The *non*-logic of quantum computation

OR:

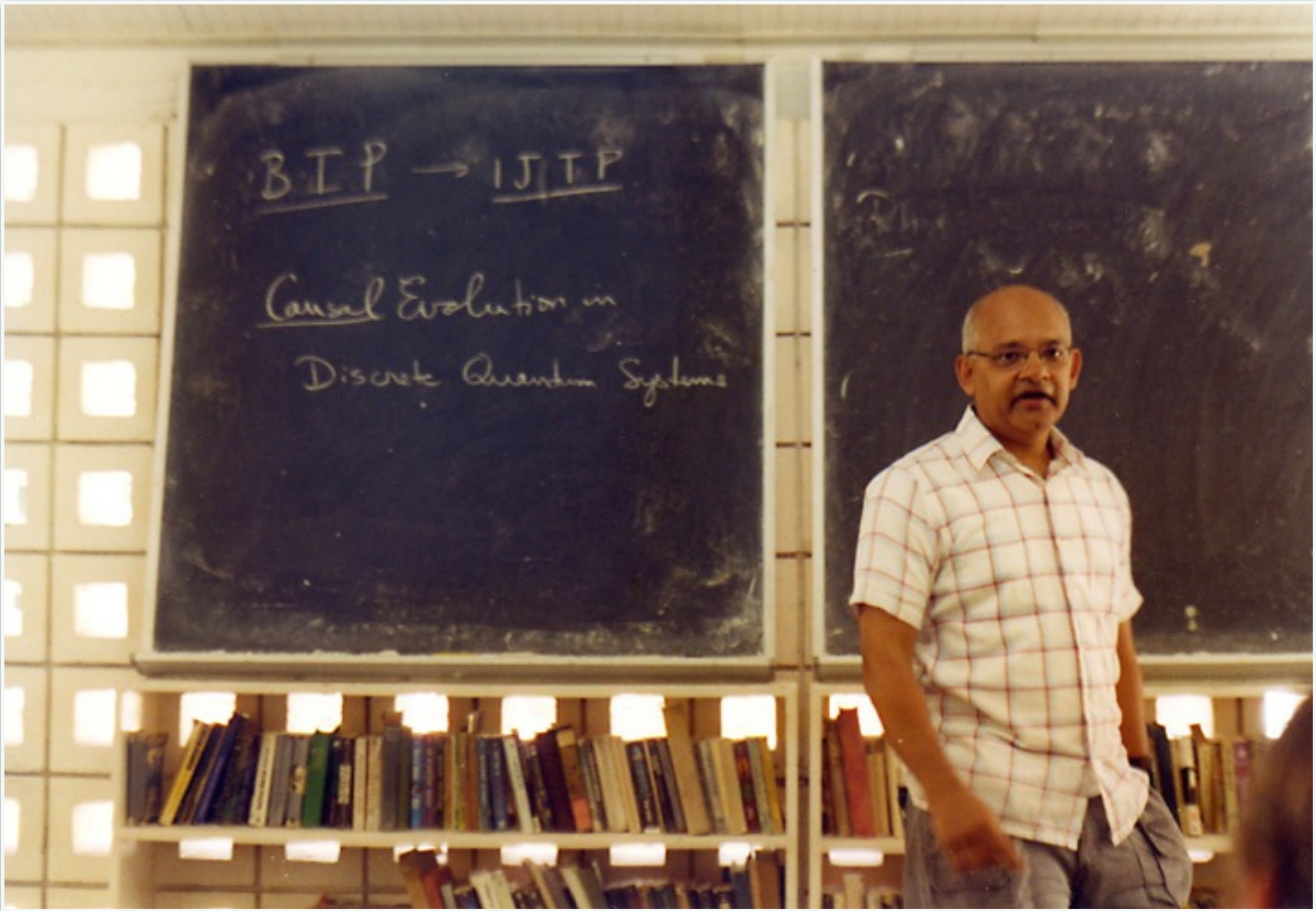
How I learned to live without propositions-as-types

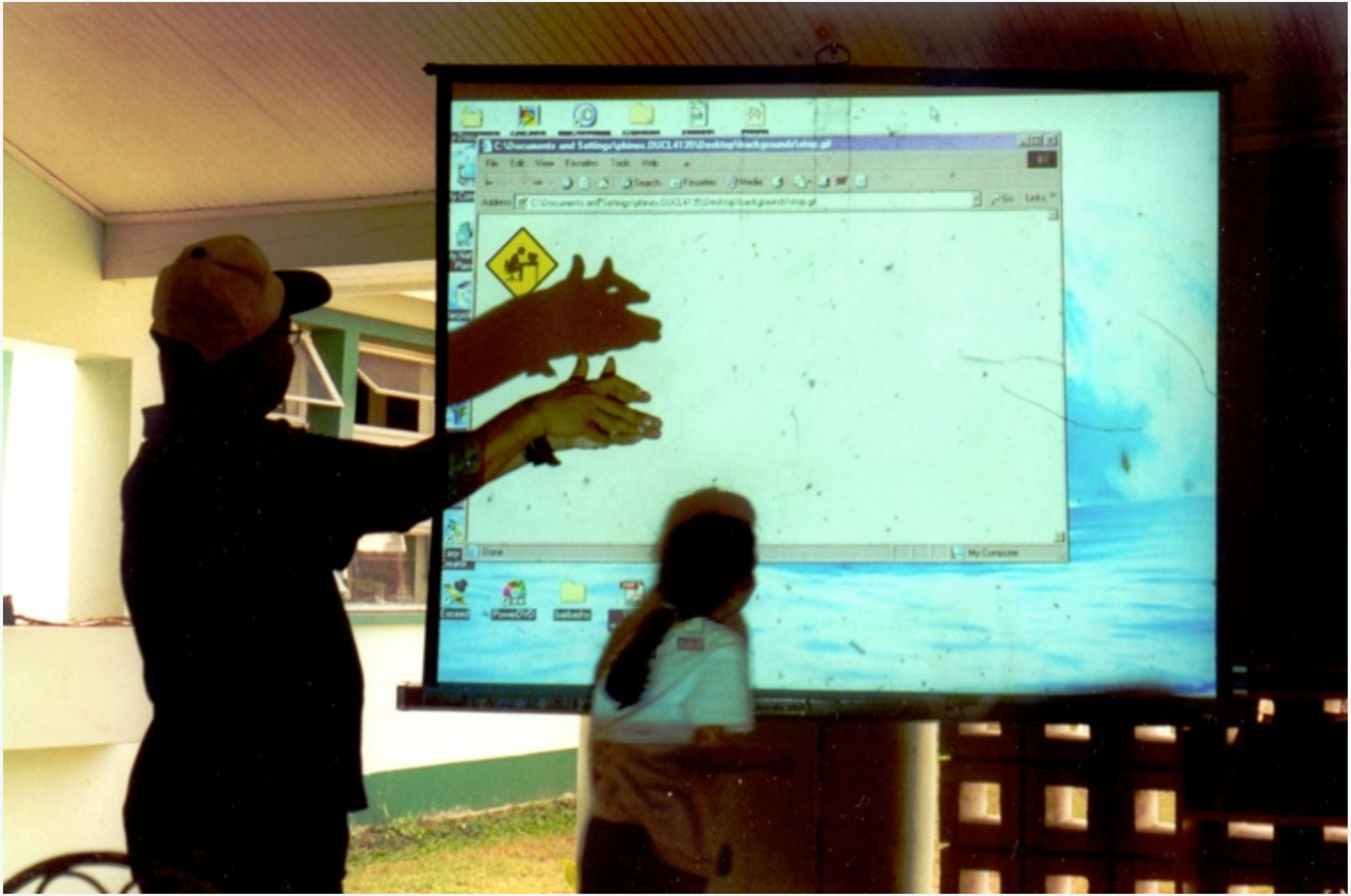
Ross Duncan

Mathematically Structured Programming Group
University of Strathclyde

2004

"The 1st occasional Bellairs workshop on semantic techniques in quantum computing"


BTP → IJTP
Causal Evolution in
Discrete Quantum Systems



What is the **logic** of quantum computation?

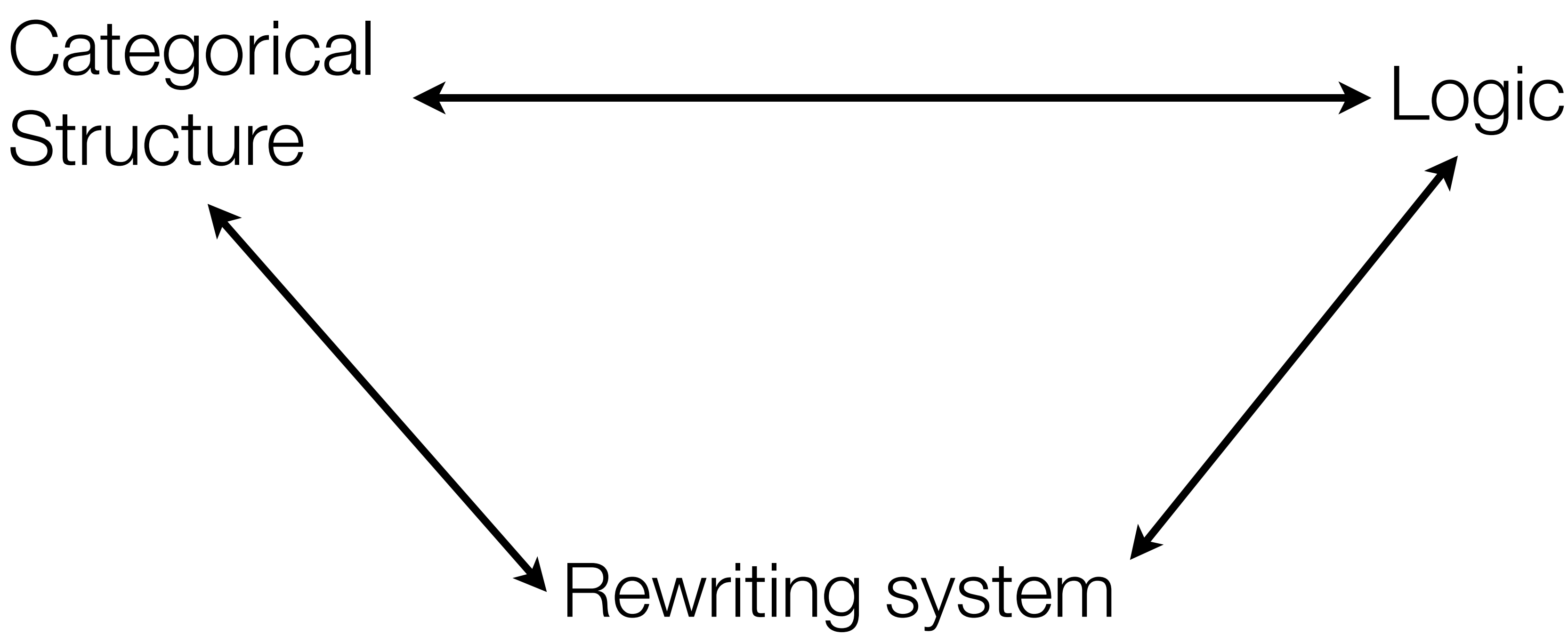
The Curry-Howard-Lambek correspondence

Cartesian closed categories

Intuitionistic Logic

Simply typed λ-calculus

General Scheme



Proofs and types

Proofs and programs are the same thing.

- Propositions are *types.*
- Many different proofs of the same theorem: *processes* producing output of that *type.*
- Less interested in the validity of propositions than the relationship between proofs

Proofs and types

Pragmatics:

- The type of a program should provide some useful information about that program.
- The type system should exclude (certain) programming errors.

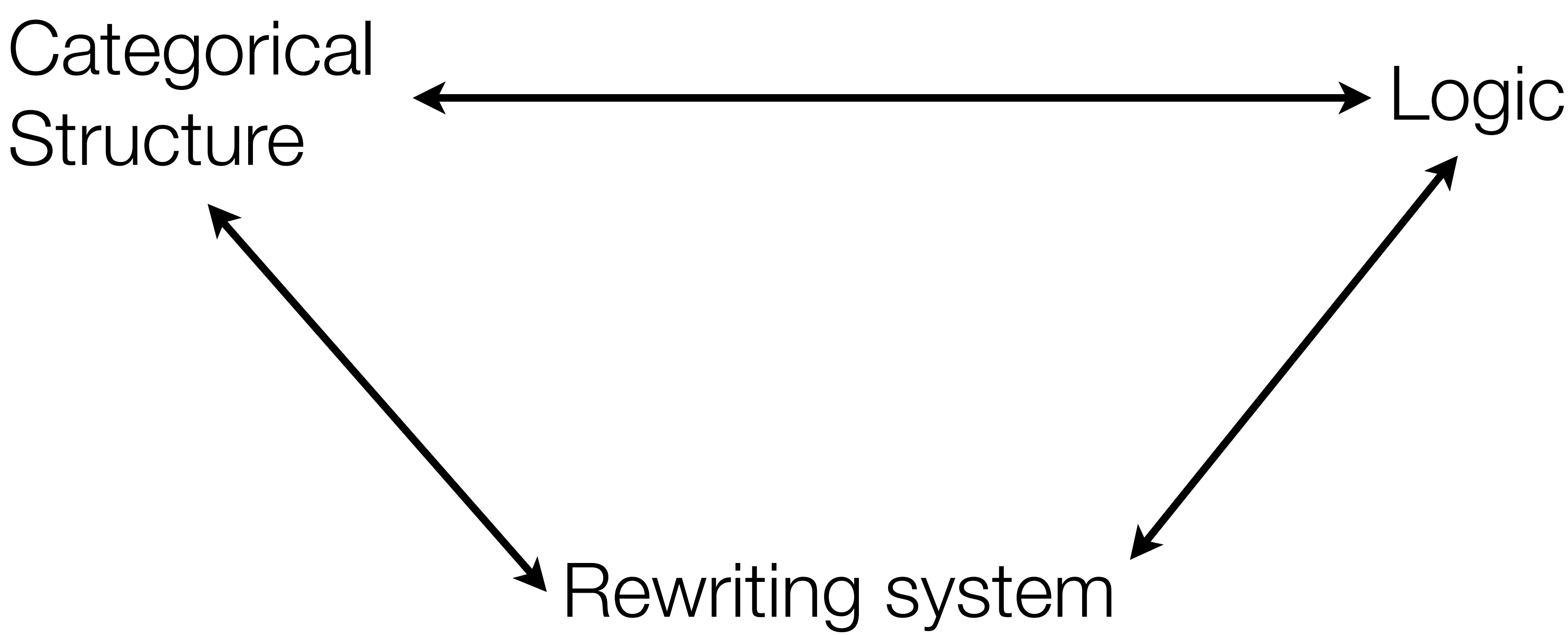
Proofs and types

Pragmatics:

- The type of a program should provide some useful information about that program.
- The type system should exclude (certain) programming errors.

“It type checks — it must be right”

The objective:



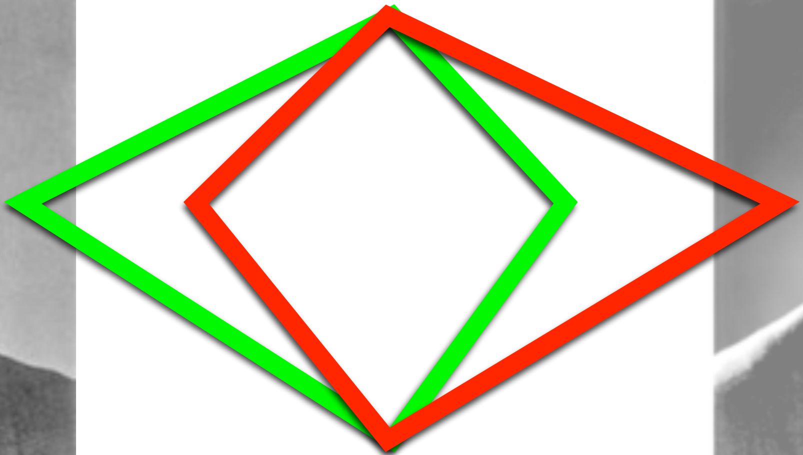
The objective:

Quantum
Categorical
Structure
??????

Quantum
Logic
??????

Quantum
Rewriting system
??????

Quantum Logic



The Birkhoff-von Neumann approach and its problems

Propositions and projectors

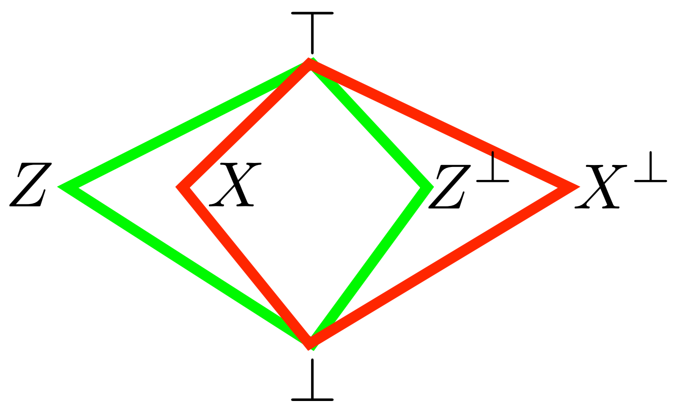
A proposition is a question with a yes/no answer:

A = *"Is the spin up?"*

but the answer will be given by a quantum measurement:

$$\psi \models A \quad \Leftrightarrow \quad p_A \left|\psi\right\rangle = \left|\psi\right\rangle$$

hence each proposition corresponds to a pair of orthogonal subspaces.

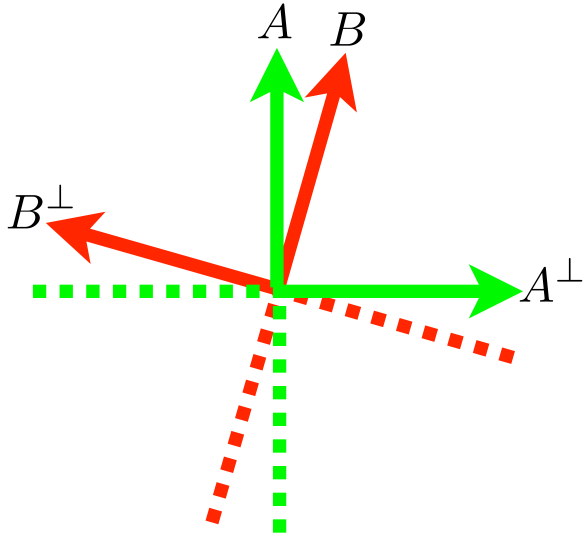


The "lattice of propositions" is simply the collection of closed subspaces ordered under inclusion.

Distributivity Fails

In general we have $p_A p_B \neq p_B p_A$ which implies the failure of distributivity.

Consider:



we have

$$\perp = (A \wedge B) \vee (A^\perp \wedge B) \neq (A \vee A^\perp) \wedge B = B$$

hence such a lattice is not distributive.

(It does satisfy a weaker law called *orthomodularity* which I won't discuss.)

No deduction theorem

Theorem: Suppose we can define a connective $\to$ such that

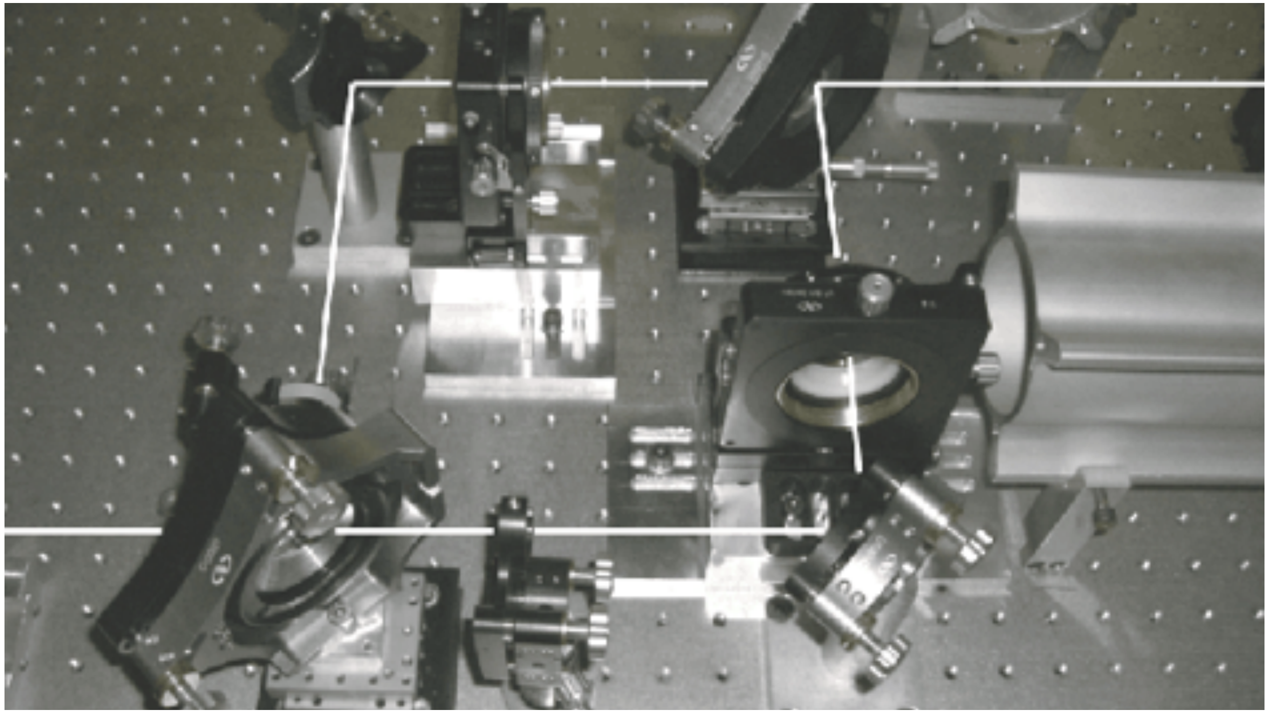
$$A \wedge X \leq B \qquad \Leftrightarrow \qquad X \leq A \to B$$

then the lattice is distributive.

Corollary: Quantum logic does not admit modus ponens.

Note that the sub-lattice defined by any set of commuting projectors is just a boolean lattice.

Quantum Mechanics



Overview of the physical theory

No-Cloning and No-Deleting

Theorem: There are no quantum operations D such that

$$D : |\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$$
$$D : |\phi\rangle \mapsto |\phi\rangle \otimes |\phi\rangle$$

unless $|\psi\rangle$ and $|\phi\rangle$ are orthogonal [Wooters & Zurek 1982]

Theorem: There are no quantum operations E such that

$$E : |\psi\rangle \mapsto |0\rangle$$
$$E : |\phi\rangle \mapsto |0\rangle$$

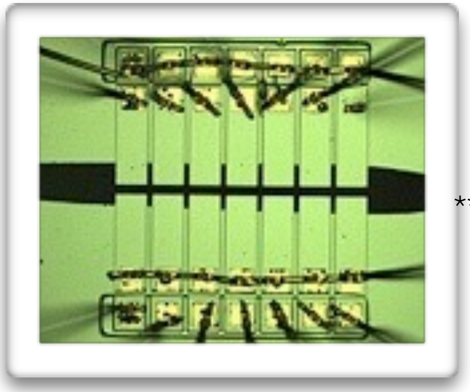
unless $|\psi\rangle$ and $|\phi\rangle$ are orthogonal [Pati & Braunstein 2000]

No-Cloning and No-Deleting

Linear types have been proposed* to capture this:

$$!A \qquad\qquad A \otimes B$$

Separate classical and quantum data in a hybrid machine



** Hensinger et al *Nature 2005*

*vanTonder 2003, Selinger and Valiron 2005, Arrighi and Dowek 2003, Altenkirch & Grattage 2005

No-Cloning and No-Deleting

Linear types have been proposed* to capture this:

S

r

Not good enough!

