Bob Coecke - Oxford University Computing Laboratory

Quantum information processing: a new light on the Q-formalism and Q-foundations

ASL 2010 North American Annual Meeting

The George Washington University
Washington, DC, March 17-20, 2010

I. von Neumann's Q-formalism & teleportation

II. Quantum algorithms & categorical quantum logic

III. QKD & abstract bases & entanglement & non-locality

Quantum information processing:
a new light on the Q-formalism and Q-foundations I

von Neumann's quantum formalism - teleportation

Bob Coecke - Oxford University Computing Laboratory

QUBITS vs. BITS
(a informal account)

A **bit**:

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

A **qubit**:

- a *continuous sphere* of values, which is ‘spanned’ (cf. rays in 2D $\mathbb{C}$-space) by two states $|0\rangle$ and $|1\rangle$.

A **qubit**:

- a *continuous sphere* of values, which is ‘spanned’ (cf. rays in 2D $\mathbb{C}$-space) by two states $|0\rangle$ and $|1\rangle$.

- transformations are restricted to *unitary* ones i.e. which preserve angles and in particular opposites.

A **qubit**:

- a *continuous sphere* of values, which is ‘spanned’ (cf. rays in 2D $\mathbb{C}$-space) by two states $|0\rangle$ and $|1\rangle$.

- transformations are restricted to *unitary* ones i.e. which preserve angles and in particular opposites.

- ‘readable’ via *quantum measurements* $M(|+\rangle, |-\rangle)$:
  - have only two possible outcomes $|+\rangle$ and $|-\rangle$,
  - change the initial state $|\psi\rangle$ to either $|+\rangle$ or $|-\rangle$,

A **qubit**:

- a *continuous sphere* of values, which is 'spanned' (cf. rays in 2D $\mathbb{C}$-space) by two states $|0\rangle$ and $|1\rangle$.

- transformations are restricted to *unitary* ones i.e. which preserve angles and in particular opposites.

- 'readable' via *quantum measurements* $M(|+\rangle, |-\rangle)$:
  - have only two possible outcomes $|+\rangle$ and $|-\rangle$,
  - change the initial state $|\psi\rangle$ to either $|+\rangle$ or $|-\rangle$,

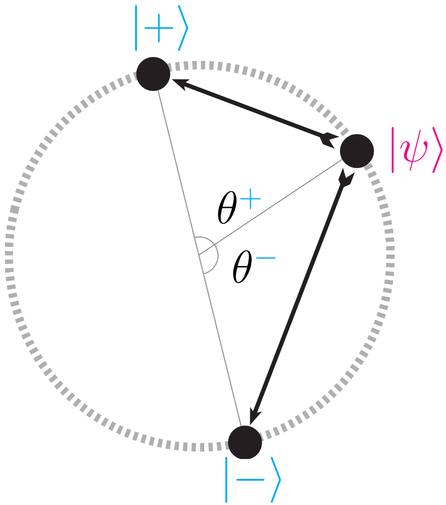
  $\Rightarrow M(|+\rangle, |-\rangle)$ <u>does not tell</u> $|\psi\rangle$ but <u>destroys</u> $|\psi\rangle$ **!**

The two transitions

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

have respective chance $\mathsf{prob}(\theta_+)$ and $\mathsf{prob}(\theta_-)$ with

$$\mathsf{prob}(\theta_+) + \mathsf{prob}(\theta_-) = 1 \quad \text{with} \quad \mathsf{prob}(\theta) = cos^2\frac{\theta}{2}\,.$$



The **state of a qubit** is described by a pair of complex numbers $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ *up to a non-zero complex multiple*.

The **state of a qubit** is described by a pair of complex numbers $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ *up to a non-zero complex multiple*.

The same state for any $z \in \mathbb{C}_0$:

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \qquad \text{and} \qquad z \cdot \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} := \begin{pmatrix} z \cdot z_1 \\ z \cdot z_2 \end{pmatrix}$$

The **state of a qubit** is described by a pair of complex numbers $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ *up to a non-zero complex multiple*.

The same state for any $z \in \mathbb{C}_0$:

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \qquad \text{and} \qquad z \cdot \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} := \begin{pmatrix} z \cdot z_1 \\ z \cdot z_2 \end{pmatrix}$$

'Bit'-inspired notation:

$$|\psi\rangle = z \cdot |0\rangle + z' \cdot |1\rangle \ .$$

with

$$|\psi\rangle = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

A (non-measurement) **transformation of a qubit** is described by a matrix of complex numbers

$$\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}$$

where $\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \perp \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ is the image of $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \perp \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

A (non-measurement) **transformation of a qubit** is described by a matrix of complex numbers

$$\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}$$

where $\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \perp \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ is the image of $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \perp \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

We have:

$$\langle U(\psi)|U(\phi)\rangle = \langle\psi|\phi\rangle \ ,$$

and in particular:

$$|\psi\rangle \perp |\phi\rangle \quad \text{then} \quad U|\psi\rangle \perp U|\phi\rangle \ .$$

The **computational basis qubit measurement** is the non-deterministic application of one of the *projectors*:

$$\mathrm{P}_0 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathrm{P}_1 := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

The **computational basis qubit measurement** is the non-deterministic application of one of the *projectors*:

$$\mathrm{P}_0 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathrm{P}_1 := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

They induce a change of state

$$|\psi\rangle \mapsto \mathrm{P}_0(|\psi\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} z_1 \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|\psi\rangle \mapsto \mathrm{P}_1(|\psi\rangle) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ z_2 \end{pmatrix} \sim \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum computation is a ‘balancing act’:

- Exploit the enlarged state space

- Avoid destruction of data by measurement

Quantum computation is a ‘balancing act’:

- Exploit the enlarged state space
- Avoid destruction of data by measurement

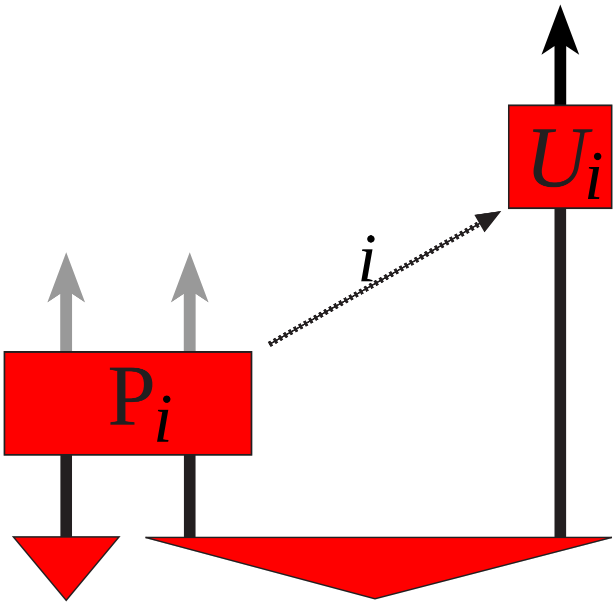
Whenever more systems are involved:

- State space blows up enormously.
- Measurement dynamics now enables information flows within networks of quantum systems.

SOME QUANTUM PHENOMENA

1. Quantum teleportation

theory: 1993; 1st experimental realisation: 1997

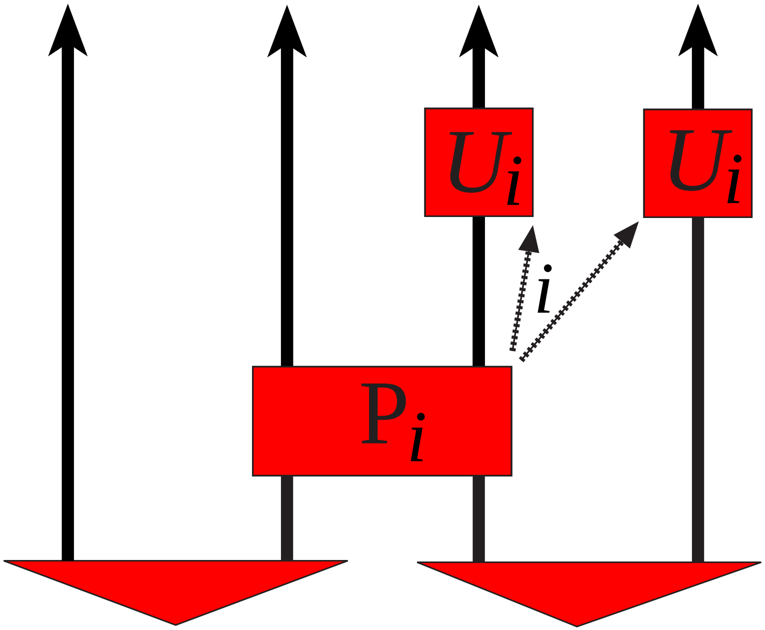


$\Rightarrow$ Measurement as a dynamic resource

$\Rightarrow$ Transmit continuous data by finite means

2. Entanglement swapping

theory: 1993; 1st experimental realisation: 2007



$\Rightarrow$ Entangle without touching

3. Public key exchange

theory: 1984, '91; you can buy one online

$\Rightarrow$ Can't be cracked

3. Public key exchange

theory: 1984, ’91; you can buy one online

$\Rightarrow$ Can’t be cracked

4. Fast algorithms

theory: 1992, ’94, ’96; science fiction

$\Rightarrow$ Generates research money and jobs!

Why this sudden new activity?

Cf. in particular the time (= 60 y) it took to discover quantum teleportation! (people weren’t looking for it)

Why this sudden new activity?

Cf. in particular the time (= 60 y) it took to discover quantum teleportation! (people weren't looking for it)

A bug became a feature, ...

after experimental confirmation of violation of the Bell inequalities by aspect and Gragnier in 1982.

THE VON NEUMANN FORMALISM
(for pure states)

pure state $\equiv$ 'closed system'

What we won't explicitly talk about:

- Continuous time Schrödinger evolution.
- Infinite spectrum observable quantities.
- Mixed states and operations

Definition. A finite-dimensional *Hilbert space* is a finite dimensional vector space $\mathcal{H}$ over the complex number field $\mathbb{C}$ with a *sesquilinear inner-product* i.e.

$$\langle - \mid - \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

which satisfies

$$\langle \psi | c_1 \cdot \psi_1 + c_2 \cdot \psi_2 \rangle = c_1 \langle \psi | \psi_1 \rangle + c_2 \langle \psi | \psi_2 \rangle$$

$$\langle c_1 \cdot \psi_1 + c_2 \cdot \psi_2 | \psi \rangle = \bar{c}_1 \langle \psi_1 | \psi \rangle + \bar{c}_2 \langle \psi_2 | \psi \rangle$$

$$\langle \psi | \phi \rangle = \overline{\langle \phi | \psi \rangle} \qquad \langle \psi | \psi \rangle \in \mathbb{R}^+$$

$$\langle \psi | \psi \rangle = 0 \ \Leftrightarrow \ \psi = \mathbf{0}$$

for all $c_1, c_2 \in \mathbb{C}$ and all $\psi, \psi_1, \psi_2 \in \mathcal{H}$.

The condition

$$\forall \psi \in \mathcal{H}_1, \phi \in \mathcal{H}_2 : \quad \langle f^\dagger(\phi) | \psi \rangle = \langle \phi | f(\psi) \rangle$$

defines the (always existing and unique) **adjoint**

$$f^\dagger : \mathcal{H}_2 \to \mathcal{H}_1 \qquad \text{of} \qquad f : \mathcal{H}_1 \to \mathcal{H}_2.$$

We have $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$ i.e. $(-)^\dagger$ is contravariant.

The condition

$$\forall \psi \in \mathcal{H}_1, \phi \in \mathcal{H}_2 : \quad \langle f^\dagger(\phi)|\psi\rangle = \langle \phi | f(\psi)\rangle$$

defines the (always existing and unique) **adjoint**

$$f^\dagger : \mathcal{H}_2 \to \mathcal{H}_1 \qquad \text{of} \qquad f : \mathcal{H}_1 \to \mathcal{H}_2.$$

We have $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$ i.e. $(-)^\dagger$ is contravariant.

A linear operator is **unitary** if, equivalently,

- its inverse exist and is equal to its adjoint,
- it preserves the inner-product.

The condition

$$\forall\psi \in \mathcal{H}_1, \phi \in \mathcal{H}_2 : \quad \langle f^\dagger(\phi)|\psi\rangle = \langle\phi|f(\psi)\rangle$$

defines the (always existing and unique) **adjoint**

$$f^\dagger : \mathcal{H}_2 \to \mathcal{H}_1 \qquad \text{of} \qquad f : \mathcal{H}_1 \to \mathcal{H}_2 .$$

We have $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$ i.e. $(-)^\dagger$ is contravariant.

A linear operator is **unitary** if, equivalently,

- its inverse exist and is equal to its adjoint,
- it preserves the inner-product.

Rays are subspaces spanned by a single vector i.e.

$$\mathsf{span}(\psi) = \{c \cdot \psi \mid c \in \mathbb{C}\} .$$

Postulate 1. [states and transformations]

The state of a quantum system $\mathcal{S}$ is described by a ray in a Hilbert space $\mathcal{H}$. Deterministic transformations of $\mathcal{S}$ are described by unitary operators acting on $\mathcal{H}$.

Self-adjoint operators satisfy $H^\dagger = H$.

Self-adjoint operators satisfy $H^\dagger = H$.

Self-adjoint idempotent operators $\mathrm{P} : \mathcal{H} \to \mathcal{H}$, i.e.

$$\mathrm{P} \circ \mathrm{P} = \mathrm{P} = \mathrm{P}^\dagger ,$$

are called **projectors**.

Self-adjoint operators satisfy $H^\dagger = H$.

Self-adjoint idempotent operators $\mathrm{P} : \mathcal{H} \to \mathcal{H}$, i.e.

$$\mathrm{P} \circ \mathrm{P} = \mathrm{P} = \mathrm{P}^\dagger ,$$

are called **projectors**.

Proposition. Each self-adjoint operator $H : \mathcal{H} \to \mathcal{H}$ admits a so-called **spectral decomposition**

$$H = \sum_i a_i \cdot \mathrm{P}_i$$

where all $a_i \in \mathbb{R}$ and all $\mathrm{P}_i : \mathcal{H} \to \mathcal{H}$ are projectors which are *mutually orthogonal* i.e.

$$\mathrm{P}_i \circ \mathrm{P}_j = O_{\mathcal{H}} \qquad \text{for} \qquad i \neq j \ .$$

Postulate 2. [measurements]

A measurement on a quantum system is described by a self-adjoint operator $H = \sum_i a_i \cdot \mathrm{P}_i$, with $\{a_i\}$ the *measurement outcomes* and $\{\mathrm{P}_i\}$ the *state changes*:

1. The initial state ψ undergoes one of the transitions

   $$\mathrm{P}_i :: \psi \mapsto \mathrm{P}_i(\psi)$$

   and the probability of the possible transitions is

   $$\mathsf{prob}(\mathrm{P}_i, \psi) = \langle \psi | \mathrm{P}_i(\psi) \rangle$$

   where ψ needs to be <u>normalized</u>.

2. The *observer* which performs the measurement receives the value a_i as a token-witness of that fact.

Remark. The measurements represented by

$$\sum_i a_i \cdot \mathrm{P}_i \qquad \text{and} \qquad \sum_i i \cdot \mathrm{P}_i$$

are 'behaviorally equivalent'.

Remark. The measurements represented by

$$\sum_i a_i \cdot \mathrm{P}_i \qquad \text{and} \qquad \sum_i i \cdot \mathrm{P}_i$$

are 'behaviorally equivalent'.

So one may think of a measurement as:

$$(\mathrm{P}_1, \ldots, \mathrm{P}_n)\,.$$

or even as:

$$\{\mathrm{P}_1, \ldots, \mathrm{P}_n\}\,.$$

The **direct sum** is

$$\mathcal{H}_1 \oplus \mathcal{H}_2 := \{(\psi, \phi) \mid \psi \in \mathcal{H}_1, \phi \in \mathcal{H}_2\}$$

A basis for $\mathcal{H}_1 \oplus \mathcal{H}_2$ is

$$\mathcal{B}_1 + \mathcal{B}_2 = \{(e_1, \mathbf{0}), \ldots, (e_n, \mathbf{0}), (\mathbf{0}, e'_1), \ldots, (\mathbf{0}, e'_m)\}.$$

The **direct sum** is

$$\mathcal{H}_1 \oplus \mathcal{H}_2 := \{(\psi, \phi) \mid \psi \in \mathcal{H}_1, \phi \in \mathcal{H}_2\}$$

A basis for $\mathcal{H}_1 \oplus \mathcal{H}_2$ is

$$\mathcal{B}_1 + \mathcal{B}_2 = \{(e_1, \mathbf{0}), \ldots, (e_n, \mathbf{0}), (\mathbf{0}, e'_1), \ldots, (\mathbf{0}, e'_m)\} \,.$$

The **tensor product** is

$$\mathcal{H}_1 \otimes \mathcal{H}_2 := \frac{\{\sum_i \alpha_i (\psi_i, \phi_i) \mid \psi_i \in \mathcal{H}_1, \phi_i \in \mathcal{H}_2\}}{\text{`bilinearity'}}$$

A basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$ is

$$\mathcal{B}_1 + \mathcal{B}_2 = \{(e_1, e'_1), \ldots, (e_i, e'_j), \ldots, (e_n, e'_m)\} \,.$$

Postulate 3. [compound systems]

The joint states of a compound quantum system are described within the tensor product of the Hilbert spaces which the states of the subsystems are described.

Enables ‘embedding’ of *single system states* via

$$\begin{tikzcd}
\mathcal{H}_1 \times \mathcal{H}_2 \arrow[r, "\xi\ \text{(bilinear)}"] \arrow[dr, "\forall\zeta\ \text{(bilinear)}"'] & \mathcal{H}_1 \otimes \mathcal{H}_2 \arrow[d, "\exists! h\ \text{(bilinear)}"] \\
& \mathcal{H}
\end{tikzcd}$$

Enables 'embedding' of *single system states* via

$$\begin{tikzcd}
\mathcal{H}_1 \times \mathcal{H}_2 \arrow[r, "\xi\ (\text{bilinear})"] \arrow[dr, "\forall\zeta\ (\text{bilinear})"'] & \mathcal{H}_1 \otimes \mathcal{H}_2 \arrow[d, "\exists! h\ (\text{bilinear})"] \\
 & \mathcal{H}
\end{tikzcd}$$

But there are a lot more states than these, ...

$$dim(\mathcal{H}_1 \oplus \mathcal{H}_2) = dim(\mathcal{H}_1) + dim(\mathcal{H}_2),$$
$$dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = dim(\mathcal{H}_1) \times dim(\mathcal{H}_2).$$

For the **Bell-state**

$$\mathsf{Bell} := |00\rangle + |11\rangle = e_1 \otimes e_1 + e_2 \otimes e_2$$

there are no $a_1, a_2, a_3, a_4 \in \mathbb{C}$ such that:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

For the **Bell-state**

$$\mathsf{Bell} := |00\rangle + |11\rangle = e_1 \otimes e_1 + e_2 \otimes e_2$$

there are no $a_1, a_2, a_3, a_4 \in \mathbb{C}$ such that:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

or equivalently, such that:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

which indicates a correspondence with the identity.

Alternative definition of the tensor product:

$$\mathcal{H}_1 \otimes \mathcal{H}_2 := \mathcal{H}_1^{(*)} \multimap \mathcal{H}_2$$

cf. the bijective correspondence:

$$\sum_{i,j} \alpha_{i,j} |\, i\, j\rangle \;\; \sim \;\; \begin{pmatrix} & \vdots & \\ \cdots & \alpha_{ij} & \cdots \\ & \vdots & \end{pmatrix} .$$

Alternative definition of the tensor product:

$$\mathcal{H}_1 \otimes \mathcal{H}_2 := \mathcal{H}_1^{(*)} \multimap \mathcal{H}_2$$

cf. the bijective correspondence:

$$\sum_{i,j} \alpha_{i,j} | \, i \, j \rangle \;\; \sim \;\; \begin{pmatrix} & \vdots & \\ \cdots & \alpha_{ij} & \cdots \\ & \vdots & \end{pmatrix} .$$

These **‘channels’** allow **information to flow** between quantum systems e.g. in the case of teleportation.

Measuring the left system for a Bell-state i.e. we apply

$$\{\mathrm{P}_0 \otimes \mathsf{id}, \mathrm{P}_1 \otimes \mathsf{id}\}$$

to the whole system we obtain

$$(\mathrm{P}_0 \otimes \mathsf{id})(\mathsf{Bell}) = |00\rangle \qquad (\mathrm{P}_1 \otimes \mathsf{id})(\mathsf{Bell}) = |11\rangle$$

Measuring the left system for a Bell-state i.e. we apply

$$\{\mathrm{P}_0 \otimes \mathsf{id}, \mathrm{P}_1 \otimes \mathsf{id}\}$$

to the whole system we obtain

$$(\mathrm{P}_0 \otimes \mathsf{id})(\mathsf{Bell}) = |00\rangle \quad (\mathrm{P}_1 \otimes \mathsf{id})(\mathsf{Bell}) = |11\rangle$$

that is, we get a certain answer if next we apply

$$\{\mathsf{id} \otimes \mathrm{P}_0, \mathsf{id} \otimes \mathrm{P}_1\} \ .$$

Representing vector $\psi \in \mathcal{H}$ by linear map

$$|\psi\rangle : \mathbb{C} \to \mathcal{H} :: 1 \mapsto \psi$$

Representing vector $\psi \in \mathcal{H}$ by linear map

$$|\psi\rangle : \mathbb{C} \to \mathcal{H} :: 1 \mapsto \psi$$

Dirac notation is formally justified by letting

- $|\psi\rangle := \psi$ and called *KET* ,
- $\langle\psi| := \psi^\dagger$ and called *BRA*,
- concatenation be composition,

Representing vector $\psi \in \mathcal{H}$ by linear map

$$|\psi\rangle : \mathbb{C} \to \mathcal{H} :: 1 \mapsto \psi$$

Dirac notation is formally justified by letting

- $|\psi\rangle := \psi$ and called *KET* ,
- $\langle\psi| := \psi^\dagger$ and called *BRA*,
- concatenation be composition,

linear map	matrix	BRA-KET
$\psi^\dagger \circ \phi$	$\begin{pmatrix} \bar{c}_1 & \ldots & \bar{c}_m \end{pmatrix} \begin{pmatrix} c'_1 \\ \vdots \\ c'_m \end{pmatrix}$	$\langle\psi \mid \phi\rangle$

Representing vector $\psi \in \mathcal{H}$ by linear map

$$|\psi\rangle : \mathbb{C} \to \mathcal{H} :: 1 \mapsto \psi$$

Dirac notation is formally justified by letting

- $|\psi\rangle := \psi$ and called *KET* ,
- $\langle\psi| := \psi^\dagger$ and called *BRA*,
- concatenation be composition,

linear map	matrix	KET-BRA
$\psi \circ \psi^\dagger$	$\begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \begin{pmatrix} \bar{c}_1 & \ldots & \bar{c}_m \end{pmatrix}$	$\mathrm{P}_\psi := |\psi\rangle\langle\psi|$

QUANTUM TELEPORTATION
(towards a logical account)

1. The 1st qubit is in state

$$|\,\psi\rangle = c_0 \cdot |\,0\rangle + c_1 \cdot |\,1\rangle\,,$$

and the 2nd and 3rd one are in the Bell-state.

1. The 1st qubit is in state

$$|\,\psi\rangle = c_0 \cdot |\,0\rangle + c_1 \cdot |\,1\rangle\,,$$

and the 2nd and 3rd one are in the Bell-state.

