Introduction to Quantum Programming and Semantics

Week 9: Complementarity

Chris Heunen

THE UNIVERSITY of EDINBURGH
informatics

Overview

- Incompatible Frobenius structures: mutually unbiased bases
- Deutsch–Jozsa algorithm: prototypical use of complementarity
- Quantum groups: strong complementarity
- Qubit gates: quantum circuits

Idea

- Measure qubit in basis $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}$, then in $\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\}$: probability of either outcome $1/2$.

Idea

- Measure qubit in basis $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}$, then in $\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\}$: probability of either outcome $1/2$.
- First measurement provides no information about second: Heisenberg's *uncertainty principle*.

Idea

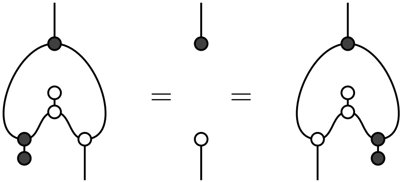
- Measure qubit in basis $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}$, then in $\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\}$: probability of either outcome $1/2$.
- First measurement provides no information about second: Heisenberg's *uncertainty principle*.
- Orthogonal bases $\{a_i\}$ and $\{b_j\}$ are complementary/unbiased if

$$\langle a_i | b_j \rangle \langle b_j | a_i \rangle = c$$

for some $c \in \mathbb{C}$.

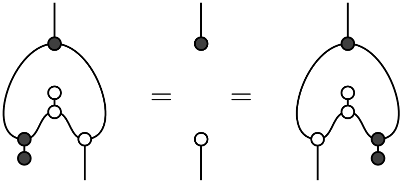
Complementarity

In braided monoidal dagger category, symmetric dagger Frobenius structures  and  on the same object are complementary if:

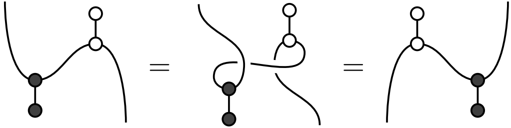


Complementarity

In braided monoidal dagger category, symmetric dagger Frobenius structures  and  on the same object are complementary if:



Black and white not obviously interchangeable. But by symmetry:



So could have added two more equalities.

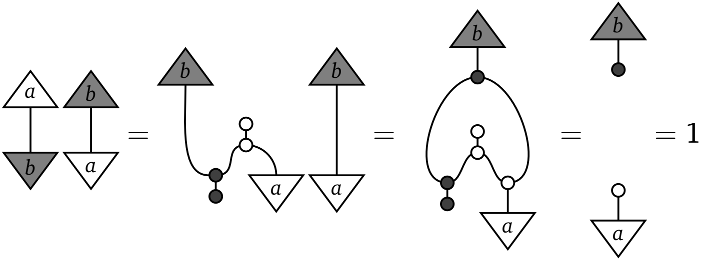
Complementarity in **FHilb**

Commutative dagger Frobenius structures in **FHilb** complementary if and only if they copy complementary bases (with $c = 1$).

Complementarity in **FHilb**

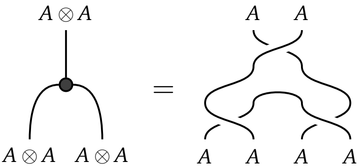
Commutative dagger Frobenius structures in **FHilb** complementary if and only if they copy complementary bases (with $c = 1$).

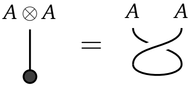
Proof. For all a in white basis, and b in black basis:



Twisted knickers

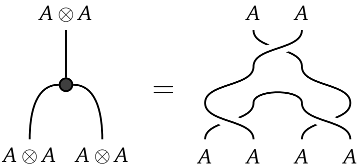
In compact dagger category, if A is self-dual, the following Frobenius structure on $A \otimes A$ is complementary to pair of pants:

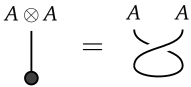


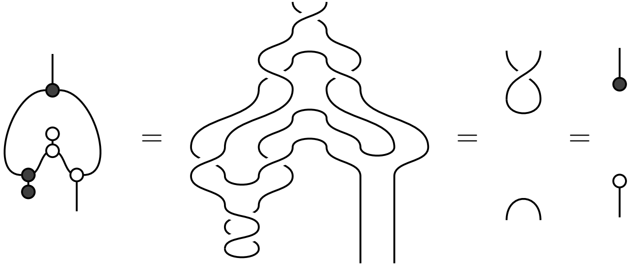


Twisted knickers

In compact dagger category, if A is self-dual, the following Frobenius structure on $A \otimes A$ is complementary to pair of pants:







So Frobenius structure on A gives complementary pair on $A \otimes A$.