** Hensinger et al *Nature 2005*

*vanTonder 2003, Selinger and Valiron 2005, Arrighi and Dowek 2003, Altenkirch & Grattage 2005

Map-State Duality

Recall that there is an isomorphism :

$$A \multimap B \cong A \otimes B$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \longleftrightarrow \quad |00\rangle + |11\rangle =: |\mathrm{Bell}_1\rangle$$

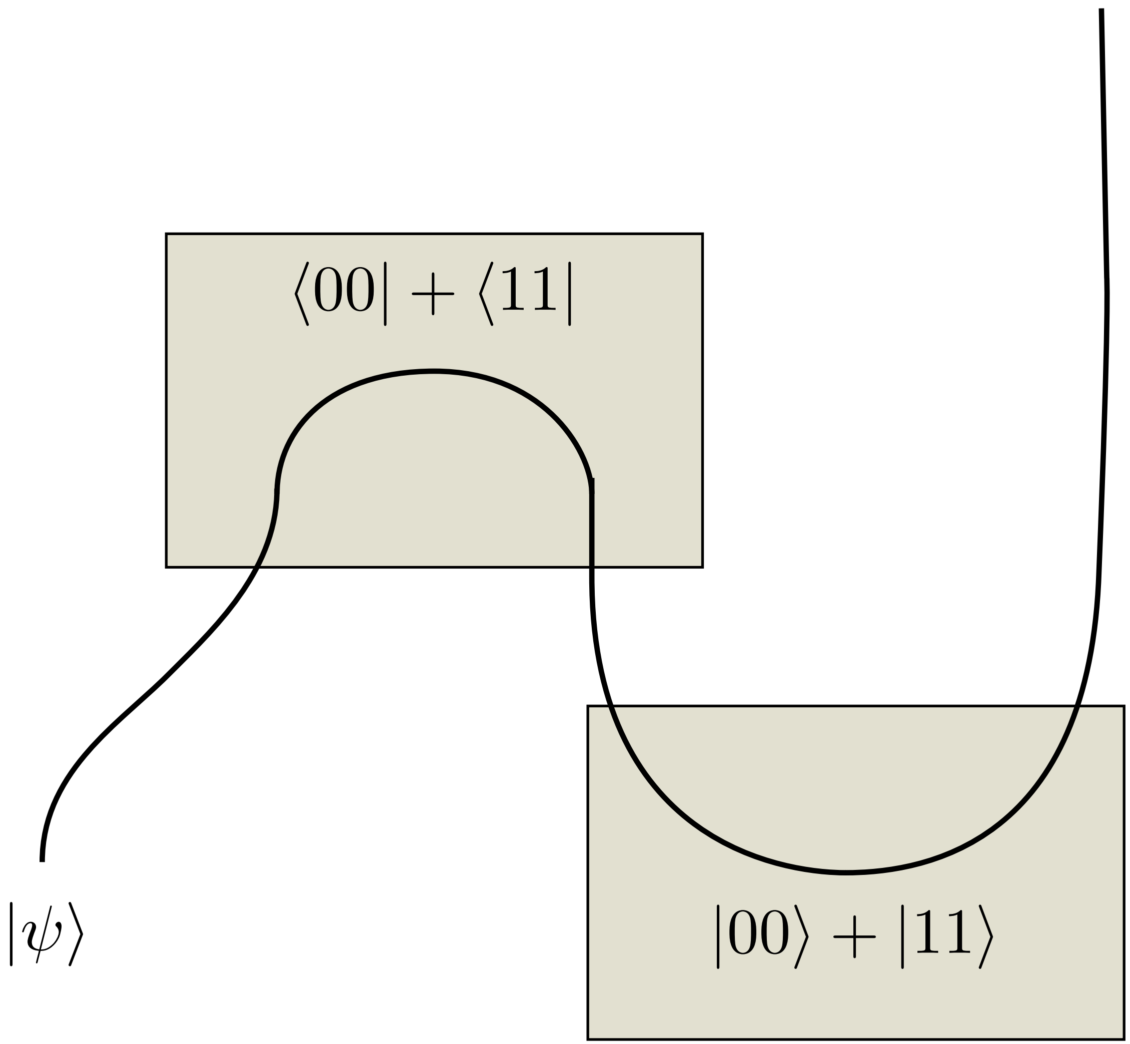
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \longleftrightarrow \quad |01\rangle + |10\rangle =: |\mathrm{Bell}_2\rangle$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \longleftrightarrow \quad |00\rangle - |11\rangle =: |\mathrm{Bell}_3\rangle$$

$$XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \longleftrightarrow \quad |01\rangle - |10\rangle =: |\mathrm{Bell}_4\rangle$$

Quantum Teleportation

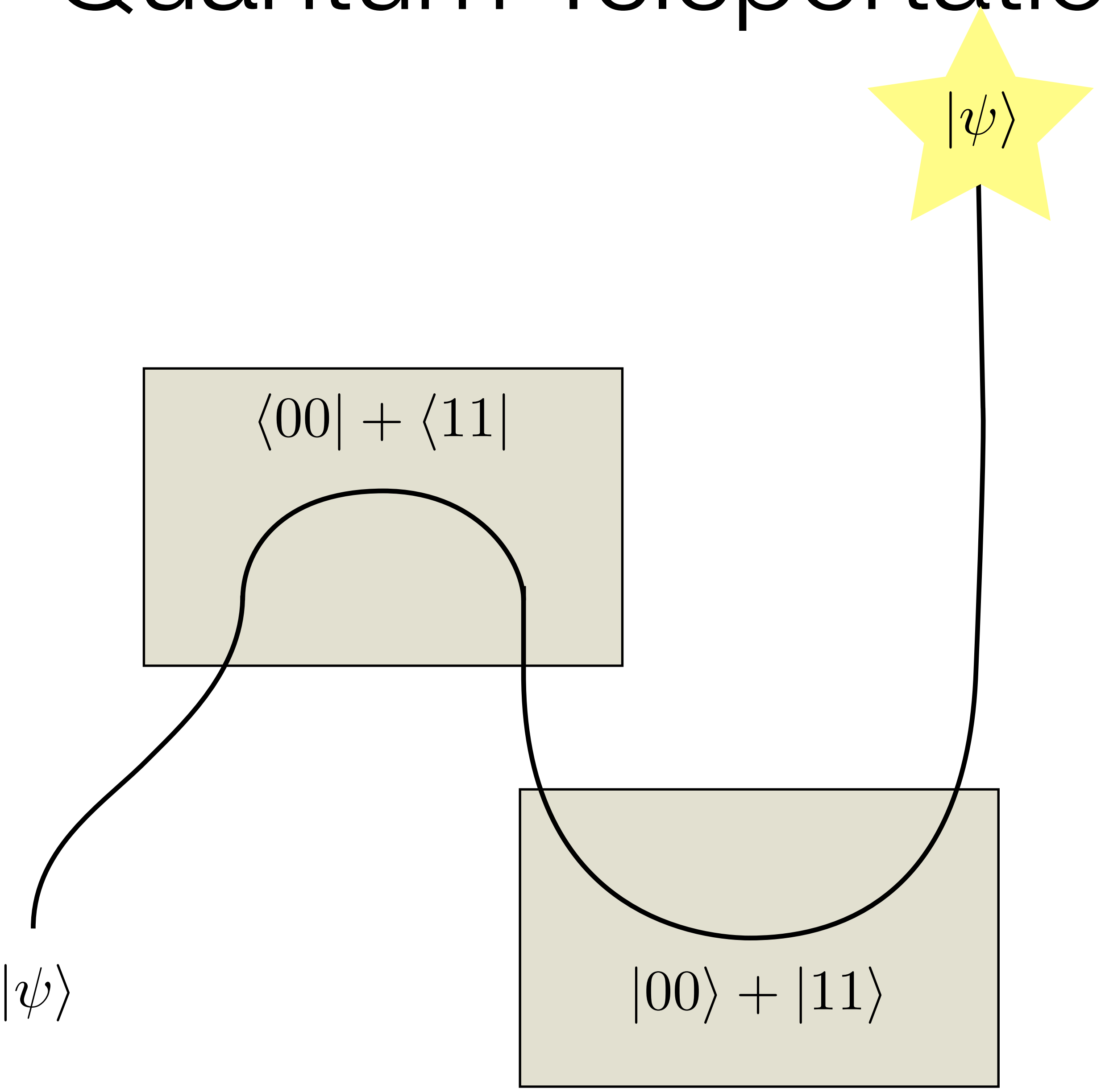
~~Alice~~
Audrey



Bob

Quantum Teleportation

~~Alice~~
Audrey



Bob

Channels via entanglement

Bennett at al:

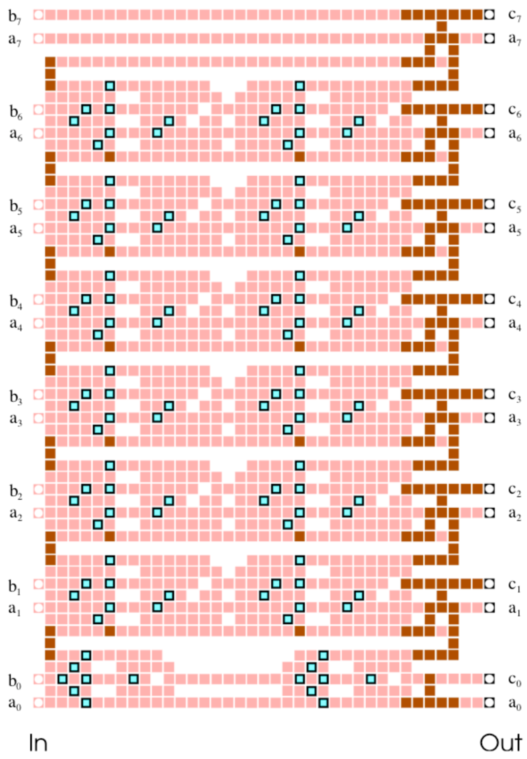
> *"Note that qubits are a directed channel resource, sent in a particular direction from the sender to the receiver; by contrast [entangled pairs] are an undirected resource shared between the sender and receiver."*

Teleporting an unknown quantum state via dual classical and EPR channels, PRL, 1993

This suggests that the type of an entangled pair should be the *linear* type $Q \parr Q$ rather than the usual $Q \to Q$.

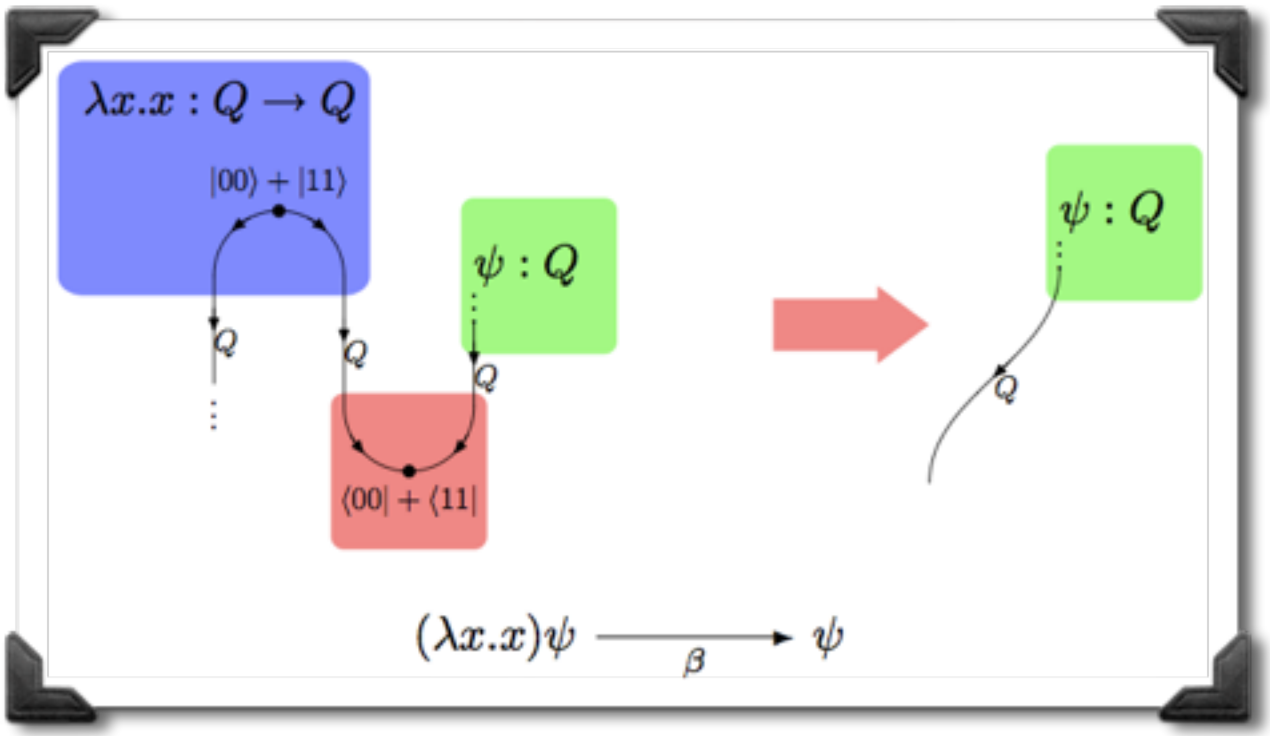
More Entanglement

Entanglement can be used for a lot more than just transmitting information:



MBQC is a universal model of computation which is based on the flow of information through large entangled states.

Propositions as types for QM



A logic based on processes not properties

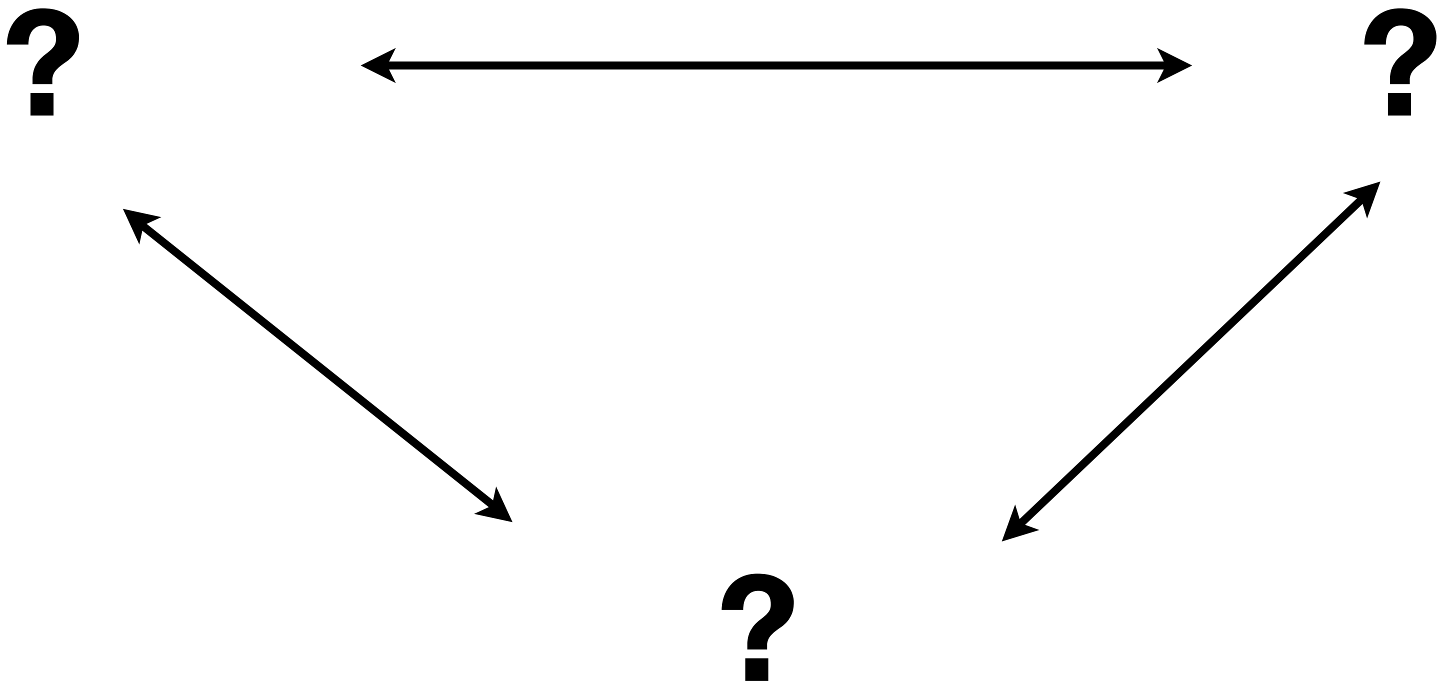
What is the quantum version?

- **We want a logic of “quantum processes”**

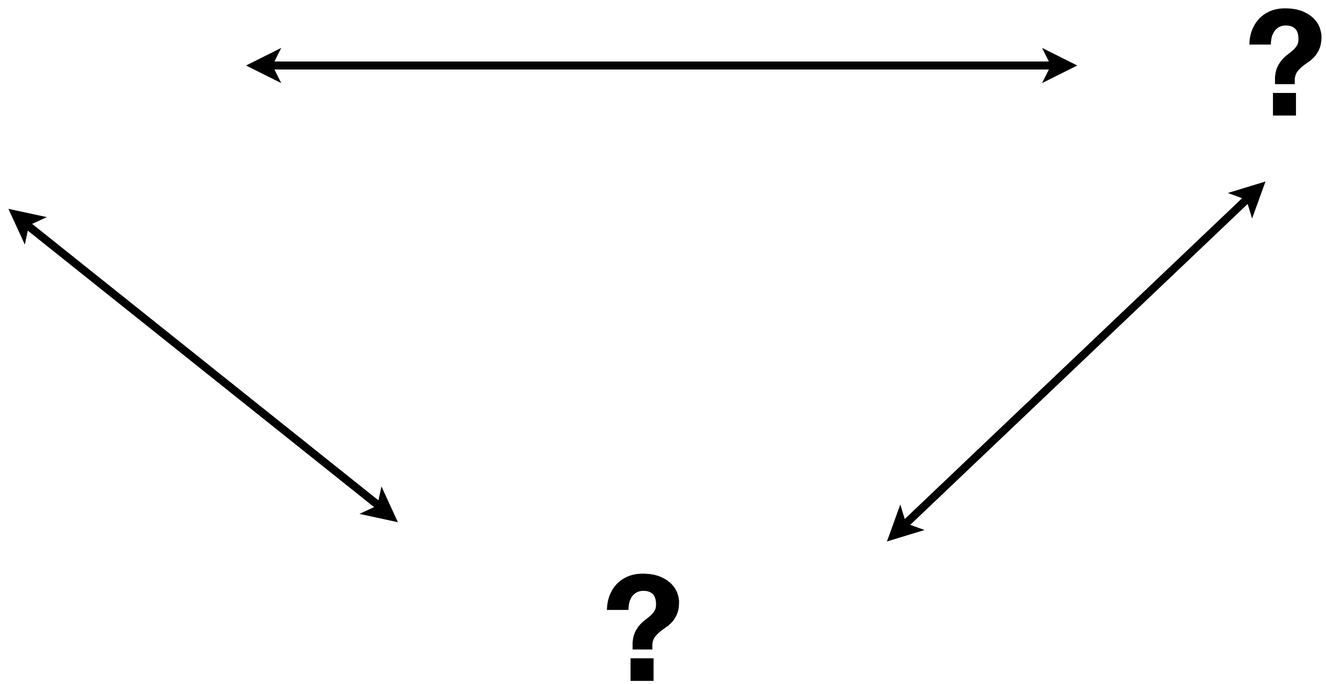
Some hints as to what this should be:

- entangled systems can’t be described by a Cartesian product
- map-state duality suggests we should have a “function-type”
- no-cloning and no-deleting imply that the underlying setting should be *linear*
- ....however we still need some way to represent non-determinism

The quantum version:



The quantum version:



The quantum version:

A categorical semantics of quantum protocols

Samson Abramsky and Bob Coecke

Oxford University Computing Laboratory,
Wolfson Building, Parks Road, Oxford OX1 3QD, UK.
samson.abramsky · bob.coecke@comlab.ox.ac.uk

The quantum version:

†-compact closed categories with †-biproducts

?

A categorical semantics of quantum protocols

Samson Abramsky and Bob Coecke

Oxford University Computing Laboratory,
Wolfson Building, Parks Road, Oxford OX1 3QD, UK.
samson.abramsky · bob.coecke@comlab.ox.ac.uk

$$
\begin{tikzcd}
Q \arrow[r, "\ulcorner 1_Q \urcorner"] \arrow[dddrr, "\Delta"'] & Q \otimes (Q^* \otimes Q) \arrow[r, "\alpha"] & (Q \otimes Q^*) \otimes Q \arrow[d, "\langle \llcorner 1_Q \lrcorner, \llcorner x \lrcorner, \llcorner z \lrcorner, \llcorner xz \lrcorner \rangle \otimes 1_Q"] \\
& & (I \oplus I \oplus I \oplus I) \otimes Q \arrow[d, "\cong"] \\
& & Q \oplus Q \oplus Q \oplus Q \arrow[d, "1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger"] \\
& & Q \oplus Q \oplus Q \oplus Q
\end{tikzcd}
$$

$$
\begin{tikzcd}
Q \arrow[r, "\ulcorner 1_Q \urcorner"] \arrow[ddddrr, "\Delta"'] & Q \otimes (Q^* \otimes Q) \arrow[r, "\alpha"] & (Q \otimes Q^*) \otimes Q \arrow[d, "\langle \llcorner 1_Q \lrcorner, \llcorner x \lrcorner, \llcorner z \lrcorner, \llcorner xz \lrcorner \rangle \otimes 1_Q"] \\
& & (I \oplus I \oplus I \oplus I) \otimes Q \arrow[d, "\cong"] \\
& & Q \oplus Q \oplus Q \oplus Q \arrow[d, "1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger"] \\
& & Q \oplus Q \oplus Q \oplus Q
\end{tikzcd}
$$

Prepare Bell state

$$
\begin{tikzcd}
Q \arrow[r, "\ulcorner 1_Q \urcorner"] \arrow[ddddrr, "\nabla"'] & Q \otimes (Q^* \otimes Q) \arrow[r, "\alpha"] & (Q \otimes Q^*) \otimes Q \arrow[d, "\langle \llcorner 1_Q \lrcorner, \llcorner x \lrcorner, \llcorner z \lrcorner, \llcorner xz \lrcorner \rangle \otimes 1_Q"] \\
 & & (I \oplus I \oplus I \oplus I) \otimes Q \arrow[d, "\cong"] \\
 & & Q \oplus Q \oplus Q \oplus Q \arrow[d, "1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger"] \\
 & & Q \oplus Q \oplus Q \oplus Q
\end{tikzcd}
$$

Relocalise

Bell basis measurement

$$
\begin{tikzcd}
Q \arrow[r, "\ulcorner 1_Q \urcorner"] \arrow[ddddrr, "\Delta"'] & Q \otimes (Q^* \otimes Q) \arrow[r, "\alpha"] & (Q \otimes Q^*) \otimes Q \arrow[d, "\langle \llcorner 1_Q \lrcorner, \llcorner x \lrcorner, \llcorner z \lrcorner, \llcorner xz \lrcorner \rangle \otimes 1_Q"] \\
 & & (I \oplus I \oplus I \oplus I) \otimes Q \arrow[d, "\cong"] \\
 & & Q \oplus Q \oplus Q \oplus Q \arrow[d, "1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger"] \\
 & & Q \oplus Q \oplus Q \oplus Q \\
 & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
Q \arrow[r, "\ulcorner 1_Q \urcorner"] \arrow[ddddrr] & Q \otimes (Q^* \otimes Q) \arrow[r, "\alpha"] & (Q \otimes Q^*) \otimes Q \arrow[d, "\langle \llcorner 1_Q \lrcorner, \llcorner x \lrcorner, \llcorner z \lrcorner, \llcorner xz \lrcorner \rangle \otimes 1_Q"] \\
& & (I \oplus I \oplus I \oplus I) \otimes Q \arrow[d, "\cong"] \\
& & Q \oplus Q \oplus Q \oplus Q \arrow[d, "1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger"] \\
& & Q \oplus Q \oplus Q \oplus Q \\
& &
\end{tikzcd}
$$