2. Perform a measurement on 1st & 2nd qubit in basis

$$\{|00\rangle + |11\rangle\,,\ |00\rangle - |11\rangle\,,\ |01\rangle + |10\rangle\,,\ |01\rangle - |10\rangle\}\,.$$

1. The 1st qubit is in state

$$|\,\psi\rangle = c_0 \cdot |\,0\rangle + c_1 \cdot |\,1\rangle\,,$$

and the 2nd and 3rd one are in the Bell-state.

2. Perform a measurement on 1st & 2nd qubit in basis

$$\{|00\rangle + |11\rangle\,,\ |00\rangle - |11\rangle\,,\ |01\rangle + |10\rangle\,,\ |01\rangle - |10\rangle\}\,.$$

3. Perform corresponding matrix on the 3rd qubit:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$|Bell\rangle^\dagger = \langle Bell| = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$$

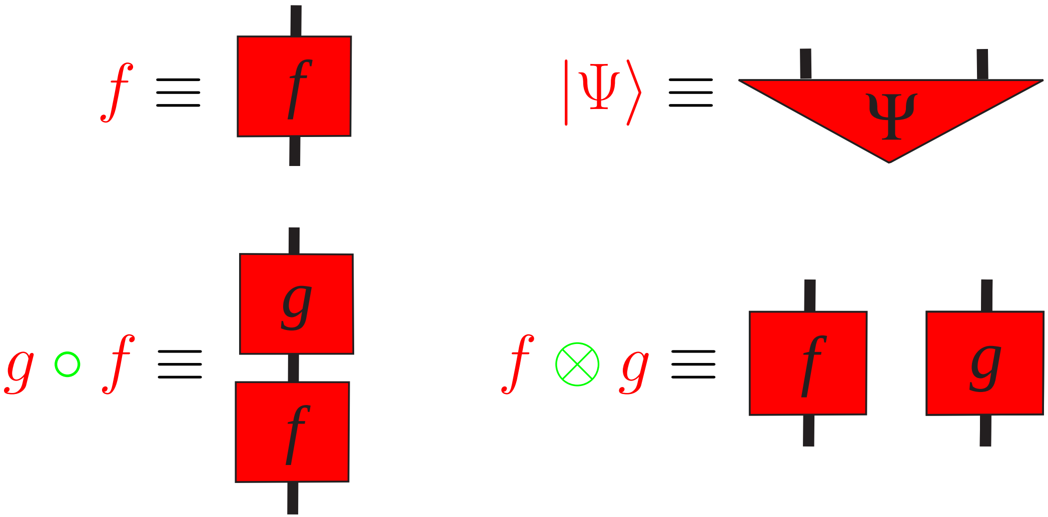
$$f \otimes g = \begin{pmatrix} f_{00}\begin{pmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{pmatrix} & f_{01}\begin{pmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{pmatrix} \\ f_{10}\begin{pmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{pmatrix} & f_{11}\begin{pmatrix} g_{00} & g_{01} \\ g_{10} & g_{11} \end{pmatrix} \end{pmatrix}$$

Lemma 0. $(f \otimes 1) \circ (1 \otimes g) = (1 \otimes g) \circ (f \otimes 1)$.

Lemma 1. $\forall\, |\Psi\rangle\ ,\ \exists\, f\ :\ |\Psi\rangle = (1 \otimes f) \circ |Bell\rangle$.

Lemma 2. $(f \otimes 1) \circ |Bell\rangle = (1 \otimes f^T) \circ |Bell\rangle$.

Lemma 3. $(\langle Bell| \otimes 1) \circ (1 \otimes |Bell\rangle)$.



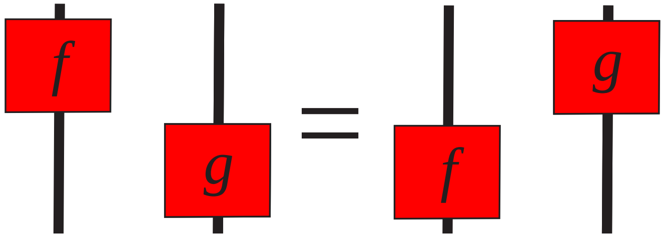
Lemma 0. $(f \otimes 1) \circ (1 \otimes g) = (1 \otimes g) \circ (f \otimes 1)$.

Lemma 1. $\forall \, |\Psi\rangle \, , \, \exists \, f \, : |\Psi\rangle = (1 \otimes f) \circ |Bell\rangle$.

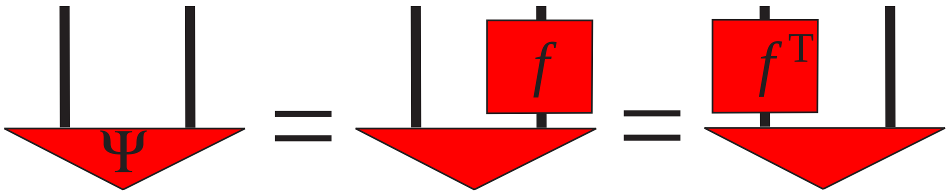
Lemma 2. $(f \otimes 1) \circ |Bell\rangle = (1 \otimes f^T) \circ |Bell\rangle$.

Lemma 3. $(\langle Bell| \otimes 1) \circ (1 \otimes |Bell\rangle) = 1$.

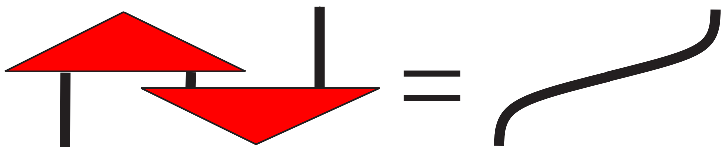
Lemma 0:

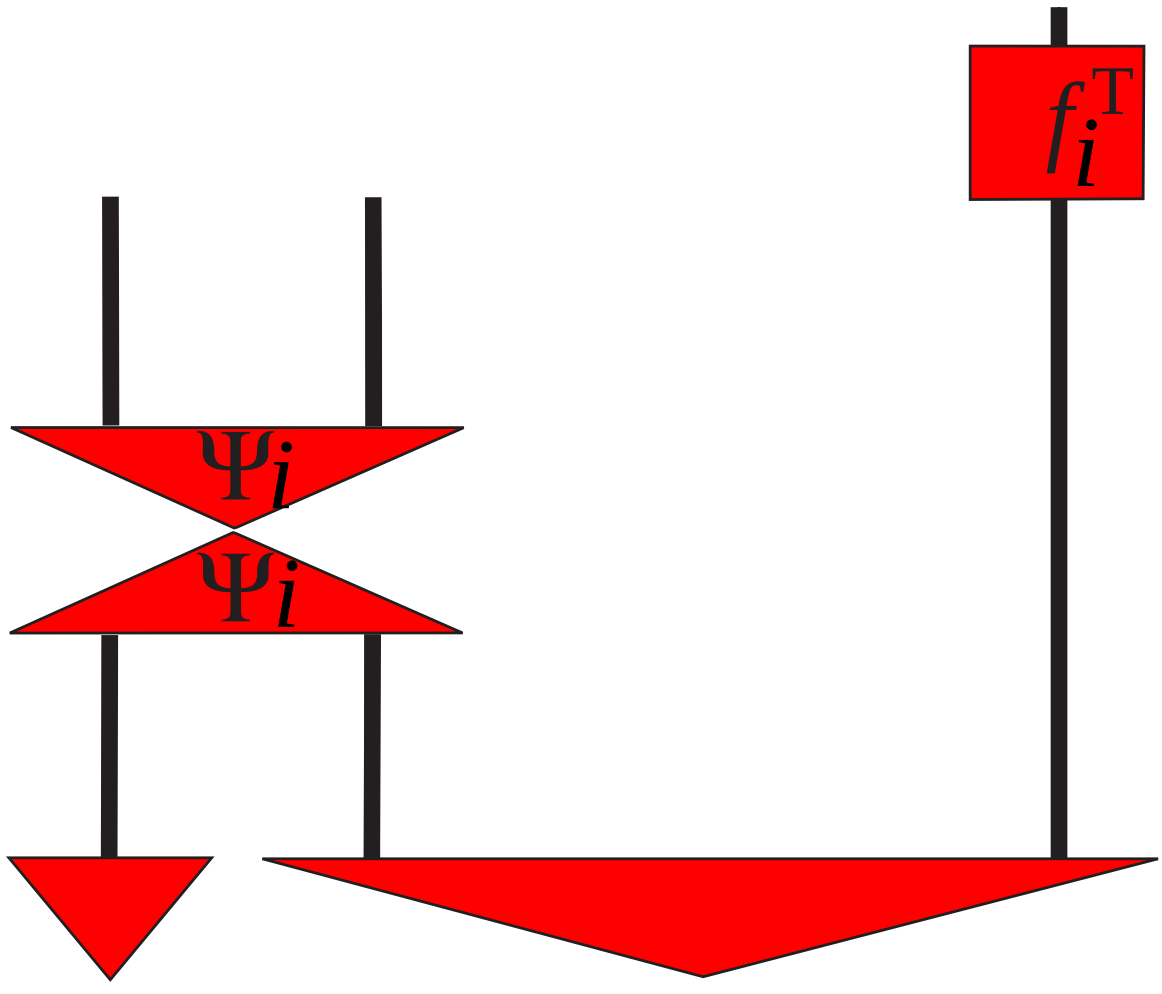


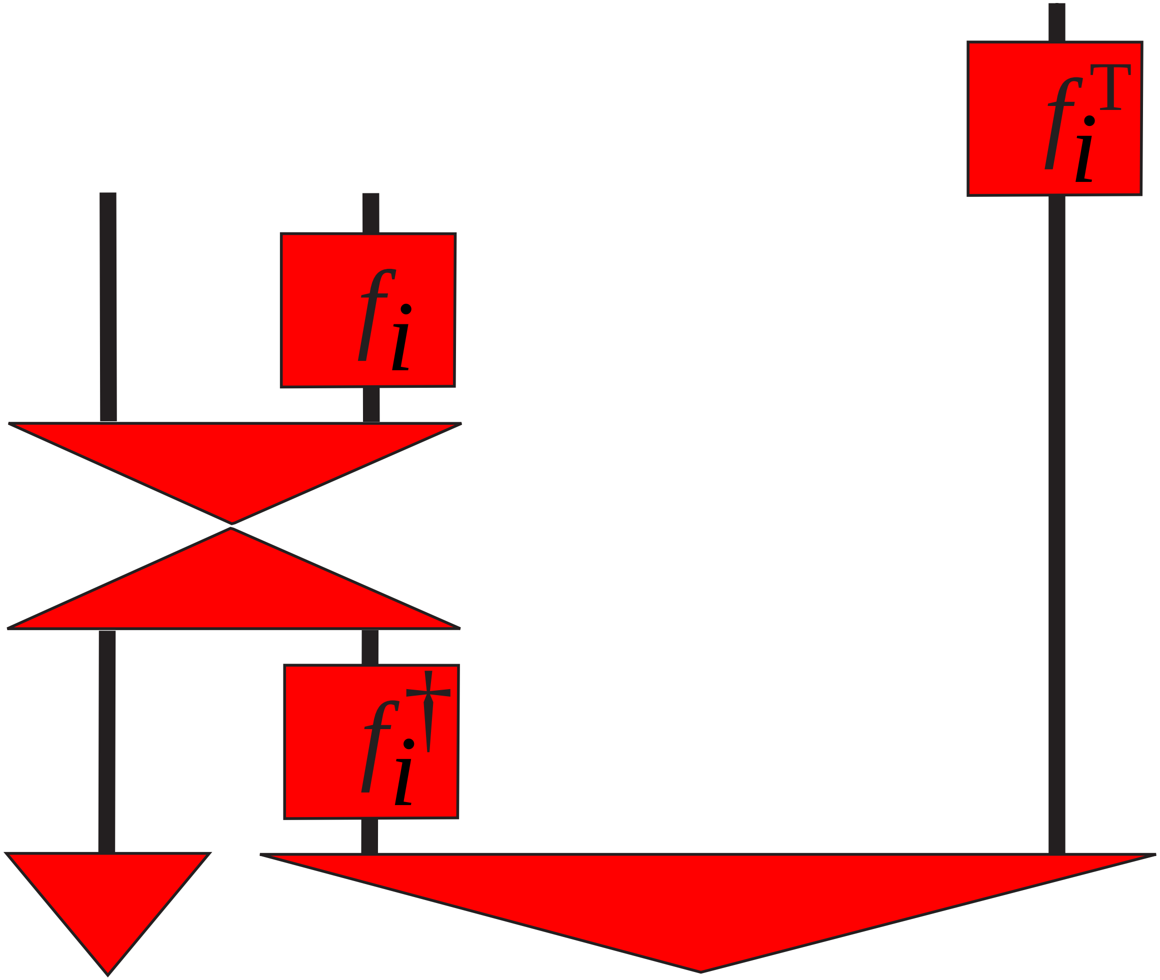
Lemma 1 & Lemma 2:

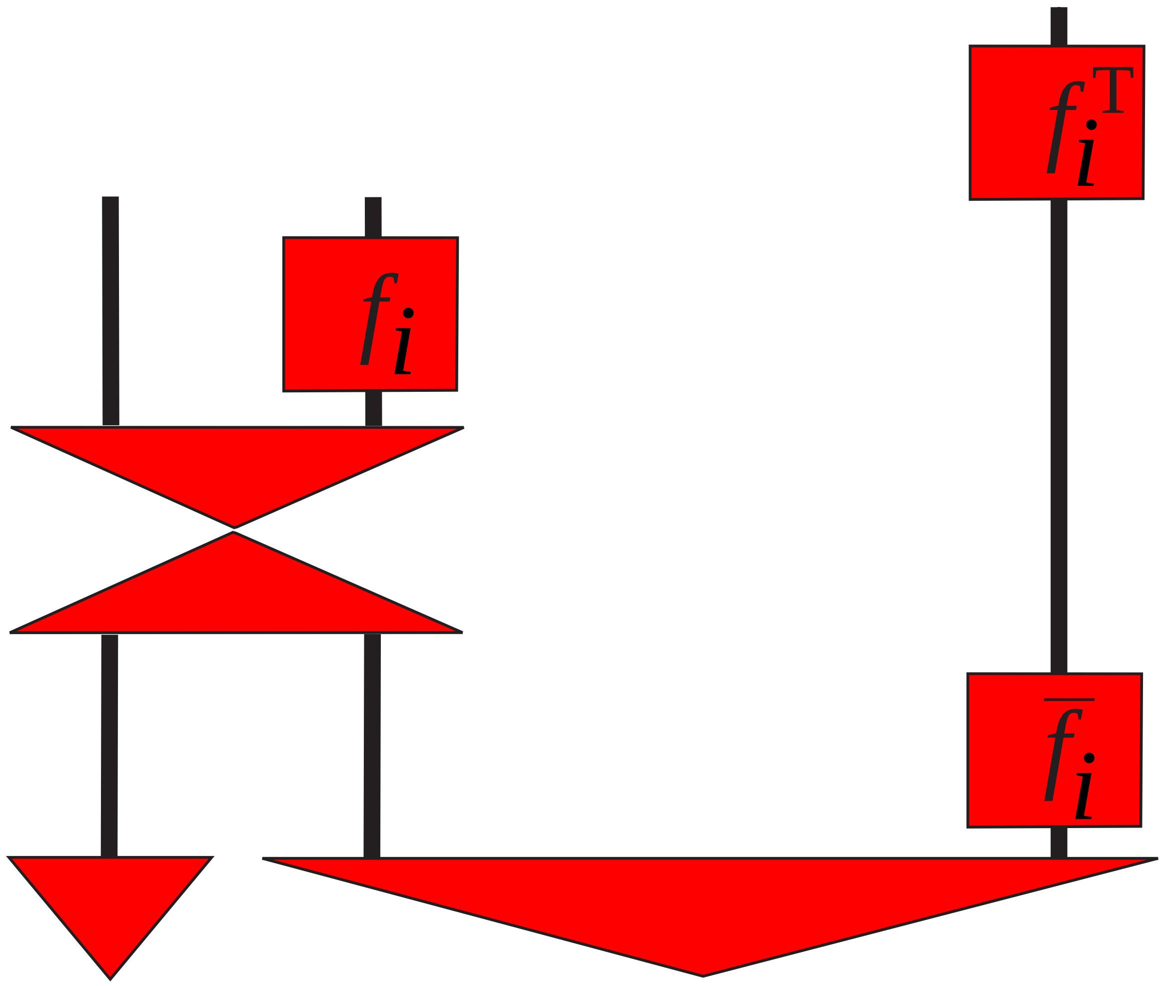


Lemma 3:

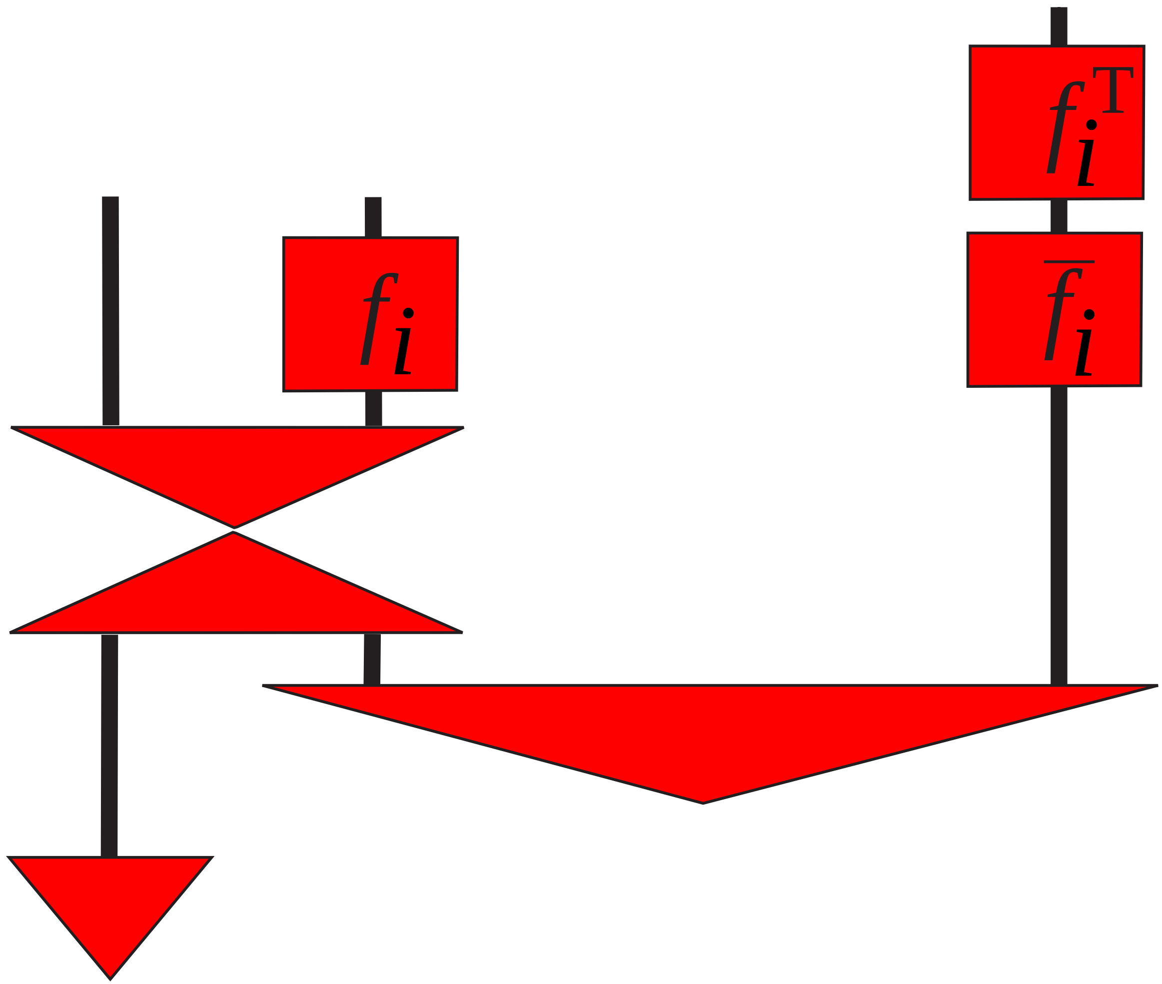



f_i^{T}
Ψ_i
Ψ_i

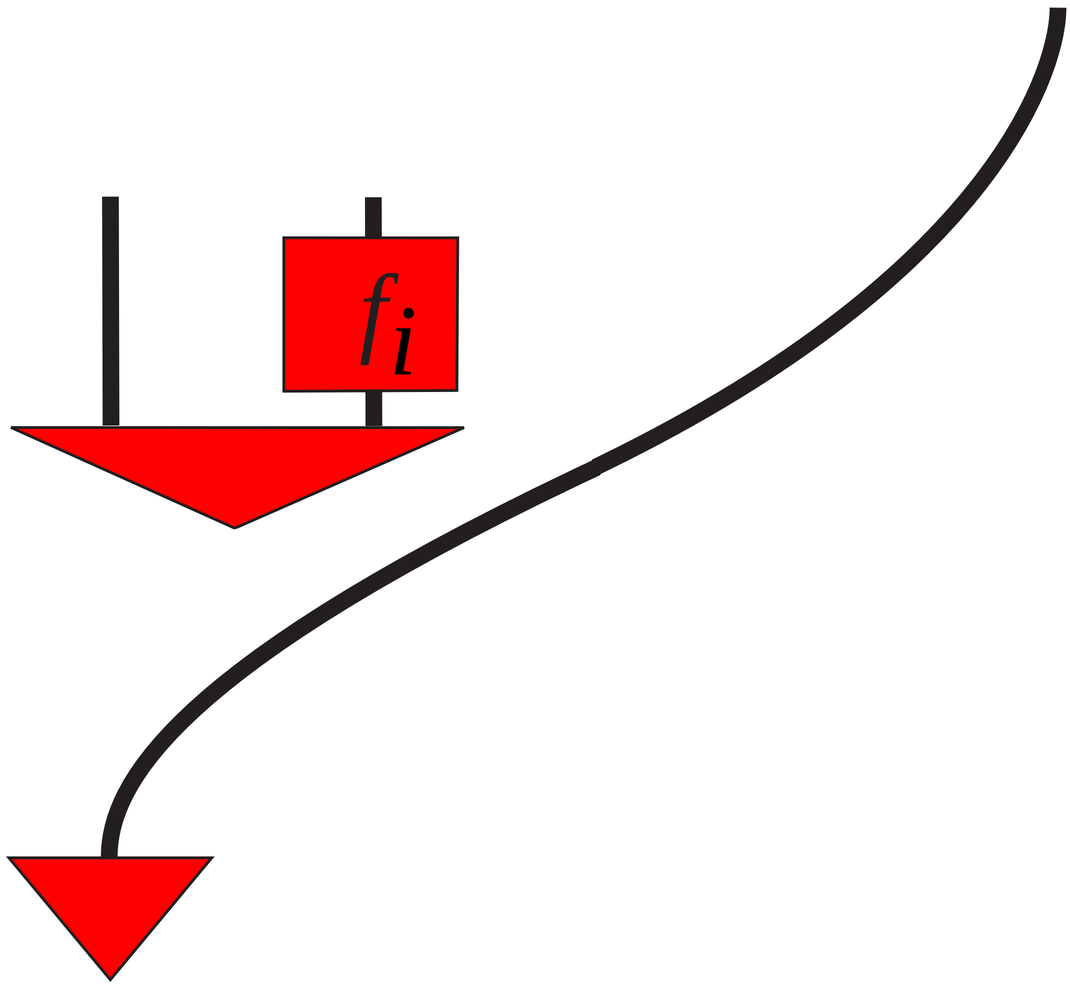

f_i
$f_i^\dagger$
f_i^{T}



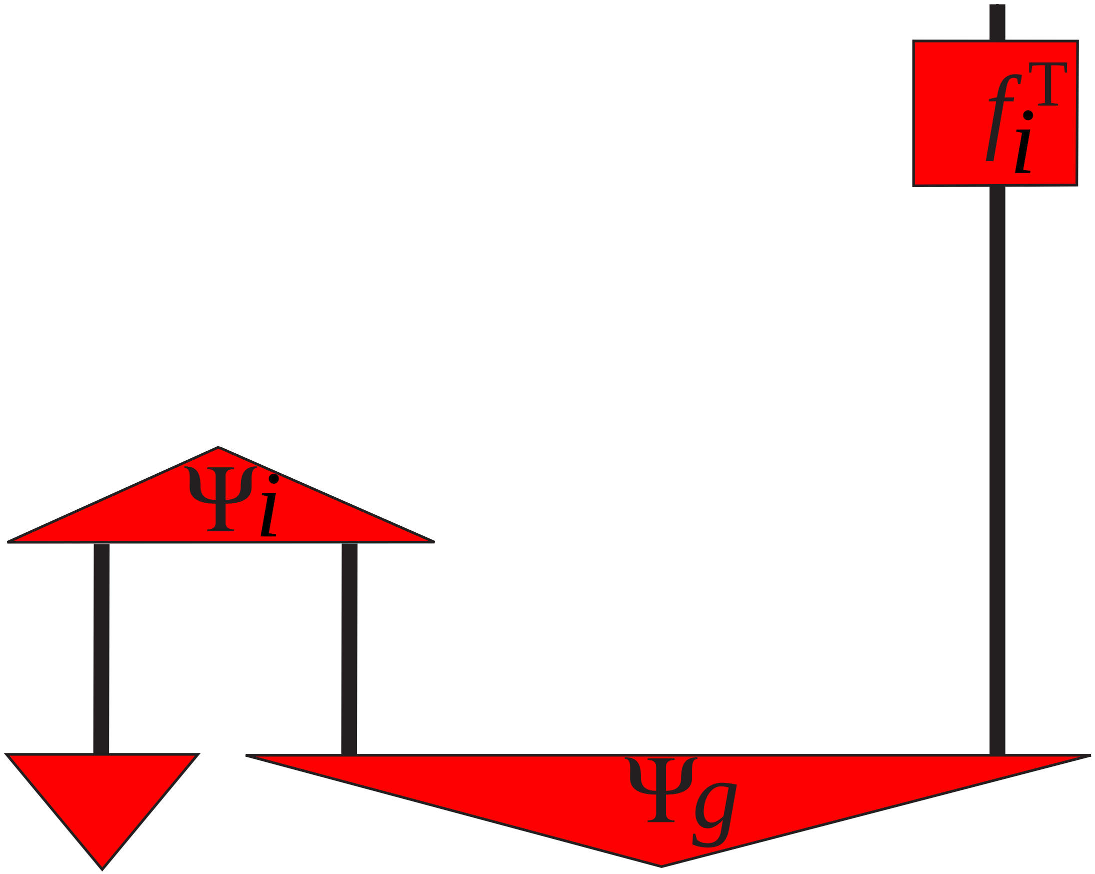
f_i
f_i^T
$\bar{f}_i$

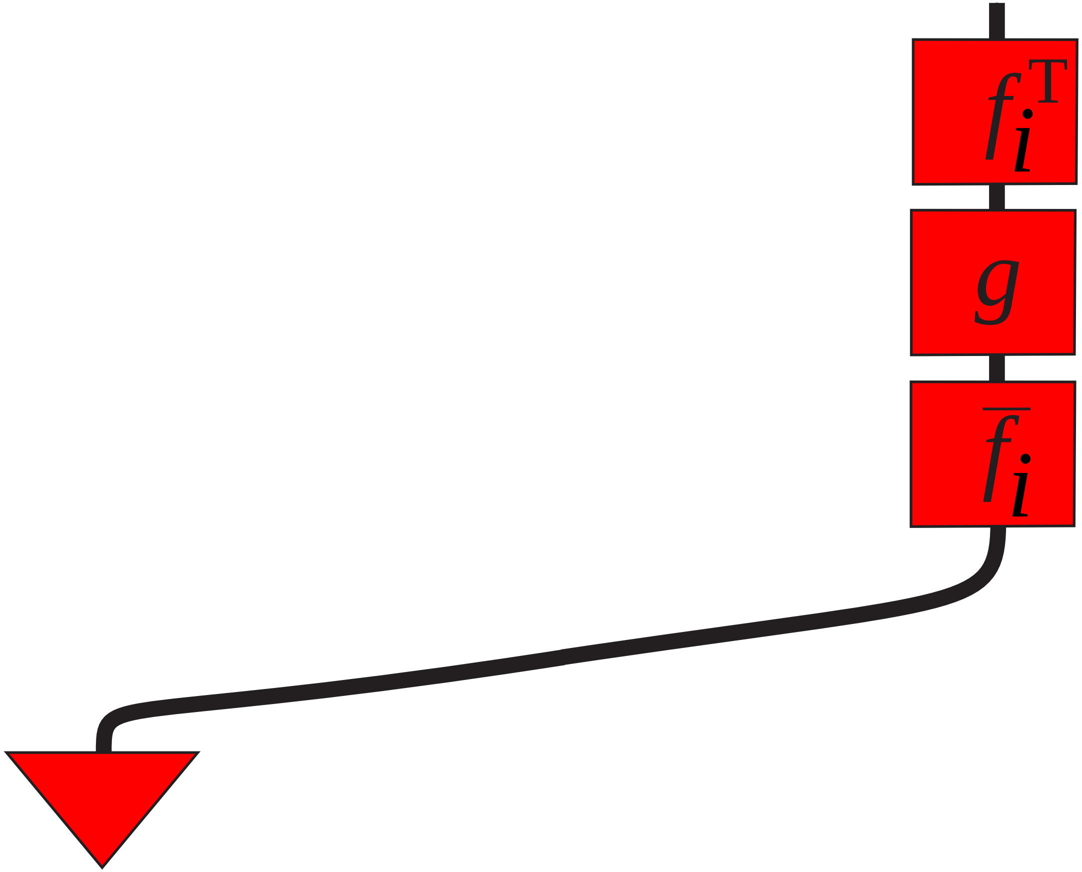


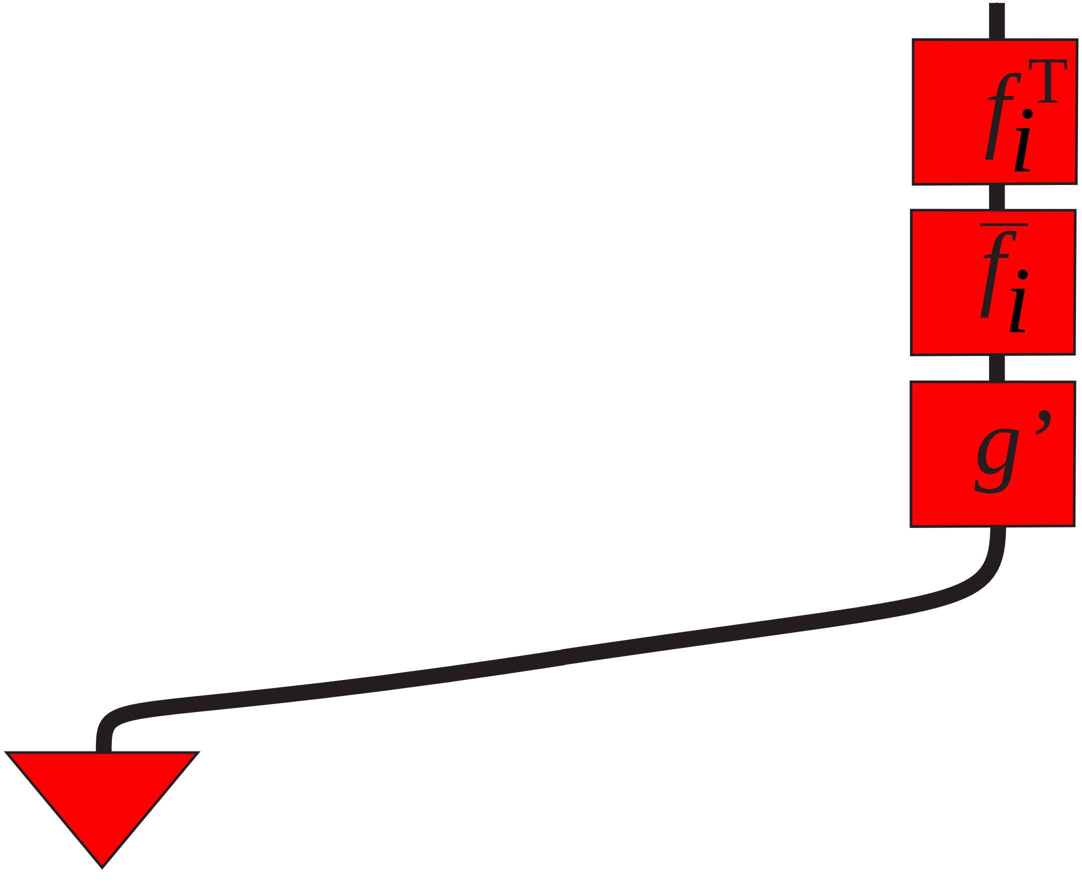
f_i
f_i^{T}
$\overline{f_i}$


f_i

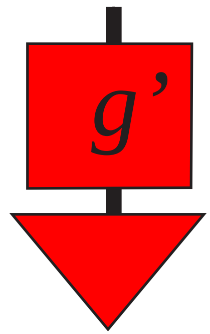
MEASUREMENT-BASED COMPUTATION


Ψ_i
f_i^{T}
Ψ_g


f_i^{T}
g
$\overline{f_i}$



f_i^{T}
$\overline{f}_i$
g'



Evaluating a function via the act of measurement

REFERENCES FOR THIS PART:

1. J. von Neumann (1932) *Mathematische Grundlagen der Quantenmechanik*. Springer-Verlag. (English translation, 1955) *Mathematical Foundations of Quantum Mechanics*. Princeton University Press.

2. P. A. M. Dirac (1947) *The Principles of Quantum Mechanics* (third edition). Oxford University Press.

3. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wooters (1993) *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Physical Review Letters **70**, 1895–1899.

4. M. Żukowski, A. Zeilinger, M. A. Horne and A. K. Ekert (1993) *'Event-ready-detectors' Bell experiment via entanglement swapping*. Physical Review Letters **71**, 4287–4290.

5. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger (1997) *Experimental Quantum Teleportation*. Nature **390**, 575–579.

6. D. Gottesman and I. L. Chuang (1999) *Quantum teleportation is a universal computational primitive*. Nature **402**, 390–393. arXiv:quant-ph/9908010

7. B. Coecke (2005) *Kindergarten quantum mechanics*. In: Quantum Theory: Reconsiderations of the Foundations III, pages 81–98. AIP Press. arXiv:quant-ph/0510032

8. `http://www.idquantique.com/`

9. `http://www.magiqtech.com/`

10. `http://www.smartquantum.com/`

Quantum information processing:
a new light on the Q-formalism and Q-foundations II

Quantum algorithms - categorical quantum logic

Bob Coecke - Oxford University Computing Laboratory

QUANTUM SPEED-UP

The quantum computational **circuit model**:

preparation $\rightsquigarrow$ unitary $\rightsquigarrow$ measurement

The quantum computational **circuit model**:

preparation $\rightsquigarrow$ unitary $\rightsquigarrow$ measurement

E.g. the **Deutsch-Jozsa algorithm**:

(p) $(|\,0\rangle + \ldots + |\,N\rangle) \otimes (|0\rangle - |1\rangle)$ with $N := 2^n - 1$

The quantum computational **circuit model**:

preparation $\rightsquigarrow$ unitary $\rightsquigarrow$ measurement

E.g. the **Deutsch-Jozsa algorithm**:

(p) $(|\,0\rangle + \ldots + |\,N\rangle) \otimes (|0\rangle - |1\rangle)$ with $N := 2^n - 1$

(u) $|\,i\,j\rangle \mapsto |\,i\,(f(i) + j)\rangle$ given $f : \mathbb{B}^n \longrightarrow \mathbb{B}$

The quantum computational **circuit model**:

preparation $\rightsquigarrow$ unitary $\rightsquigarrow$ measurement

E.g. the **Deutsch-Jozsa algorithm**:

(p) $(|\,0\rangle + \ldots + |\,N\rangle) \otimes (|0\rangle - |1\rangle)$ with $N := 2^n - 1$

(u) $|\,i\,j\rangle \mapsto |\,i\,(f(i) + j)\rangle$ given $f : \mathbb{B}^n \longrightarrow \mathbb{B}$

(m) measure 1st n qubits in basis $\{|\,0\rangle + \ldots + |\,N\rangle, \ldots\}$

The quantum computational **circuit model**:

preparation $\rightsquigarrow$ unitary $\rightsquigarrow$ measurement

E.g. the **Deutsch-Jozsa algorithm**:

(p) $(|\,0\rangle + \ldots + |\,N\rangle) \otimes (|0\rangle - |1\rangle)$ with $N := 2^n - 1$

(u) $|\,i\,j\rangle \mapsto |\,i\,(f(i) + j)\rangle$ given $f : \mathbb{B}^n \longrightarrow \mathbb{B}$

(m) measure 1st n qubits in basis $\{|\,0\rangle + \ldots + |\,N\rangle, \ldots\}$

Parallelism: 1 measurement $\Rightarrow$ global property of f.

Step 1: *encode* $f : \mathbb{B}^n \rightarrow \mathbb{B}$ *as a (reversible) unitary:*

$$U_f :: |\, i\, j\rangle \mapsto |\, i\, (f(i) + j)\rangle$$

Step 1: *encode* $f : \mathbb{B}^n \to \mathbb{B}$ *as a (reversible) unitary:*

$$U_f :: |\, i\; j\rangle \mapsto |\, i\, (f(i) + j)\rangle$$

Step 2: *apply* f *to all the inputs at once:*

$$U_f(|\,0\rangle + \ldots + |\,N\rangle, |0\rangle) = |\,i\; f(0)\rangle + \ldots + |\,N\; f(N)\rangle$$

Step 1: *encode* $f : \mathbb{B}^n \to \mathbb{B}$ *as a (reversible) unitary:*

$$U_f :: |\, i\, j\rangle \mapsto |\, i\, (f(i) + j)\rangle$$

Step 2: *apply* f *to all the inputs at once:*

$$U_f(|\, 0\rangle + \ldots + |\, N\rangle, |0\rangle) = |\, i\, f(0)\rangle + \ldots + |\, N\, f(N)\rangle$$

Step 3: *observe that what you aimed for fails since measuring exposes one term and destroys all others.*

Step 1: *encode* $f : \mathbb{B}^n \longrightarrow \mathbb{B}$ *as a (reversible) unitary:*

$$U_f :: |\, i\, j\rangle \mapsto |\, i\, (f(i) + j)\rangle$$

Step 2: *apply* f *to all the inputs at once:*

$$U_f(|\,0\rangle + \ldots + |\,N\rangle, |0\rangle) = |\,i\, f(0)\rangle + \ldots + |\,N\, f(N)\rangle$$

Step 3: *observe that what you aimed for fails since measuring exposes one term and destroys all others.*

Step 4: *be really really clever by now doing:*

$$U_f(|\,0\rangle + \ldots + |\,N\rangle, |0\rangle - |1\rangle)$$

Step 1: *encode* $f : \mathbb{B}^n \to \mathbb{B}$ *as a (reversible) unitary:*

$$U_f :: |\, i\, j\rangle \mapsto |\, i\, (f(i) + j)\rangle$$

Step 2: *apply* f *to all the inputs at once:*

$$U_f(|\, 0\rangle + \ldots + |\, N\rangle, |0\rangle) = |\, i\, f(0)\rangle + \ldots + |\, N\, f(N)\rangle$$

Step 3: *observe that what you aimed for fails since measuring exposes one term and destroys all others.*

Step 4: *be really really clever by now doing:*

$$U_f(|\, 0\rangle + \ldots + |\, N\rangle, |0\rangle - |1\rangle)$$

Step 5: *then measure 1st* n *qubits in basis:*

$$\{|\, 0\rangle + \ldots + |\, N\rangle, \ldots\}$$

Indeed, one computes that:

$$U_f\left(\left(\sum_i |\, i\rangle\right) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = \left(\sum_i (-1)^{f(i)} |\, i\rangle\right) \otimes (|0\rangle - |1\rangle)$$

Indeed, one computes that:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = (\sum_i (-1)^{f(i)} |\, i\rangle) \otimes (|0\rangle - |1\rangle)$$

so for f constant:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = \pm(\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)$$

Indeed, one computes that:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = (\sum_i (-1)^{f(i)} |\, i\rangle) \otimes (|0\rangle - |1\rangle)$$

so for f constant:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = \pm(\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)$$

and that

$$\left\langle (\sum_i (-1)^{f(i)} |\, i\rangle) \otimes (|0\rangle - |1\rangle) \middle\| (\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle) \right\rangle = 0$$

Indeed, one computes that:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = (\sum_i (-1)^{f(i)} |\, i\rangle) \otimes (|0\rangle - |1\rangle)$$

so for f constant:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = \pm(\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)$$

and that

$$\left\langle \sum_i (-1)^{f(i)} |\, i\rangle \middle| \sum_i |\, i\rangle \right\rangle = 0$$

Indeed, one computes that:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = (\sum_i (-1)^{f(i)} |\, i\rangle) \otimes (|0\rangle - |1\rangle)$$

so for f constant:

$$U_f\left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)\right) = \pm(\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)$$

and that

$$\sum_i (-1)^{f(i)} = 0$$

Indeed, one computes that:

$$U_f \left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle) \right) = (\sum_i (-1)^{f(i)} |\, i\rangle) \otimes (|0\rangle - |1\rangle)$$

so for f constant:

$$U_f \left((\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle) \right) = \pm (\sum_i |\, i\rangle) \otimes (|\, 0\rangle - |\, 1\rangle)$$

and that

$$\sum_i (-1)^{f(i)} = 0$$

whenever f is 'balanced'.

Indeed, one computes that:

$$U_f\left((\sum_i |\,i\rangle) \otimes (|\,0\rangle - |\,1\rangle)\right) = (\sum_i (-1)^{f(i)} |\,i\rangle) \otimes (|0\rangle - |1\rangle)$$

so for f constant:

$$U_f\left((\sum_i |\,i\rangle) \otimes (|\,0\rangle - |\,1\rangle)\right) = \pm(\sum_i |\,i\rangle) \otimes (|\,0\rangle - |\,1\rangle)$$

and that

$$\sum_i (-1)^{f(i)} = 0$$

whenever f is 'balanced'.

In one go we distinguish constant from balanced functions, ...

Indeed, one computes that:

$$U_f\left((\sum_i |\,i\rangle)\otimes(|\,0\rangle - |\,1\rangle)\right) = (\sum_i (-1)^{f(i)}|\,i\rangle)\otimes(|0\rangle - |1\rangle)$$

so for f constant:

$$U_f\left((\sum_i |\,i\rangle)\otimes(|\,0\rangle - |\,1\rangle)\right) = \pm(\sum_i |\,i\rangle)\otimes(|\,0\rangle - |\,1\rangle)$$

and that

$$\sum_i (-1)^{f(i)} = 0$$

whenever f is 'balanced'.

In one go we distinguish constant from balanced functions, ... so what?

Why quantum computing?

Contra: The Deutsch-Jozsa algorithm is useless.

Why quantum computing?

Contra: The Deutsch-Jozsa algorithm is useless.

Pro: Shor's 'very similar' factoring algorithm is exponentially faster than faster than know classical one.

Why quantum computing?

Contra: The Deutsch-Jozsa algorithm is useless.

Pro: Shor's 'very similar' factoring algorithm is exponentially faster than faster than know classical one.

Contra: There aren't many other quantum algorithms nor might there ever be a device to run them on.

Why quantum computing?

Contra: The Deutsch-Jozsa algorithm is useless.

Pro: Shor's 'very similar' factoring algorithm is exponentially faster than faster than know classical one.

Contra: There aren't many other quantum algorithms nor might there ever be a device to run them on.

Pro: Quantum computing is also about:

- Communication and cryptographic protocols.
- The fresh perspective yields in new physics.
- Fresh data and concepts for quantum foundations.
- Fresh challenges for the quantum formalism.

The quantum formalism

[von Neumann 1932] Formalized quantum mechanics in “Mathematische Grundlagen der Quantenmechanik”

The quantum formalism

[von Neumann 1932] Formalized quantum mechanics in "Mathematische Grundlagen der Quantenmechanik"

[von Neumann to Birkhoff 1935] "I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more." (sic)

The quantum formalism

[von Neumann 1932] Formalized quantum mechanics in "Mathematische Grundlagen der Quantenmechanik"

[von Neumann to Birkhoff 1935] "I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more." (sic)

[Birkhoff and von Neumann 1936] "The LOGIC of Quantum Mechanics", *Annals of Mathematics*.

The quantum formalism

[von Neumann 1932] Formalized quantum mechanics in "Mathematische Grundlagen der Quantenmechanik"

[von Neumann to Birkhoff 1935] "I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more." (sic)

[Birkhoff and von Neumann 1936] "The LOGIC of Quantum Mechanics", *Annals of Mathematics*.

[1936 – 2000] many attempts followed, ...

The quantum formalism

[von Neumann 1932] Formalized quantum mechanics in “Mathematische Grundlagen der Quantenmechanik”

[von Neumann to Birkhoff 1935] “I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more.” (sic)

[Birkhoff and von Neumann 1936] “The LOGIC of Quantum Mechanics”, *Annals of Mathematics*.

[1936 – 2000] many attempts followed, ... and FAILED.

Meanwhile, new physical phenomena :

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical insights:

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical insights:

— tensor product key to quantum theory —

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical insights:

— tensor product key to quantum theory —

Meanwhile, new logic:

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical insights:

— tensor product key to quantum theory —

Meanwhile, new logic:

— linear logics & interaction logic —

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical insights:

— tensor product key to quantum theory —

Meanwhile, new logic:

— linear logics & interaction logic —

Meanwhile, new algebra:

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical insights:

— tensor product key to quantum theory —

Meanwhile, new logic:

— linear logics & interaction logic —

Meanwhile, new algebra:

— monoidal categories —

Meanwhile, new physical phenomena :

— quantum informatic protocols —

Meanwhile, new physical insights:

— tensor product key to quantum theory —

Meanwhile, new logic:

— linear logics & interaction logic —

Meanwhile, new algebra:

— monoidal categories $\equiv$ pictures —

WHY MONOIDAL CATEGORIES?

BECAUSE THEY ARE EVERYWHERE!

... let’s start with food, ...

1. Let A be a raw potato.

1. Let A be a raw potato.

A admits many *states* e.g. dirty, clean, skinned, ...

1. Let A be a raw potato.

A admits many *states* e.g. dirty, clean, skinned, ...

2. We want to *process* A into cooked potato B.

B admits many *states* e.g. boiled, fried, deep fried, baked with skin, baked without skin, ...

1. Let A be a raw potato.

A admits many *states* e.g. dirty, clean, skinned, ...

2. We want to *process* A into cooked potato B.

B admits many *states* e.g. boiled, fried, deep fried, baked with skin, baked without skin, ... Let

$$A \xrightarrow{f} B \qquad A \xrightarrow{f'} B \qquad A \xrightarrow{f''} B$$

be boiling, frying, baking.

1. Let A be a raw potato.

A admits many *states* e.g. dirty, clean, skinned, ...