Pauli basis

Three mutually complementary bases of $\mathbb{C}^2$:

$$
\begin{aligned}
&X \text{ basis} && \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} \\
&Y \text{ basis} && \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix} \right\} \\
&Z \text{ basis} && \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}
\end{aligned}
$$

Pauli basis

Three mutually complementary bases of $\mathbb{C}^2$:

$$
\begin{array}{ll}
X \text{ basis} & \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \right\} \\
Y \text{ basis} & \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} \right\} \\
Z \text{ basis} & \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\}
\end{array}
$$

- Largest family of complementary bases for $\mathbb{C}^2$: no four bases all mutually unbiased.

Pauli basis

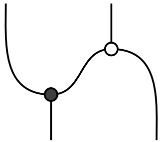
Three mutually complementary bases of $\mathbb{C}^2$:

$$
\begin{array}{ll}
X \text{ basis} & \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \right\} \\
Y \text{ basis} & \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} \right\} \\
Z \text{ basis} & \left\{ \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\}
\end{array}
$$

- Largest family of complementary bases for $\mathbb{C}^2$: no four bases all mutually unbiased.
- What is the maximum number of mutually complementary bases in a given dimension? Only known for prime power dimensions p^n.

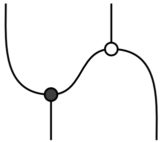
Characterisation

Symmetric dagger Frobenius structures in braided monoidal dagger category are complementary if and only if the following is unitary:

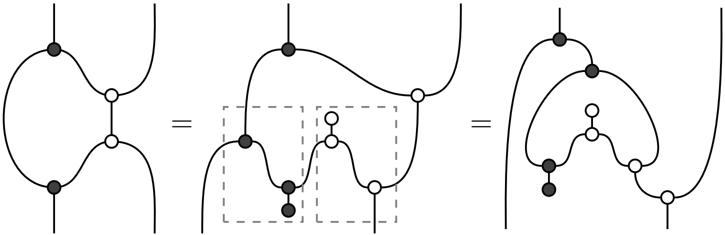


Characterisation

Symmetric dagger Frobenius structures in braided monoidal dagger category are complementary if and only if the following is unitary:

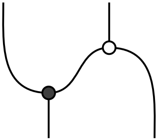


Proof. Compose with adjoint:

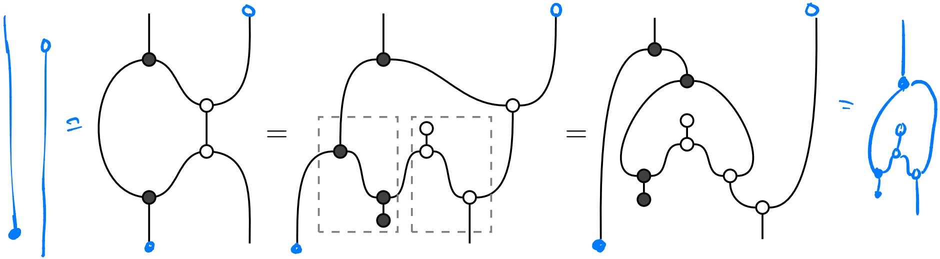


Characterisation

Symmetric dagger Frobenius structures in braided monoidal dagger category are complementary if and only if the following is unitary:



Proof. Compose with adjoint:



Conversely, if is identity, compose with white counit on top right, black unit on bottom left, to get complementarity.