Classical communication

$$
\begin{tikzcd}
Q \arrow[r, "\ulcorner 1_Q \urcorner"] \arrow[ddddrr, "\Delta"'] & Q \otimes (Q^* \otimes Q) \arrow[r, "\alpha"] & (Q \otimes Q^*) \otimes Q \arrow[d, "\langle \llcorner 1_Q \lrcorner, \llcorner x \lrcorner, \llcorner z \lrcorner, \llcorner xz \lrcorner \rangle \otimes 1_Q"] \\
& & (I \oplus I \oplus I \oplus I) \otimes Q \arrow[d, "\cong"] \\
& & Q \oplus Q \oplus Q \oplus Q \arrow[d, "1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger"] \\
& & Q \oplus Q \oplus Q \oplus Q
\end{tikzcd}
$$

Unitary correction

$$
\begin{tikzcd}
Q \arrow[r, "\ulcorner 1_Q \urcorner"] \arrow[ddddrr, "\nabla"'] & Q \otimes (Q^* \otimes Q) \arrow[r, "\alpha"] & (Q \otimes Q^*) \otimes Q \arrow[d, "\langle \llcorner 1_Q \lrcorner, \llcorner x \lrcorner, \llcorner z \lrcorner, \llcorner xz \lrcorner \rangle \otimes 1_Q"] \\
 & & (I \oplus I \oplus I \oplus I) \otimes Q \arrow[d, "\cong"] \\
 & & Q \oplus Q \oplus Q \oplus Q \arrow[d, "1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger"] \\
 & & Q \oplus Q \oplus Q \oplus Q
\end{tikzcd}
$$

Specification

An invitation:

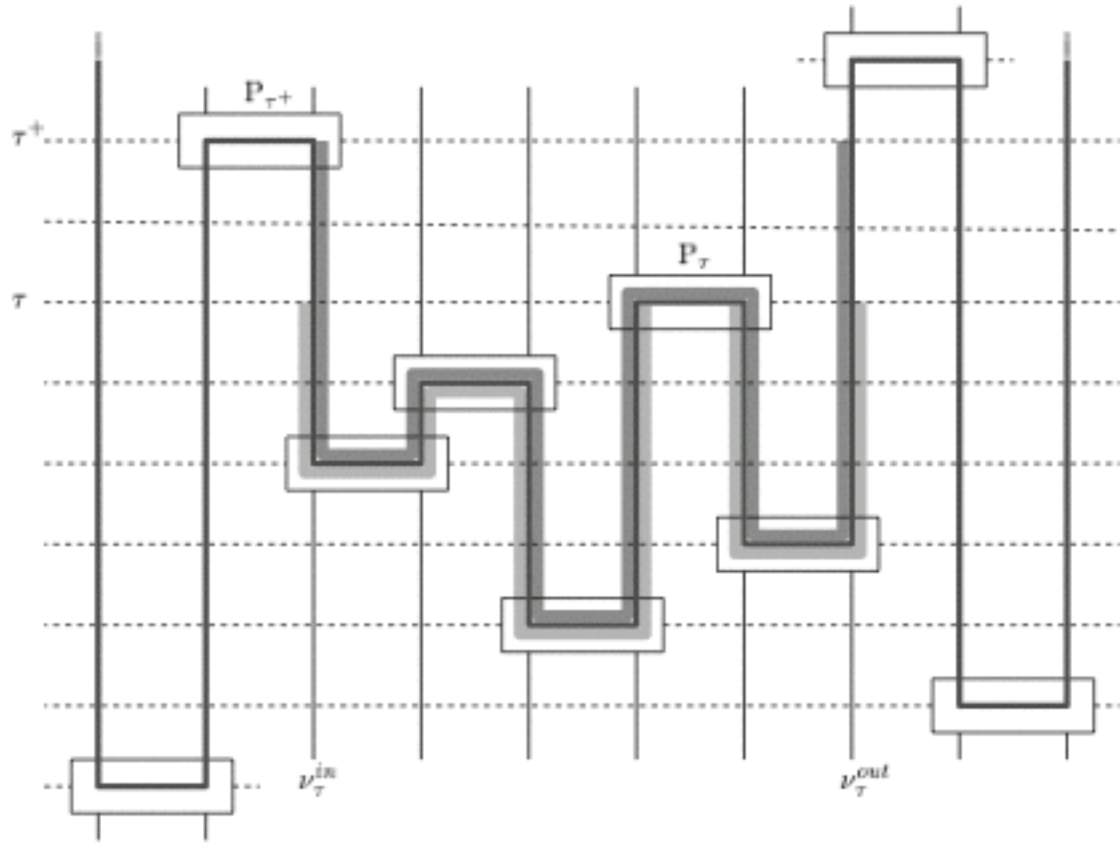
Programming Research Group

THE LOGIC OF ENTANGLEMENT.
AN INVITATION.

(VERSION 0.9999)

Bob Coecke

PRG-RR-03-12



An invitation:

Programming Research Group

THE LOGIC OF ENTANGLEMENT.

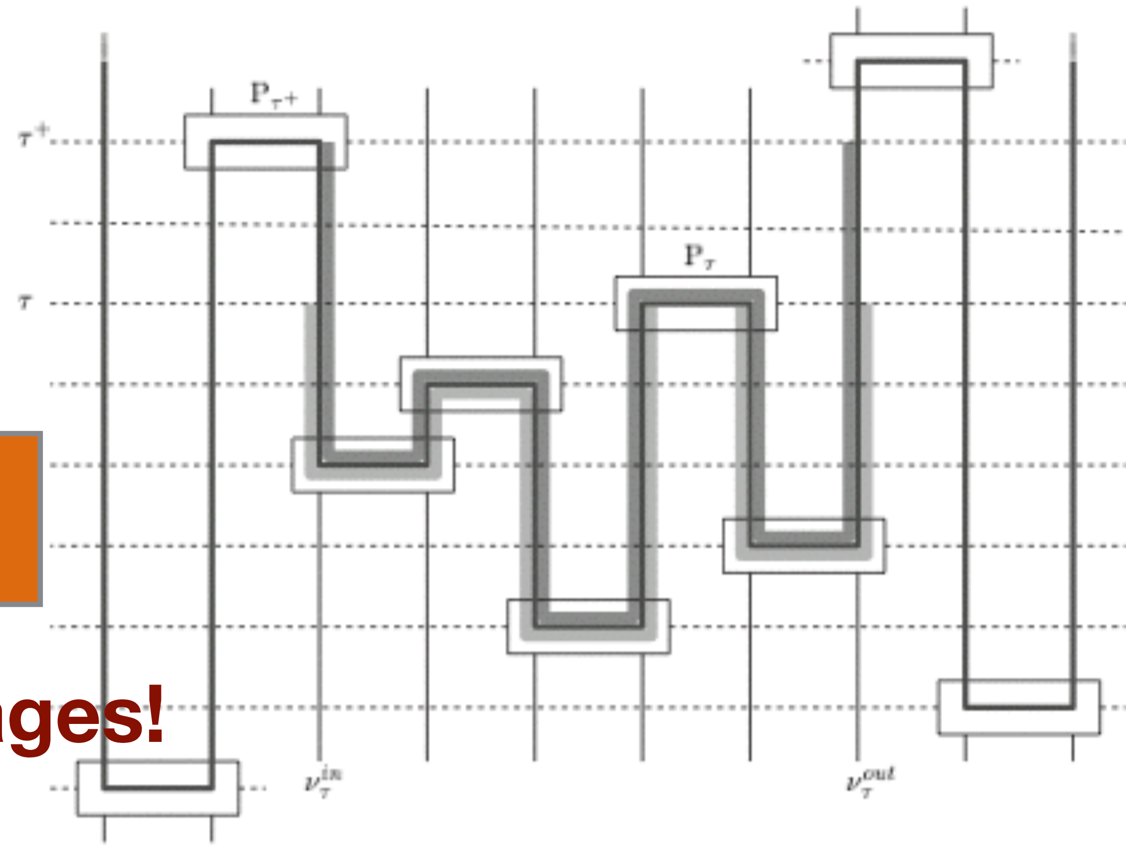
AN INVITATION.

(VERSION 0.9999)

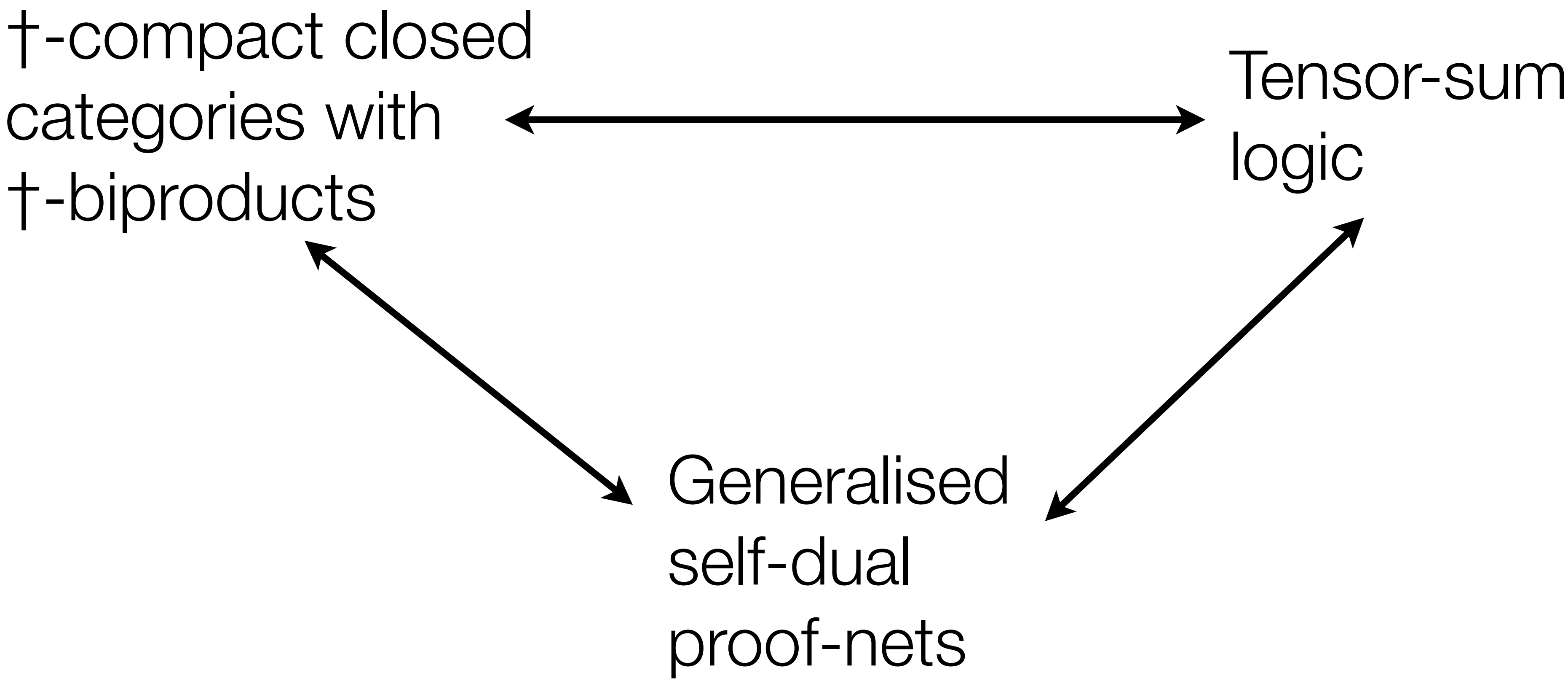
Bob Coecke

PRG-RR-03-12

161 pages!



The quantum version:



The connectives

Classical logic

$$\neg\neg A = A$$
$$\neg(A \wedge B) = \neg A \vee \neg B$$
$$\neg(A \vee B) = \neg A \wedge \neg B$$

	conjunction	disjunction
	$\bigwedge$	$\bigvee$

The connectives

Linear logic

(MALL)

$$A^{\perp\perp} = A$$
$$(A \otimes B)^{\perp} = A^{\perp} \parr B^{\perp}$$
$$(A \parr B)^{\perp} = A^{\perp} \otimes B^{\perp}$$
$$(A \& B)^{\perp} = A^{\perp} \oplus B^{\perp}$$
$$(A \oplus B)^{\perp} = A^{\perp} \& B^{\perp}$$

	conjunction	disjunction
multiplicative	$\otimes$	$\parr$
additive	$\&$	$\oplus$

The connectives

Tensor-sum "logic"

$$A^{**} = A$$
$$(A \otimes B)^* = A^* \otimes B^*$$
$$(A \oplus B)^* = A^* \oplus B^*$$

multiplicative	$\otimes$
additive	$\oplus$

A professional opinion:

J.-Y. Girard, *The Blind Spot*, 2006

A professional opinion:

"One must leave it in the department of atrocities..."

J.-Y. Girard, *The Blind Spot*, 2006

"Here one witnesses a frank divorce between the logical viewpoint and the category-theoretic viewpoint, for which $\otimes = \parr$ is not absurd. Thus, in algebra, the tensor is often equal to the cotensor, for instance in finite dimensional vector spaces ... This remark illustrates the gap separating logic and categories, by the way quite legitimate activities, that one should not try to crush one upon another."

Tensor-Sum Logic

Tensor-sum logic is a Gentzen system, designed to capture the structure of a certain free category on some generators $\mathcal{A}$.

- Essentially it is MALL with self-dual connectives
- Every proof has an interpretation as an arrow of $F\mathcal{A}$
- Every arrow of $F\mathcal{A}$ has a corresponding proof
- The system is cut-eliminating, and the cut-elimination procedure is sound wrt the interpretation.

Tensor-Sum Logic

Tensor-sum logic is a Gentzen system, designed to capture the structure of a certain free category on some generators $\mathcal{A}$.

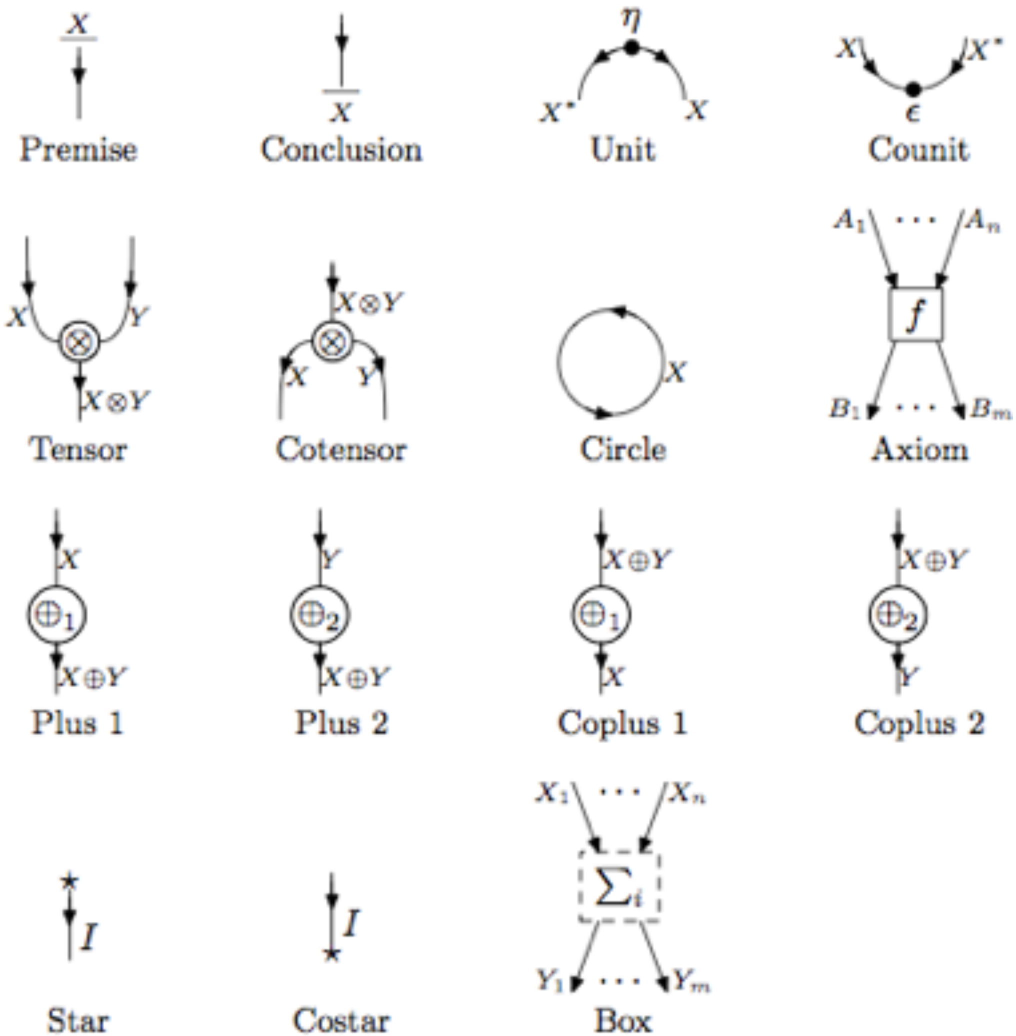
- Essentially it is MALL with self-dual connectives
- Every proof has an interpretation as an arrow of $F\mathcal{A}$
- Every arrow of $F\mathcal{A}$ has a corresponding proof
- The system is cut-eliminating, and the cut-elimination procedure is sound wrt the interpretation.

It has some *oddities* as a logical system:

- Every entailment $A \vdash B$ is derivable with a *zero proof*
- Self-duality allows the formation of *self-cuts*
  - the empty sequent is derivable in many *inequivalent ways*

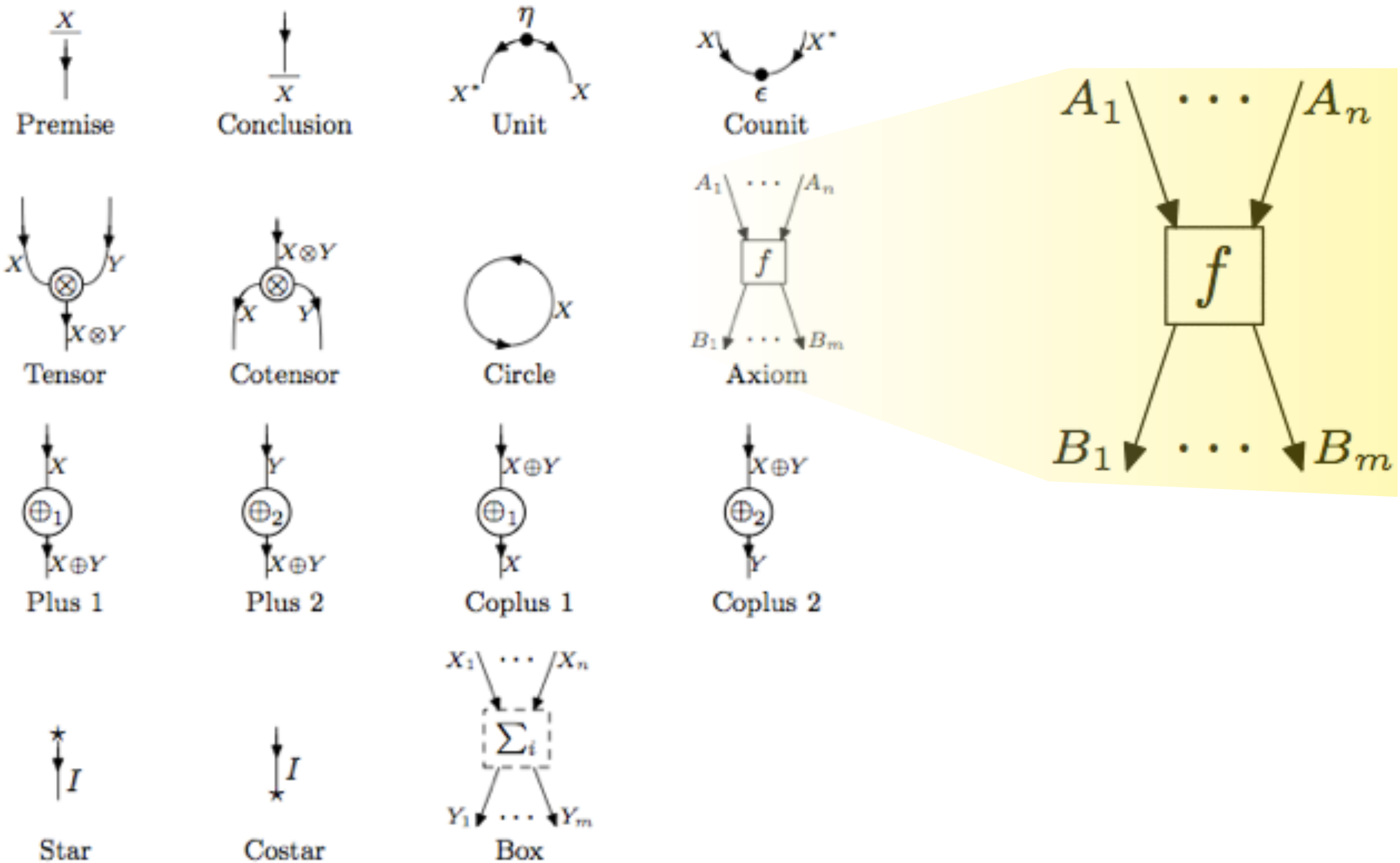
Proof-nets for tensor and sum

Define a system of proof-nets with non-logical axioms:



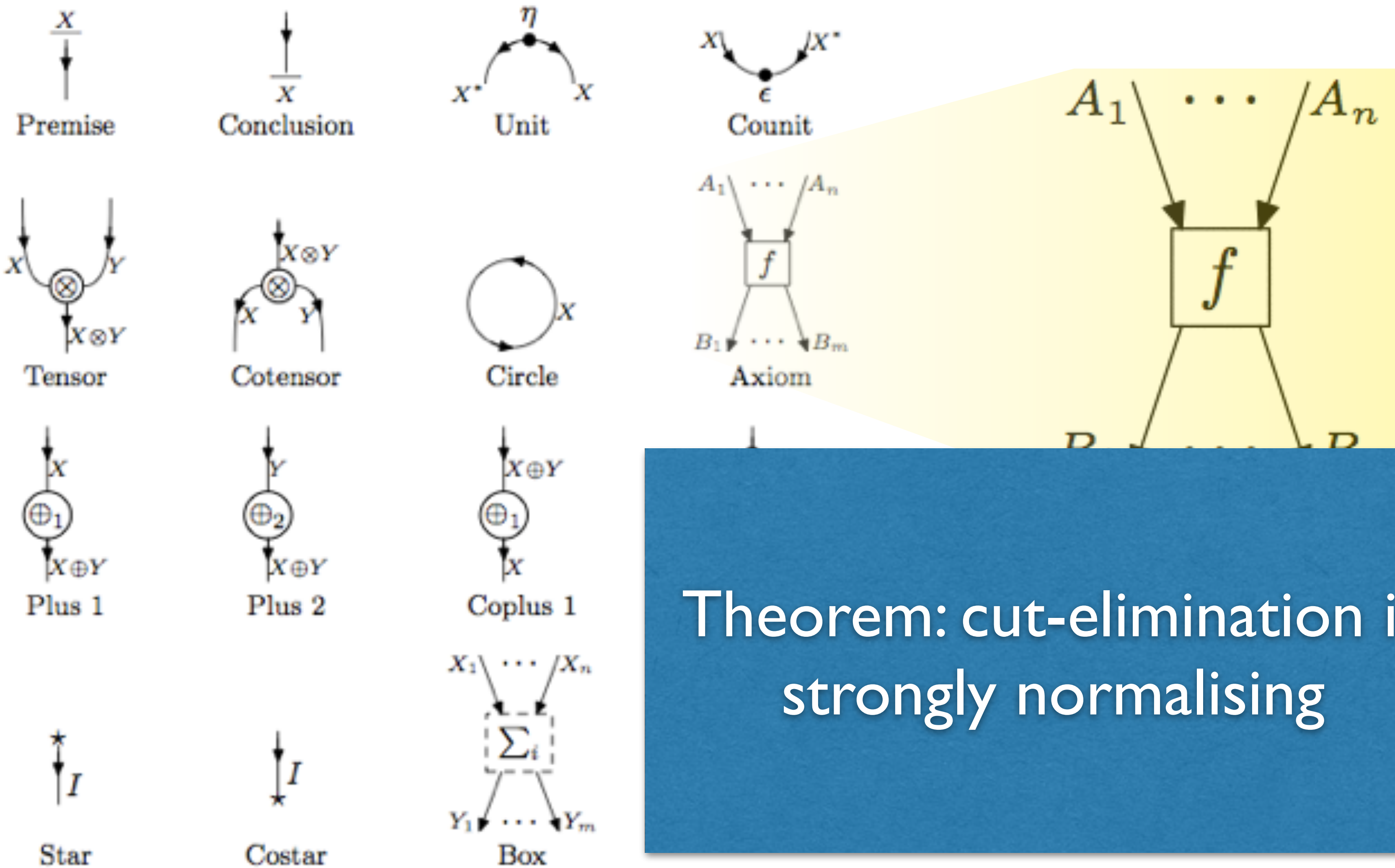
Proof-nets for tensor and sum

Define a system of proof-nets with non-logical axioms:



Proof-nets for tensor and sum

Define a system of proof-nets with non-logical axioms:



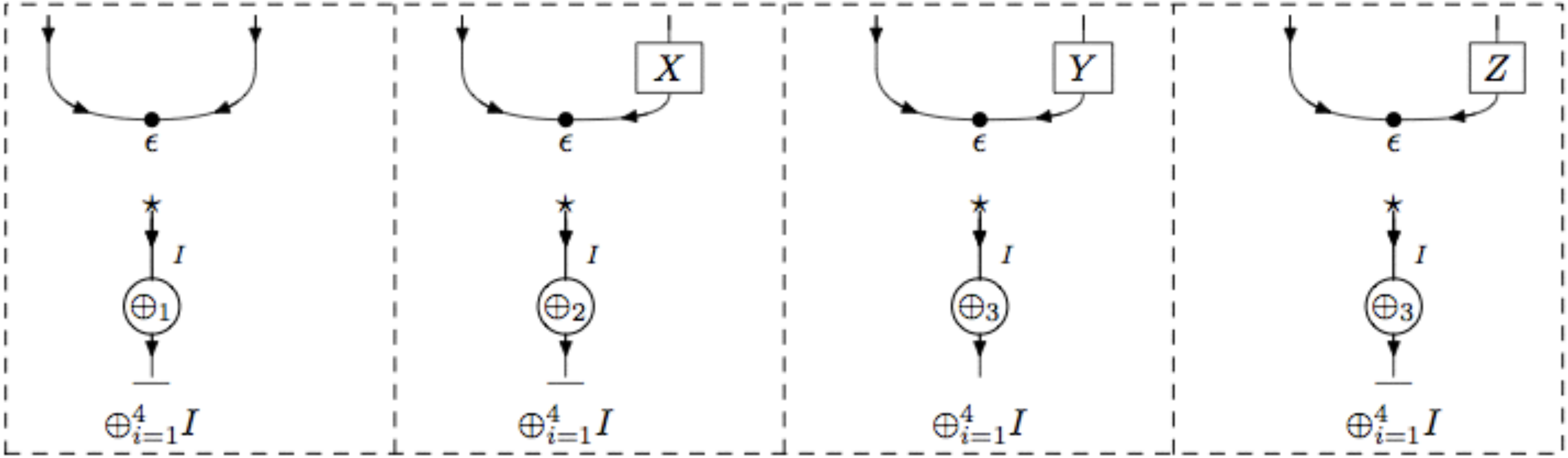
Theorem: cut-elimination is strongly normalising

Example: teleportation

The shared Bell state and the input qubit:

Example: teleportation

The Bell basis measurement

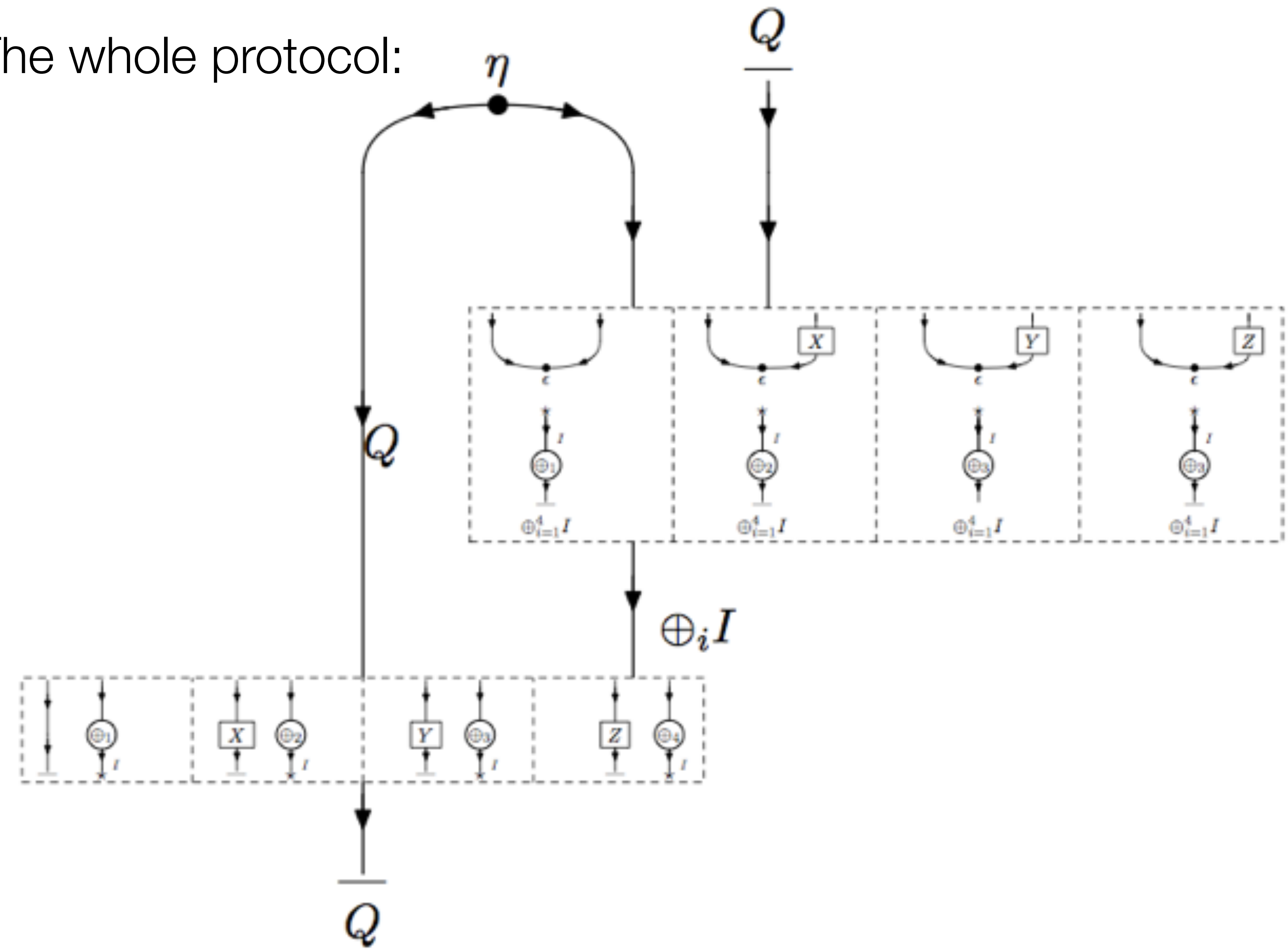


Example: teleportation

The classically controlled corrections:

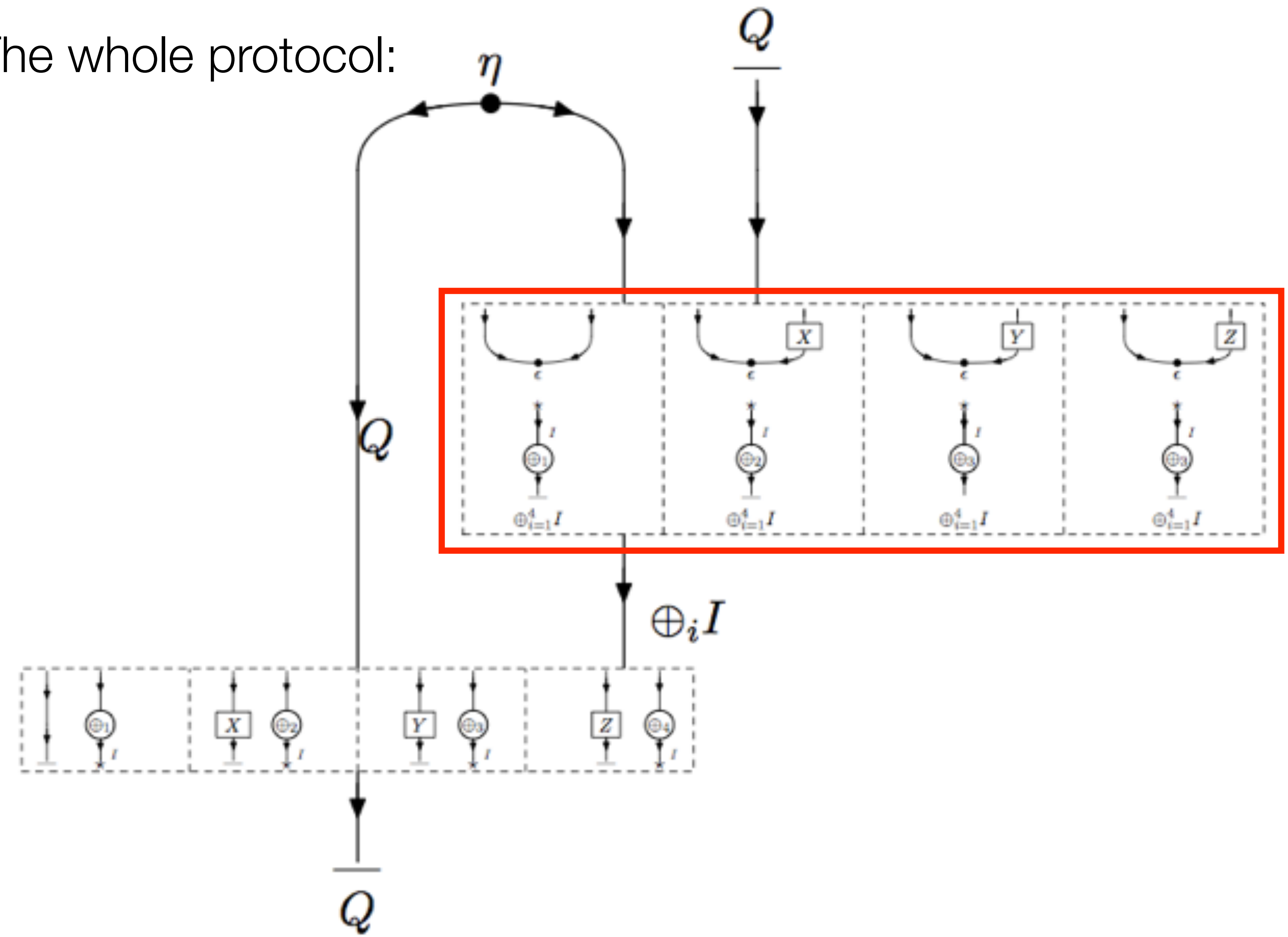
Example: teleportation

The whole protocol:

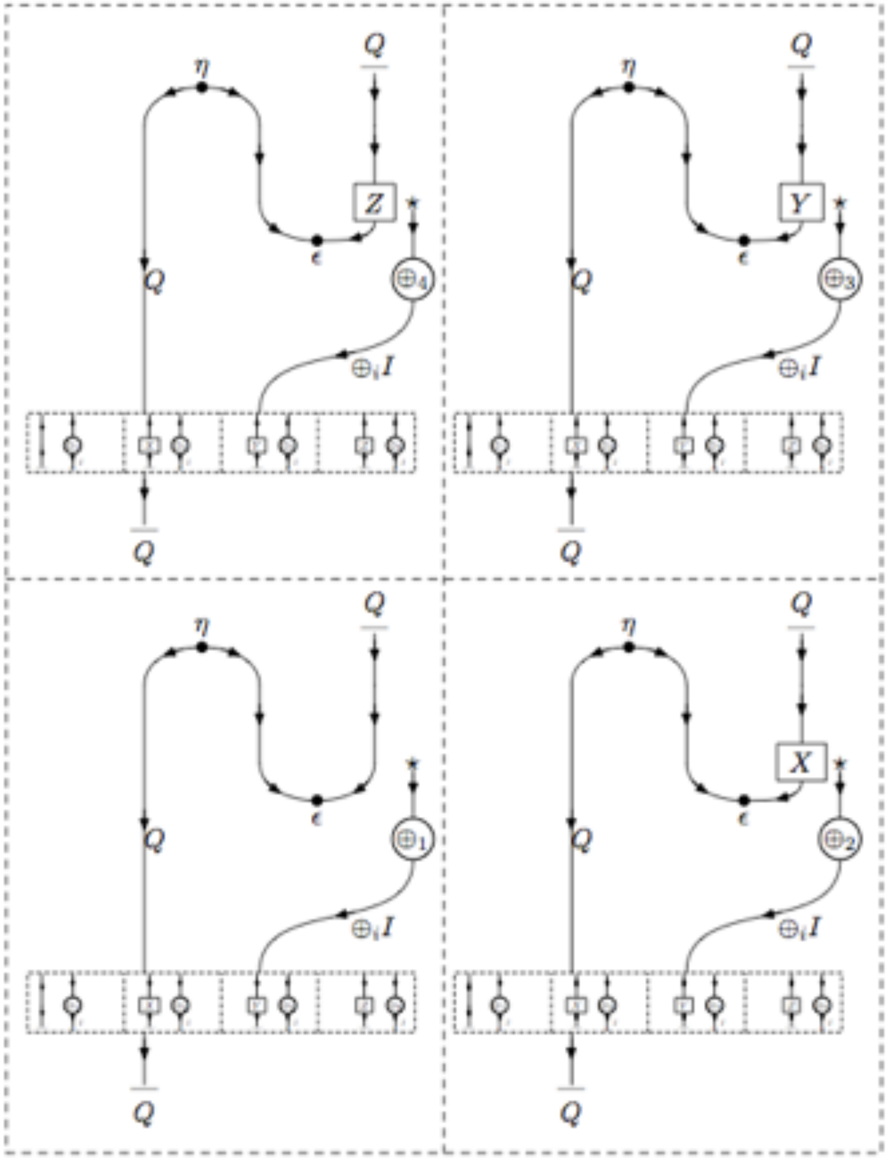


Example: teleportation

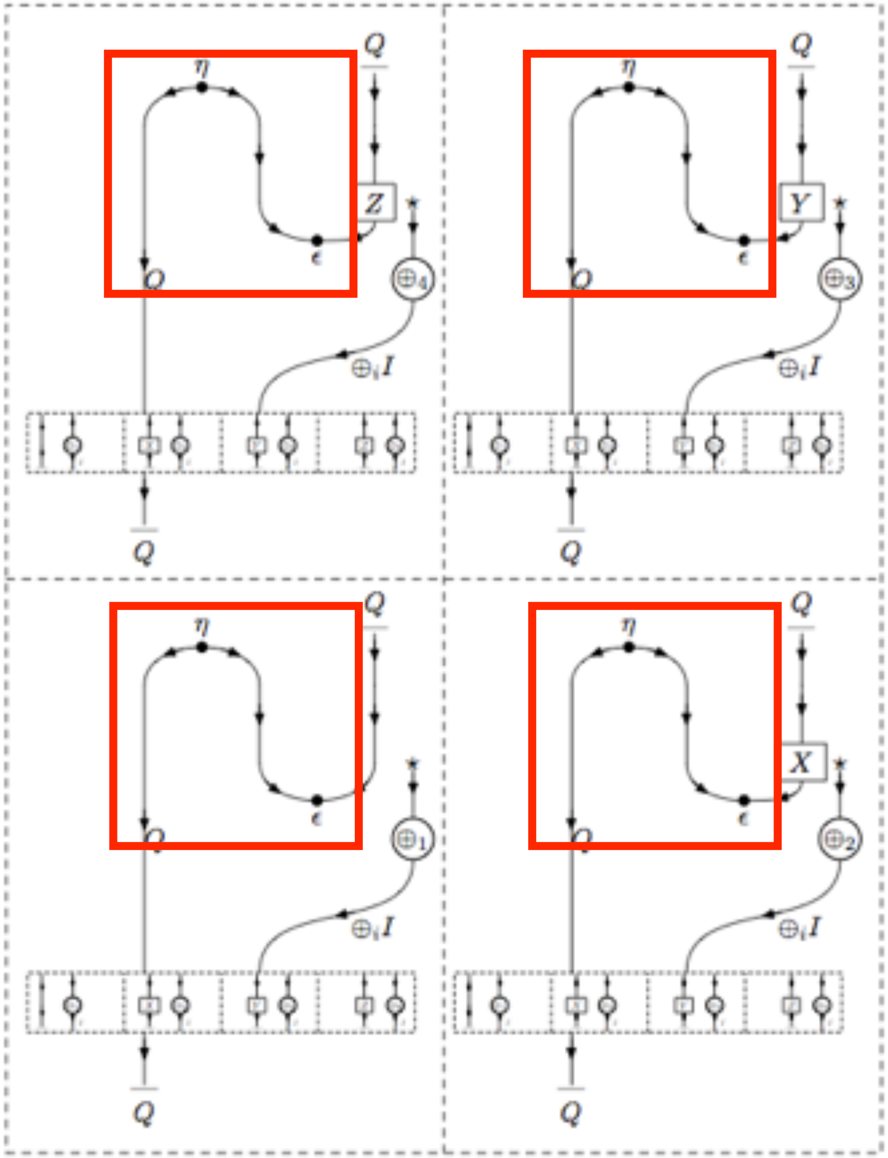
The whole protocol:



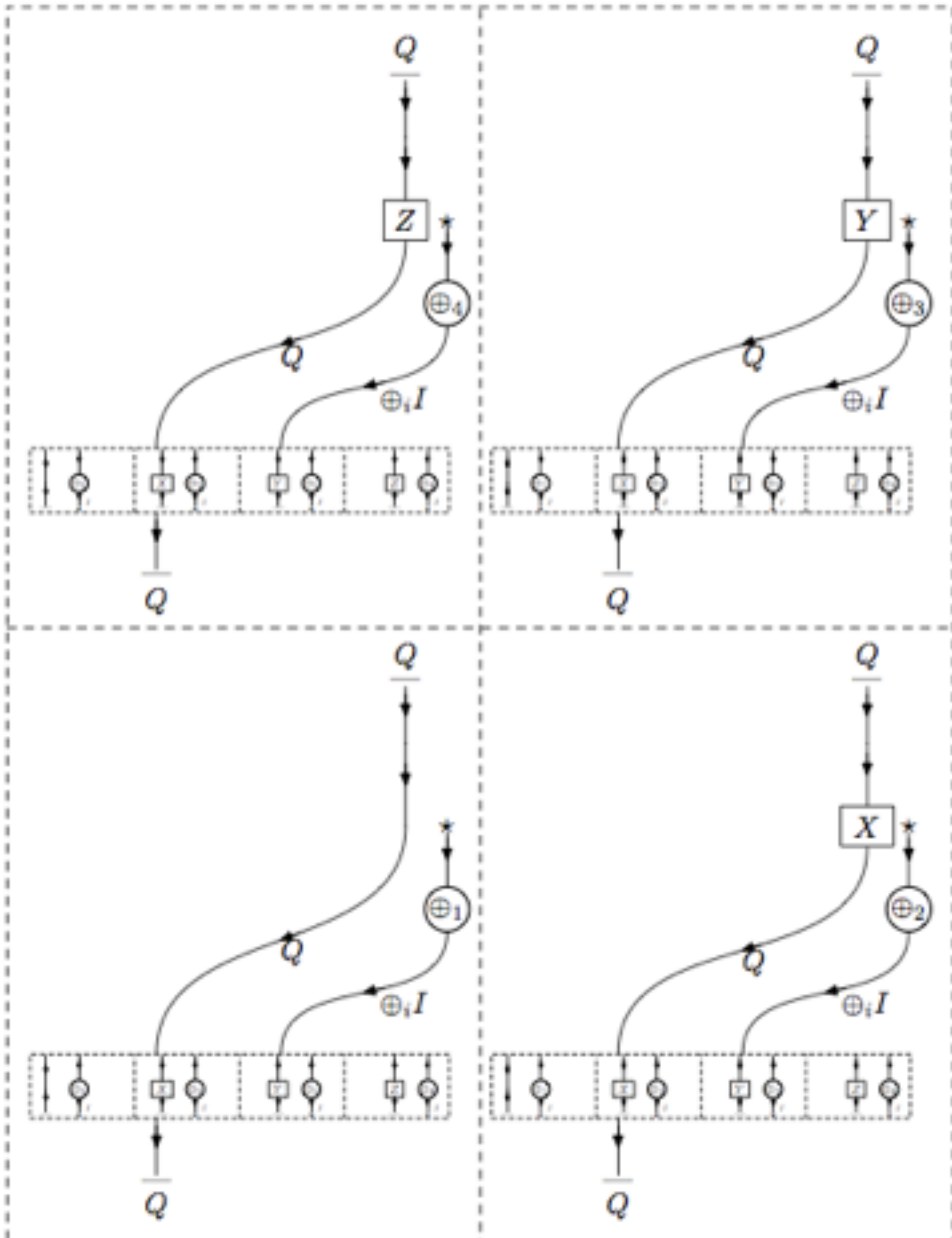
Example: teleportation



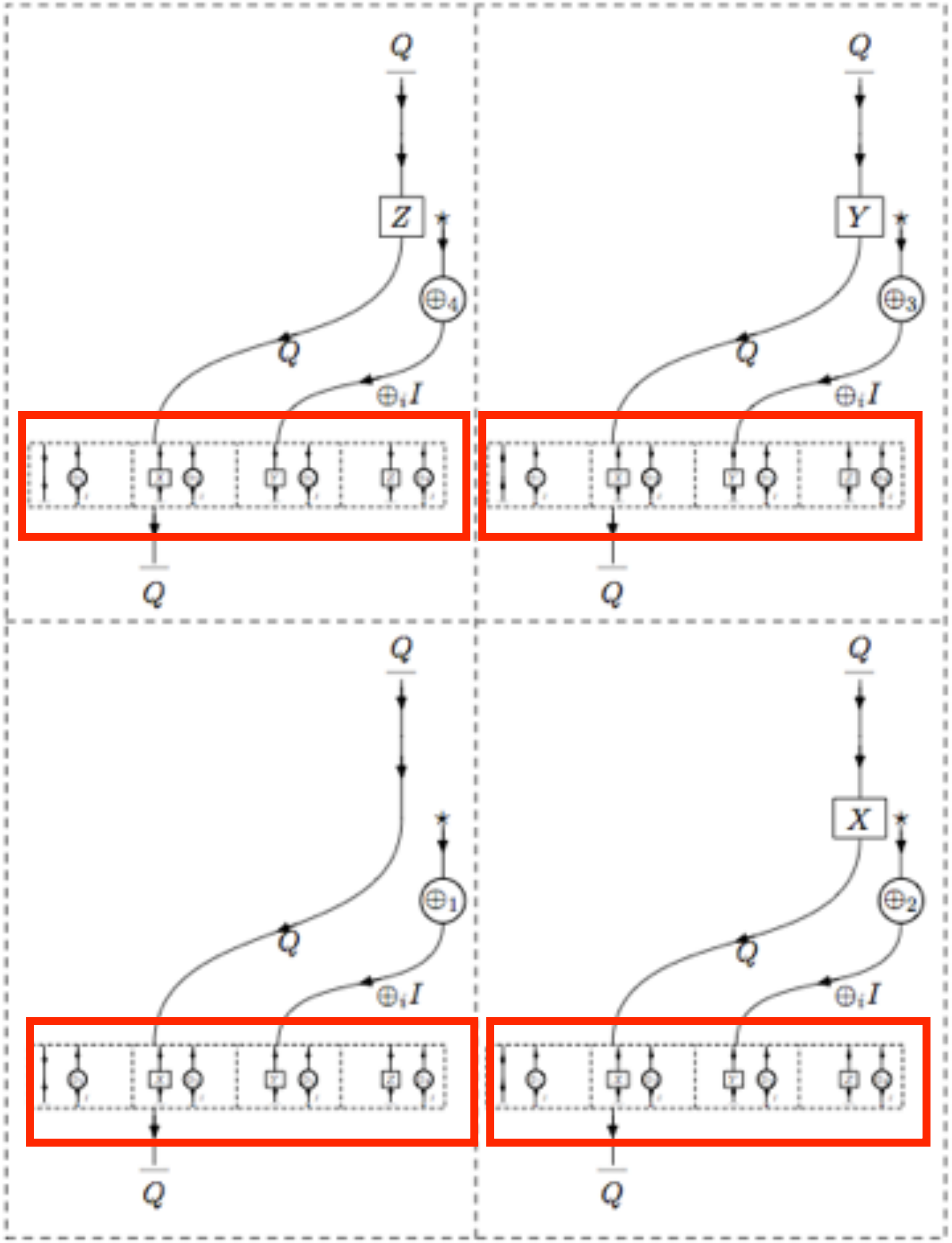
Example: teleportation



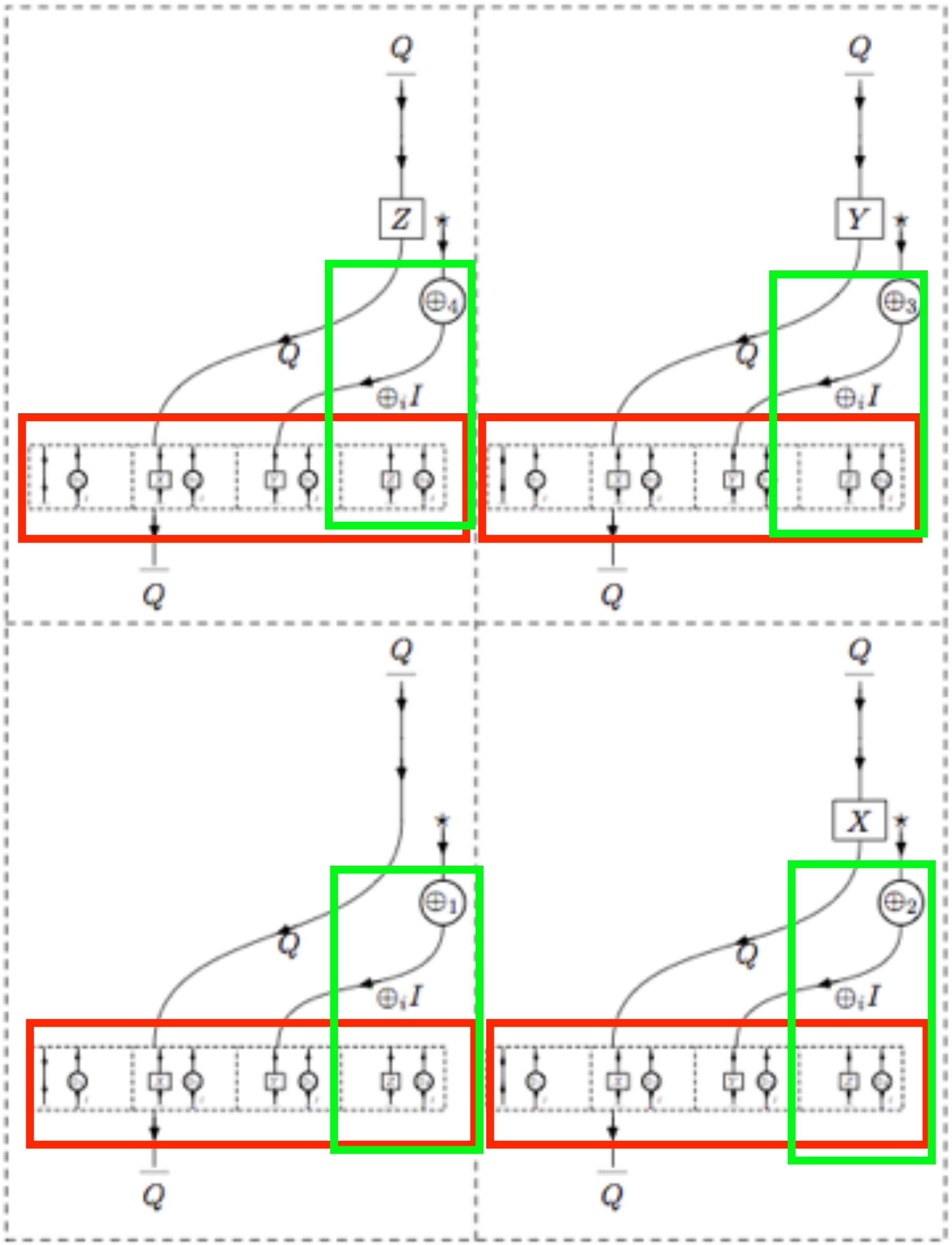
Example: teleportation



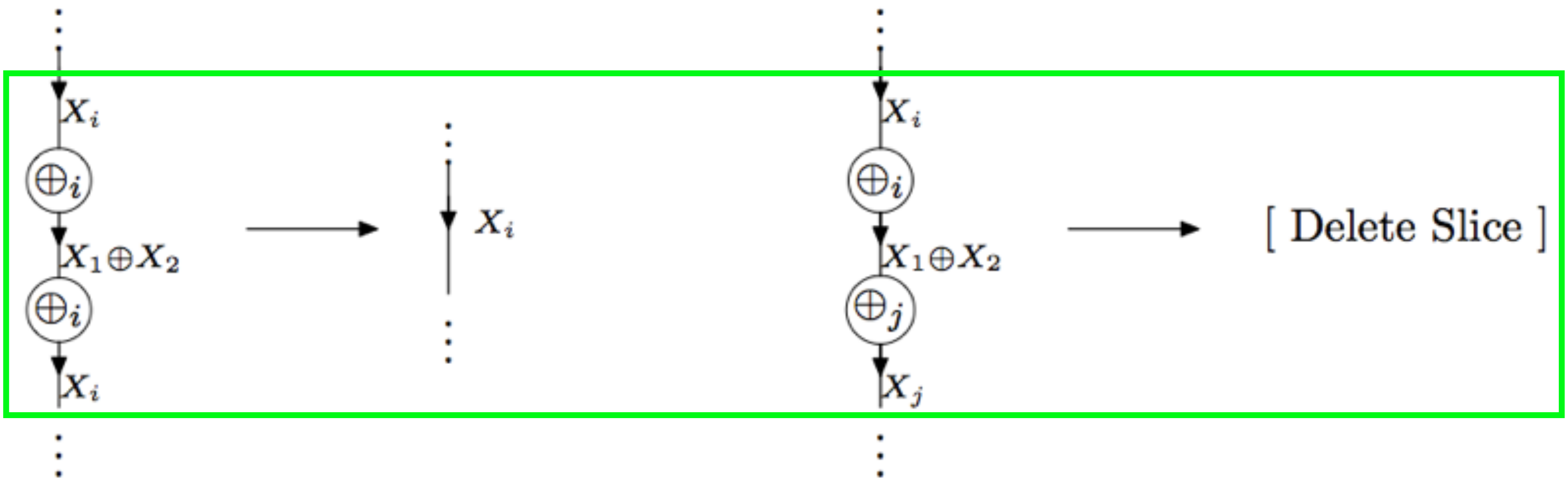
Example: teleportation



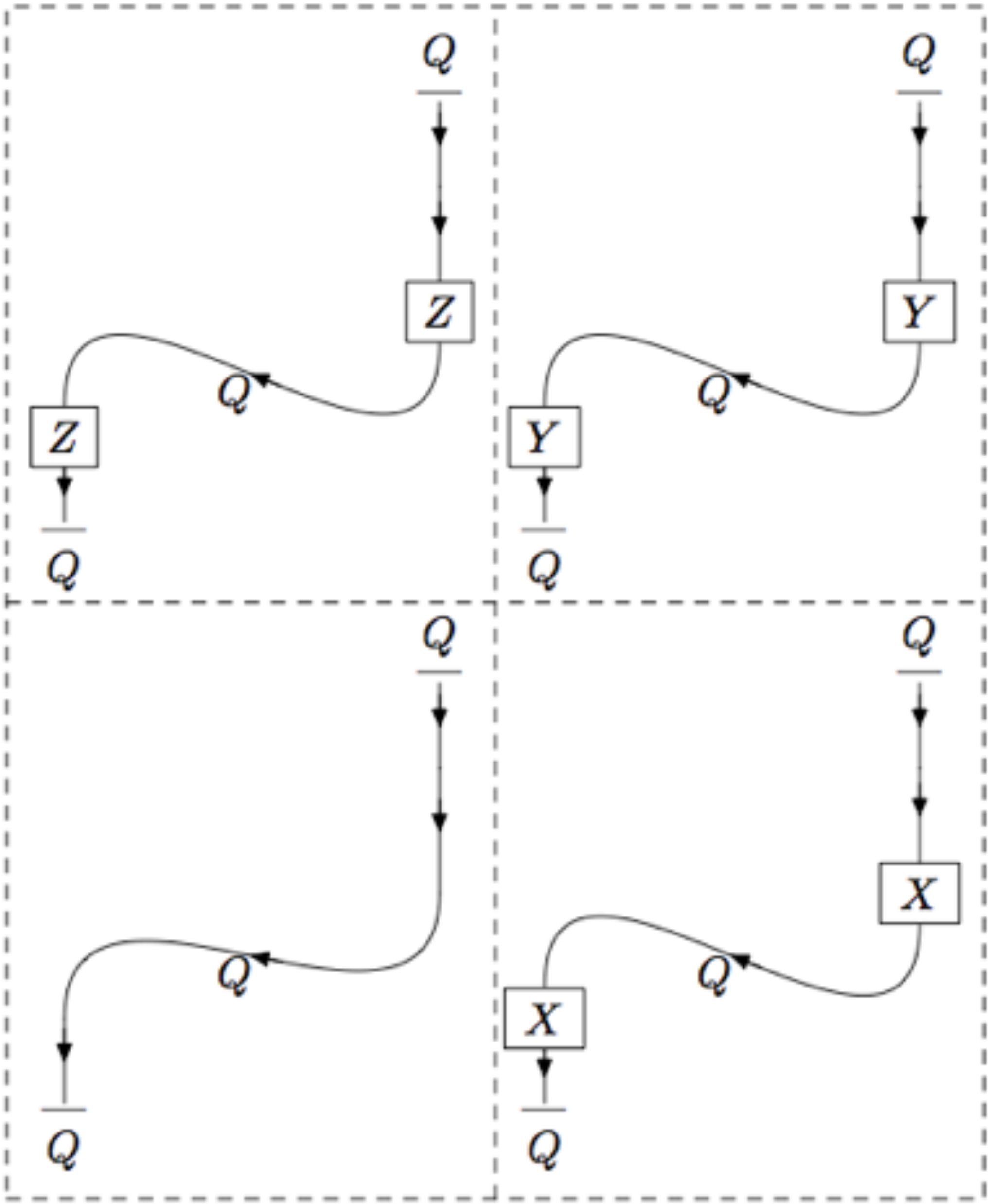
Example: teleportation



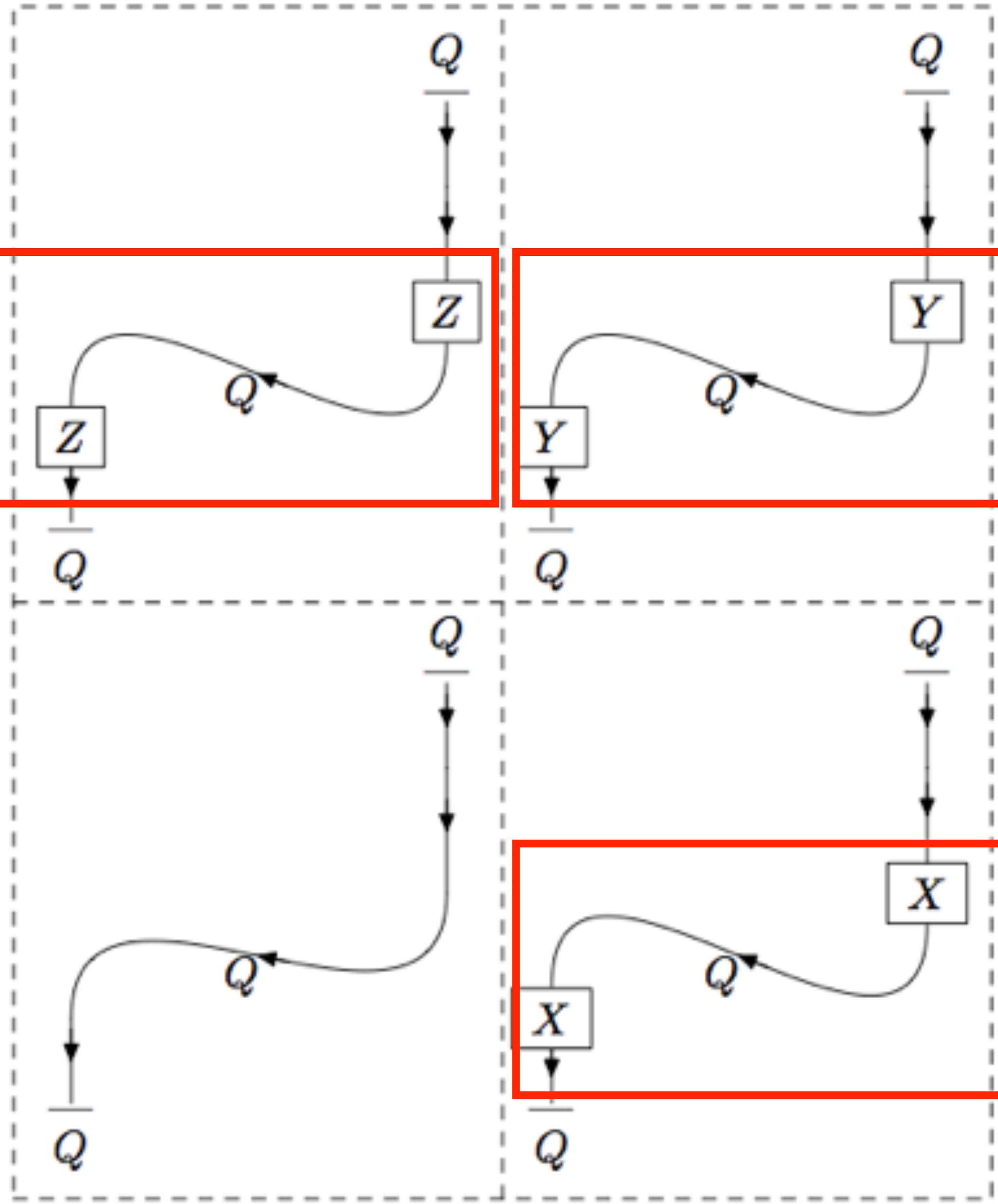
Example: teleportation



Example: teleportation



Example: teleportation

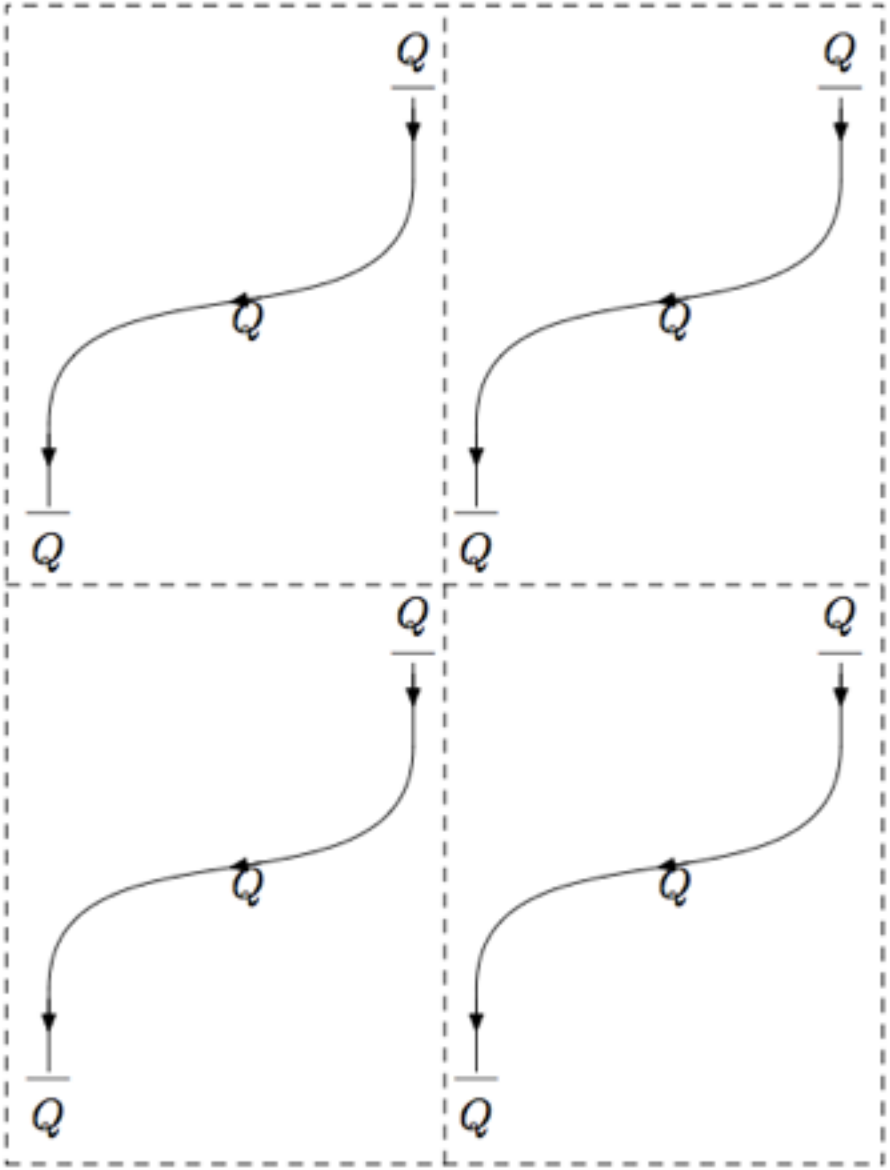


$Z^2 = 1_Q$

$Y^2 = 1_Q$

$X^2 = 1_Q$

Example: teleportation



Full completeness

Theorem: Let $\mathbf{P}$ be a compact symmetric polycategory. There is an equivalence of categories between $\mathbf{Circ}(\mathbf{P})$ and $\mathbf{PN}(\mathbf{P})$.

The biproduct

We used the biproduct to encode the branching nature of quantum processes.

- The diagonal map shows the possibility of different choices:

$$Q \xrightarrow{\Delta} Q \oplus Q$$

- But what about the codiagonal?

$$Q \oplus Q \xrightarrow{\nabla} Q$$

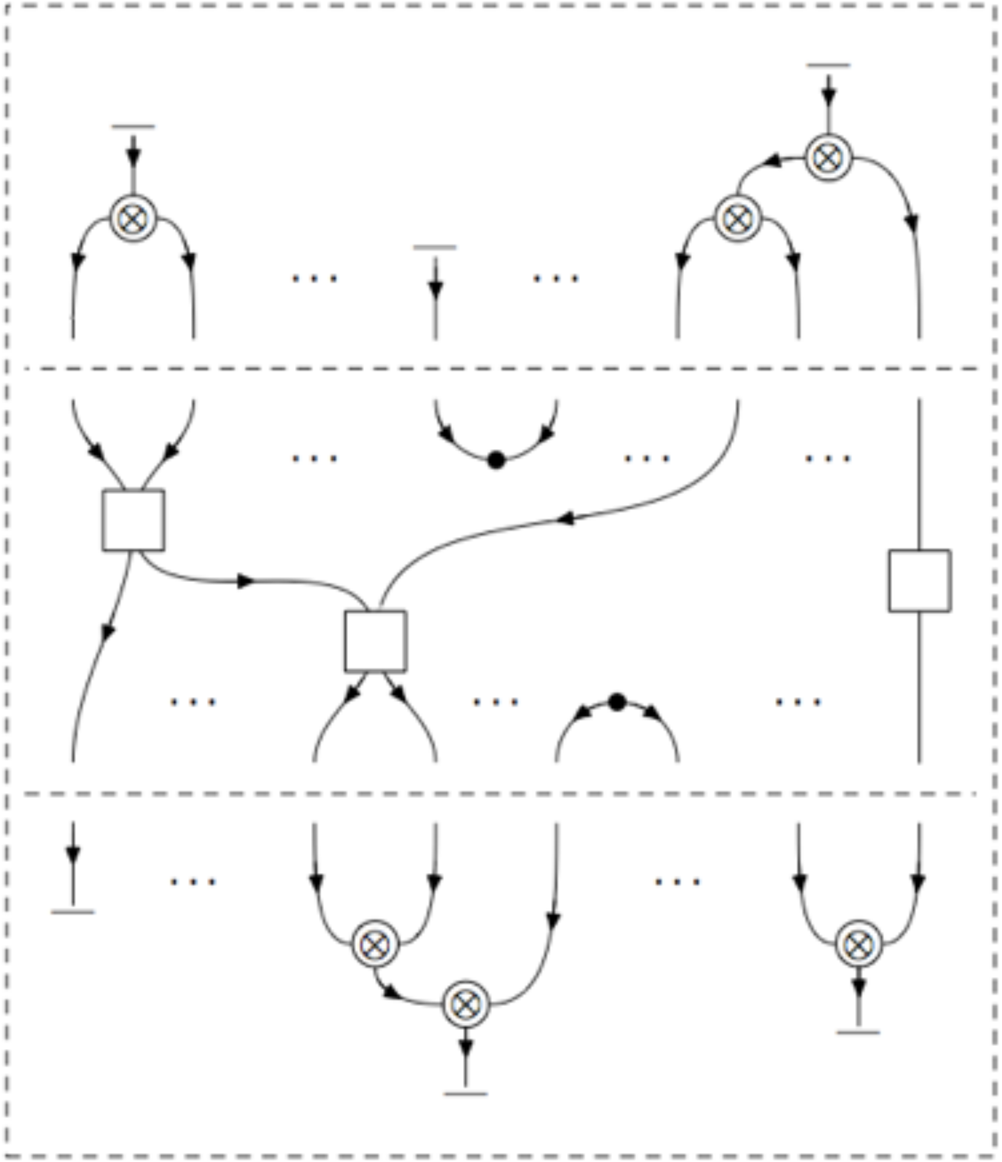
- Semantically this corresponds to superposition rather than probabilistic mixing --- the wrong interpretation
- To properly address the issue of probabilities in QM we use Selinger's CPM construction

Normal form theorem

Pure logic, determined by premise

A unique A-labelled circuit

Pure logic determined by conclusion



Types for entanglement?

Can we regain the the separation between $\otimes$ and $\parr$ to talk about entanglement?