2. We want to *process* A into cooked potato B.

B admits many *states* e.g. boiled, fried, deep fried, baked with skin, baked without skin, ... Let

$$A \xrightarrow{f} B \qquad A \xrightarrow{f'} B \qquad A \xrightarrow{f''} B$$

be boiling, frying, baking. *States* are *processes*

$$\mathrm{I} := \text{unspecified} \xrightarrow{\psi} A.$$

3. Let

$$A \xrightarrow{g \circ f} C$$

be the *composite process* of first boiling $A \xrightarrow{f} B$ and then salting $B \xrightarrow{g} C$.

3. Let

$$A \xrightarrow{g \circ f} C$$

be the *composite process* of first boiling $A \xrightarrow{f} B$ and then salting $B \xrightarrow{g} C$. Let

$$X \xrightarrow{\mathbf{1}_X} X$$

be doing nothing. We have $\mathbf{1}_Y \circ \xi = \xi \circ \mathbf{1}_X = \xi$.

4. Let $A \otimes D$ be potato A and carrot D

4. Let $A \otimes D$ be potato A and carrot D and let

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E$$

be boiling potato while frying carrot.

4. Let $A \otimes D$ be potato A and carrot D and let

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E$$

be boiling potato while frying carrot. Let

$$C \otimes F \xrightarrow{x} M$$

be mashing spice-cook-potato and spice-cook-carrot.

5. Total *process*:

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E \xrightarrow{g \otimes k} C \otimes F \xrightarrow{x} M = A \otimes D \xrightarrow{x \circ (g \otimes k) \circ (f \otimes h)} M.$$

5. Total *process*:

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E \xrightarrow{g \otimes k} C \otimes F \xrightarrow{x} M = A \otimes D \xrightarrow{x \circ (g \otimes k) \circ (f \otimes h)} M.$$

6. *Recipe* = *composition structure* on *processes*.

5. Total *process*:

$$A \otimes D \xrightarrow{f\otimes h} B \otimes E \xrightarrow{g\otimes k} C \otimes F \xrightarrow{x} M = A \otimes D \xrightarrow{x\circ(g\otimes k)\circ(f\otimes h)} M\,.$$

6. *Recipe* = *composition structure* on *processes*.

7. *Law*:

5. Total *process*:

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E \xrightarrow{g \otimes k} C \otimes F \xrightarrow{x} M = A \otimes D \xrightarrow{x \circ (g \otimes k) \circ (f \otimes h)} M\,.$$

6. *Recipe* = *composition structure* on *processes*.

7. *Law governing recipes*:

$$(\mathbf{1}_B \otimes g) \circ (f \otimes \mathbf{1}_C) = (f \otimes \mathbf{1}_D) \circ (\mathbf{1}_A \otimes g)$$

5. Total *process*:

$$A \otimes D \xrightarrow{f \otimes h} B \otimes E \xrightarrow{g \otimes k} C \otimes F \xrightarrow{x} M = A \otimes D \xrightarrow{x \circ (g \otimes k) \circ (f \otimes h)} M\,.$$

6. *Recipe* = *composition structure* on *processes*.

7. *Law governing recipes*:

$$(\mathbf{1}_B \otimes g) \circ (f \otimes \mathbf{1}_C) = (f \otimes \mathbf{1}_D) \circ (\mathbf{1}_A \otimes g)$$

i.e.

boil potato then fry carrot = fry carrot then boil potato

7. A more general law on recipes:

$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h)$$

i.e.

boil pot then salt pot, while, fry car then pepper car

$$||$$

boil pot while fry car, then, salt pot while pepper car

Very successful in **proof theory** and **programming**:

proof theory	**programming**
Propositions	Data Types
Proofs	Programs

BLUE = systems

Red = processes

Very successful in **proof theory** and **programming**:

proof theory	**programming**
Propositions	Data Types
Proofs	Programs

BLUE = systems

Red = processes

but also applies to:

biology	**chemistry**	**physics**
Biological syst.	Chemical syst	Physical syst
Biological proc	Chemical proc	Physical proc

— *(physical) data in monoidal category* —

Systems:

$$A \qquad B \qquad C$$

Processes:

$$A \xrightarrow{f} A \qquad A \xrightarrow{g} B \qquad B \xrightarrow{h} C$$

Compound systems:

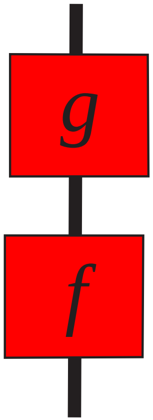
$$A \otimes B \qquad \mathrm{I} \qquad A \otimes C \xrightarrow{f \otimes g} B \otimes D$$

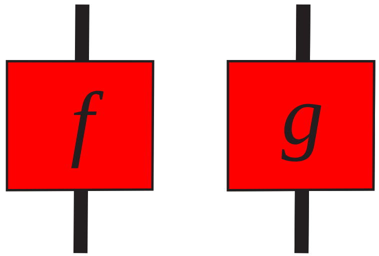
Temporal composition:

$$A \xrightarrow{h \circ g} C \; := \; A \xrightarrow{g} B \xrightarrow{h} C \qquad A \xrightarrow{1_A} A$$

— *graphical notation* —

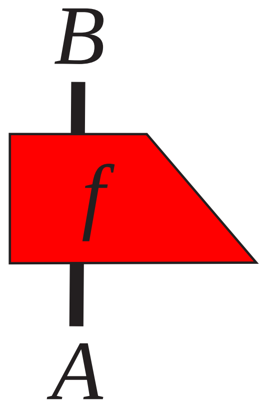
— *graphical notation* —

$g \circ f \equiv$ 

$f \otimes g \equiv$ 

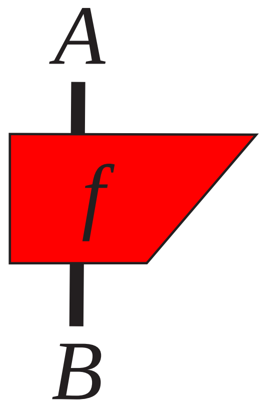
— *graphical notation* —

$$f \; : A \longrightarrow B$$



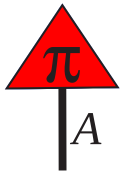
— *graphical notation* —

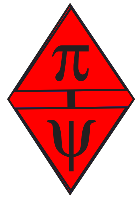
$$f^{\dagger} : B \to A$$



— *graphical notation* —

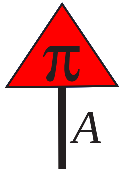
$\psi : \mathrm{I} \longrightarrow A$ $\qquad$ $\pi : A \longrightarrow \mathrm{I}$ $\qquad$ $\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

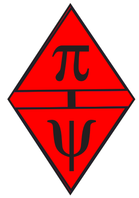




— *graphical notation* —

$\psi : \mathrm{I} \longrightarrow A$ $\qquad$ $\pi : A \longrightarrow \mathrm{I}$ $\qquad$ $\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

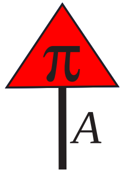


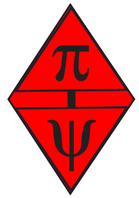


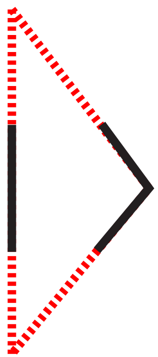
$$| \quad \rangle$$

— *graphical notation* —

$\psi : \mathrm{I} \longrightarrow A$ $\qquad$ $\pi : A \longrightarrow \mathrm{I}$ $\qquad$ $\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

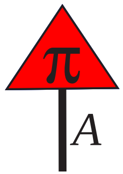


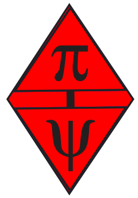


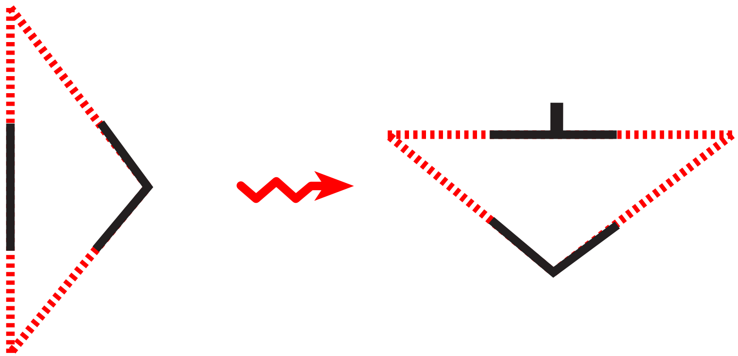


— *graphical notation* —

$\psi : \mathrm{I} \longrightarrow A$ $\qquad$ $\pi : A \longrightarrow \mathrm{I}$ $\qquad$ $\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

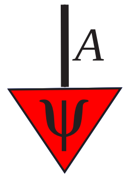




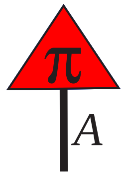


— *graphical notation* —

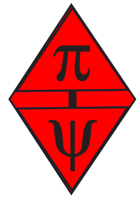
$\psi : \mathrm{I} \longrightarrow A$



$\pi : A \longrightarrow \mathrm{I}$



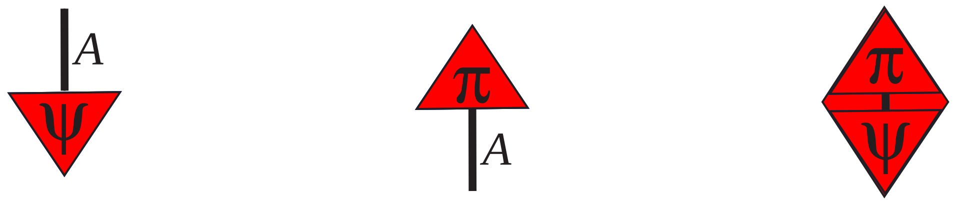
$\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

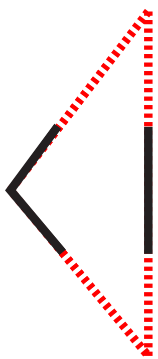


$\langle \; |$

— *graphical notation* —

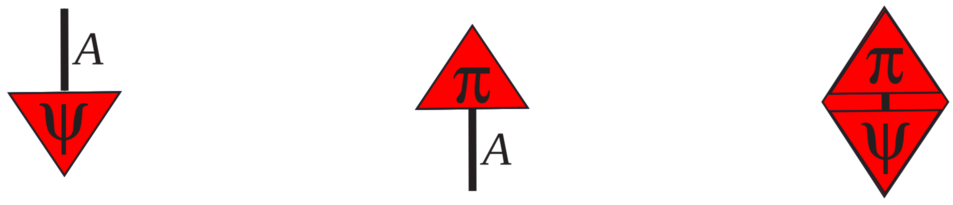
$\psi : \mathrm{I} \longrightarrow A$ $\qquad$ $\pi : A \longrightarrow \mathrm{I}$ $\qquad$ $\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

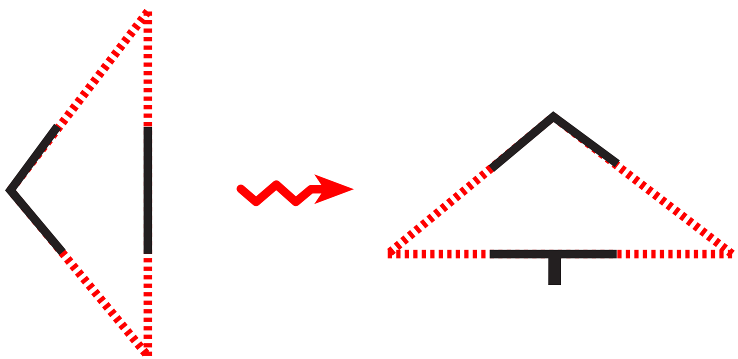




— *graphical notation* —

$\psi : \mathrm{I} \longrightarrow A$ $\pi : A \longrightarrow \mathrm{I}$ $\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

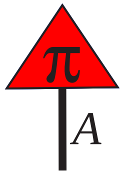




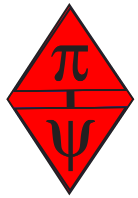
— *graphical notation* —

$\psi : \mathrm{I} \longrightarrow A$

$\pi : A \longrightarrow \mathrm{I}$



$\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

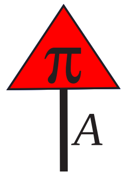


$$\langle \quad | \quad \rangle$$

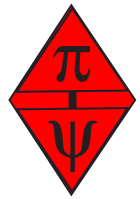
— *graphical notation* —

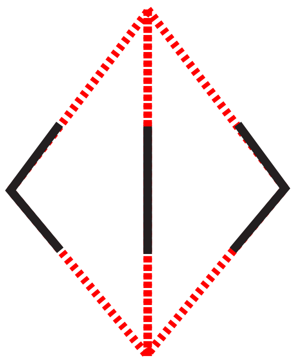
$\psi : \mathrm{I} \longrightarrow A$

$\pi : A \longrightarrow \mathrm{I}$



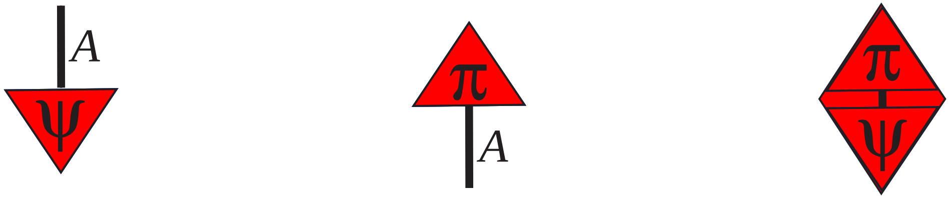
$\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$

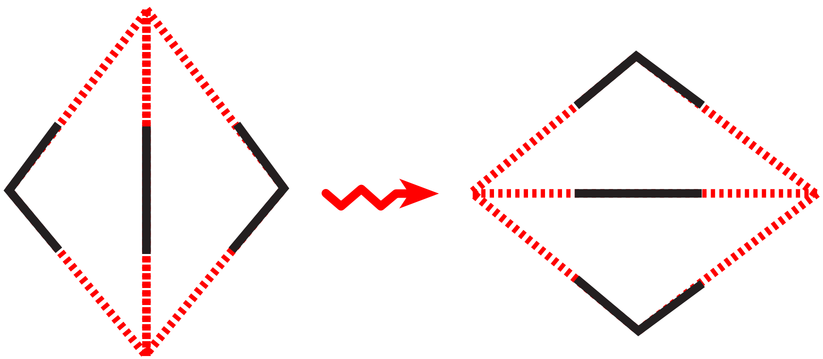




— *graphical notation* —

$\psi : \mathrm{I} \longrightarrow A$ $\qquad$ $\pi : A \longrightarrow \mathrm{I}$ $\qquad$ $\pi \circ \psi : \mathrm{I} \longrightarrow \mathrm{I}$





— *graphical notation* —

Thm. [Joyal & Street ’91] ***An equational statement between expressions in symmetric monoidal categorical language holds if and only if it is derivable in the graphical notation via homotopy*.**

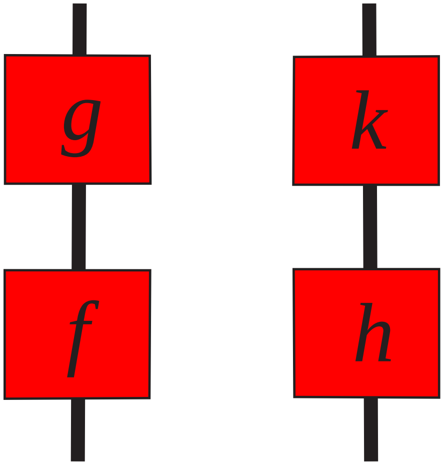
— *merely a new notation?* —

— *merely a new notation?* —

$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h)$$

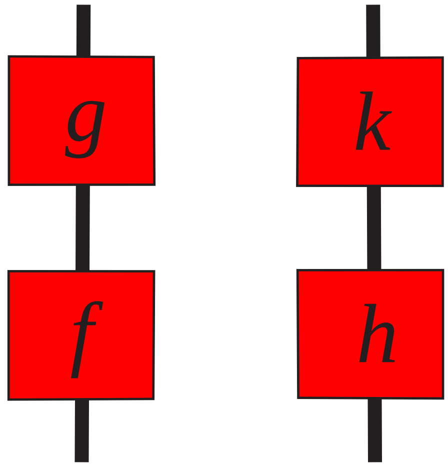
— ***merely a new notation?*** —

$$(g \circ f) \otimes (k \circ h)$$



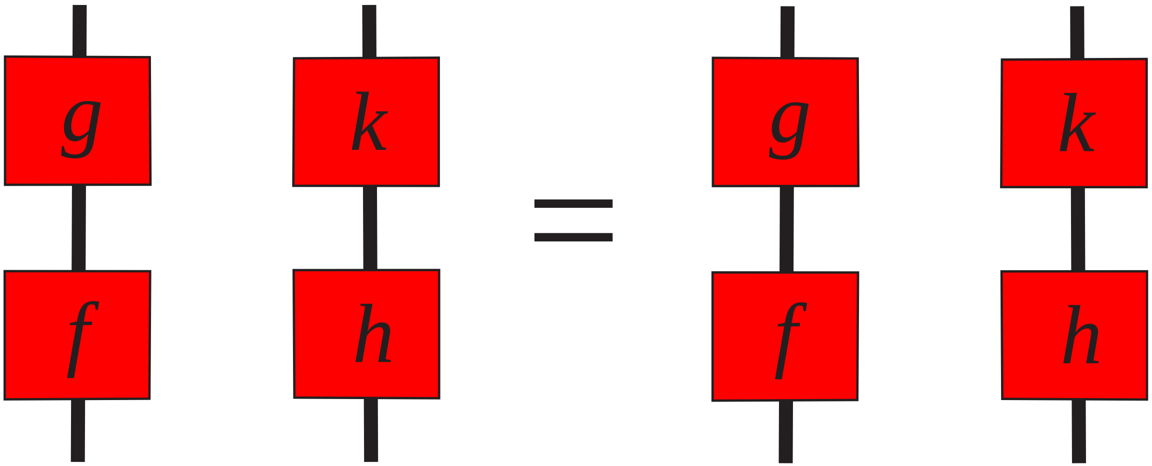
— ***merely a new notation?*** —

$$(g \otimes k) \circ (f \otimes h)$$

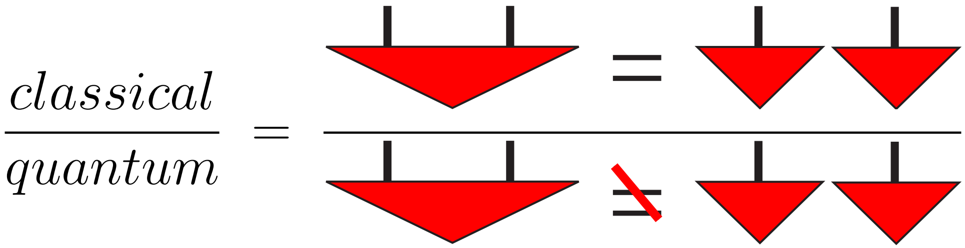


— *merely a new notation?* —

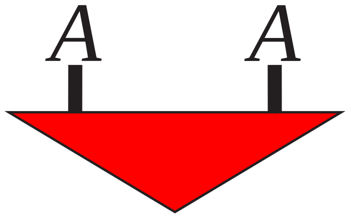
$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h)$$

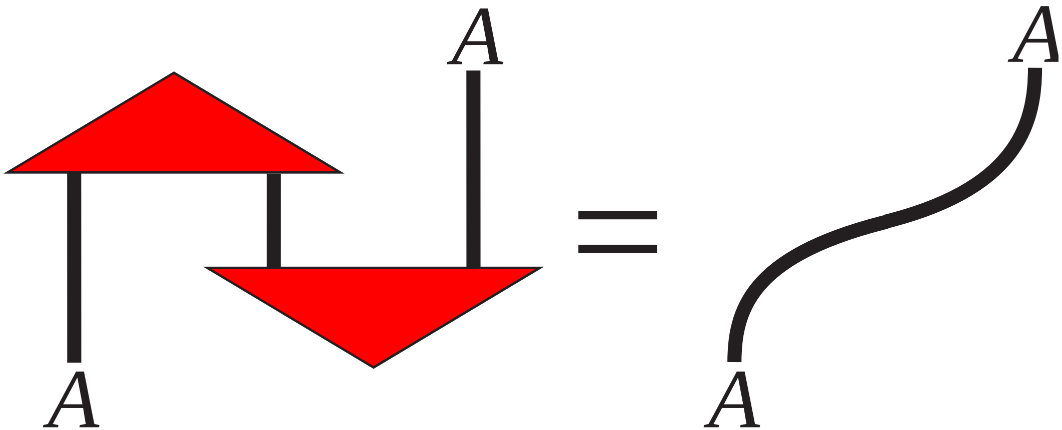


— *(pure) Classical vs. Quantum* —



— *quantum-like* —



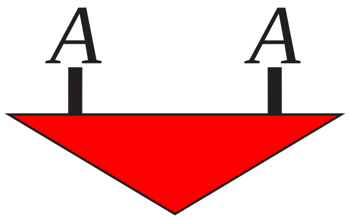


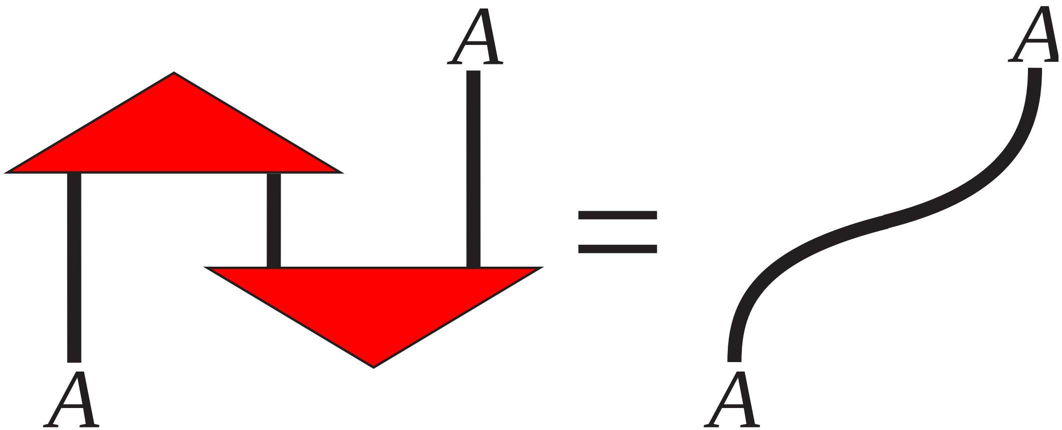
— *quantum-like* —

$$(A\,,\eta : \mathrm{I} \longrightarrow A \otimes A)$$

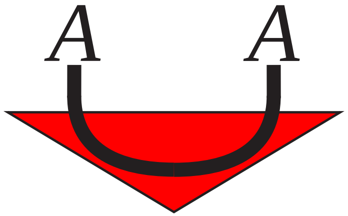
$$\begin{tikzcd}
A & \mathrm{I} \otimes A \arrow[l, "\simeq"'] & (A \otimes A) \otimes A \arrow[l, "\eta^\dagger \otimes 1_A"'] \\
A \arrow[u, "1_A"] \arrow[r, "\simeq"'] & A \otimes \mathrm{I} \arrow[r, "1_A \otimes \eta"'] & A \otimes (A \otimes A) \arrow[u, "\simeq"']
\end{tikzcd}$$