Complementarity in **Rel**

If G, H are nontrivial groups, these are complementary groupoids:

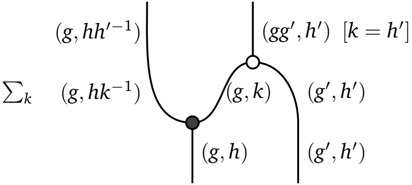
- objects $g \in G$, morphisms $g \xrightarrow{(g,h)} g$, with $(g, h') \bullet (g, h) = (g, hh')$
- objects $h \in H$, morphisms $h \xrightarrow{(g,h)} h$, with $(g', h) \circ (g, h) = (gg', h)$

Complementarity in **Rel**

If G, H are nontrivial groups, these are complementary groupoids:

- objects $g \in G$, morphisms $g \xrightarrow{(g,h)} g$, with $(g,h') \bullet (g,h) = (g,hh')$
- objects $h \in H$, morphisms $h \xrightarrow{(g,h)} h$, with $(g',h) \circ (g,h) = (gg',h)$

Proof.



Every input related to unique output, so unitary.

Groupoid allows complementary one just when every object has number of outgoing morphisms.

The Deutsch-Jozsa algorithm

Solves certain problem faster than possible classically

- Typical exact quantum decision algorithm (no approximation)
- Problem artificial, but other important algorithms very similar:
  - Shor's factoring algorithm
  - Grover's search algorithm
  - the hidden subgroup problem
- 'All or nothing' nature makes it categorical

The Deutsch-Jozsa algorithm

Problem:

- Given 2-valued function $A \xrightarrow{f} \{0, 1\}$ on a finite set A.
- Constant if takes just a single value on every element of A.
- Balanced if takes value 0 on exactly half the elements of A.
- You are promised that f is either constant or balanced.
  You must decide which.

The Deutsch-Jozsa algorithm

Problem:

- Given 2-valued function $A \xrightarrow{f} \{0, 1\}$ on a finite set A.
- Constant if takes just a single value on every element of A.
- Balanced if takes value 0 on exactly half the elements of A.
- You are promised that f is either constant or balanced.
  You must decide which.

Best classical strategy:

- Sample f on $\frac{1}{2}|A| + 1$ elements of A.
  If different values then balanced, otherwise constant.

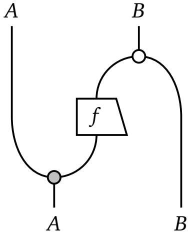
The Deutsch-Jozsa algorithm

Quantum Deutsch-Jozsa uses f only *once*!
How to access f? Can only apply unitary operators...

The Deutsch-Jozsa algorithm

Quantum Deutsch-Jozsa uses f only *once*!
How to access f? Can only apply unitary operators...
Must embed $A \xrightarrow{f} \{0, 1\}$ into an *oracle*.

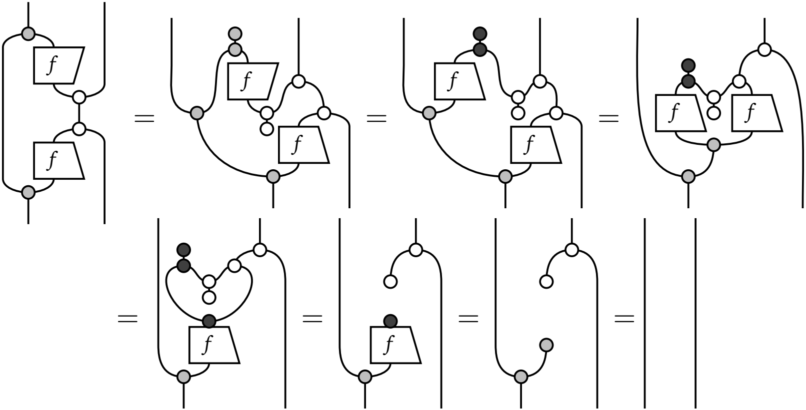
Given Frobenius structures (A, ⅄, ⫯) and (B, ⅄, ⫯) in monoidal dagger category, oracle is morphism $A \xrightarrow{f} B$ making the following unitary:



Where to find oracles

Let (A, ◍), (B, ●) and (B, ○) be symmetric dagger Frobenius.
If ●, ○ complementary, self-conjugate comonoid homomorphism
(A, ◍) $\xrightarrow{f}$ (B, ●) is oracle.