- Entangled states do not form a subspace
- Do double gluing on $\mathbf{fdHilb}$
  - $\otimes$ gives product states
  - $\parr$ gives **all** states
- Hence $\otimes$ is a subtype of $\parr$

How many types anyway?

Defn: A state S is said to be *SLOCC reachable* from state S' if there is a sequence of stochastic local operations and classical communications producing S from S'

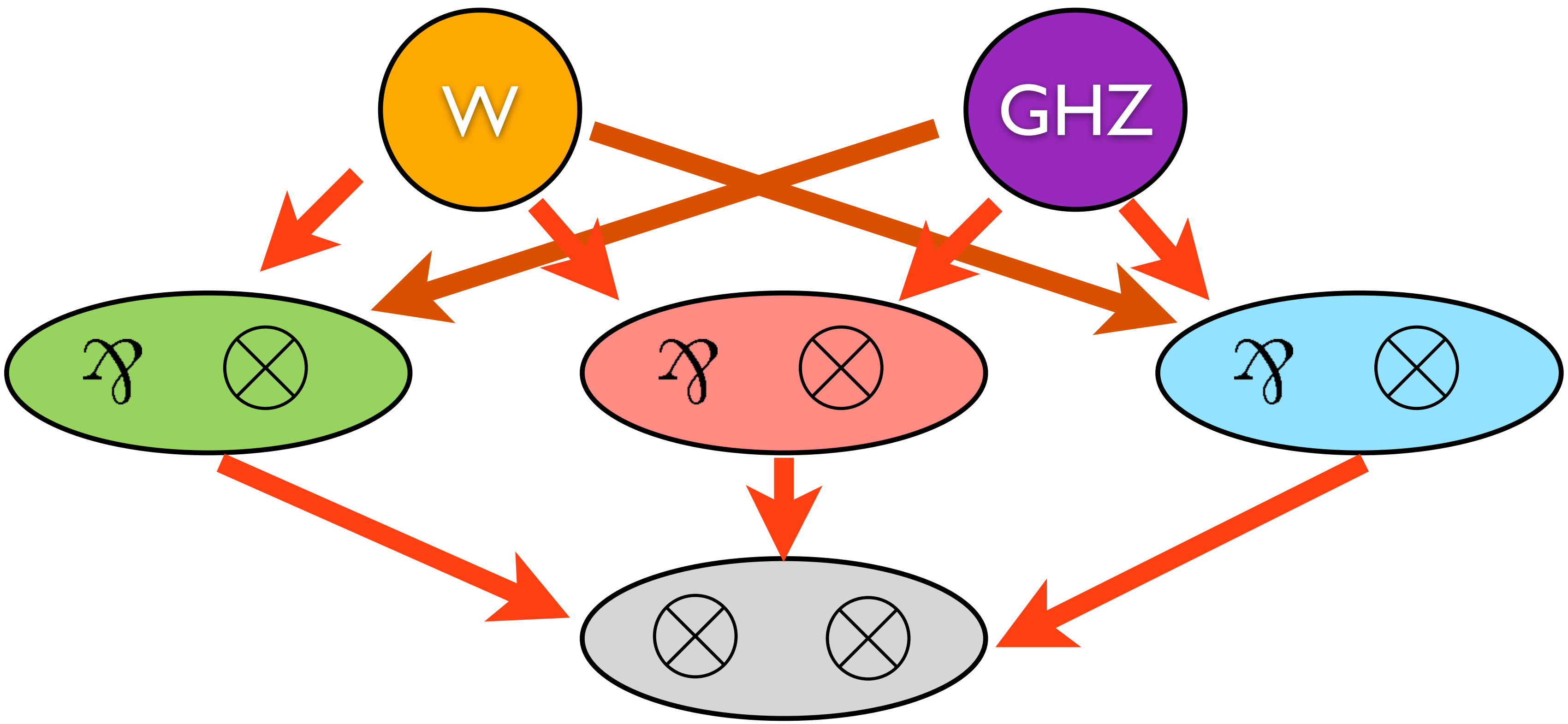
Defn: If S and S' are mutually SLOCC reachable then they are *SLOCC equivalent*.

How many types anyway?

Prop: For 2-qubit states there are 2 SLOCC classes:

How many types anyway?

Prop: For 3-qubit states there are 6 SLOCC classes:



How many types anyway?

Prop: For 4-qubit states there are **uncountably many** SLOCC classes

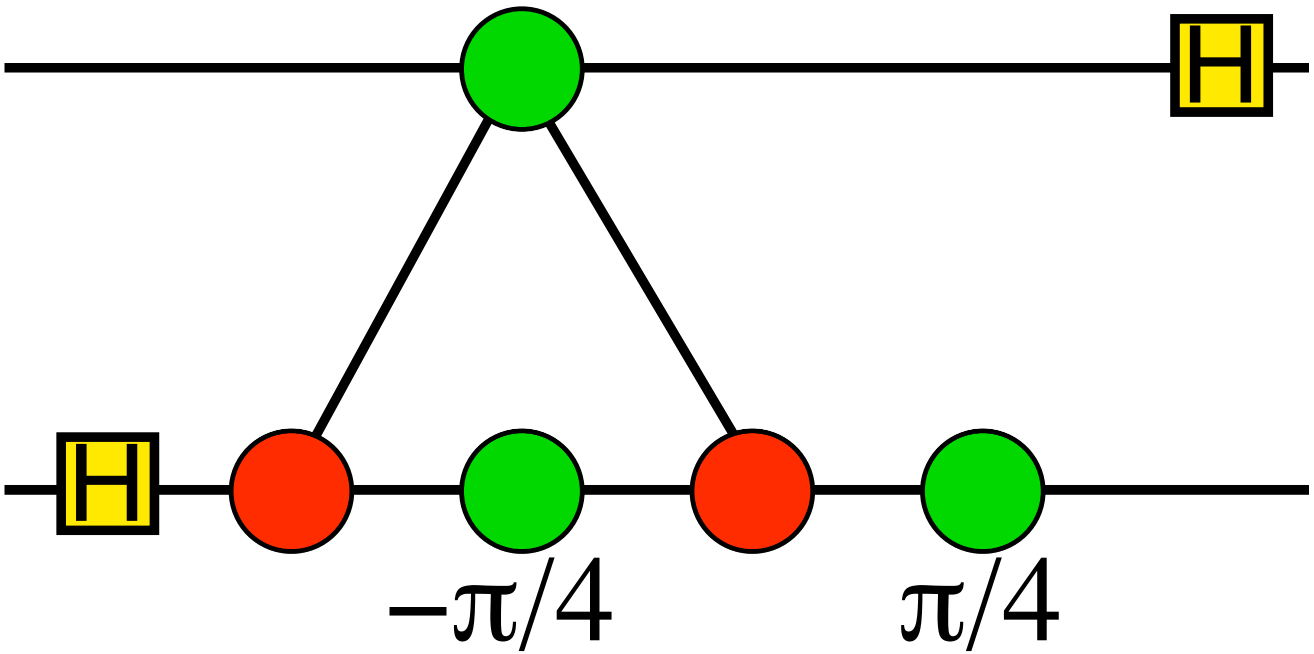
How many types anyway?

Prop: For 4-qubit states there are **uncountably many** SLOCC classes

Forget about types to describe entanglement

Just look at the terms

The ZX-calculus



Quantum processes, diagrammatically

“Classical” Quantum States

When can a quantum state be treated as if classical?

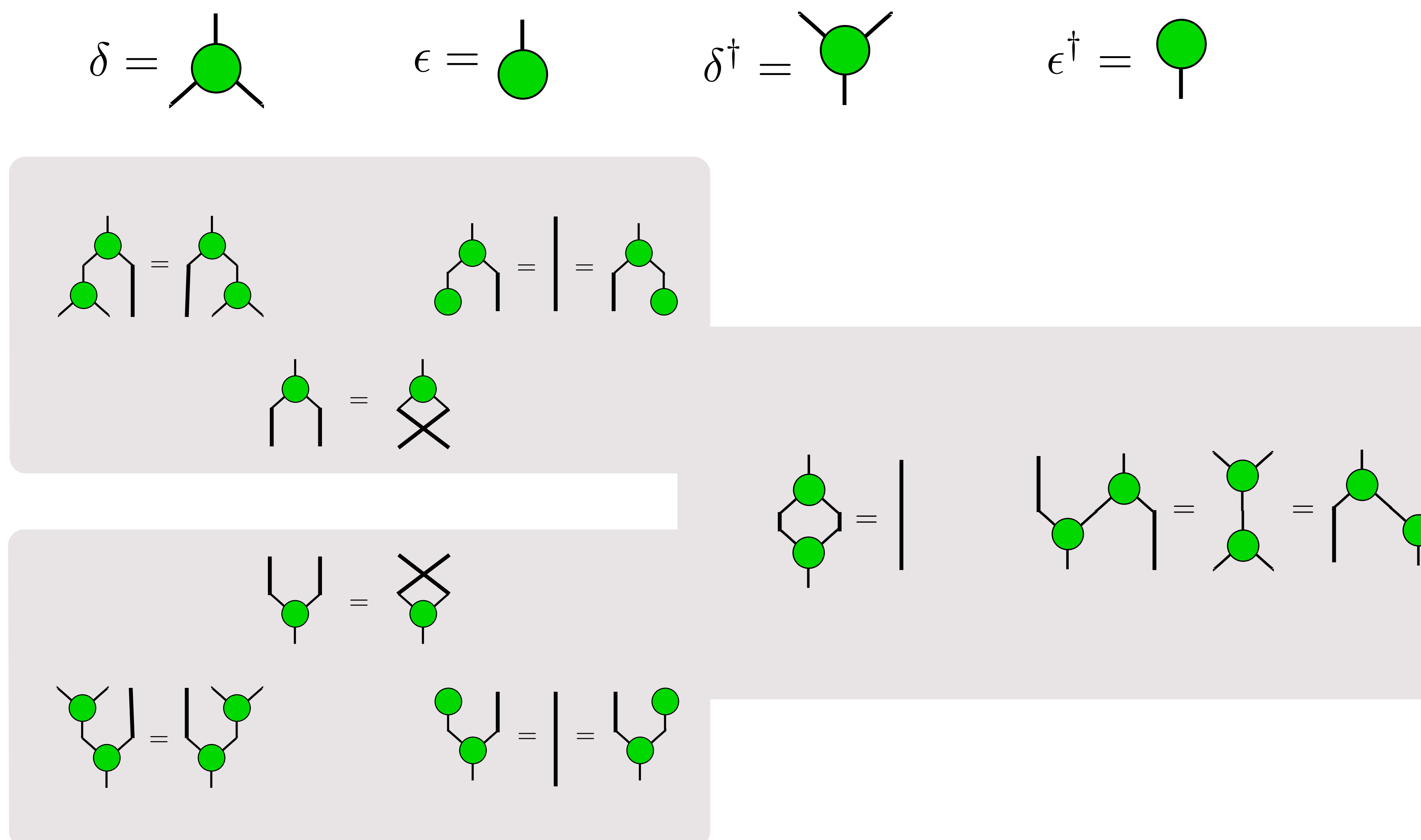
- no-go theorems allow copying and deleting of *orthogonal* states;

In other words:

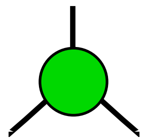
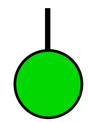
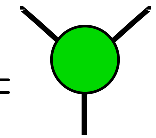
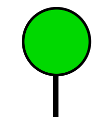
- A quantum state may be copied and deleted if it is an eigenstate of some *known observable.*

We’ll use this property to formalise *observables* in terms of *copying* and *deleting* operations.

Classical Structures

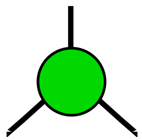
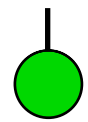
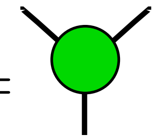
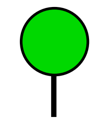


Classical Structures

$\delta =$  $\epsilon =$  $\delta^\dagger =$  $\epsilon^\dagger =$ 

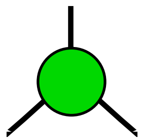
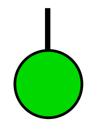
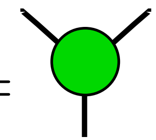
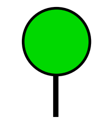
In other words: a classical structure is a *special commutative †-Frobenius algebra*

Classical Structures

$\delta =$  $\epsilon =$  $\delta^\dagger =$  $\epsilon^\dagger =$ 

Theorem: in $\mathbf{FDHilb}$, classical structures are in bijective correspondence to bases. [Coecke, Pavlovic, Vicary]

Classical Structures

$\delta =$  $\epsilon =$  $\delta^\dagger =$  $\epsilon^\dagger =$ 

Theorem: in $\mathbf{FDHilb}$, classical structures are in bijective correspondence to bases. [Coecke, Pavlovic, Vicary]

Each (well behaved) observable defines a basis, therefore :
every observable defines a classical structure!

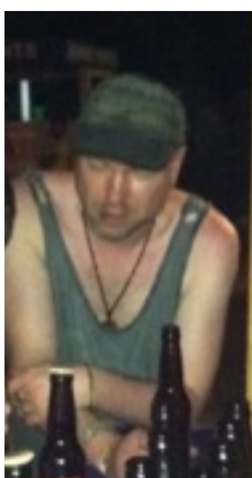
Classical Structures

Still not enough!

every observable defines a classical structure!

Enough equations (probably)

Final ingredient: complementarity



New Journal of Physics

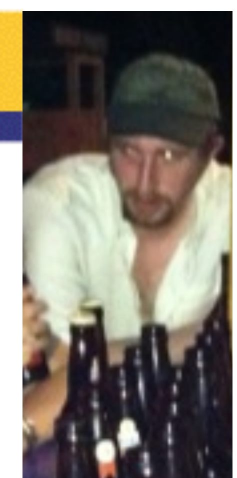
The open-access journal for physics

Interacting quantum observables: categorical algebra and diagrammatics

Bob Coecke[1] **and Ross Duncan**[2]

[1] Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

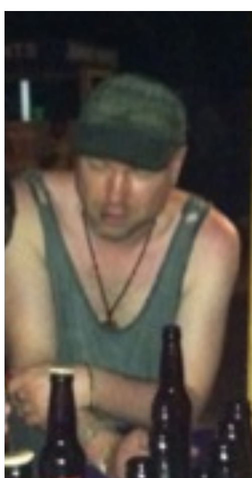
[2] Laboratoire d'Information Quantique, Université Libre de Bruxelles, Boulevard du Triomphe, B-1050, Bruxelles, Belgium



Enough equations (probably)

Final ingredient: complementarity

Only 86 pages!



New Journal of Physics

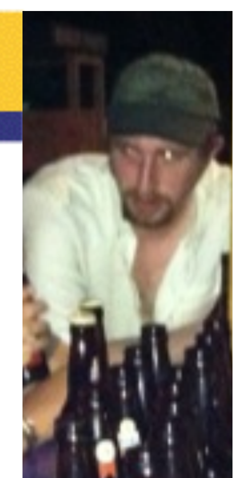
The open-access journal for physics

Interacting quantum observables: categorical algebra and diagrammatics

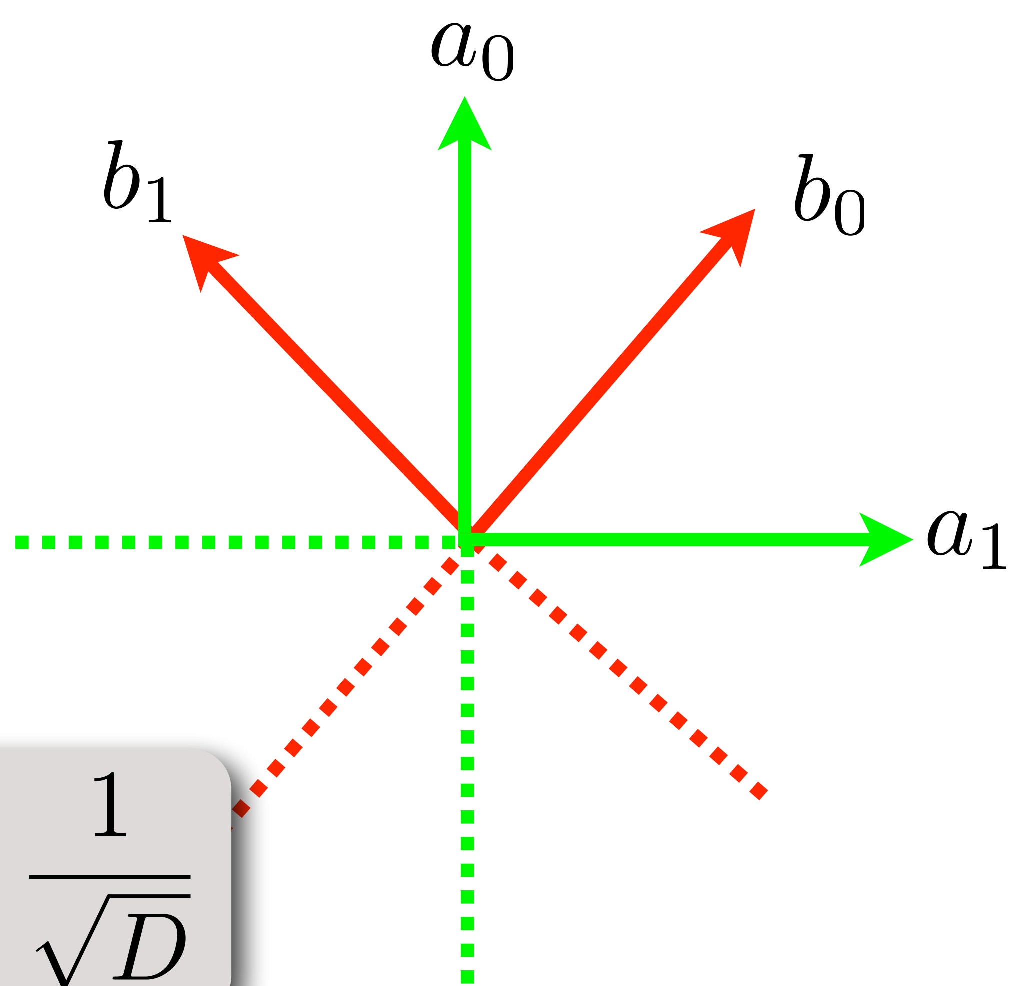
Bob Coecke[1] **and Ross Duncan**[2]

[1] Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

[2] Laboratoire d'Information Quantique, Université Libre de Bruxelles, Boulevard du Triomphe, B-1050, Bruxelles, Belgium



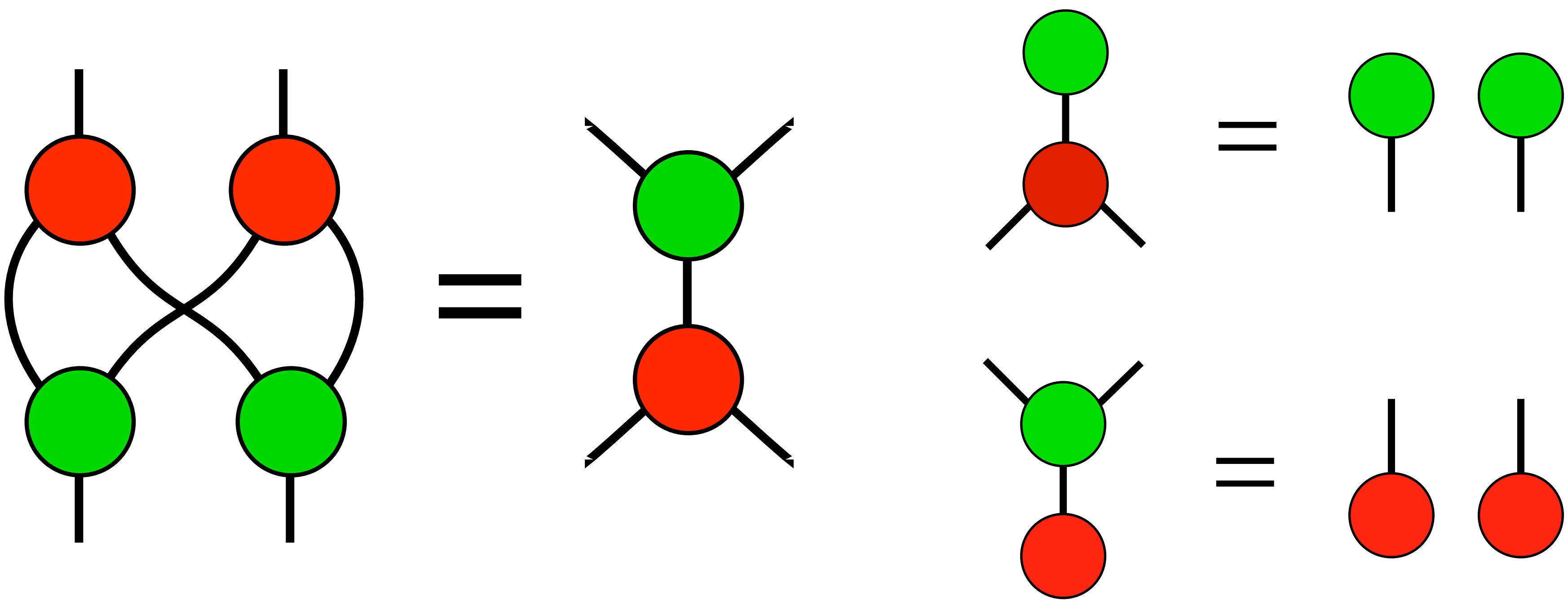
Complementary Observables



$$|\langle a_i \mid b_j \rangle| = \frac{1}{\sqrt{D}}$$

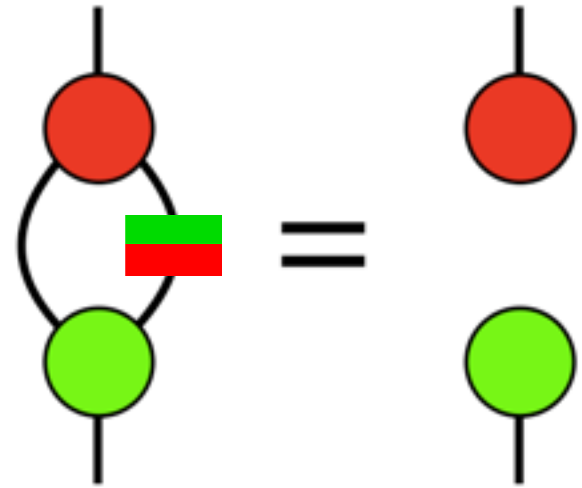
Strong Complementarity

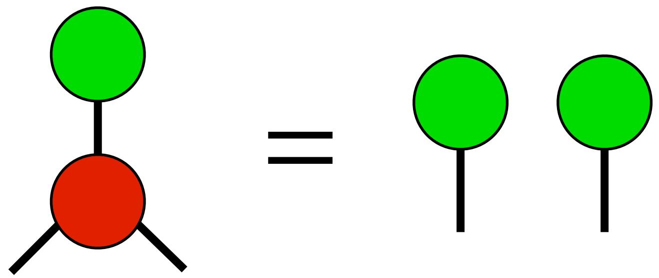
Strongly complementary observables form a *bialgebra*

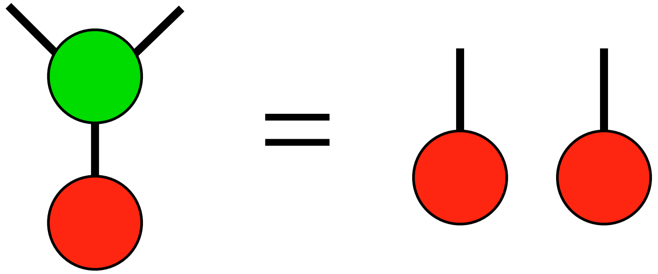


Strongly complementary observables form Hopf algebras

Theorem:







Remark: under the assumption of *enough classical points* the “strong” assumption is not needed; simple complementarity suffices

Strong Complementarity

Many useful properties now follow… too many to discuss!

