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 \{ (1, 0), (0, 1) \}, then in \{ \frac{1}{\sqrt{2}} (1, 1), \frac{1}{\sqrt{2}} (1, -1) \}: probability of either outcome 1/2.
Idea

- Measure qubit in basis \{ \left( \begin{array}{c} 1 \\ 0 \end{array} \right), \left( \begin{array}{c} 0 \\ 1 \end{array} \right) \}, \text{ then in } \{ \frac{1}{\sqrt{2}} \left( \begin{array}{c} 1 \\ 1 \end{array} \right), \frac{1}{\sqrt{2}} \left( \begin{array}{c} 1 \\ -1 \end{array} \right) \}: \text{ probability of either outcome } 1/2.

- First measurement provides no information about second: Heisenberg’s *uncertainty principle*. 
Idea

- Measure qubit in basis \{ (\frac{1}{0}) , (0\frac{1}{1}) \}, then in \{ \frac{1}{\sqrt{2}} (\frac{1}{1}) , \frac{1}{\sqrt{2}} (\frac{1}{-1}) \}: 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 $\triangleright$ and $\triangleleft$ on the same object are complementary if:
Complementarity

In braided monoidal dagger category, symmetric dagger Frobenius structures $\triangleright$ and $\triangleleft$ on the same object are **complementary** if:

\[
\begin{align*}
\begin{array}{c}
\text{Diagram 1} \quad = \quad \text{Diagram 2} \quad = \\
\text{Diagram 3}
\end{array}
\end{align*}
\]

Black and white not obviously interchangeable. But by symmetry:

\[
\begin{align*}
\begin{array}{c}
\text{Diagram 4} \quad = \quad \text{Diagram 5} \quad = \\
\text{Diagram 6}
\end{array}
\end{align*}
\]

So could have added two more equalities.
Complementarity in $\text{FHilb}$

Commutative dagger Frobenius structures in $\text{FHilb}$ complementary if and only if they copy complementary bases (with $c = 1$).
Complementarity in $\text{FHilb}$

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

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

\[
\begin{align*}
\begin{array}{ccc}
\begin{array}{ccc}
a & b & b \\
\downarrow & & \downarrow \\
b & & a
\end{array}
& = &
\begin{array}{ccc}
b & a \\
\downarrow & & \downarrow \\
a & & a
\end{array}
& = &
\begin{array}{ccc}
b & \\
\downarrow & & \downarrow \\
a & & a
\end{array}
& = &
\begin{array}{ccc}
b \\
\downarrow & & \downarrow \\
a
\end{array}
= 1
\end{array}
\end{align*}
\]
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 $\mathbb{C}^2$:

- **$X$ basis**:
  \[
  \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}
  \]

- **$Y$ basis**:
  \[
  \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}
  \]

- **$Z$ basis**:
  \[
  \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}
  \]
Pauli basis

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

- **X basis** $\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$

- **Y basis** $\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}$

- **Z basis** $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$

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

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

- **X basis**
  $$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$$

- **Y basis**
  $$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}$$

- **Z basis**
  $$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

- 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 complementary if and only if the following is unitary:

\[ \text{Diagram with two circles connected by a line} \]
Characterisation

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

Proof. Compose with adjoint:
Characterisation

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

\[
\text{Proof. Compose with adjoint:}
\]

Conversely, if is identity, compose with white counit on top right, black unit on bottom left, to get complementarity.
Complementarity in \textbf{Rel}

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

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

**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 $f : A \rightarrow \{0, 1\}$ 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 \((A, \&_A, \*$\_A*)\) and \((B, \&_B, \*$\_B*)\) in monoidal dagger category, *oracle* is morphism \( A \xrightarrow{f} B \) making the following unitary:
Where to find oracles

Let \((A, \otimes), (B, \otimes)\) and \((B, \otimes)\) be symmetric dagger Frobenius. If \(\otimes\) complementary, self-conjugate comonoid homomorphism \((A, \otimes) \overset{f}{\rightarrow} (B, \otimes)\) is oracle.

