \end{array}$$

But we don't assume a pair-like structure, i.e.

$$\text{whole} \neq \sum \text{components}$$

This turns out to comprise the absence of

$$A \xrightarrow{\Delta} A \otimes A \qquad A \otimes B \xrightarrow{\pi} A$$

## No-cloning & No-deleting

Wooters-Zurek 1982; Pati-Braunstein 2000

Crucial for secure quantum cryptography.

Is this connected to resource sensitive languages and recent models for concurrency and interaction in distributed computation?

Yes

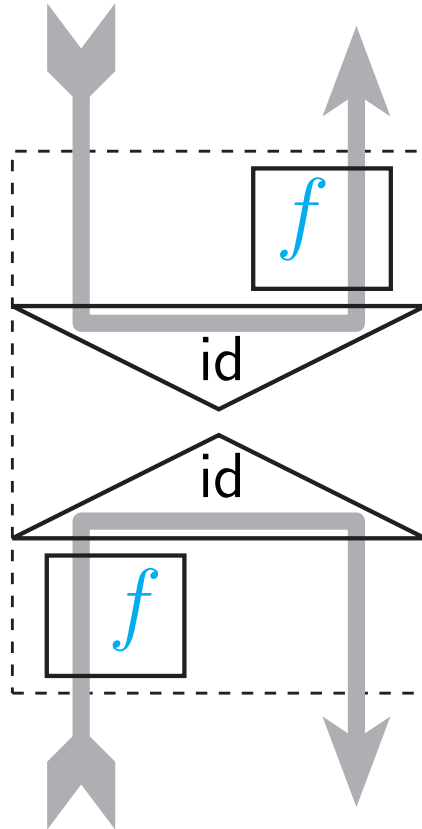
Categories will enable us to capture the quantum information flow (= geometry of the line) syntactically, and compare it to the resource-sensitive and concurrent CS semantics.

No-cloning & no-deleting refute existence of

$$\begin{array}{ll} A \xrightarrow{\Delta} A \otimes A & A \otimes B \xrightarrow{\pi} A \\ A \vdash A \wedge A & A \wedge B \vdash A \end{array}$$

What more do we need for quantum theory?

# Dissection of $P_f$



$$P_f = f \otimes \text{id}; \lrcorner \text{id} \lrcorner; \lrcorner \text{id} \lrcorner; \text{id} \otimes f$$

(cf. unraveling a program into commands)