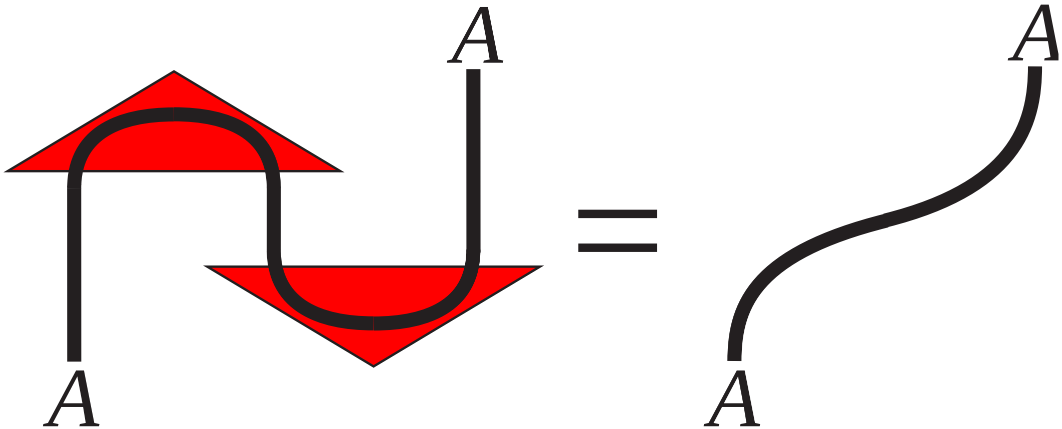
— *quantum-like* —



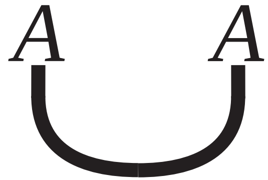


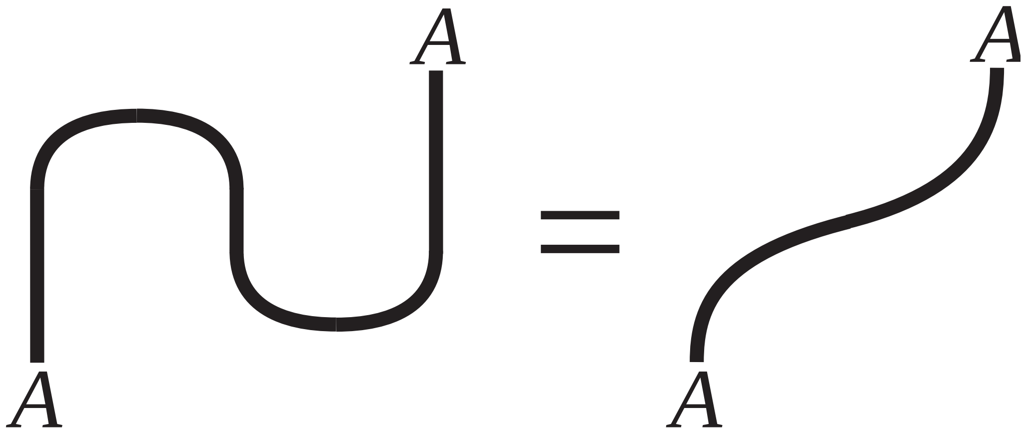
— *quantum-like* —



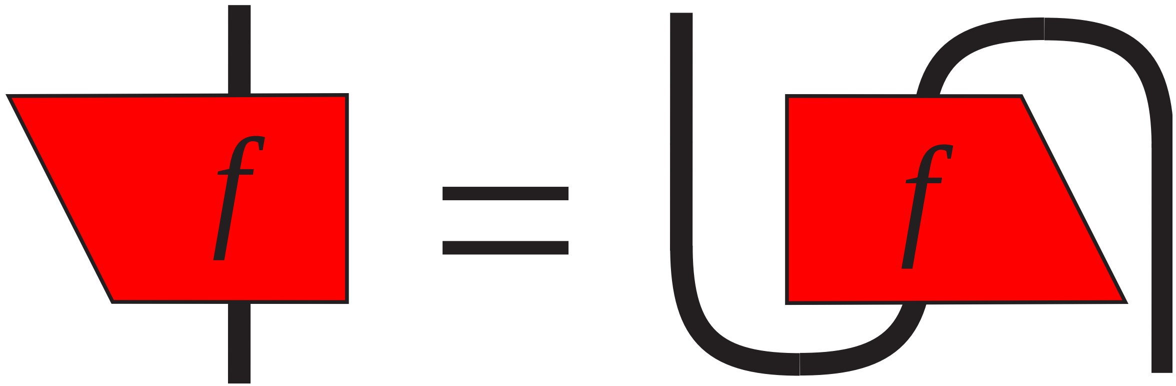


— *quantum-like* —

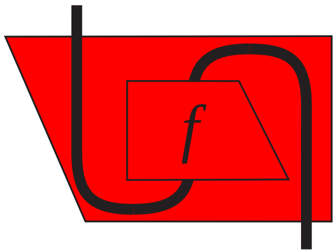




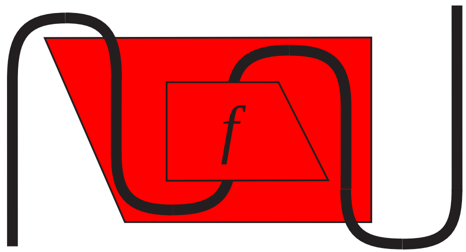
— *quantum-like* —



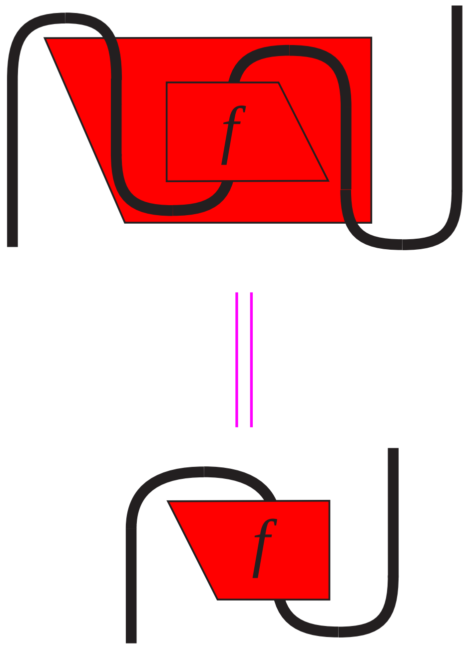
— *sliding* —



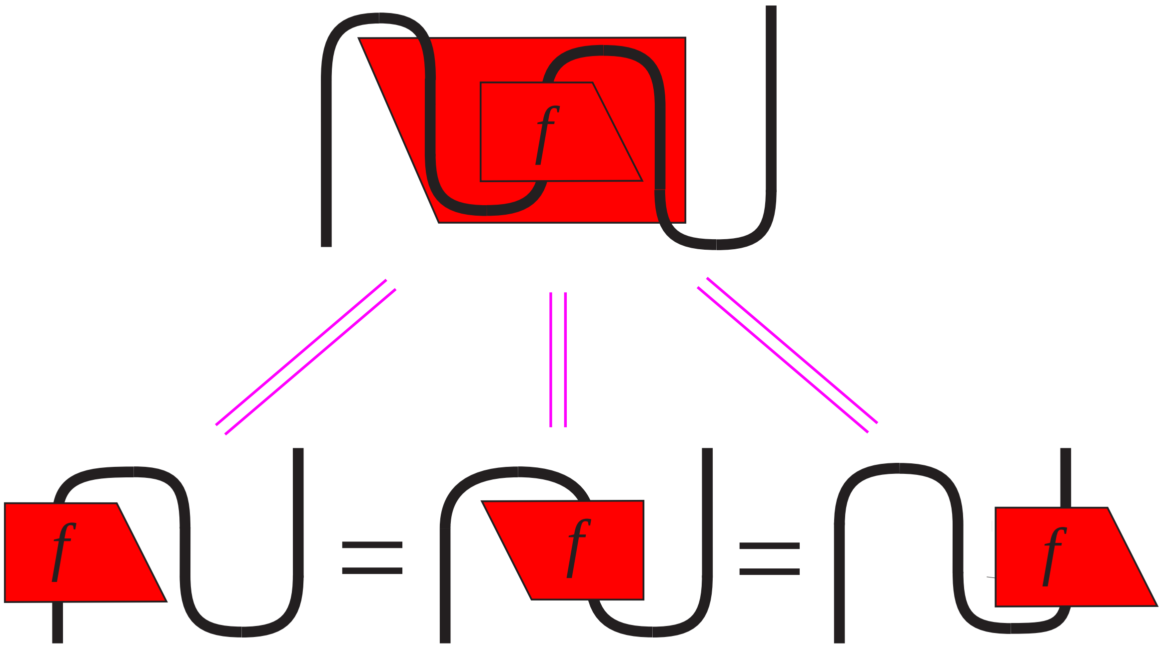
— *sliding* —



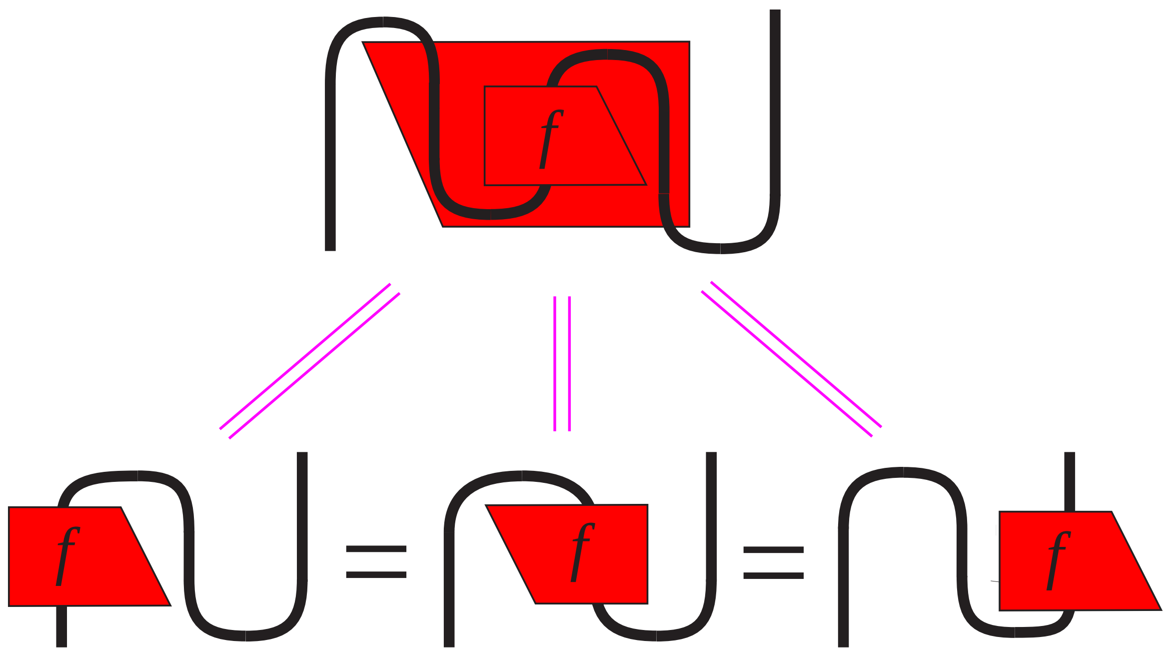
— *sliding* —



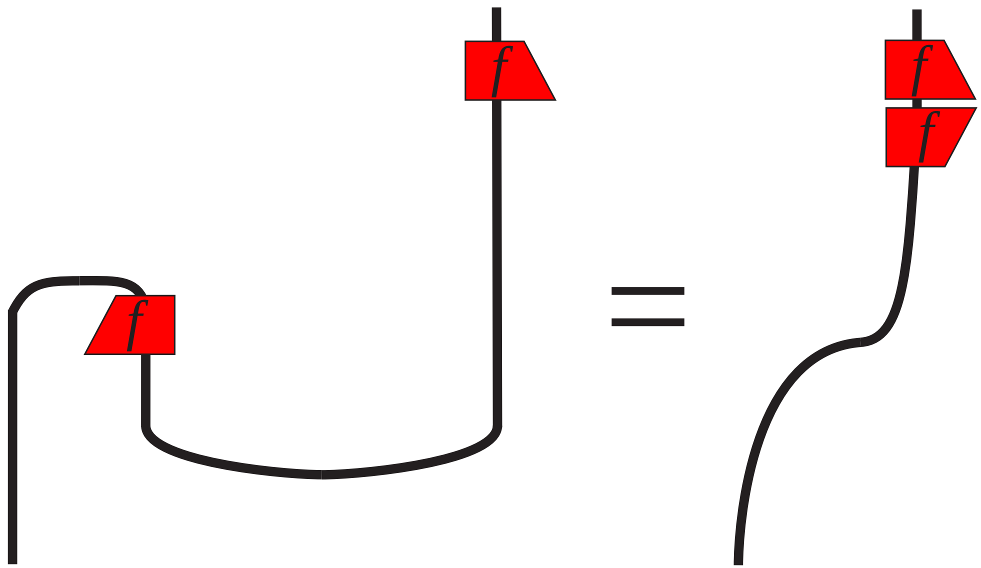
— *sliding* —

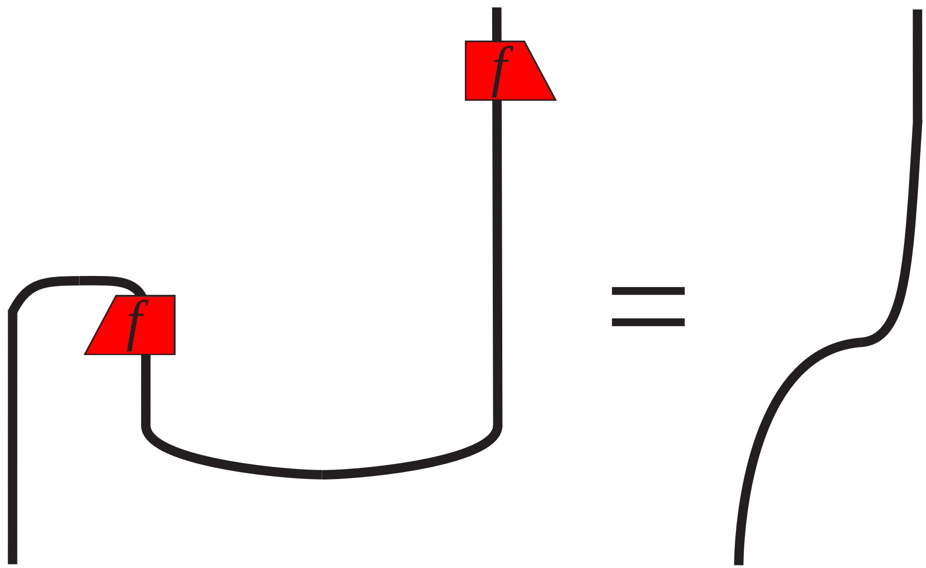


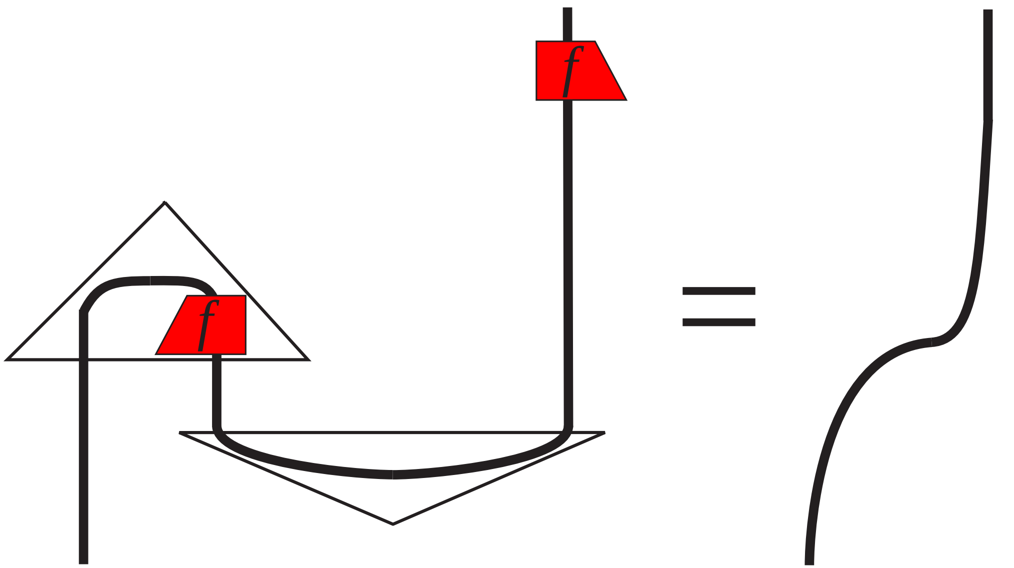
— *sliding* —

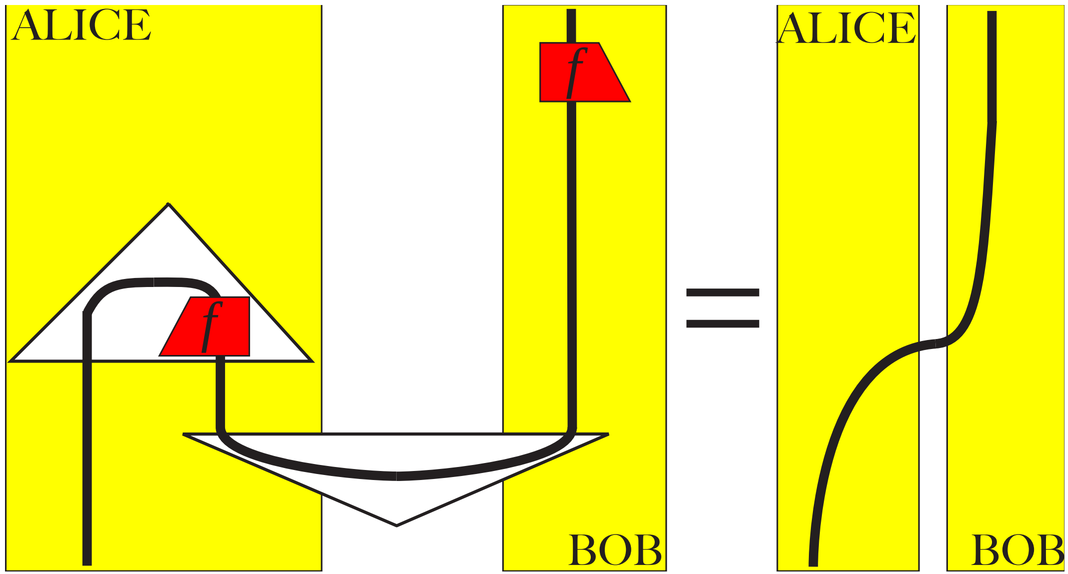


In QM: cups = Bell-states, caps =Bell-effects, π-rotations = transpose

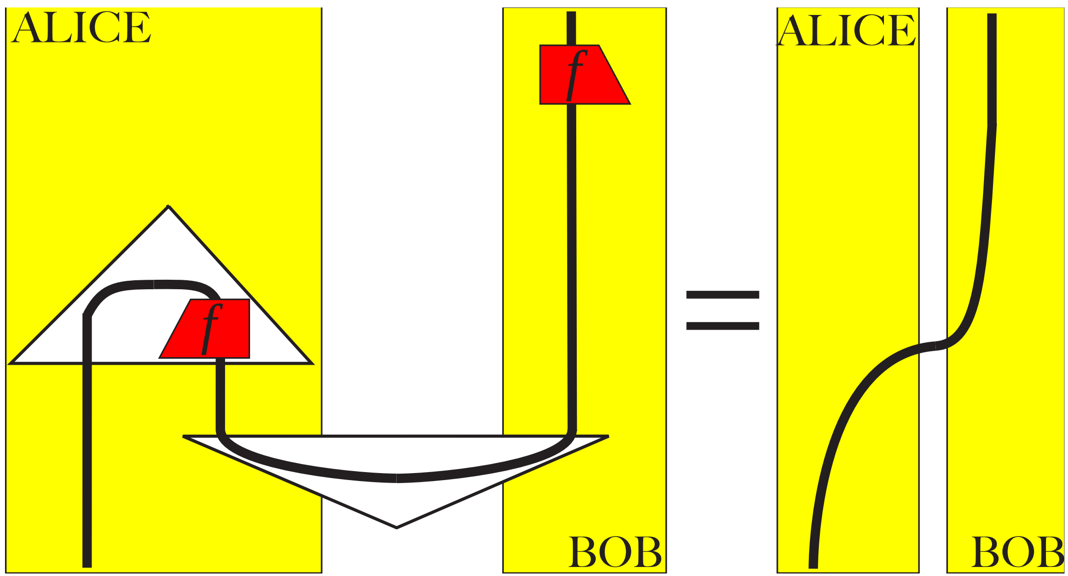

f
f
=
f
f


f
f
=

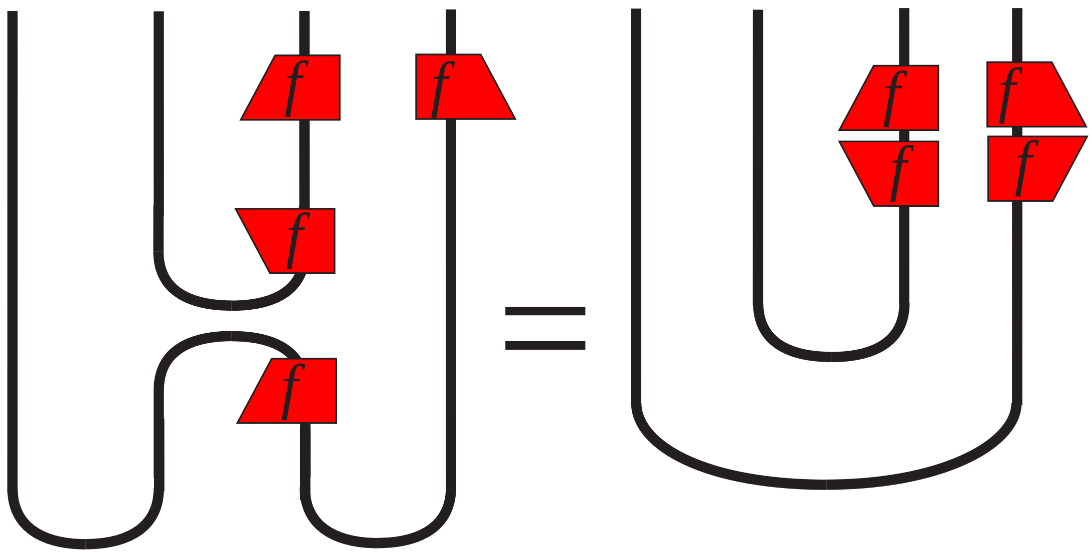

f
f



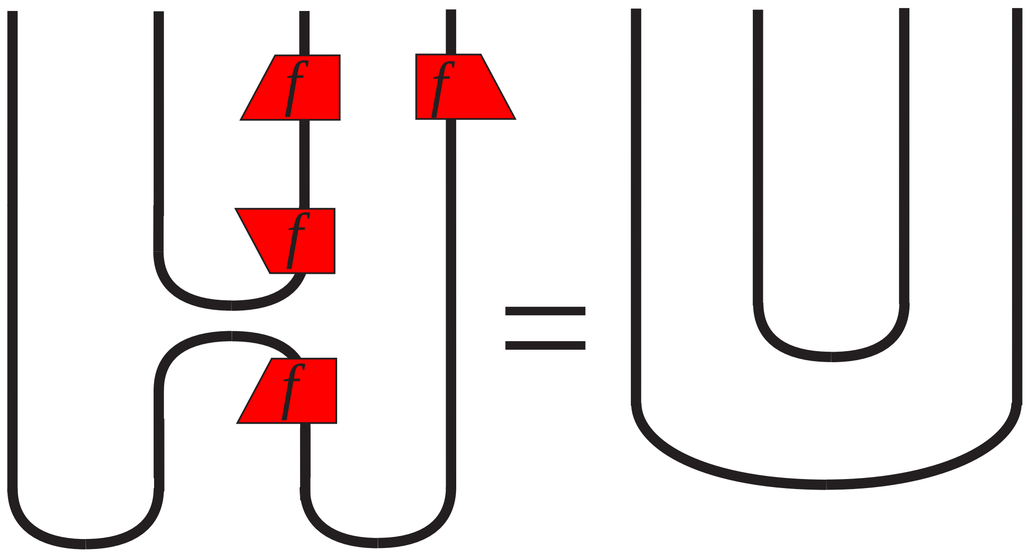
ALICE
f
f
BOB
=
ALICE
BOB

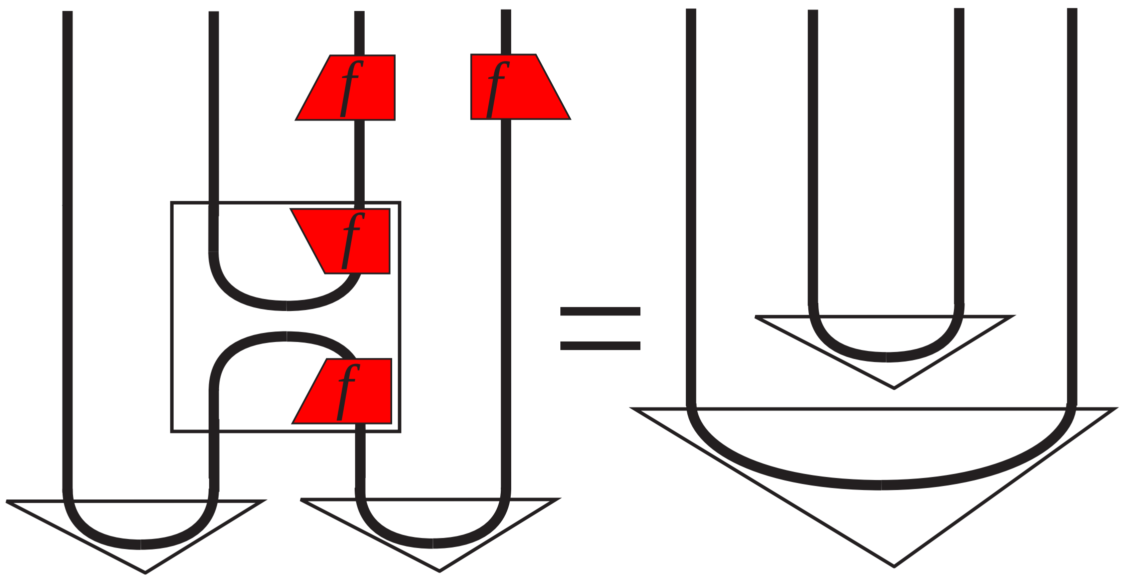


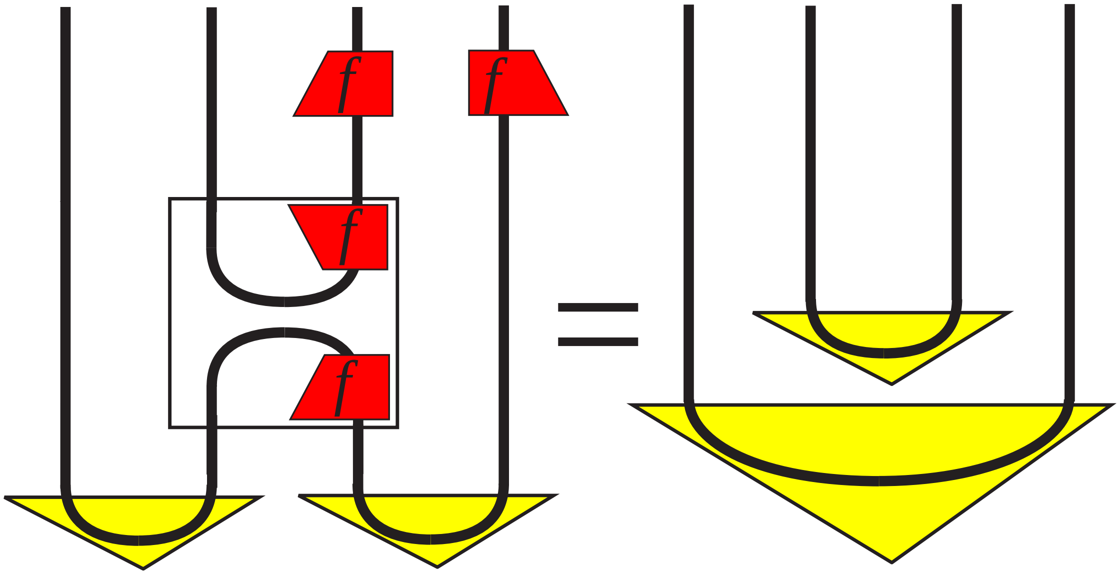
$\Rightarrow$ **quantum teleportation**



f
f
f
f
=
f
f
f
f


f
f
f
f
=


f
f
f
f
=



$\Rightarrow$ **Entanglement swapping**

— *examples* —

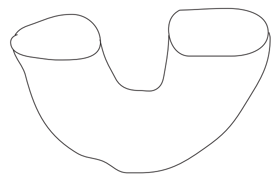
FdHilb :

$$\eta_{\mathcal{H}} : \mathbb{C} \to \mathcal{H} \otimes \mathcal{H} :: 1 \mapsto \sum_i |ii\rangle$$

Rel :

$$\eta_X = \{(*, (x, x)) | x \in X\} \subseteq \{*\} \times (X \times X)$$

n-Cob :



— *completeness* —

Thm. [ ] *An equational statement between expressions in symmetric monoidal categorical language holds if and only if it is derivable in the graphical notation via homotopy*.

— *completeness* —

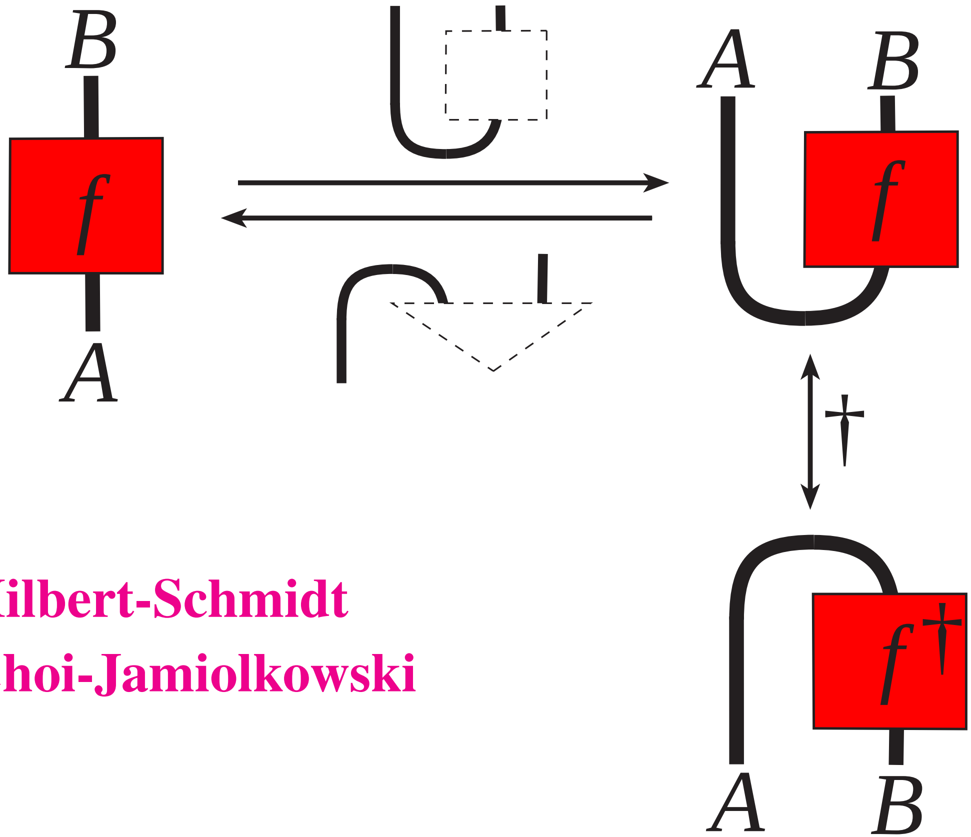
Thm. [Selinger '05] *An equational statement between expressions in dagger compact symmetric monoidal categorical language holds if and only if it is derivable in the graphical notation via homotopy*.

— *completeness* —

Thm. [Selinger '05] *An equational statement between expressions in dagger compact symmetric monoidal categorical language holds if and only if it is derivable in the graphical notation via homotopy.*

Thm. [Selinger '08] *An equational statement between expressions in dagger compact symmetric monoidal categorical language holds if and only if it is derivable for Hilbert spaces, linear maps, composition thereoff, Bell-states, tensor product, and adjoints.*

— *yanking as deduction* —



- **Hilbert-Schmidt**
- **Choi-Jamiolkowski**

THE NO CLONING THEOREM

If

$$U(\psi_1 \otimes \phi_0) = \psi_1 \otimes \psi_1 \qquad U(\psi_2 \otimes \phi_0) = \psi_2 \otimes \psi_2$$

If

$$U(\psi_1 \otimes \phi_0) = \psi_1 \otimes \psi_1 \qquad U(\psi_2 \otimes \phi_0) = \psi_2 \otimes \psi_2$$

then

$$\langle U(\psi_1 \otimes \phi_0) | U(\psi_2 \otimes \phi_0) \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

If

$$U(\psi_1 \otimes \phi_0) = \psi_1 \otimes \psi_1 \qquad U(\psi_2 \otimes \phi_0) = \psi_2 \otimes \psi_2$$

then

$$\langle U(\psi_1 \otimes \phi_0) | U(\psi_2 \otimes \phi_0) \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

$$\langle \psi_1 \otimes \phi_0 | \psi_2 \otimes \phi_0 \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

If

$$U(\psi_1 \otimes \phi_0) = \psi_1 \otimes \psi_1 \qquad U(\psi_2 \otimes \phi_0) = \psi_2 \otimes \psi_2$$

then

$$\langle U(\psi_1 \otimes \phi_0) | U(\psi_2 \otimes \phi_0) \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

$$\langle \psi_1 \otimes \phi_0 | \psi_2 \otimes \phi_0 \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

$$\langle \psi_1 | \psi_2 \rangle \langle \psi_0 | \psi_0 \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle$$

If

$$U(\psi_1 \otimes \phi_0) = \psi_1 \otimes \psi_1 \qquad U(\psi_2 \otimes \phi_0) = \psi_2 \otimes \psi_2$$

then

$$\langle U(\psi_1 \otimes \phi_0) | U(\psi_2 \otimes \phi_0)\rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

$$\langle \psi_1 \otimes \phi_0 | \psi_2 \otimes \phi_0 \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

$$\langle \psi_1 | \psi_2 \rangle \langle \psi_0 | \psi_0 \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle$$

$$\langle \psi_1 | \psi_2 \rangle = \langle \psi_1 | \psi_2 \rangle^2$$

If

$$U(\psi_1 \otimes \phi_0) = \psi_1 \otimes \psi_1 \qquad U(\psi_2 \otimes \phi_0) = \psi_2 \otimes \psi_2$$

then

$$\langle U(\psi_1 \otimes \phi_0) | U(\psi_2 \otimes \phi_0)\rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

$$\langle \psi_1 \otimes \phi_0 | \psi_2 \otimes \phi_0 \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle$$

$$\langle \psi_1 | \psi_2 \rangle \langle \psi_0 | \psi_0 \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle$$

$$\langle \psi_1 | \psi_2 \rangle = \langle \psi_1 | \psi_2 \rangle^2$$

$$\langle \psi_1 | \psi_2 \rangle = 0 \qquad \text{or} \qquad \langle \psi_1 | \psi_2 \rangle = 1$$

i.e. ψ_1 and ψ_2 need to be either equal or orthogonal.

— *no-cloning vs. natural diagonal* —

$$\{\Delta_A : A \longrightarrow A \otimes A\}_A$$

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\Delta_A"'] & B \arrow[d, "\Delta_B"] \\
A \otimes A \arrow[r, "f \otimes f"'] & B \otimes B
\end{tikzcd}$$

— *no-cloning vs. natural diagonal* —

$$\{\Delta_{\mathcal{H}} :: |\,i\,\rangle \mapsto |\,i\,i\,\rangle\}_{\mathcal{H}}$$

$$\begin{tikzcd}
\mathbb{C} \arrow[rr, "1\mapsto|0\rangle+|1\rangle"] \arrow[d, "1\mapsto 1\otimes 1"'] \arrow[drr, phantom, "\text{NO!}"] & & \mathbb{C}\oplus\mathbb{C} \arrow[d, "\begin{array}{l}|0\rangle\mapsto|00\rangle\\ |1\rangle\mapsto|11\rangle\end{array}"] \\
\mathbb{C}\otimes\mathbb{C} \arrow[rr, "1\otimes 1\mapsto(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)"'] & & (\mathbb{C}\oplus\mathbb{C})\otimes(\mathbb{C}\oplus\mathbb{C})
\end{tikzcd}$$