Proof.
The Deutsch-Jozsa algorithm

Let $A \xrightarrow{f} \{0, 1\}$ be given function, and $|A| = n$. Choose complementary bases $\bigcirc = \mathbb{C}^2$, $\bigcirc = \mathbb{C}[\mathbb{Z}_2]$. Let $b = \left( \begin{array}{c} 1 \\ -1 \end{array} \right)$, a copyable state of $\bigcirc$.

The **Deutsch–Jozsa algorithm** is this morphism:

1. Prepare initial states
2. Apply a unitary map
3. Measure the first system
4. Prepare initial states
Deutsch-Jozsa simplifies

The Deutsch–Jozsa algorithm simplifies to:

\[
\frac{1}{\sqrt{2}} \frac{1}{n} f b
\]

**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:

\[
\begin{align*}
\begin{array}{c}
f \\
\end{array} &= \\
\begin{array}{c}
x \\
\end{array}
\end{align*}
\]
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:

\[
\begin{align*}
    f &= x \\
    b &= 1/\sqrt{2} \\
    1/n &= 
\end{align*}
\]

So history is:

\[
\begin{align*}
    b &= b \\
    1/\sqrt{2} &= 1/\sqrt{2} \\
    1/n &= 1/n \\
    \pm 1 &= \pm 1 \\
    1/\sqrt{2} &= 1/\sqrt{2}
\end{align*}
\]

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 $A^f \rightarrow \{0, 1\}$ is balanced, the Deutsch-Jozsa history is impossible.

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

\[
\begin{array}{c}
\text{b} \\
\downarrow \\
\text{f} \\
\text{= 0}
\end{array}
\]

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:

\[
\begin{array}{c}
\bigtriangleup \\
\downarrow \\
\bigtriangledown \\
0
\end{array}
\]

Recall \( b = \left( \begin{array}{c} 1 \\ -1 \end{array} \right) \). Hence the final history equals 0.
Bialgebras

Complementary classical structures in $\text{FHilb}$ are mutually unbiased bases. How to build them?
Bialgebras

Complementary classical structures in $\text{FHilb}$ 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

$\Upsilon: g \mapsto g \otimes g$

$\triangleleft: g \otimes h \mapsto gh$

$\Phi: g \mapsto 1$

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

Complementary classical structures in \textbf{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

\[
\begin{align*}
\mathcal{Y}: g & \mapsto g \otimes g \\
\mathcal{A}: g \otimes h & \mapsto gh
\end{align*}
\]

\[
\begin{align*}
\mathcal{O}: g & \mapsto 1 \\
\mathcal{O}: 1 & \mapsto \sum_{g \in G} g
\end{align*}
\]

Some nice relationships emerge between $\mathcal{Y}$ and $\mathcal{A}$.
Bialgebras

In a braided monoidal category, a bialgebra consists of a monoid \((A, \cdot, \varepsilon)\) and a comonoid \((A, \triangledown, \varphi)\) satisfying:

\[
\begin{align*}
\triangledown & \Rightarrow \varepsilon, \\
\varphi & \Rightarrow \varepsilon,
\end{align*}
\]

Example: monoid \(M\) is a bialgebra in \(\text{Set}\) and hence in \(\text{Rel}\) and \(\text{FHilb}\):

\[
\begin{align*}
\varepsilon &: \ x \mapsto (x, x), \\
\varphi &: \ (x, y) \mapsto xy, \\
\varepsilon &: \ 1 \mapsto 1_M.
\end{align*}
\]
In a braided monoidal category, a bialgebra consists of a monoid $(A, \cdot, \mathbb{1})$ and a comonoid $(A, \varepsilon, \epsilon)$ satisfying:

Example: monoid $M$ is a bialgebra in $\textbf{Set}$ and hence in $\textbf{Rel}$ and $\textbf{FHilb}$

$$\varepsilon^\prime: m \mapsto (m, m) \quad \varepsilon: m \mapsto \bullet \quad \cdot: (m, n) \mapsto mn \quad \mathbb{1}: \bullet \mapsto \mathbb{1}_M.$$
Frobenius hates bialgebras

In a braided monoidal category, if a monoid \((A, \hat{\cdot}, \hat{\bullet})\) and comonoid \((A, \hat{\cdot}', \hat{\bullet}')\) form a Frobenius structure and a bialgebra, then \(A \cong I\).
Frobenius hates bialgebras

In a braided monoidal category, if a monoid \((A, \cdot, \varepsilon)\) and comonoid \((A, \delta, \epsilon)\) form a Frobenius structure and a bialgebra, then \(A \cong I\).