## The algebra of entanglement

1. a monoidal involution on objects,

$$A \mapsto A^*$$

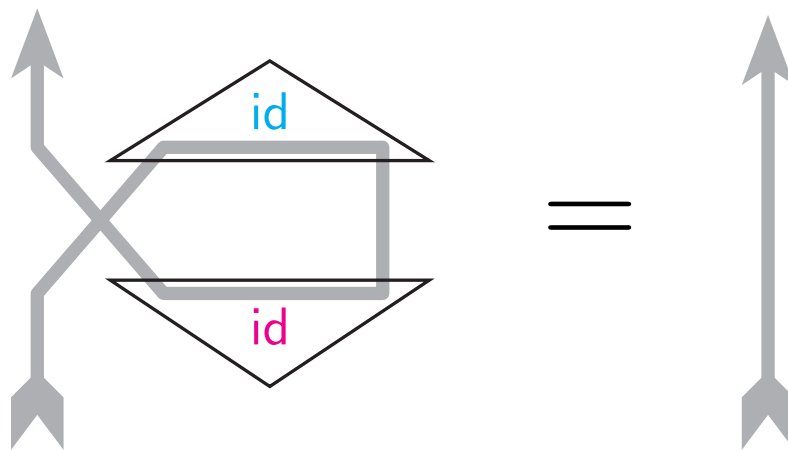
2. for each involutive pair a morphism

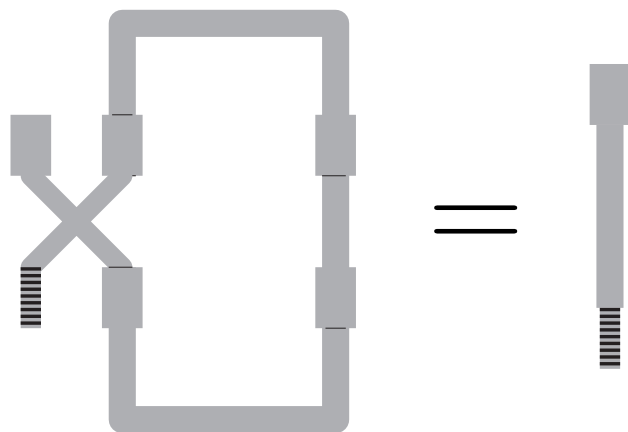
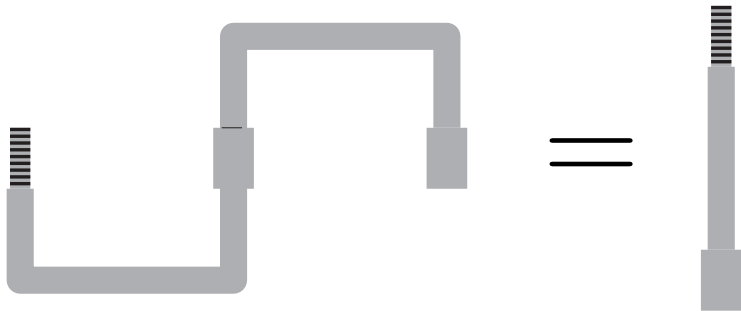
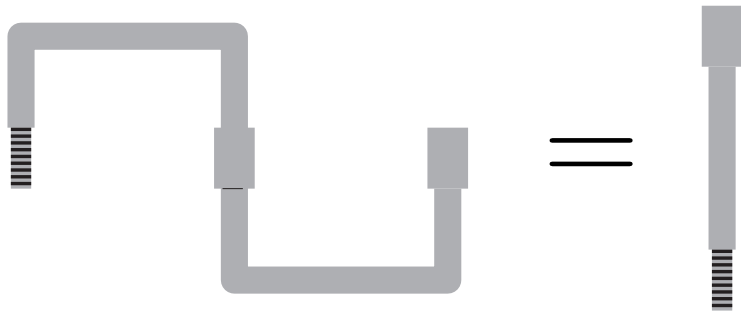
$$\ulcorner \text{id} \urcorner : I \rightarrow A \otimes A^*$$

3. a monoidal duality on morphisms,

$$f : A \rightarrow B \mapsto f^\dagger : B \rightarrow A$$

such that





## Scalars:

- Unit 1 as  $\text{id}_I$ .
- Integers as  $\lfloor \text{id}_A \rfloor \circ \lceil \text{id}_A \rceil$
- Reals as  $s \circ s^\dagger$
- Probabilities  $[0, 1]$  as  $|\langle \phi | \psi \rangle|$ .

contained in  $\underline{\mathbf{C}}(I, I)$  for  $I$  the  $\otimes$ -unit, and each scalar induces “natural” scalar multiplication.

## Unitarity:

$$U^\dagger = U^{-1}$$

## Inner-product:

$$\langle \phi | \psi \rangle := \phi^\dagger \circ \psi$$

for  $\phi: I \rightarrow A$  and  $\psi: I \rightarrow B$ . We have:

$$\langle U \circ \psi | U \circ \phi \rangle = \langle \psi | \phi \rangle$$

$$\langle f^\dagger \circ \psi | \phi \rangle = \langle \psi | f \circ \phi \rangle$$

# Example

**objects:** sets

**morphisms:** relations

**tensor:** cartesian product

**Additional data:**

$$X^* := X \quad R^\dagger := R^c$$

$$\eta := \{(*, (x, x)) \mid x \in X\} \subseteq \{*\} \times (X \times X)$$

**Matrices in any involutive abelian semiring** provide a model generalizing relations, that is, matrices in the Boolean semiring.

Other examples are inner-product spaces, free compact closed categories generated by self-dual categories,  $n$ -cobordisms, . . .

What do we miss to have all ingredients of von Neumann's formalism?

An operation  $\oplus$  on  $\underline{\mathbf{C}}$  which now stands for

“plugging histories together”

where history = picture = branch = world, and which has pair-like nature (= biproduct).

Disjunctive/probabilistic content:

$$Q \oplus Q$$

Producing a “sphere” from two “germs”:

$$Q \simeq I \oplus I$$

A **qubit measurement** becomes

$$\langle \mathbf{P}_+, \mathbf{P}_- \rangle : Q \rightarrow Q \oplus Q$$

where

$$\mathbf{P}_\# = \pi_\#^\dagger \circ \pi_\# : Q \rightarrow Q$$

with

$$\langle \pi_+^\dagger, \pi_-^\dagger \rangle : Q \rightarrow I \oplus I$$

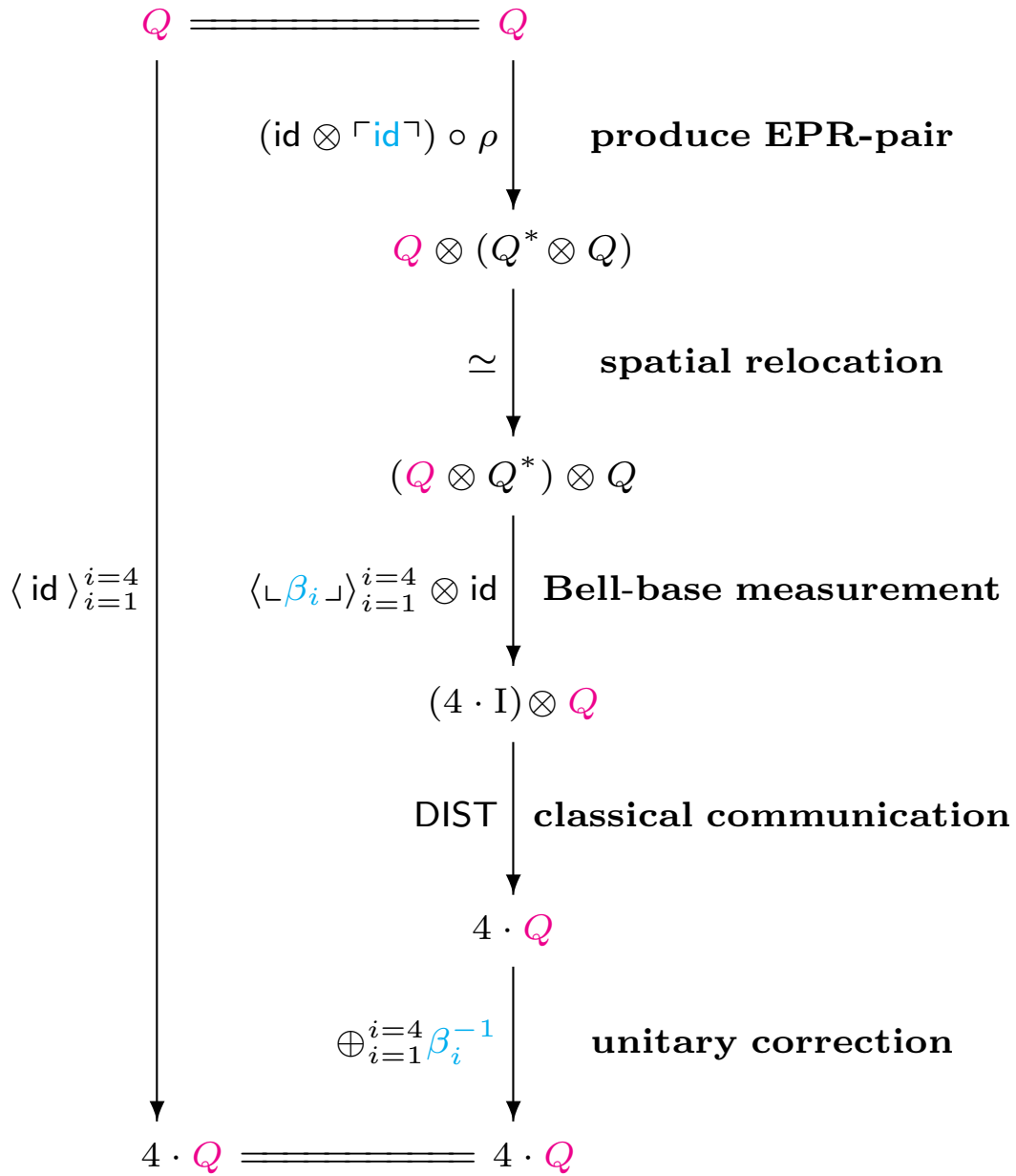
unitary.

**Classical information flow** is distributivity,

$$(I \oplus I) \otimes Q \xrightarrow{\text{DIST}} (I \otimes Q) \oplus (I \otimes Q) \simeq Q \oplus Q$$