$$|00\rangle + |11\rangle \neq (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$$

— *no-cloning vs. natural diagonal* —

$$\{\Delta_X :: x \mapsto (x,x)\}_X$$

$$\begin{tikzcd}
\{*\} \arrow[rr, "{\{(*,0),(*,1)\}}"] \arrow[d, "{\{(*,(*,*))\}}"'] \arrow[drr, phantom, "\textcolor{red}{\text{NO!}}"] & & \{0,1\} \arrow[d, "{\{(0,(0,0)),(1,(1,1))\}}"] \\
\{*\}\times\{*\} \arrow[rr, "{\{(*,0),(*,1)\}\times\{(*,0),(*,1)\}}"'] & & \{0,1\}\times\{0,1\}
\end{tikzcd}$$

$$\{(0,0),(1,1)\} \neq \{0,1\}\times\{0,1\}$$

— *no-cloning vs. natural diagonal* —

Thm. [Abramsky'09] *In a compact symmetric monoidal category with a uniform copying operation, i.e. a monoidal natural transformation* $\{\Delta_A : A \to A \otimes A\}_A$*, every morphism is a scalar multiple of the identity.*

— *no-cloning vs. natural diagonal* —

Thm. [Abramsky'09] *In a compact symmetric monoidal category with a uniform copying operation, i.e. a monoidal natural transformation $\{\Delta_A : A \to A \otimes A\}_A$, every morphism is a scalar multiple of the identity.*

Remark. This results can be lifted to a **no-broadcasting theorem** by relying on Selinger's CPM-construction.

	pure C	mixed C	pure Q	mixed Q
broadcastable:	`yes`	`YES`	`no`	`no`
cloneable:	`yes`	`NO`	`no`	`no`

— *high-level QM-methods in linguistics* —

— *high-level QM-methods in linguistics* —

Lambek grammar of a sentence:

— *high-level QM-methods in linguistics* —

Lambek grammar of a sentence:

Meaning of the words in it:

$$\overrightarrow{John} \otimes \overrightarrow{does} \otimes \overrightarrow{not} \otimes \overrightarrow{like} \otimes \overrightarrow{Mary}$$

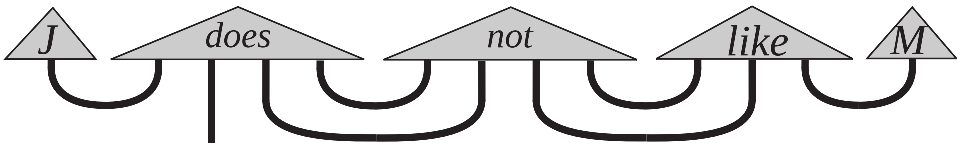
— *high-level QM-methods in linguistics* —

Lambek grammar of a sentence:

Meaning of the words in it:

$$\overrightarrow{John} \otimes \overrightarrow{does} \otimes \overrightarrow{not} \otimes \overrightarrow{like} \otimes \overrightarrow{Mary}$$

Interpret cups and caps in **FdHilb** and compose:



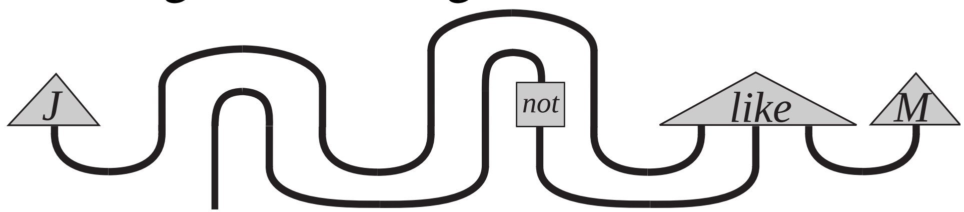
— *high-level QM-methods in linguistics* —

Lambek grammar of a sentence:

Meaning of the words in it:

$$\overrightarrow{John} \otimes \overrightarrow{does} \otimes \overrightarrow{not} \otimes \overrightarrow{like} \otimes \overrightarrow{Mary}$$

Substitute logical meanings of words:



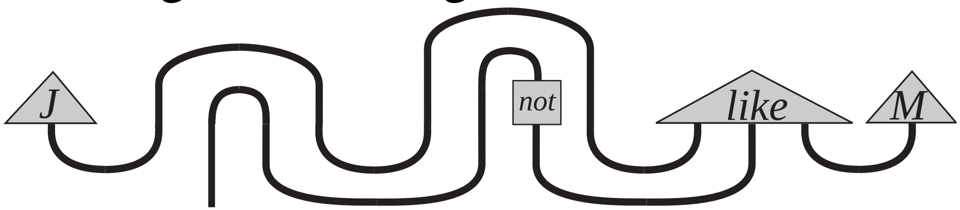
— *high-level QM-methods in linguistics* —

Lambek grammar of a sentence:

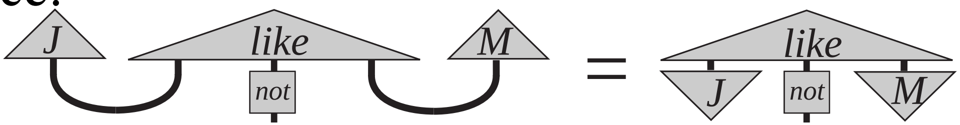
Meaning of the words in it:

$$\overrightarrow{John} \otimes \overrightarrow{does} \otimes \overrightarrow{not} \otimes \overrightarrow{like} \otimes \overrightarrow{Mary}$$

Substitute logical meanings of words:



Reduce:



REFERENCES FOR THIS PART:

1. W. K. Wootters and W. Zurek (1982) *A single quantum cannot be cloned*. Nature **299**, 802–803.
2. A. Joyal and R. Street (1991) *The Geometry of tensor calculus* I. Advances in Mathematics **88**, 55–112.
3. D. Deutsch and R. Jozsa (1992) *Rapid solutions of problems by quantum computation*. Proceedings of the Royal Society of London A **439**, 553–558.
4. H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher (1996) *Noncommuting mixed states cannot be broadcast*. Physical Review Letters **76**, 2818–2821.
5. P. W. Shor (1997) *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM Journal on Computing **26**, 1484–1509.
6. M. Rédei (1997) *Why John von Neumann did not like the Hilbert space formalism of quantum mechanics (and what he liked instead)*. Studies in History and Philosophy of Modern Physics **27**, 493–510.
7. S. Abramsky and B. Coecke (2004) *A categorical semantics of quantum protocols*. In: Proceedings of 19th IEEE-LiCS, pages 415–425. IEEE Press. arXiv:quant-ph/0402130
8. S. Abramsky (2009) *No-cloning in categorical quantum mechanics*. In: Semantic Techniques for Quantum Computation, pages 1–28, Cambridge UP. arXiv:0910.2401
9. B. Coecke (2010) *Quantum picturalism*. Contemporary Physics **51**, 59–83. arXiv:0908.1787
10. P. Selinger (2010) *Finite dimensional Hilbert spaces are complete for dagger compact closed categories*. Electronic Notes in Theoretical Computer Science, to appear.
11. B. Coecke, M. Sadrzadeh and S. Clark (2010) *Mathematical foundations for a compositional distributional model of meaning*. Forthcoming.

Quantum information processing: a new light on the Q-formalism and Q-foundations III

QKD - classicality & complementarity - entanglement - non-locality

Bob Coecke - Oxford University Computing Laboratory

QUANTUM KEY DISTRIBUTION

— *complementarity* —

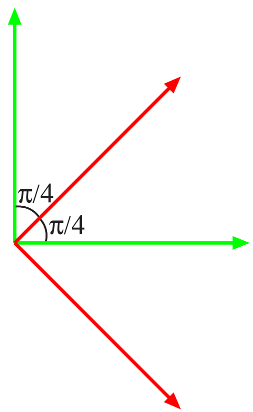
Two bases

$$\{|0\rangle, \ldots, |n\rangle\} \quad \text{and} \quad \{|0\rangle, \ldots, |n\rangle\}$$

are **complementary** (or **unbiased**) if

$$|\langle\, i \,\|\, j \,\rangle| = \frac{1}{\sqrt{n}}$$

yielding equal transition probabilities.



— ***key distribution*** —

step 1.

- Alice encodes bit **either** in green or red basis.

— *key distribution* —

step 1.

- Alice encodes bit **either** in green or red basis.

step 2.

- Alice sends qubit to Bob.

— *key distribution* —

step 1.

- Alice encodes bit **either** in green or red basis.

step 2.

- Alice sends qubit to Bob.

step 3.

- Bob decodes qubit **either** in green or red basis.

— *key distribution* —

step 1.

- Alice encodes bit **either** in green or red basis.

step 2.

- Alice sends qubit to Bob.

step 3.

- Bob decodes qubit **either** in green or red basis.

step 4.

- Alice and Bob (publicly) compare their choices of bases and retain only bits for which bases match.

— *key distribution* —

step 1.

- Alice encodes bit **either** in green or red basis.

step 2.

- Alice sends qubit to Bob.

step 3.

- Bob decodes qubit **either** in green or red basis.

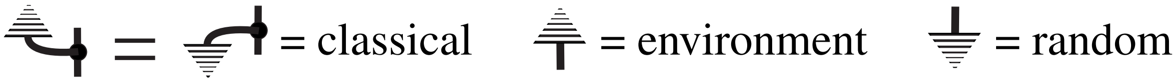
step 4.