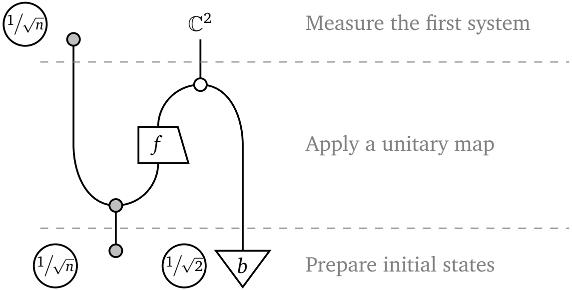
Proof.



The Deutsch-Jozsa algorithm

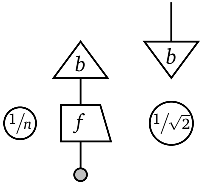
Let $A \xrightarrow{f} \{0,1\}$ be given function, and $|A| = n$.
Choose complementary bases ● $= \mathbb{C}^2$, ○ $= \mathbb{C}[\mathbb{Z}_2]$.
Let $b = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, a copyable state of ○.

The Deutsch–Jozsa algorithm is this morphism:



Deutsch-Jozsa simplifies

The Deutsch–Jozsa algorithm simplifies to:



Proof. Duplicate copyable state *b* through white dot, and apply noncommutative spider theorem to cluster of gray dots.

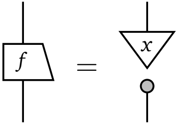
Deutsch-Jozsa correctness: constant

If $A \xrightarrow{f} \{0, 1\}$ is constant, the Deutsch-Jozsa history is certain.

Deutsch-Jozsa correctness: constant

If $A \xrightarrow{f} \{0,1\}$ is constant, the Deutsch-Jozsa history is certain.

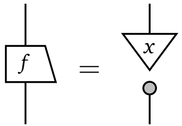
Proof. If $f(a) = x$ for all $a \in A$, oracle $H \xrightarrow{f} \mathbb{C}^2$ decomposes as:



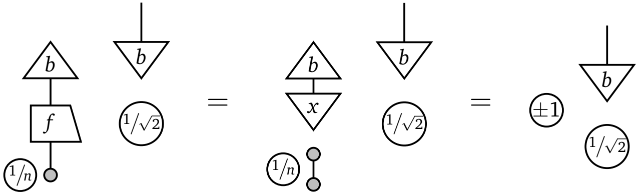
Deutsch-Jozsa correctness: constant

If $A \xrightarrow{f} \{0,1\}$ is constant, the Deutsch-Jozsa history is certain.

Proof. If $f(a) = x$ for all $a \in A$, oracle $H \xrightarrow{f} \mathbb{C}^2$ decomposes as:



So history is:



This has norm 1, so the history is certain.

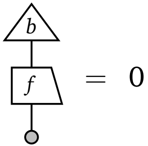
Deutsch-Jozsa correctness:balanced

If $A \xrightarrow{f} \{0, 1\}$ is balanced, the Deutsch–Jozsa history is impossible.

Deutsch-Jozsa correctness:balanced

If $A \xrightarrow{f} \{0,1\}$ is balanced, the Deutsch–Jozsa history is impossible.

Proof. The function f is balanced just when the following holds:

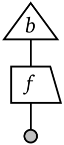


Recall $b = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Deutsch-Jozsa correctness:balanced

If $A \xrightarrow{f} \{0,1\}$ is balanced, the Deutsch–Jozsa history is impossible.

Proof. The function f is balanced just when the following holds:



$= \ 0$

Recall $b = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Hence the final history equals 0.

Bialgebras

Complementary classical structures in **FHilb** are mutually unbiased bases. How to build them?

Bialgebras

Complementary classical structures in **FHilb** are mutually unbiased bases. How to build them?

One standard way: let G be finite group, and consider Hilbert space with basis $\{g \in G\}$, with

 $: g \mapsto g \otimes g$

 $: g \mapsto 1$

 $: g \otimes h \mapsto gh$

 $: 1 \mapsto \sum_{g \in G} g$

Bialgebras

Complementary classical structures in **FHilb** are mutually unbiased bases. How to build them?