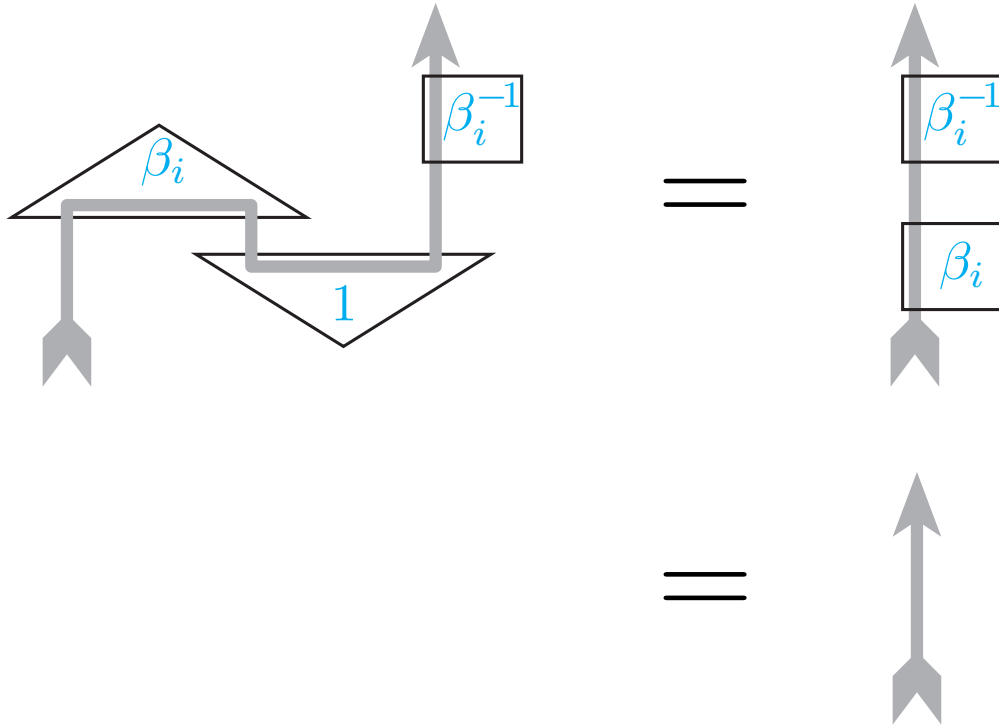
$$(Q_1 \oplus Q_2) \otimes Q \xrightarrow{\text{DIST}} (Q_1 \otimes Q) \oplus (Q_2 \otimes Q)$$

# Theorem.



i.e.

$$\rho_Q ; \text{id} \otimes \ulcorner \text{id} \urcorner ; \alpha ; \langle \lfloor \beta_i \rfloor \rangle_{i=1}^{i=4} \otimes \text{id} ; \text{DIST} ; \bigoplus_{i=1}^{i=4} \beta_i^{-1} = \text{id}$$



## Beyond von Neumann's 1932 Q.M.

**We increased resolution.** We now see the quantum information flow. **We extended scope.** We added classical data and information flow. **Types reflect kinds,** and there are many more of them.

**The formalism is high-level.** We have a compact purely formal language and intuitive geometrical proofs, but with a categorical logical and syntactic counterpart, namely **linear logic with dual self-dual connectives.**

**We emphasized essence.** We abstract over non-crucial things and allowed new degrees of axiomatic freedom, enabling **relational reasoning:** sets, relations and the cartesian product satisfy the axiomatics.

**A bonus.** The probability rule can be derived in our formalism while in von Neumann's formalism it is a postulate.

## Direct applications

**Intuitive** analysis and design of computational schemes and protocols, and general **operational** reasoning about quantum systems.

A step stone towards **automated** analysis, design and reasoning about quantum systems

E.g. **measurement based quantum computing** is both from soft- and hardware perspective very promising, and relies completely on the structure of entanglement.

In particular, qualifying and quantifying **multipartite entanglement** and obtaining a better understanding of its properties is the current holy grail of quantum information.

## A transdisciplinary perspective

What did we do so far? We definitely did

- high-level quantum informatics,

but, also

- physics in informatic perspective.

Why did it take 60 years and 6 persons for

- teleportation to be invented?

Why did it took 70 years to have

- a complete quantum formalism and logic
- which recognizes the compositional nature of entanglement,

and as such

- trivializes teleportation?

Since many of the tools were either

- not available (yet), or,
- not being considered (yet).

Now they do exist and were developed by

- computer scientists.

So why didn't physicist invent them?

- Many physicists couldn't care less.
- They looked in the wrong direction.
- They used inappropriate methodologies.
- They followed old-fashion paradigms.

Computer science has something to offer to other sciences — other than “the computer”!

- Logical and structural reasoning.
- The operational methodology.
- Fresh paradigms.

E.g.

- Interaction and concurrency.
- Open systems.
- Qualitative reasoning about information.
- Continuous vs. discrete.
- Hybrid systems.

# EPILOGUE