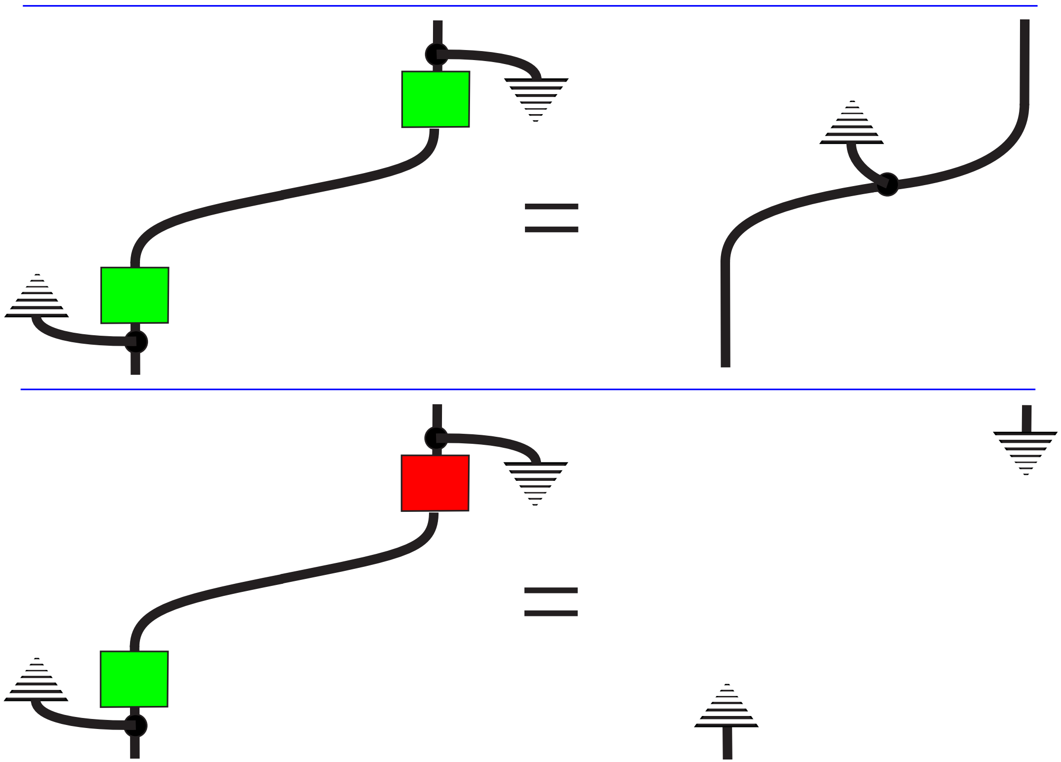
- Alice and Bob (publicly) compare their choices of bases and retain only bits for which bases match.

step 5.

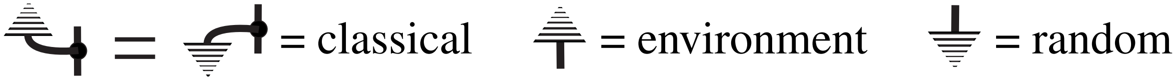
- Alice and Bob compare part of their resulting key.

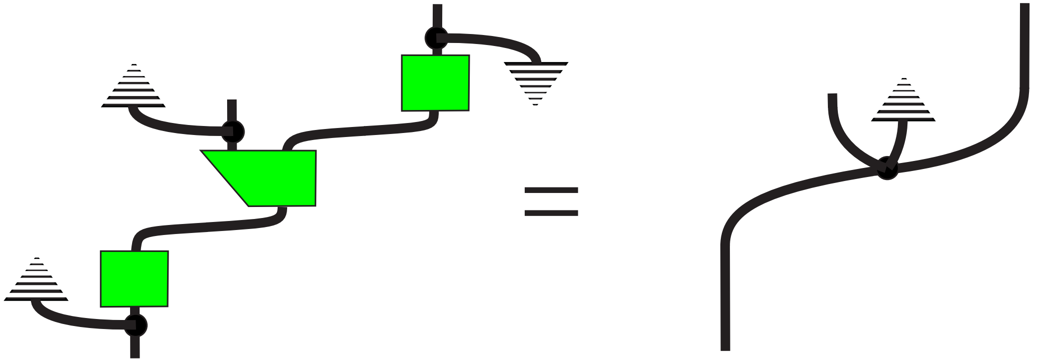
— *key distribution* —

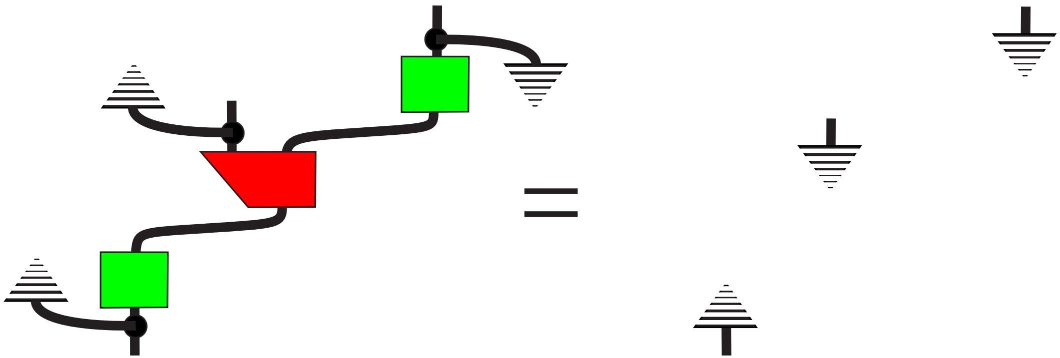




— *key distribution* —





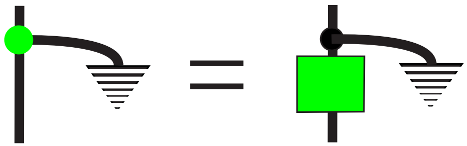


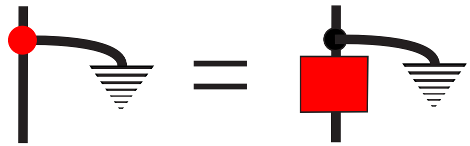
— *underlying complementarity calculus* —

The ingredients:

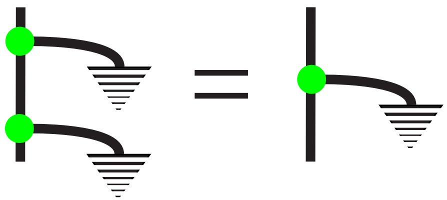
— *underlying complementarity calculus* —

The ingredients:

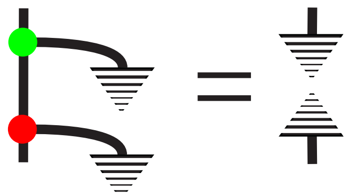




The Rules:



idempotence



'antipotence'

Everything else follows from this.

— *underlying complementarity calculus* —

In fact, everything reduces to the structure of:

OBSERVABLES/CLASSICALITY

— *observables and classical data* —

$\boxed{\text{quantum data cannot be copied nor deleted}}$

— *observables and classical data* —

quantum data cannot be copied nor deleted

classical data CAN be copied and deleted

— *observables and classical data* —

NON-FEATURE:

quantum data cannot be copied nor deleted

FEATURE:

classical data CAN be copied and deleted

— *observables and classical data* —

NON-FEATURE:

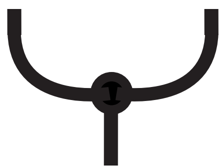
quantum data cannot be copied nor deleted

FEATURE:

classical data CAN be copied and deleted

OBSERVABLE:

copying operation + **deleting operation**



— *observables and classical data* —

A commutative monoid is a set A with a binary map

$$- \bullet - : A \times A \to A$$

which is commutative, associative and unital i.e

$$(a \bullet b) \bullet c = a \bullet (b \bullet c) \quad a \bullet b = b \bullet a \quad a \bullet 1 = a$$

— *observables and classical data* —

A commutative monoid is a set A with a binary map

$$\mu(-,-) : A \times A \to A$$

which is commutative, associative and unital i.e

$$\mu(\mu(a,b),c) = \mu(a,\mu(b,c)) \quad \mu(a,b) = \mu(b,a) \quad \mu(a,1) = a$$

— *observables and classical data* —

A commutative monoid is a set A with a binary map

$$\mu : A \times A \to A$$

which is commutative, associative and unital i.e

$$\mu\circ(\mu\times 1_A) = \mu\circ(1_A\times\mu) \quad \mu = \mu\circ\sigma \quad \mu\circ(1_A\times e) = 1_A$$

with:

$$\sigma : A \times A \to A \times A :: (a, b) \mapsto (b, a)$$

$$e : \{*\} \to A :: * \mapsto 1$$

— *observables and classical data* —

A commutative monoid is a set A with a binary map

$$\mu : A \times A \to A$$

which is commutative, associative and unital i.e

$$\mu\circ(\mu\times 1_A) = \mu\circ(1_A\times\mu) \quad \mu = \mu\circ\sigma \quad \mu\circ(1_A\times e) = 1_A$$

A cocomutative comonoid is a set A with a binary map

$$\delta : A \to A \times A$$

which is cocommutative, coassociative and counital i.e

$$(\delta\times 1_A)\circ\delta = (1_A\times\delta)\circ\delta \quad \delta = \sigma\circ\delta \quad (1_A\times e')\circ\delta = 1_A$$

— *observables and classical data* —

A commutative monoid is object A with morphism

$$\mu : A \otimes A \to A$$

which is commutative, associative and unital i.e

$$\mu\circ(\mu\otimes 1_A) = \mu\circ(1_A\otimes\mu) \quad \mu = \mu\circ\sigma \quad \mu\circ(1_A\otimes e) = 1_A$$

A cocomutative comonoid is object A with morphism

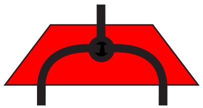
$$\delta : A \to A \otimes A$$

which is cocommutative, coassociative and counital i.e

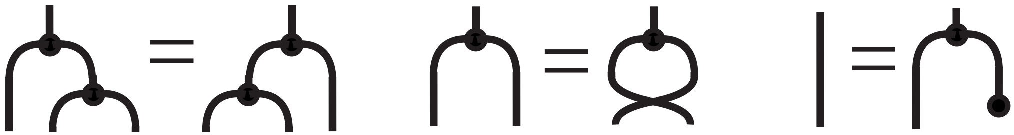
$$(\delta\otimes 1_A)\circ\delta = (1_A\otimes\delta)\circ\delta \quad \delta = \sigma\circ\delta \quad (1_A\otimes e')\circ\delta = 1_A$$

— *observables and classical data* —

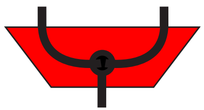
A commutative monoid is object A with morphisms

 $: A \otimes A \to A$  $: \mathrm{I} \to A$

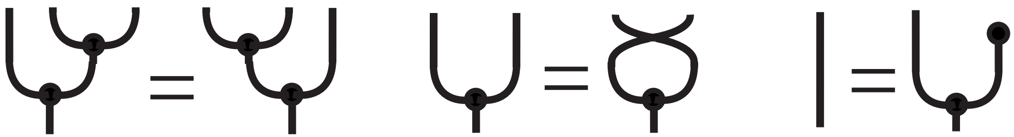
s.t.



A cocommutative comonoid is object A with morphisms

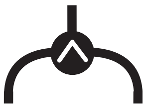
 $: A \to A \otimes A$  $: A \to \mathrm{I}$

s.t.

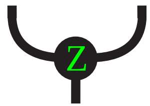


— *observables and classical data* —

FSet:



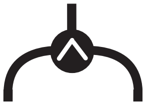
$$:: \begin{cases} |00\rangle, |01\rangle, |10\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



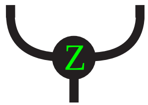
$$:: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$

— *observables and classical data* —

FSet:



$$:: \begin{cases} |00\rangle, |01\rangle, |10\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$

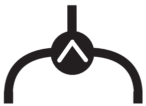


$$:: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$

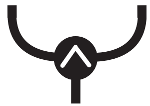
Z is the only commutative comonoid on $\{0, 1\}$ in **FSet**.

— *observables and classical data* —

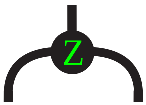
FRel:



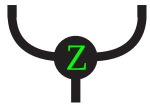
$$:: \begin{cases} |00\rangle, |01\rangle, |10\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



$$:: \begin{cases} |0\rangle \mapsto |00\rangle, |01\rangle, |10\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$



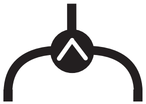
$$:: \begin{cases} |00\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



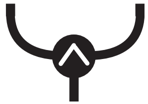
$$:: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$

— *observables and classical data* —

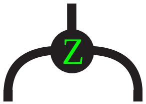
FdHilb:



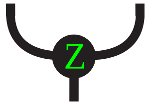
$$:: \begin{cases} |00\rangle, |01\rangle, |10\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



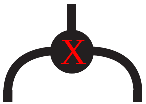
$$:: \begin{cases} |0\rangle \mapsto |00\rangle, |01\rangle, |10\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$



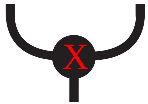
$$:: \begin{cases} |00\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



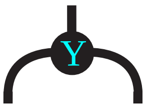
$$:: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$



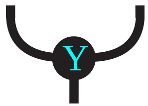
$$:: \begin{cases} |++\rangle \mapsto |+\rangle \\ |--\rangle \mapsto |-\rangle \end{cases}$$



$$:: \begin{cases} |+\rangle \mapsto |++\rangle \\ |-\rangle \mapsto |--\rangle \end{cases}$$



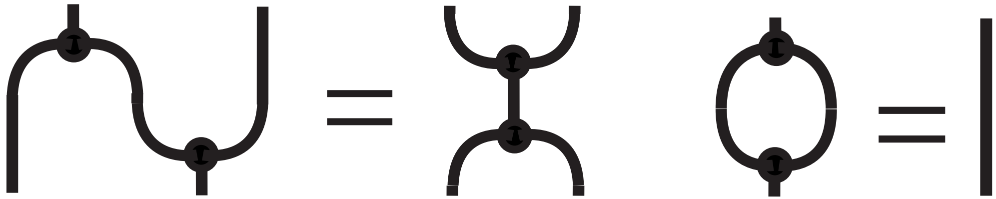
$$:: \begin{cases} |\sharp\,\sharp\rangle \mapsto |\sharp\rangle \\ |==\rangle \mapsto |=\rangle \end{cases}$$



$$:: \begin{cases} |\sharp\rangle \mapsto |\sharp\,\sharp\rangle \\ |=\rangle \mapsto |==\rangle \end{cases}$$

— *observables and classical data* —

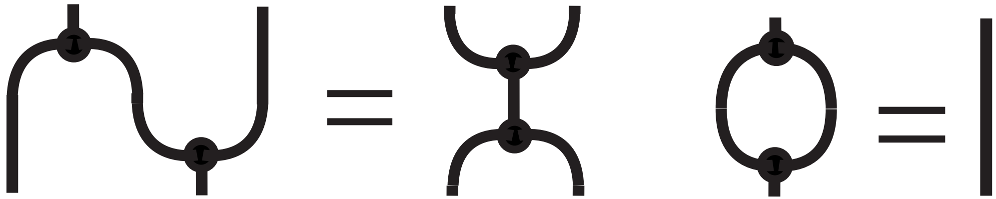
If a (co)commutative (co)monoid satisfies



it is a dagger special commutative Frobenius algebra.

— *observables and classical data* —

If a (co)commutative (co)monoid satisfies



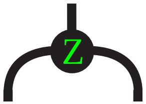
it is a dagger special commutative Frobenius algebra.

Thm. (with Pavlovic & Vicary) In **FHilb** these †CFAs exactly correspond with orthonormal bases on the underlying Hilbert space via the correspondence:

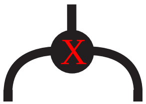
$$\{|\,i\,\rangle\}_i \quad \longleftrightarrow \quad |\,i\,\rangle \mapsto |\,ii\,\rangle$$

— *observables and classical data* —

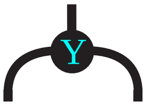
FdHilb examples:



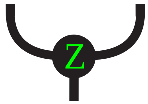
$$:: \begin{cases} |00\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



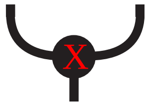
$$:: \begin{cases} |++\rangle \mapsto |+\rangle \\ |--\rangle \mapsto |-\rangle \end{cases}$$



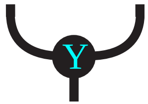
$$:: \begin{cases} |\sharp\,\sharp\rangle \mapsto |\sharp\rangle \\ |=\,=\rangle \mapsto |=\rangle \end{cases}$$



$$:: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$



$$:: \begin{cases} |+\rangle \mapsto |++\rangle \\ |-\rangle \mapsto |--\rangle \end{cases}$$

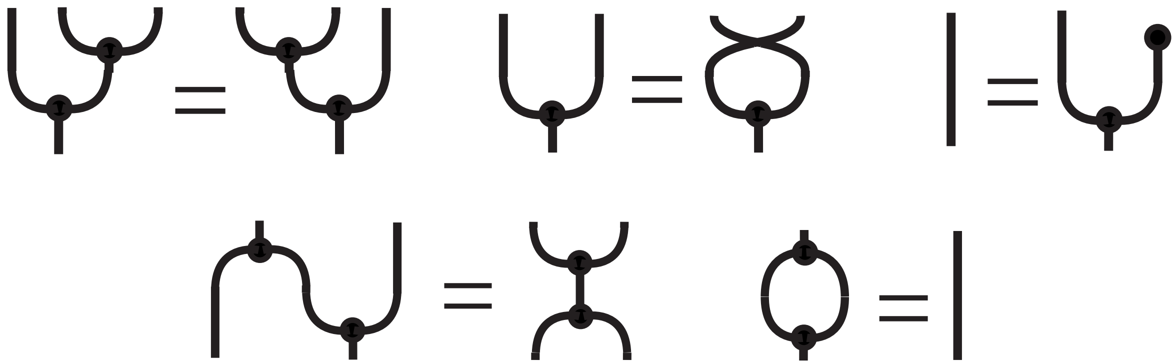


$$:: \begin{cases} |\sharp\rangle \mapsto |\sharp\,\sharp\rangle \\ |=\rangle \mapsto |=\,=\rangle \end{cases}$$

— *observables and classical data* —

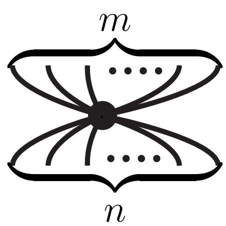
A **†CFA** is a pair:

which is such that:



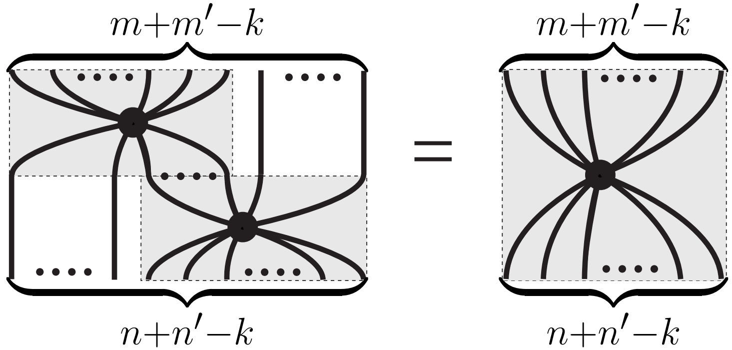
— *observables and classical data* —

A **†CFA** is a family:

'spiders' $= \Big\{$ 

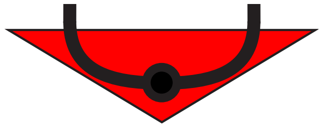
$\Big| \; n, m \in \mathbb{N} \Big\}$

which is such that, for $k > 0$:



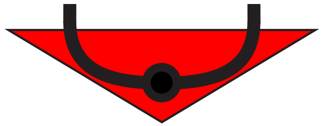
— $(0, 2)$-*spiders = "Bell-states"* —

Definition. Each dag. spec. comm. Frobenius algebra induces a 2-frontleg/0-backleg spider, the Bell-state:

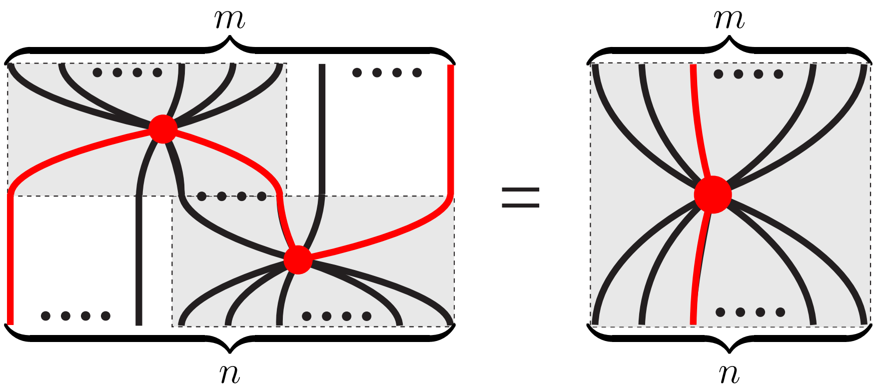


— $(0,2)$*-spiders = "Bell-states"* —

Definition. Each dag. spec. comm. Frobenius algebra induces a 2-frontleg/0-backleg spider, the Bell-state:



Proposition. Bell-states satisfy 'yanking':



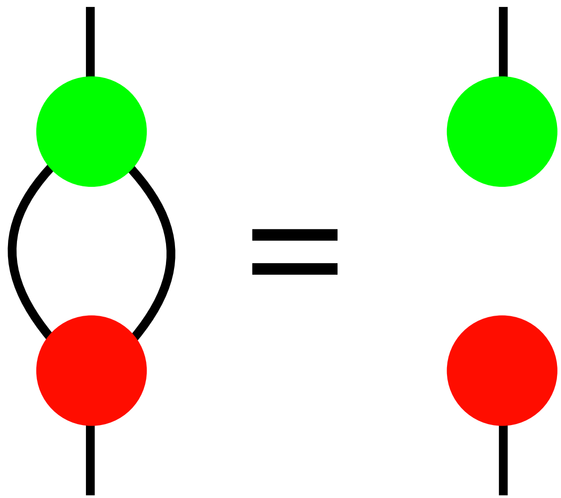
COMPLEMENTARY BASES

— *observables and classical data* —

Thm. [C & Duncan '08] Complementarity means:

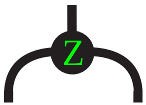
— *observables and classical data* —

Thm. [C & Duncan '08] Complementarity means:

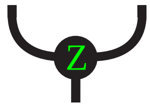


— *observables and classical data* —

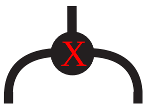
FdHilb:



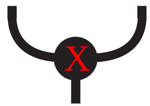
$$:: \begin{cases} |00\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



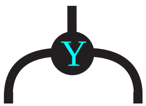
$$:: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$



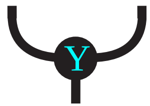
$$:: \begin{cases} |+\,+\rangle \mapsto |+\rangle \\ |-\,-\rangle \mapsto |-\rangle \end{cases}$$



$$:: \begin{cases} |+\rangle \mapsto |+\,+\rangle \\ |-\rangle \mapsto |-\,-\rangle \end{cases}$$



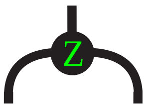
$$:: \begin{cases} |\sharp\ \sharp\rangle \mapsto |\sharp\rangle \\ |=\,=\rangle \mapsto |=\rangle \end{cases}$$



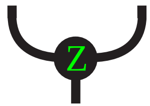
$$:: \begin{cases} |\sharp\rangle \mapsto |\sharp\ \sharp\rangle \\ |=\rangle \mapsto |=\,=\rangle \end{cases}$$

— *observables and classical data* —

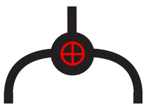
FRel:



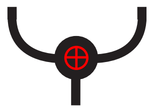
$$:: \begin{cases} |00\rangle \mapsto |0\rangle \\ |11\rangle \mapsto |1\rangle \end{cases}$$



$$:: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{cases}$$



$$:: \begin{cases} |00\rangle, |11\rangle \mapsto |0\rangle \\ |01\rangle, |10\rangle \mapsto |1\rangle \end{cases}$$



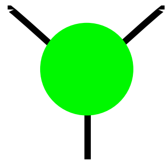
$$:: \begin{cases} |0\rangle \mapsto |00\rangle, |11\rangle \\ |1\rangle \mapsto |01\rangle, |10\rangle \end{cases}$$

$\Rightarrow$ Complementarity can be modeled with relations!

Coecke & Edwards ’08: 0808.1037. Pavlovic ’08: 0812.2266. Evans et al ’09: 0909.4453.