One standard way: let G be finite group, and consider Hilbert space with basis $\{g \in G\}$, with

: $g \mapsto g \otimes g$

: $g \mapsto 1$

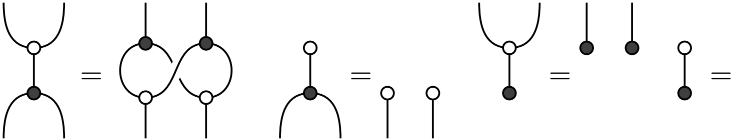
: $g \otimes h \mapsto gh$

: $1 \mapsto \sum_{g \in G} g$

Some nice relationships emerge between  and .

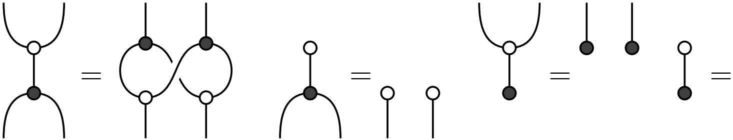
Bialgebras

In a braided monoidal category, a bialgebra consists of a monoid
(A,, ) and a comonoid (A,, ) satisfying:



Bialgebras

In a braided monoidal category, a bialgebra consists of a monoid $(A,$ , $)$ and a comonoid $(A,$ , $)$ satisfying:



Example: monoid M is a bialgebra in **Set** and hence in **Rel** and **FHilb**

: $m \mapsto (m, m)$ : $m \mapsto \bullet$ : $(m, n) \mapsto mn$ : $\bullet \mapsto 1_M$.

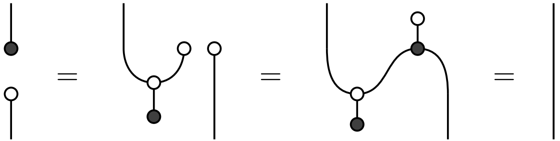
Frobenius hates bialgebras

In a braided monoidal category, if a monoid (A, , ) and comonoid (A, , ) form a Frobenius structure and a bialgebra, then $A \simeq I$.

Frobenius hates bialgebras

In a braided monoidal category, if a monoid (A,,) and comonoid (A,,) form a Frobenius structure and a bialgebra, then $A \simeq I$.

Proof. Will show  and  are inverses. The bialgebra laws already require  $\circ$  $= \mathrm{id}_I$. For the other composite:



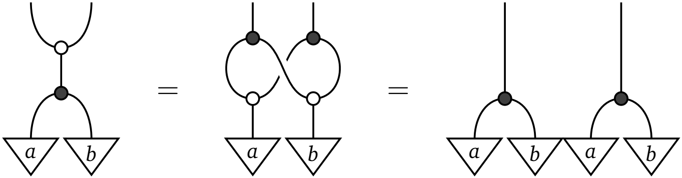
Copyable states

In a braided monoidal category if  and  form a bialgebra, then copyable states for  are a monoid under .

Copyable states

In a braided monoidal category if and form a bialgebra, then copyable states for are a monoid under .

Proof. Associativity is immediate. Unitality comes down to third bialgebra law: is copyable for . Have to prove well-definedness. Let a and b be copyable states for .



Hence -copyable states are indeed closed under .

Strong complementarity

- Consider $\mathbb{C}^2$ in **FHilb**. Computational basis $\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}$ gives dagger Frobenius structure . Orthogonal basis $\{\begin{pmatrix}e^{i\varphi}\\e^{i\theta}\end{pmatrix}, \begin{pmatrix}e^{i\varphi}\\-e^{i\theta}\end{pmatrix}\}$ gives dagger Frobenius structure . Complementary, but only a bialgebra if $\varphi = \theta = 0$.

Strong complementarity

- Consider $\mathbb{C}^2$ in **FHilb**. Computational basis $\{\binom{1}{0}, \binom{0}{1}\}$ gives dagger Frobenius structure. Orthogonal basis $\{\begin{pmatrix} e^{i\varphi} \\ e^{i\theta} \end{pmatrix}, \begin{pmatrix} e^{i\varphi} \\ -e^{i\theta} \end{pmatrix}\}$ gives dagger Frobenius structure. Complementary, but only a bialgebra if $\varphi = \theta = 0$.

- In a braided monoidal dagger category, two dagger symmetric Frobenius structures are strongly complementary when they are complementary, and also form a bialgebra.