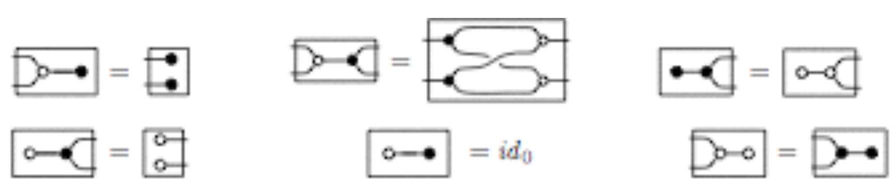
I claim that such interacting algebras are a **fundamental new structure** for computer science

See work of Sobocinski and various coauthors

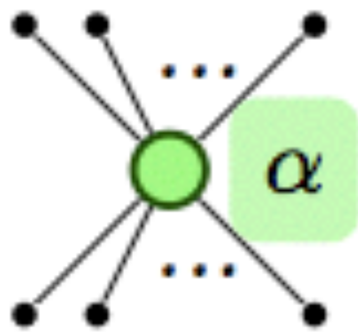
Interacting Bialgebras are Frobenius

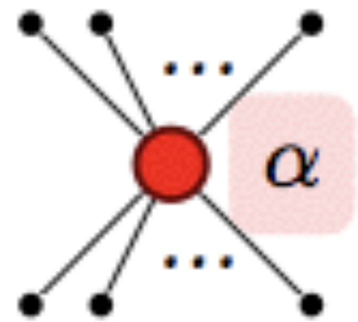
Filippo Bonchi[1], Paweł Sobociński[2] and Fabio Zanasi[1]

[1] ENS de Lyon, Université de Lyon, CNRS, INRIA, France
[2] University of Southampton, UK



ZX-calculus syntax



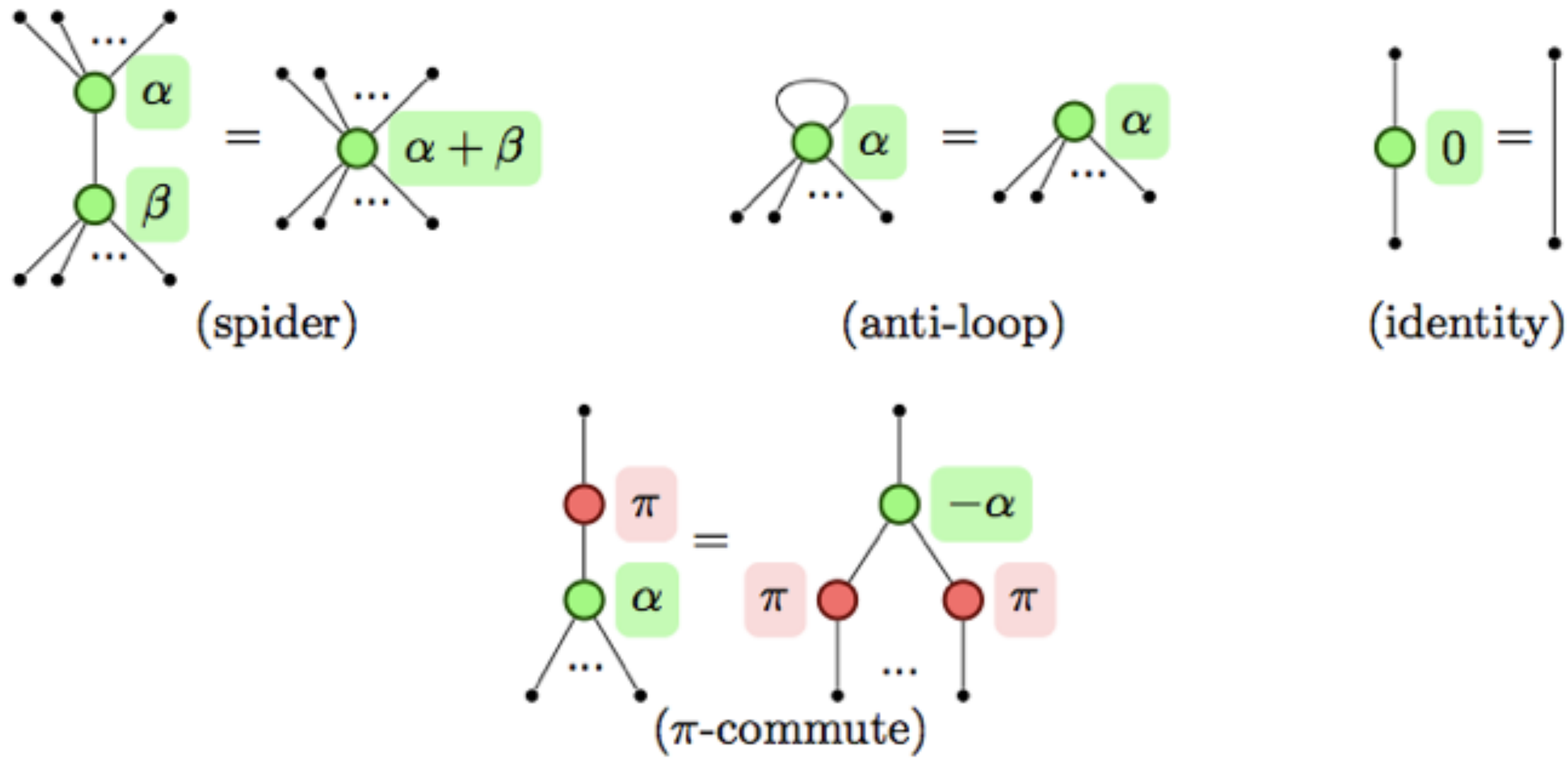


Defn: A *diagram* is an undirected open graph generated by the above vertices.

Defn: let $\mathbb{D}$ be the dagger compact category of diagrams s.t.

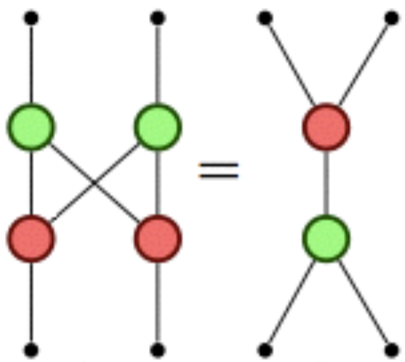
$$(\cdot)^\dagger : \alpha \mapsto -\alpha$$

Equations

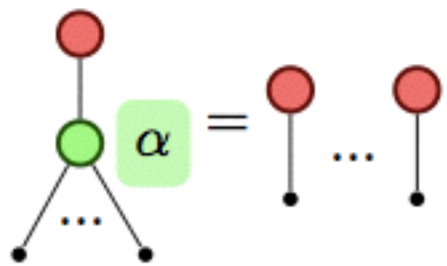


α
β
$=$
$\alpha + \beta$
(spider)
α
$=$
α
(anti-loop)
0
$=$
(identity)
π
α
$=$
$-\alpha$
π
π
(π-commute)

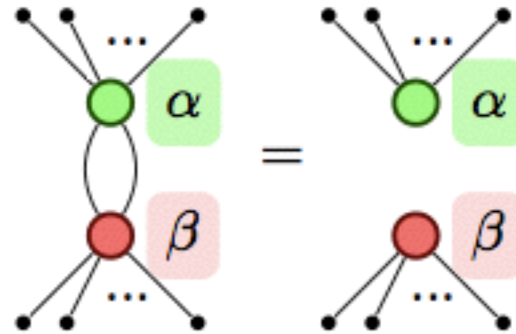
Equations



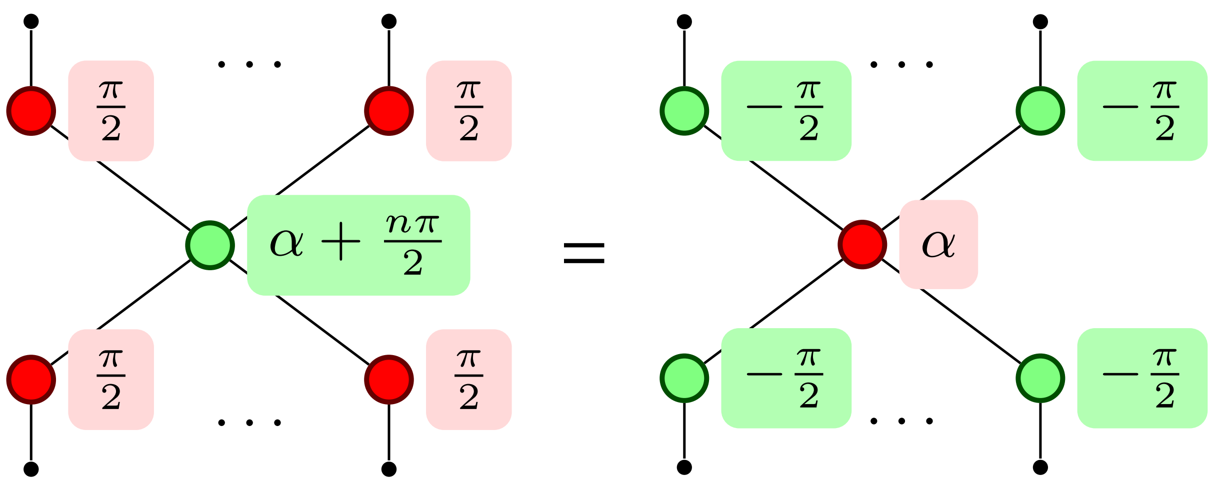
(bialgebra)



(copying)

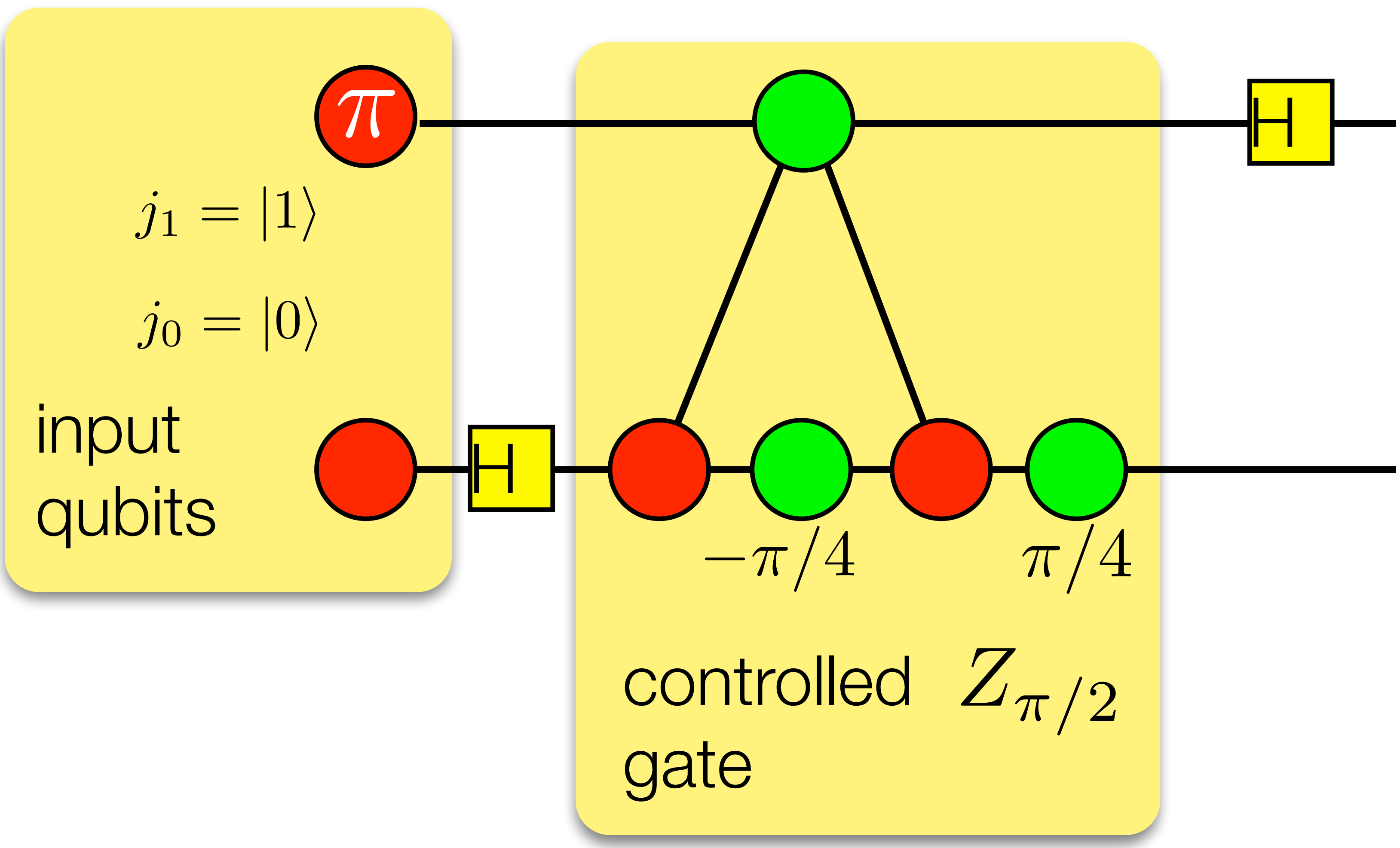


(hopf)

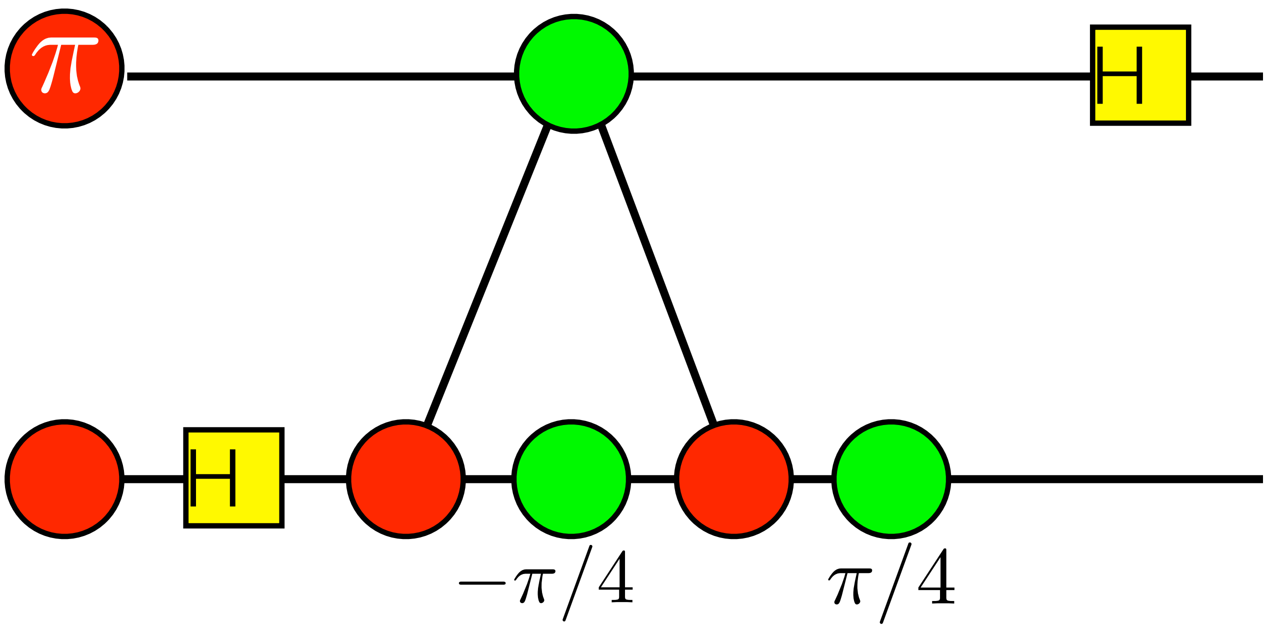


(colour change)

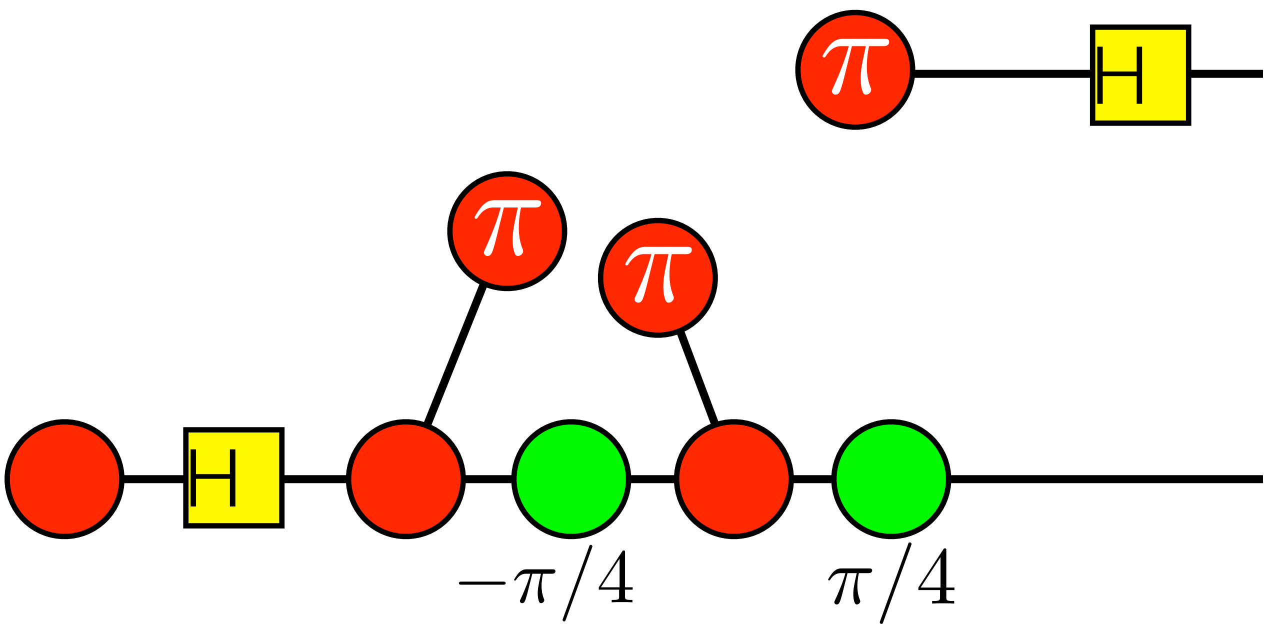
Example: 2-Qubit Quantum Fourier Transform



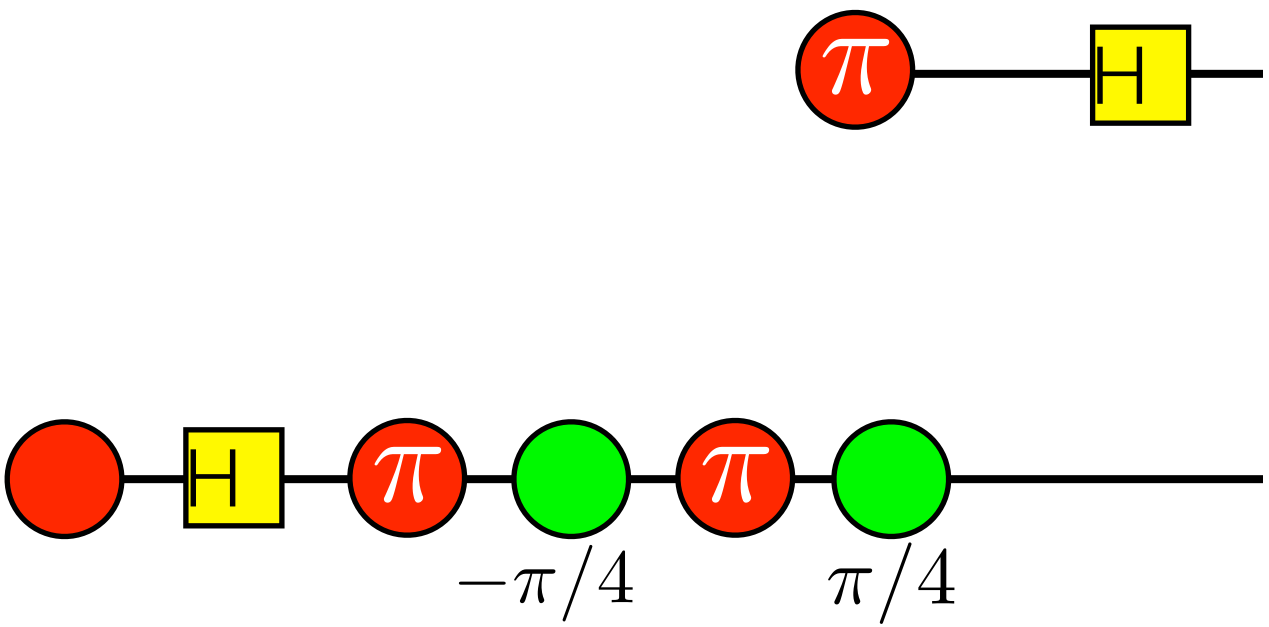
Example: 2-Qubit Quantum Fourier Transform



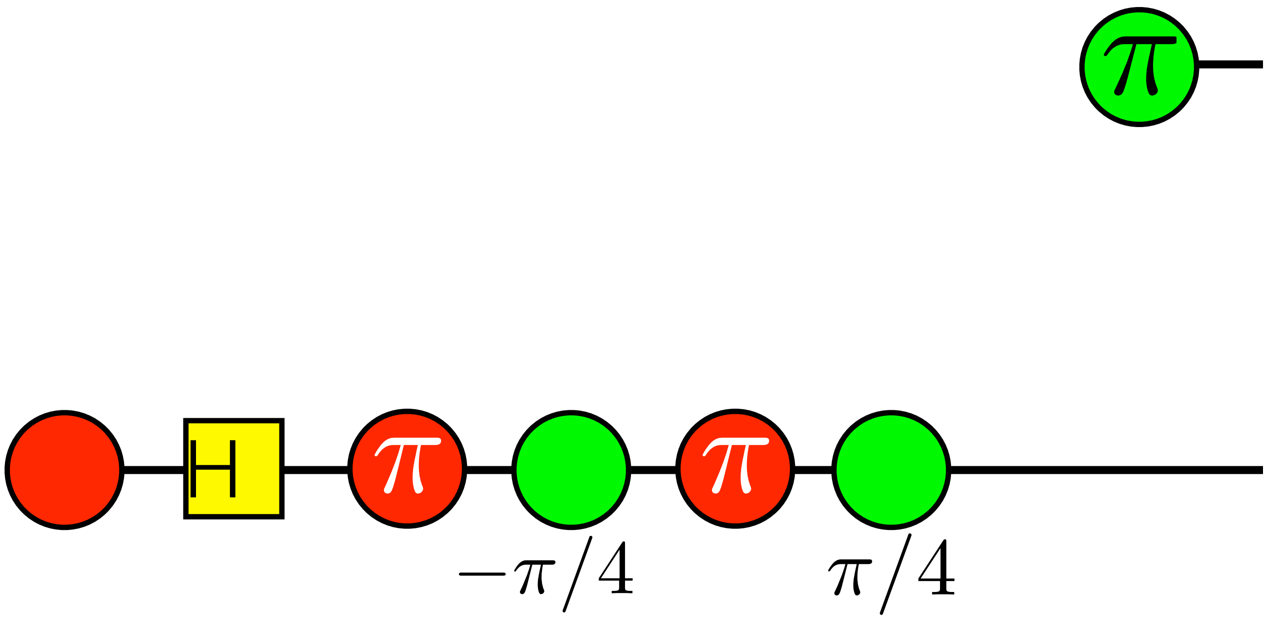
Example: 2-Qubit Quantum Fourier Transform