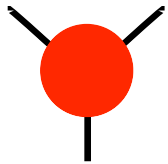
— *computing with spiders* —

Z-spin:



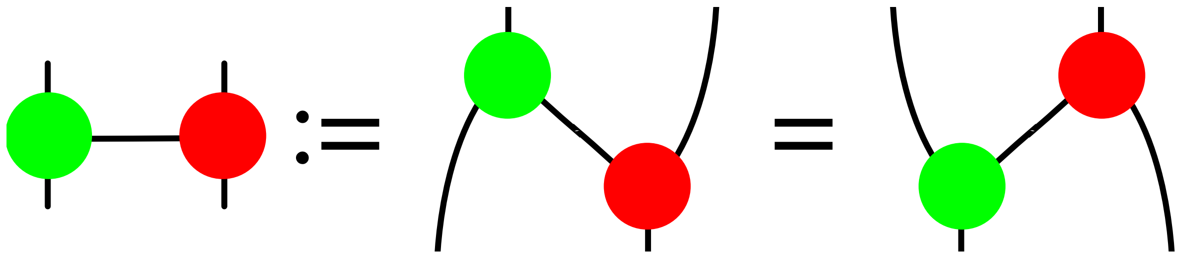
$$\delta_Z : |i\rangle \mapsto |ii\rangle$$

X-spin:

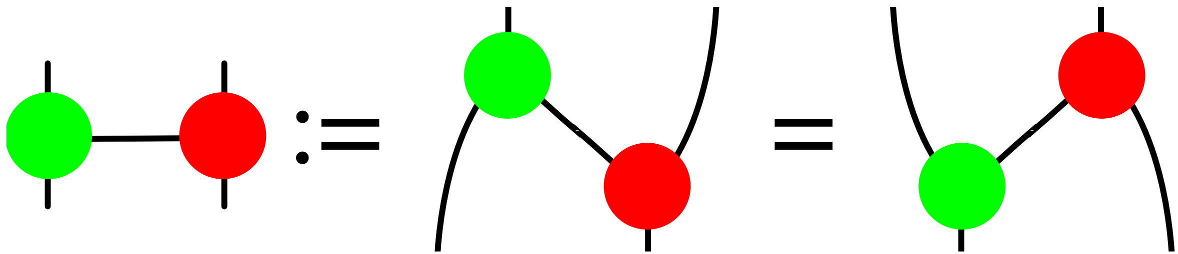


$$\delta_X : |\pm\rangle \mapsto |\pm\pm\rangle$$

— *computing with spiders* —



— *computing with spiders* —



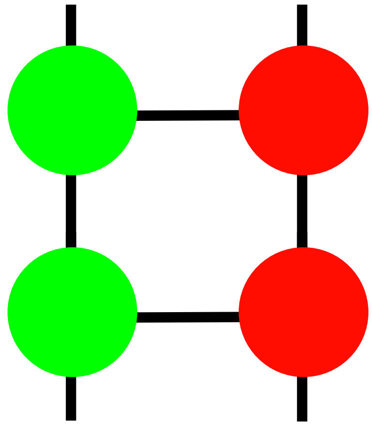
i.e.

$$(\delta_Z^\dagger \otimes 1) \circ (1 \otimes \delta_X) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = CNOT$$

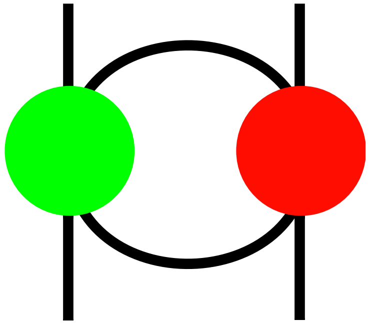
— *computing with spiders* —

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = ?$$

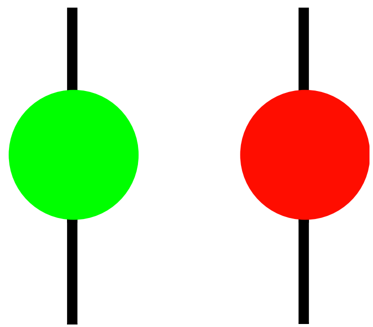
— *computing with spiders* —



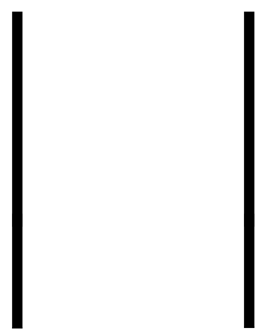
— *computing with spiders* —



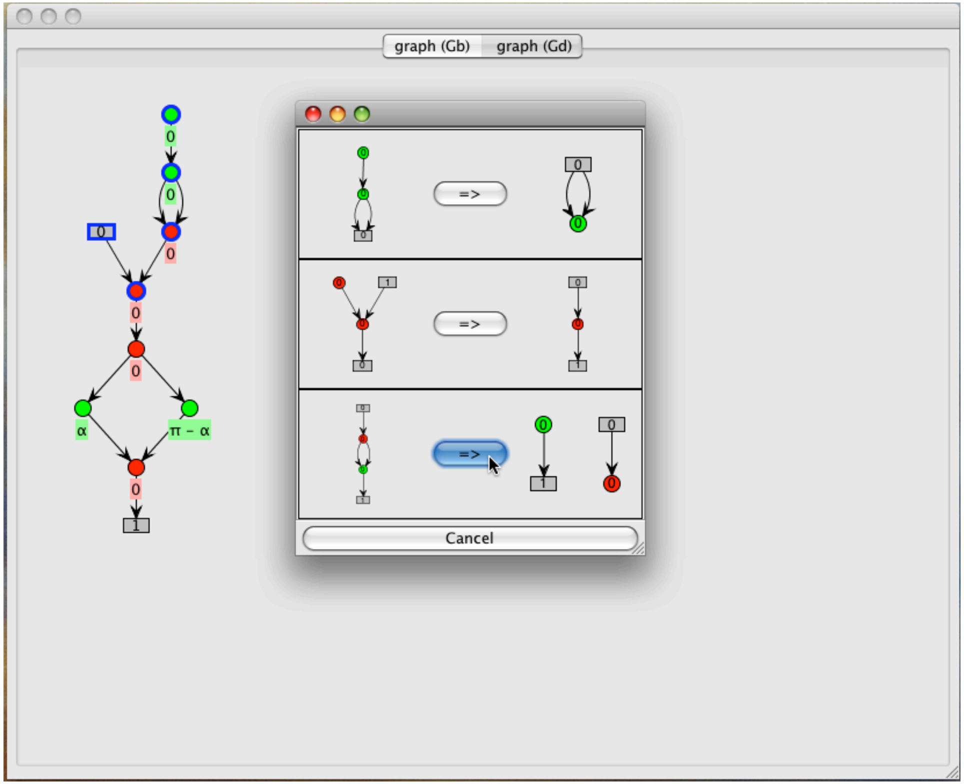
— *computing with spiders* —



— *computing with spiders* —



quantomatic – *Dixon / Duncan / Kissinger*



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

ENTANGLEMENT

Classifying entanglement: Two multipartite quantum states **compare** if by (possibly probabilistic) either local or classical means one can be turned into the other.

Classifying entanglement: Two multipartite quantum states **compare** if by (possibly probabilistic) either local or classical means one can be turned into the other.

Two qubits:

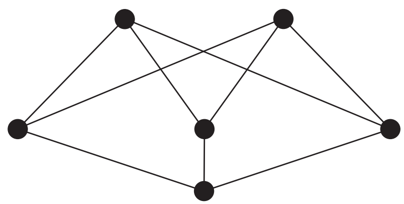
Proof: A linear map either has an inverse or not.

Classifying entanglement: Two multipartite quantum states **compare** if by (possibly probabilistic) either local or classical means one can be turned into the other.

Two qubits:

Proof: A linear map either has an inverse or not.

Three qubits:



Proof: Significantly non-trivial.

GHZ-SLOCC-class representative:

$$GHZ = |000\rangle + |111\rangle$$

Many applications in quantum computing e.g. fault-tolerance; canonical witness of quantum non-locality.

GHZ-SLOCC-class representative:

$$GHZ = |000\rangle + |111\rangle$$

Many applications in quantum computing e.g. fault-tolerance; canonical witness of quantum non-locality.

W-SLOCC-class representative:

$$W = |001\rangle + |010\rangle + |100\rangle$$

Occurs naturally in condensed matter physics

GHZ-SLOCC-class representative:

$$GHZ = |000\rangle + |111\rangle$$

Many applications in quantum computing e.g. fault-tolerance; canonical witness of quantum non-locality.

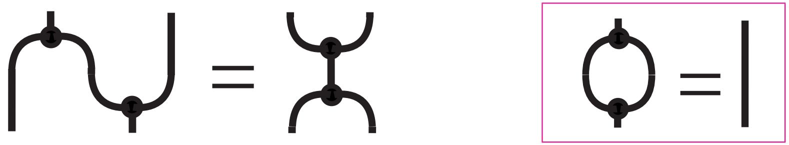
W-SLOCC-class representative:

$$W = |001\rangle + |010\rangle + |100\rangle$$

Occurs naturally in condensed matter physics

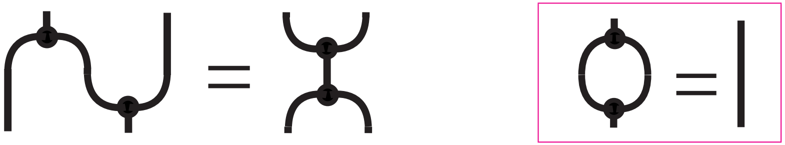
Beyond these it's a total mess: continuous classes for which the structure nor applications are known (there are some notable exceptions such as graph states).

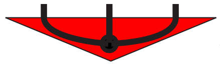
Proposition. [CK'10] A special CFA on $\mathbb{C}^2$, i.e.



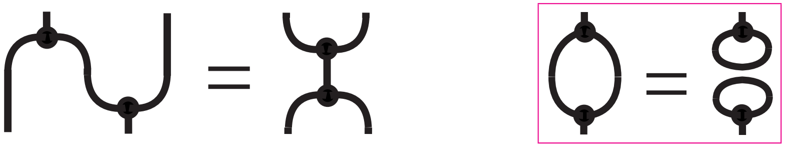
induces a GHZ-class state , and vice versa.

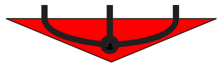
Proposition. [CK'10] A special CFA on $\mathbb{C}^2$, i.e.



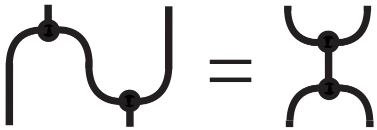
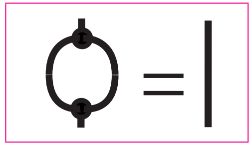
induces a GHZ-class state , and vice versa.

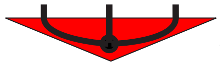
Proposition. [CK'10] An anti-special CFA on $\mathbb{C}^2$, i.e.



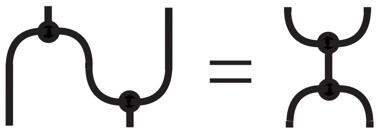
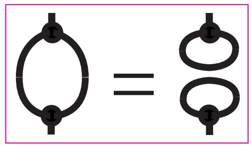
induces a W-class state , and vice versa.

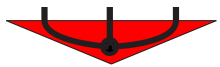
Proposition. [CK'10] A special CFA on $\mathbb{C}^2$, i.e.

induces a GHZ-class state , and vice versa.

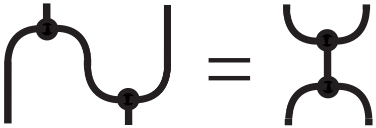
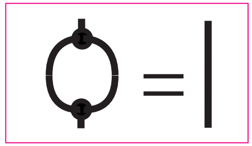
Proposition. [CK'10] An anti-special CFA on $\mathbb{C}^2$, i.e.

induces a W-class state , and vice versa.

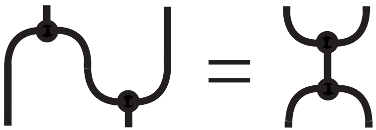
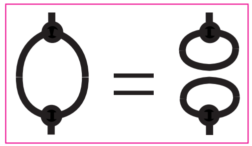
Proposition. Every CFA on $\mathbb{C}^2$ is either special or anti-special; every monoid on $\mathbb{C}^2$ extends to an CFA.

Proposition. [CK’10] A special CFA on $\mathbb{C}^2$, i.e.

induces a GHZ-class state , and vice versa.

Proposition. [CK’10] A anti-special CFA on $\mathbb{C}^2$, i.e.

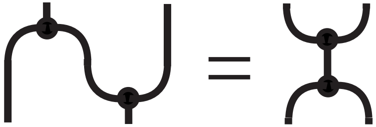
 

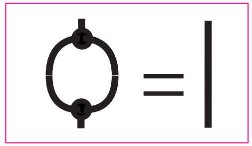
induces a W-class state , and vice versa.

Proposition. Every CFA on $\mathbb{C}^2$ is either special or anti-special; every monoid on $\mathbb{C}^2$ extends to an CFA.

$\Rightarrow$ **algebra meets entanglement classification.**

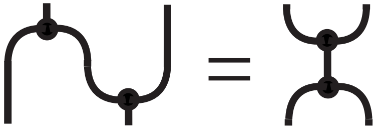
Proposition. [CK'10] A special CFA on $\mathbb{C}^2$, i.e.

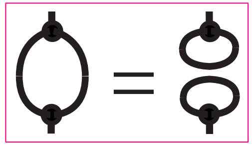




induces a GHZ-class state , and vice versa.

Proposition. [CK'10] A anti-special CFA on $\mathbb{C}^2$, i.e.





induces a W-class state , and vice versa.

Proposition. Every CFA on $\mathbb{C}^2$ is either special or anti-special; every monoid on $\mathbb{C}^2$ extends to an CFA.

Conjecture: all behaviors arise from composition.

NON-LOCALITY

Value assignment: Given a particular quantum state, assign to all measurements definite outcomes.

Value assignment: Given a particular quantum state, assign to all measurements definite outcomes.

Hidden-variable representation for a state: A probability distribution over value assignments which produces the quantum mechanical probabilities.

Value assignment: Given a particular quantum state, assign to all measurements definite outcomes.

Hidden-variable representation for a state: A probability distribution over value assignments which produces the quantum mechanical probabilities.

Bell's thm: this is not possible for the Bell-state i.e. no hidden-variable representation exists.

Value assignment: Given a particular quantum state, assign to all measurements definite outcomes.

Hidden-variable representation for a state: A probability distribution over value assignments which produces the quantum mechanical probabilities.

Bell's thm: this is not possible for the Bell-state i.e. no hidden-variable representation exists.

GHZ thm: this is not possible for the GHZ-state, in fact, no value assignment even exists.

Value assignment: Given a particular quantum state, assign to all measurements definite outcomes.

Hidden-variable representation for a state: A probability distribution over value assignments which produces the quantum mechanical probabilities.

Bell's thm: this is not possible for the Bell-state i.e. no hidden-variable representation exists.

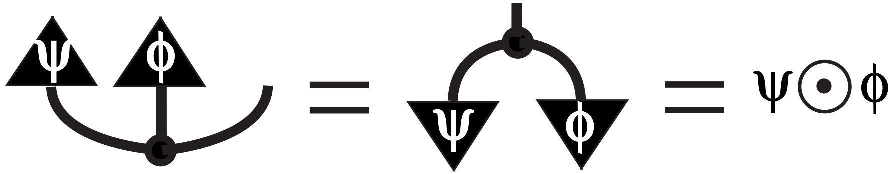
GHZ thm: this is not possible for the GHZ-state, in fact, no value assignment even exists.

The argument takes place in the Clifford fragment; Clifford circuits can be efficiently classically simulated.

For a GHZ-state measurement outcomes on two of the sub-systems determine the state of third sub-system:

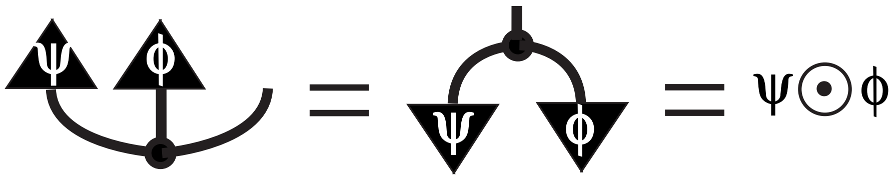
$$= \psi \odot \phi$$

For a GHZ-state measurement outcomes on two of the sub-systems determine the state of third sub-system:



This always yields an Abelian group on those states that our unbiased for the ‘GHZ-basis’.

For a GHZ-state measurement outcomes on two of the sub-systems determine the state of third sub-system:



This always yields an Abelian group on those states that our unbiased for the ‘GHZ-basis’.

In the case of X- and Y-measurements this is Z_4, with:

- the X-eigenstate $|+\rangle$ is the unit
- the X-eigenstate $|-\rangle$ is the involution
- the Y-eigenstates $|\sharp\rangle$ and $|=\rangle$ are the remainder

For the unit $|+\rangle$ and the involution $|-\rangle$ we have:

$$|+\rangle \odot |+\rangle = |+\rangle \quad |+\rangle \odot |-\rangle = |-\rangle \quad |-\rangle \odot |-\rangle = |+\rangle$$

i.e. even occurrences of $|-\rangle$ in correlations.

For the unit $|+\rangle$ and the involution $|-\rangle$ we have:

$$|+\rangle \odot |+\rangle = |+\rangle \quad |+\rangle \odot |-\rangle = |-\rangle \quad |-\rangle \odot |-\rangle = |+\rangle$$

i.e. even occurrences of $|-\rangle$ in correlations.

For $|=\rangle$ and $|\sharp\rangle$ we have:

$$|\sharp\rangle \odot |=\rangle = |+\rangle \quad |=\rangle \odot |=\rangle = |-\rangle \quad |\sharp\rangle \odot |\sharp\rangle = |=\rangle$$

i.e. odd occurrences of $\{|-\rangle, |=\rangle\}$ in correlations.

$$\{|+\rangle, |-\rangle\} \times \{|+\rangle, |-\rangle\} \times \{|+\rangle, |-\rangle\}$$

$$\{|+\rangle, |-\rangle\} \times \{|\sharp\rangle, |=\rangle\} \times \{|\sharp\rangle, |=\rangle\}$$

$$\{|\sharp\rangle, |=\rangle\} \times \{|+\rangle, |-\rangle\} \times \{|\sharp\rangle, |=\rangle\}$$

$$\{|\sharp\rangle, |=\rangle\} \times \{|\sharp\rangle, |=\rangle\} \times \{|+\rangle, |-\rangle\}$$

Above line: three red observables have even $\{|-\rangle\}$-occurrences

Below line: each row has odd $\{|-\rangle, |=\rangle\}$-occurrences $\Rightarrow$ three rows together have odd $\{|-\rangle, |=\rangle\}$-occurrences $\Rightarrow$ since blue observables occur twice for the same system and hence don't contribute to signs, three red observables have odd $\{|-\rangle\}$-occurrences.

CONTRADICTION

REFERENCES FOR THIS PART:

1. J. Swinger (1960) *Unitary operator bases*. Proceedings of the National Academy of Sciiences of the USA, **46**, 570–579.
2. C. H. Bennett and G. Brassard (1984) *Quantum cryptography: Public key distribution and coin tossing*. In *Proceedings of IEEE-CCSSP*, pages 175–179.
3. S. Popescu, and D. Rohrlich (1994) *Nonlocality as an axiom*. Foundations of Physics **24**, 379–385.
4. M. A. Nielsen (1999) *Conditions for a class of entanglement transformations*. Physical Review Letters **83**, 436–439. arXiv:quant-ph/9811053
5. W. Dür, G. Vidal and J. I. Cirac (2000) *Three qubits can be entangled in two inequivalent ways*. Physical Review A **62**, 062314. arXiv:quant-ph/0005115
6. M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest and H.-J. Briegel (2006) *Entanglement in graph states and its applications*. arXiv:quant-ph/0602096
7. B. Coecke, D. Pavlovic, and J. Vicary (2008) *A new description of orthogonal bases*. arXiv:0810.0812
8. B. Coecke and R. W. Duncan (2008) *Interacting quantum observables*. In: Proceedings of ICALP, pp. 298–310, LNCS 5126, Springer-Verlag. arXiv:0906.4725
9. J. Anders and D. E. Browne (2009) *Computational power of correlations*. Physical Review Letters **102**, 050502. arXiv:0805.1002
10. B. Coecke and A. Kissinger (2010) *The compositional structure of multipartite quantum entanglement*. arXiv:1002.2540
11. B. Coecke and S. Perdrix (2010) *Environment and classical channels in categorical quantum mechanics*. Forthcoming.

Diagrammatic QM logic introductions:

Appetizer: ***Kindergarten quantum mechanics.***
arXiv:quant-ph/0510032.

Survey: ***Quantum picturalism.***
arXiv:0908.1787.

Relevant category theory:

Appetizer: ***Introducing categories to the practicing physicist.***
arXiv:0808.1032.

Categories for the practicing physicist. (with Paquette)
arXiv:0905.3010.

A survey of graphical languages for monoidal categories. (Selinger)
arXiv:0908.3347

More advanced technical papers:

- S. Abramsky and B. Coecke (2004) *A categorical semantics of quantum protocols*. In:

Proceedings of 19th IEEE conference on Logic in Computer Science, pages 415–425. IEEE Press. arXiv:quant-ph/0402130. Revised version (2009): *Categorical quantum mechanics*. In: Handbook of Quantum Logic and Quantum Structures, K. Engesser, D. M. Gabbay and D. Lehmann (eds), pages 261–323. Elsevier. arXiv:0808.1023

- P. Selinger (2007) *Dagger compact closed categories and completely positive maps*. Electronic Notes in Theoretical Computer Science **170**, 139–163. http://www.mathstat.dal.ca/∼selinger/papers.html♯dagger

- B. Coecke and D. Pavlovic (2007) *Quantum measurements without sums*. In: Mathematics of Quantum Computing and Technology, G. Chen, L. Kauffman and S. Lamonaco (eds), pages 567–604. Taylor and Francis. arXiv:quant-ph/0608035

- J. Vicary (2008) *A categorical framework for the quantum harmonic oscillator*. International Journal of Theoretical Physics **47**, 3408–3447. arXiv:0706.0711

- B. Coecke, D. Pavlovic, and J. Vicary (2008) *A new description of orthogonal bases*. arXiv:0810.0812

- B. Coecke and R. W. Duncan (2008) *Interacting quantum observables*. In: Proceedings of ICALP, pp. 298–310, LNCS 5126, Springer-Verlag. arXiv:0906.4725

- S. Abramsky (2009) *No-cloning in categorical quantum mechanics*. In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 1–28, Cambridge University Press. arXiv:0910.2401

- B. Coecke and B. Edwards (2008) *Toy quantum categories*. Electronic Notes in Theoretical Computer Science, to appear. arXiv:0808.1037

- B. Coecke, E. O. Paquette and D. Pavlovic (2009) *Classical and quantum structuralism*. In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 29–69, Cambridge University Press. arXiv:0904.1997
- L. Dixon and R. Duncan (2009) *Graphical reasoning in compact closed categories for quantum computation*. Annals of Mathematics and Artificial Intelligence **56**, 23–42.
- P. Selinger (2010) *Finite dimensional Hilbert spaces are complete for dagger compact closed categories*. Electronic Notes in Theoretical Computer Science, to appear. http://www.mathstat.dal.ca/∼selinger/papers.html♯finhilb
- B. Coecke and A. Kissinger (2010) *The compositional structure of multipartite quantum entanglement*. arXiv:1002.2540
- B. Coecke, B. Edwards and R. W. Spekkens (2010) *Phase groups and the origin of non-locality for qubits*. Electronic Notes in Theoretical Computer Science, to appear.
- B. Coecke and S. Perdrix (2010) *Environment and classical channels in categorical quantum mechanics*. Forthcoming.