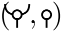
Strong complementarity in **FHilb**

In **FHilb**, strongly complementary symmetric dagger Frobenius structures, one of which is commutative, correspond to finite groups.

Strong complementarity in **FHilb**

In **FHilb**, strongly complementary symmetric dagger Frobenius structures, one of which is commutative, correspond to finite groups.

Proof.

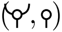
- Given strongly complementary symmetric dagger Frobenius structures, the states that are self-conjugate, copyable and deletable for  form a group under .
- By the classification theorem for commutative dagger Frobenius structures, there is an entire basis of such states for .

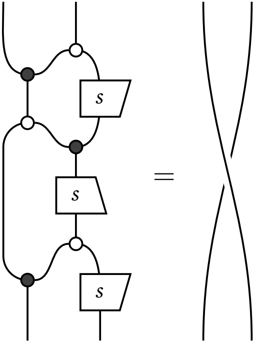
```
f(a,b) {
    bit c := a;
    a := b;
    b := c;

    return (.a, .b);
}
```

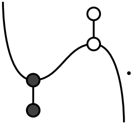
```
                          a = 0    b = 0
a := a XOR b;               0        0
b := b XOR a;               0        0
a := a XOR b;               0        0
```

CNOT(a,b) = (a, a XOR b)

Qubit gates

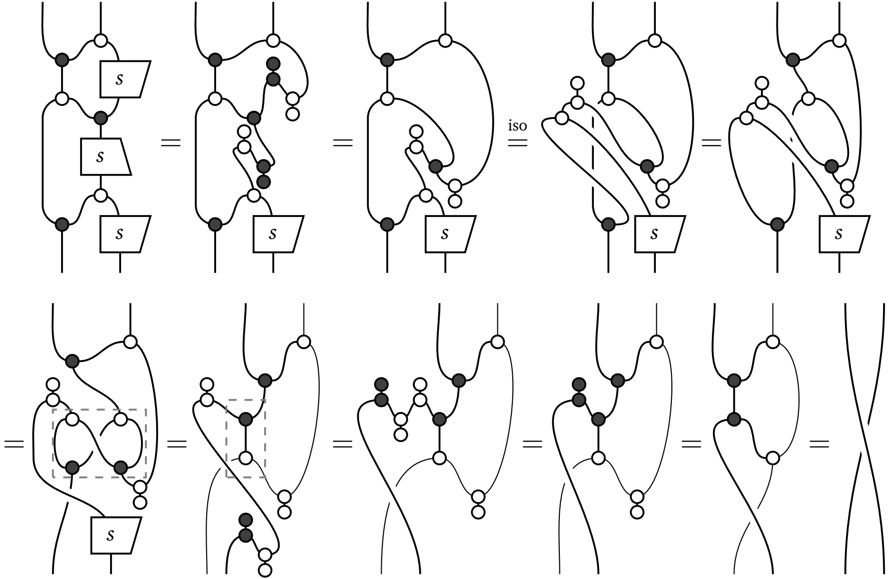
In a braided monoidal dagger category, let  and  be complementary classical structures with antipode s. Then the first bialgebra law holds if and only if:



where $s =$  .

Qubit gates

Proof.



Qubit gates in **FHilb**

Fix A to be qubit $\mathbb{C}^2$; let (,) copy computational basis $\{|0\rangle, |1\rangle\}$, and (,) copy the X basis. The three antipodes s become identities.

The three unitaries reduce to three CNOT gates:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Qubit gates in **FHilb**

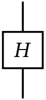
Fix A to be qubit $\mathbb{C}^2$; let $(\bullet, \bullet)$ copy computational basis $\{|0\rangle, |1\rangle\}$, and $(\circ, \circ)$ copy the X basis. The three antipodes s become identities.

The three unitaries reduce to three CNOT gates:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

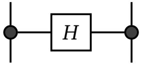
These two classical structures are transported into each other by Hadamard gate:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} =$$



Controlled Z

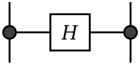
The CZ gate in **FHilb** can be defined as follows.