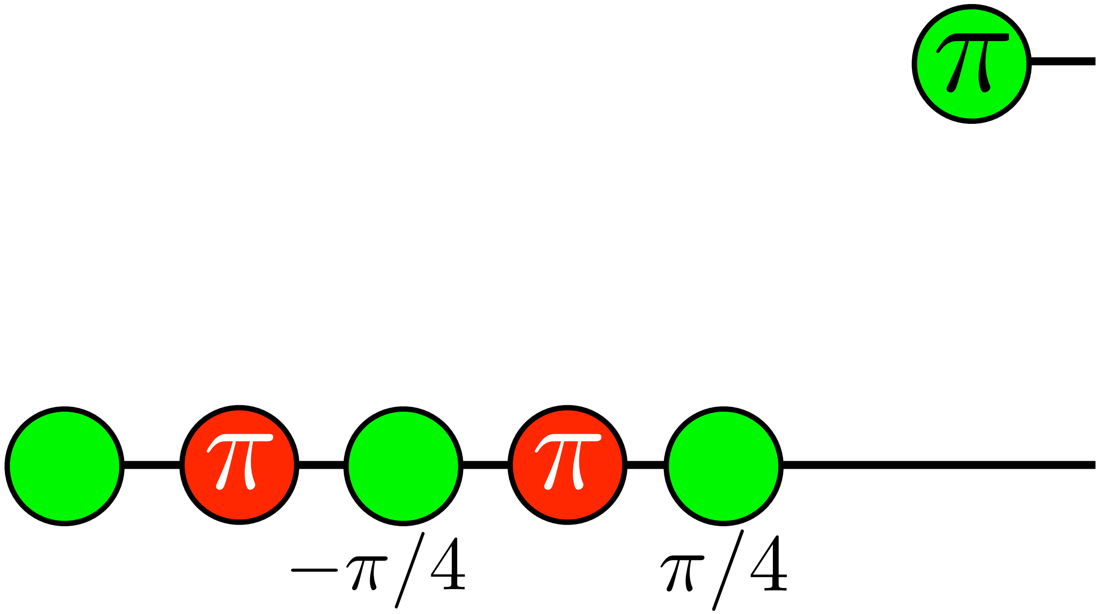
Example: 2-Qubit Quantum Fourier Transform



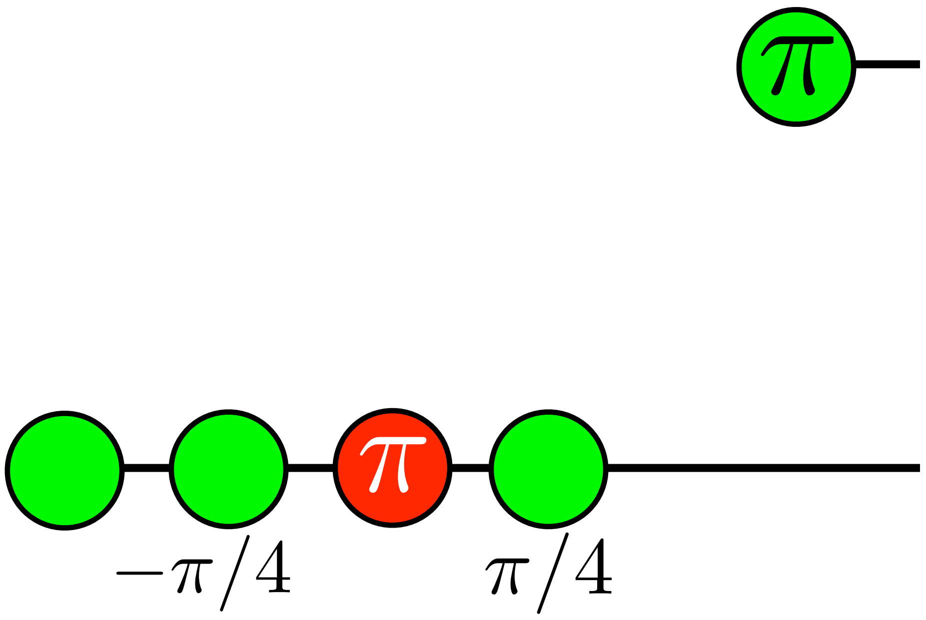
Example: 2-Qubit Quantum Fourier Transform



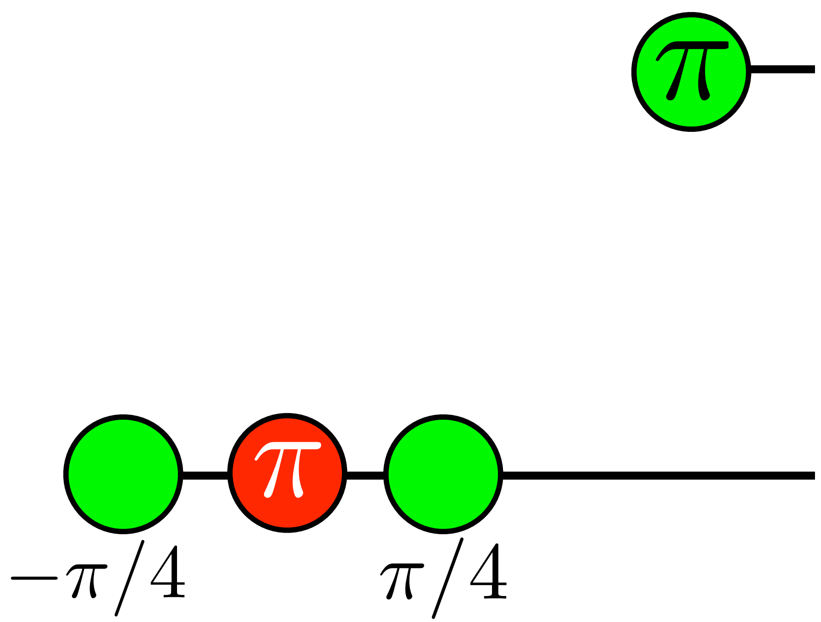
Example: 2-Qubit Quantum Fourier Transform



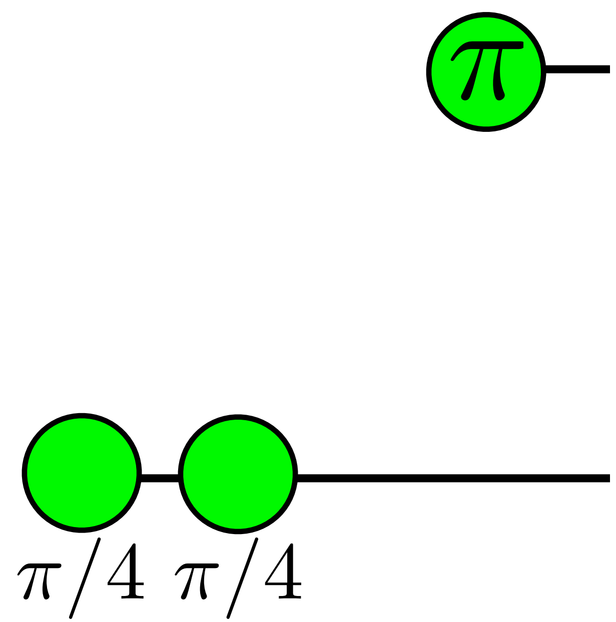
Example: 2-Qubit Quantum Fourier Transform



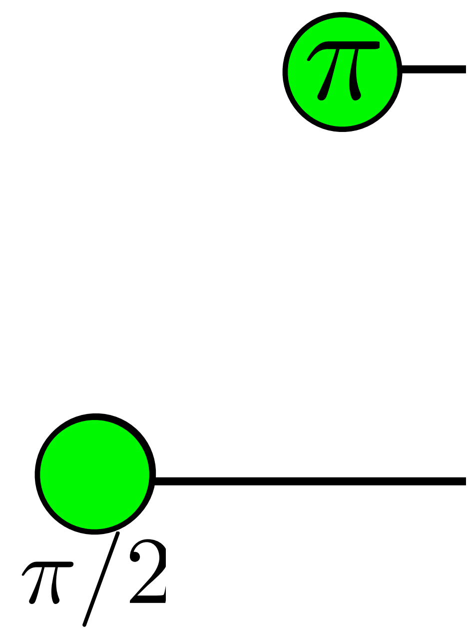
Example: 2-Qubit Quantum Fourier Transform



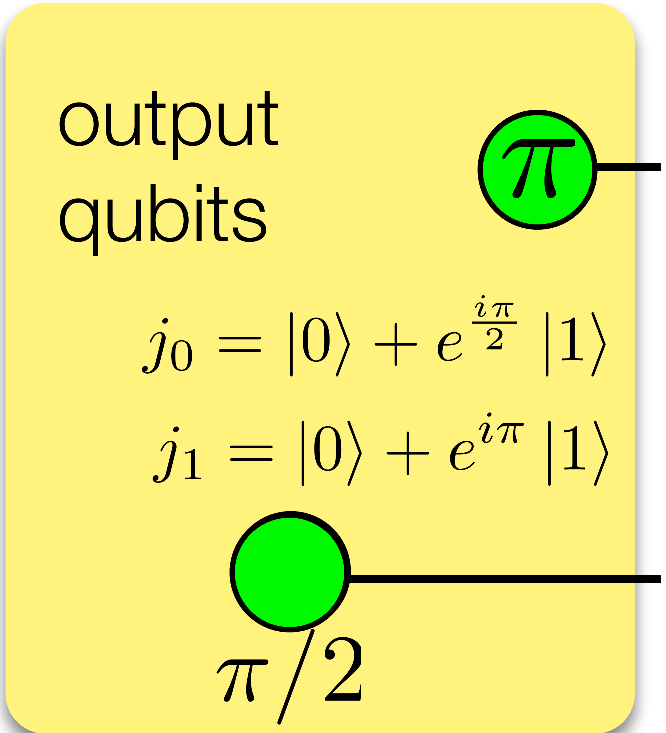
Example: 2-Qubit Quantum Fourier Transform



Example: 2-Qubit Quantum Fourier Transform



Example: 2-Qubit Quantum Fourier Transform

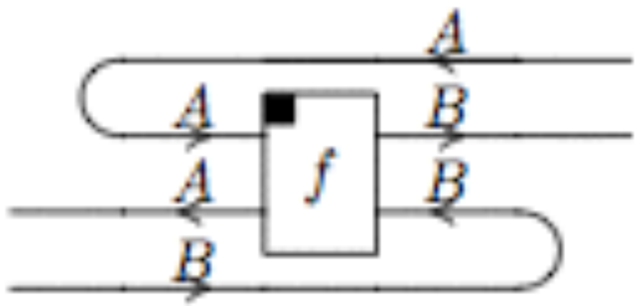


Extensions (1)

The calculus as presented does not deal with non-determinism or probabilities. Two extensions:

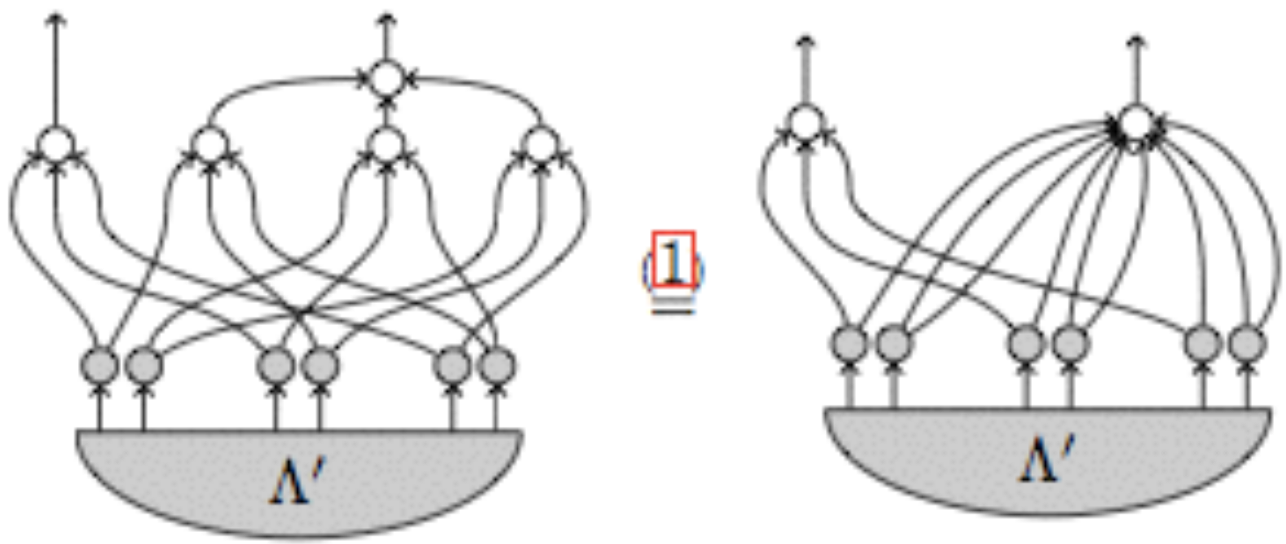
- Conditional vertices:

- Selinger's CPM construction:



Extensions (2)

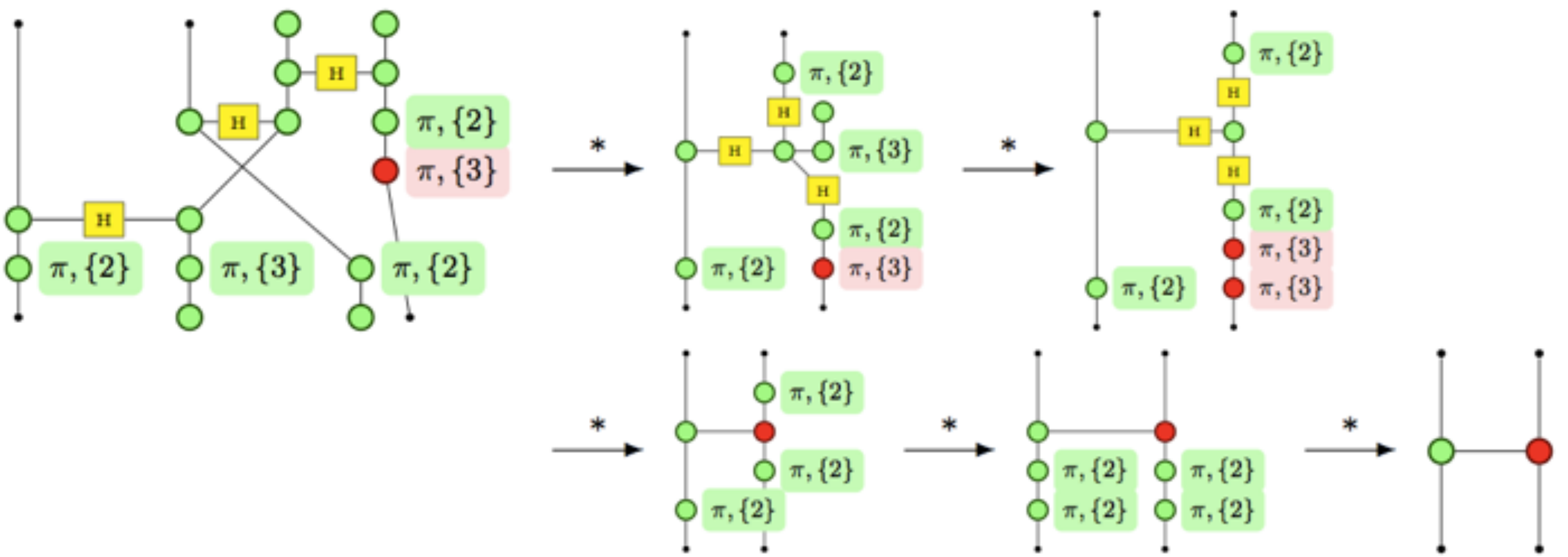
The CPM approach was used to prove that *strong complementarity* is equivalent to *non-locality:*



... justifying the claim that this is a fundamental notion for QM

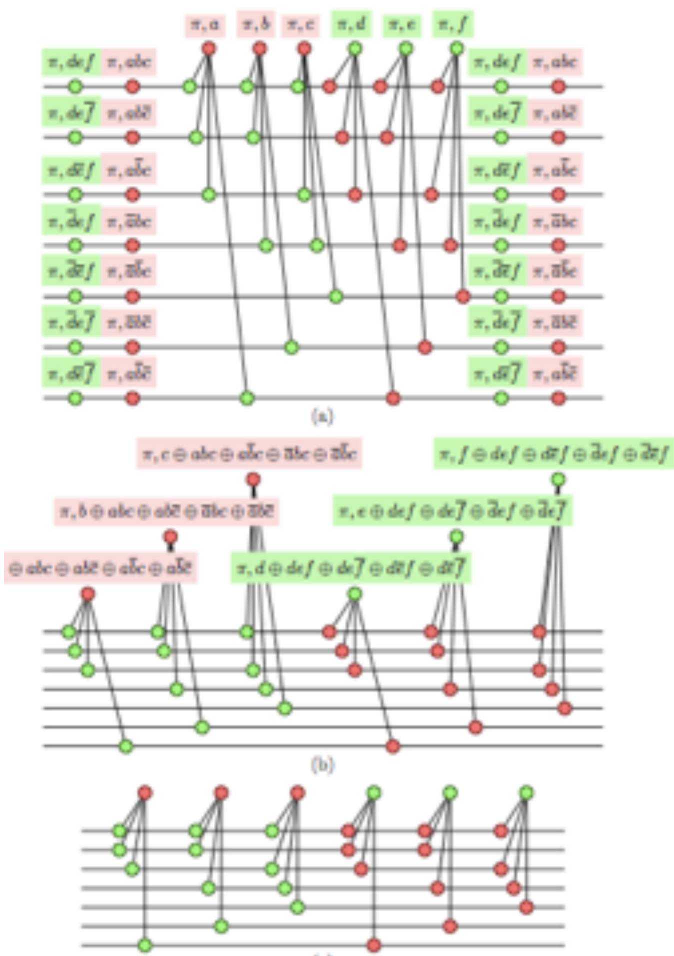
Extensions (3)

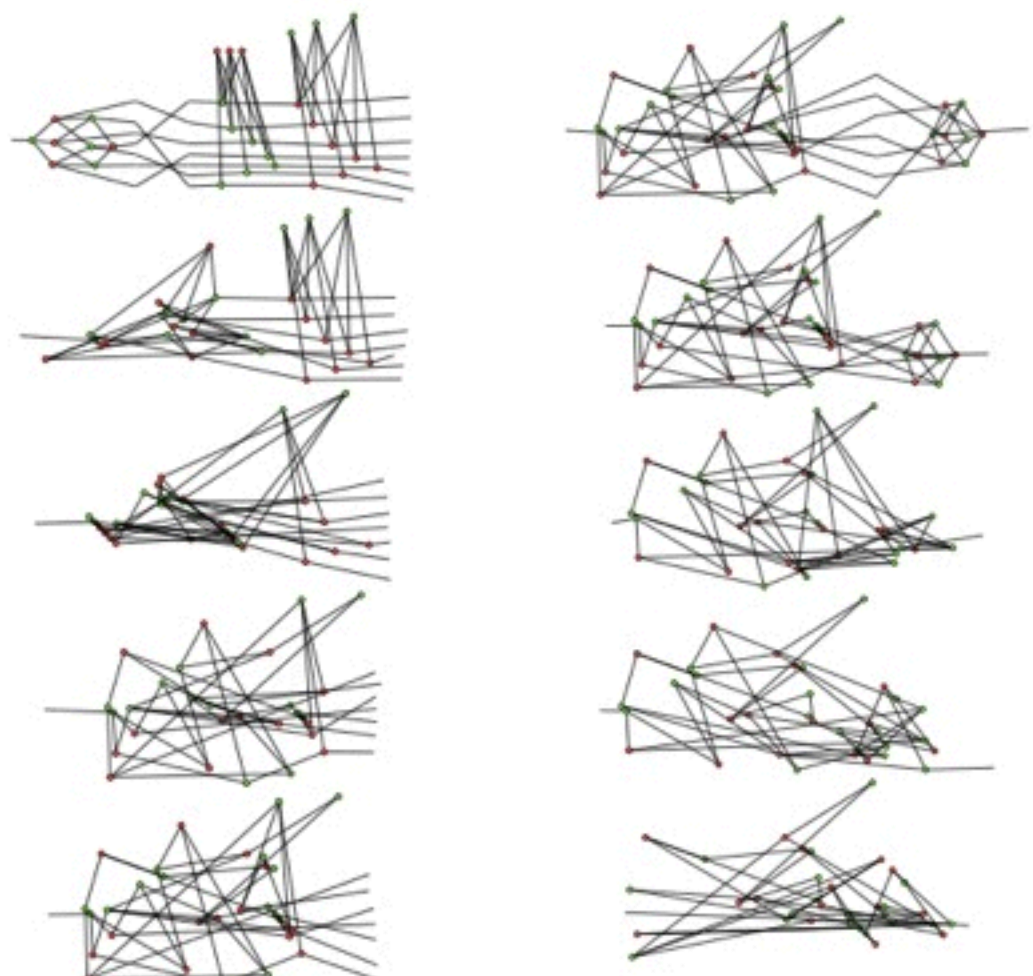
The conditional vertices approach was used to prove the correctness of quantum programs:



Extensions (3)

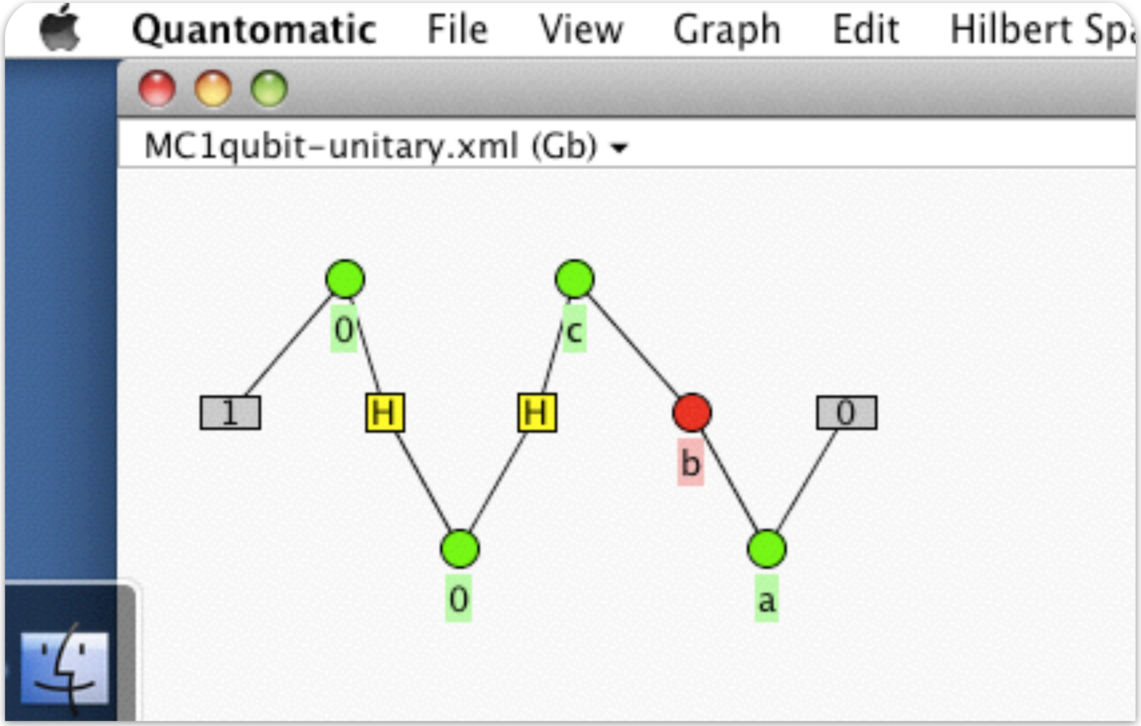
... and error-correcting codes:





Advertising

Graphical tool for doing graphical calculations:



http://dream.inf.ed.ac.uk/projects/quantomatic/

Happy Birthday Prakash!