**Proof.** Will show \(\varepsilon\) and \(\delta\) are inverses. The bialgebra laws already require \(\delta \circ \varepsilon = \text{id}_I\). For the other composite:
Copyable states

In a braided monoidal category if \( \triangleright \) and \( \triangleright \rhd \) form bialgebra, then copyable states for \( \triangleright \) are monoid under \( \triangleright \).
Copyable states

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

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

\[
\begin{align*}
\begin{array}{c}
\begin{tikzpicture}
\draw (-0.5,0) -- (-0.5,1);
\draw (0.5,0) -- (0.5,1);
\draw (0,1) -- (0,2);
\draw (-0.5,1) -- (0,1);
\draw (0.5,1) -- (0,1);
\draw (0,2) -- (0,3);
\filldraw[fill=black] (-0.5,0) circle (0.1);
\filldraw[fill=black] (0.5,0) circle (0.1);
\filldraw[fill=white] (0,1) circle (0.1);
\filldraw[fill=black] (0,2) circle (0.1);
\end{tikzpicture}
\end{array}
\end{align*}
\]

Hence $\triangleright$-copyable states are indeed closed under $\otimes$.
Strong complementarity

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

- Consider $\mathbb{C}^2$ in $\text{FHilb}$. Computational basis $\{(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$ gives dagger Frobenius structure $\triangleleft$. 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 $\triangle$. 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 $\mathbf{FHilb}$

In $\mathbf{FHilb}$, strongly complementary symmetric dagger Frobenius structures, one of which is commutative, correspond to finite groups.
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 \((\mathcal{Y}, \mathcal{F})\) form a group under \(\otimes\).
- By the classification theorem for commutative dagger Frobenius structures, there is an entire basis of such states for \(\mathcal{Y}\).
Qubit gates

In a braided monoidal dagger category, let $(\otimes, \oplus)$ and $(\Uparrow, \circledast)$ be complementary classical structures with antipode $s$. Then the first bialgebra law holds if and only if:

\[ s^2 = \frac{24}{31} \]
Qubit gates

Proof.
Qubit gates in FHilb

Fix $A$ to be qubit $\mathbb{C}^2$; let $(\otimes, \bullet)$ copy computational basis $\{|0\rangle, |1\rangle\}$, and $(\bigvee, \bigvee)$ 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 $(\otimes, \oplus)$ copy computational basis $\{|0\rangle, |1\rangle\}$, and $(\bigwedge, \bigvee)$ 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 \textbf{FHilb} can be defined as follows.

\[ \text{CZ} = \begin{array}{c}
\text{H}
\end{array} \]
Controlled Z

The CZ gate in FHilb can be defined as follows.

\[ CZ = \begin{array}{c}
\end{array} \]

Proof. Rewrite as:

\[ CZ = \begin{array}{c}
\end{array} \]

Hence

\[ CZ = (\text{id} \otimes H) \circ \text{CNOT} \circ (\text{id} \otimes H) = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1
\end{pmatrix} \]
Controlled Z

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

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

Proof.
Measurement-based computing

Single-qubit unitaries can be implemented via **Euler angles**: unitary $\mathbb{C}^2 \rightarrow \mathbb{C}^2$ allows phases $\varphi, \psi, \theta$ with $u = Z_\theta \circ X_\psi \circ Z_\varphi$, where $Z_\theta$ is rotation in $Z$ basis over angle $\theta$, and $X_\varphi$ in $X$ basis over angle $\varphi$. 
Measurement-based computing

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

If unitary $C^2 \xrightarrow{u} C^2$ in $\text{FHilb}$ has Euler angles $\varphi, \psi, \theta$, then:
**Proof.** Use phased spider theorem to reduce to:

\[ \varphi H \psi H \theta H \]

But by transport lemma, this is just:

\[ \varphi \psi \theta \]

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