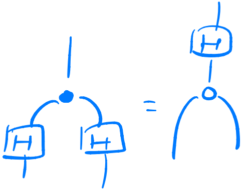
CZ = 

Controlled Z

The CZ gate in **FHilb** can be defined as follows.

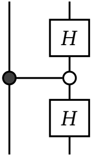
CZ =

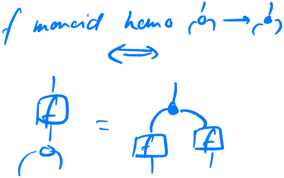




Proof. Rewrite as:

CZ =





Hence

$$\mathrm{CZ} = (\mathrm{id} \otimes H) \circ \mathrm{CNOT} \circ (\mathrm{id} \otimes H) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

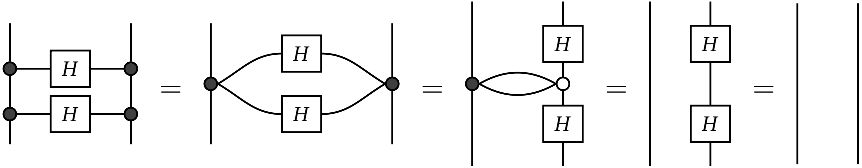
Controlled Z

If $(A,$ $)$ and $(A,$ $)$ complementary classical structures in braided monoidal dagger category, and $A \xrightarrow{H} A$ satisfies $H \circ H = \mathrm{id}_A$, then CZ makes sense and satisfies $\mathrm{CZ} \circ \mathrm{CZ} = \mathrm{id}$.

Controlled Z

If $(A, \bullet)$ and $(A, \circ)$ complementary classical structures in braided monoidal dagger category, and $A \xrightarrow{H} A$ satisfies $H \circ H = \mathrm{id}_A$, then CZ makes sense and satisfies $\mathrm{CZ} \circ \mathrm{CZ} = \mathrm{id}$.

Proof.



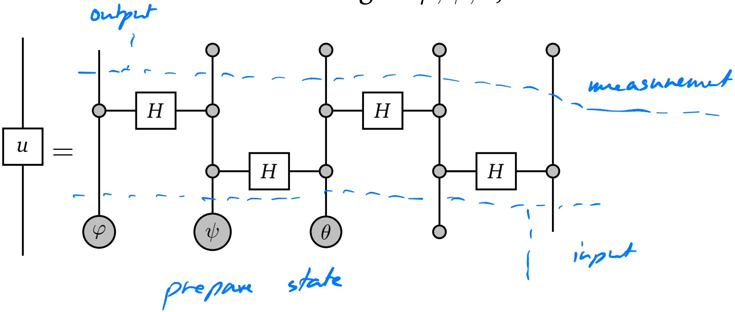
Measurement-based computing

Single-qubit unitaries can be implemented via Euler angles: unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ allows phases φ, ψ, θ with $u = Z_\varphi \circ X_\psi \circ Z_\theta$, where Z_θ is rotation in Z basis over angle θ, and X_φ in X basis over angle φ.

Measurement-based computing

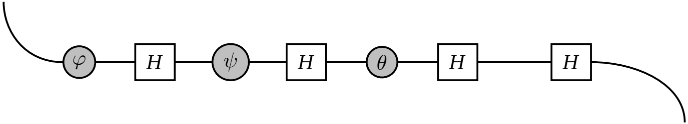
Single-qubit unitaries can be implemented via Euler angles: unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ allows phases φ, ψ, θ with $u = Z_\varphi \circ X_\psi \circ Z_\theta$, where Z_θ is rotation in Z basis over angle θ, and X_φ in X basis over angle φ.

If unitary $\mathbb{C}^2 \xrightarrow{u} \mathbb{C}^2$ in **FHilb** has Euler angles φ, ψ, θ, then:

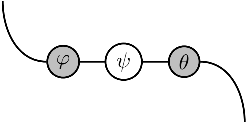


Measurement-based computing

Proof. Use phased spider theorem to reduce to:



But by transport lemma, this is just:



which equals u, by definition of the Euler angles.

Summary

- Incompatible Frobenius structures: mutually unbiased bases
- Deutsch-Jozsa algorithm: prototypical use of complementarity
- Quantum groups: strong complementarity
- Qubit gates: use in quantum circuits