# Introduction to Quantum Programming and Semantics

## Week 2: Categories, Hilbert spaces

Chris Heunen

THE UNIVERSITY *of* EDINBURGH
informatics

# Categorical semantics

Want:

- Compositionality: $[\![\texttt{F; G}]\!] = [\![\texttt{G}]\!] \circ [\![\texttt{F}]\!]$
- Concurrency: $[\![\texttt{F par G}]\!] = [\![\texttt{F}]\!] \otimes [\![\texttt{G}]\!]$
- Recursion: $[\![\texttt{F(X)}]\!] = [\![\texttt{F}]\!]([\![\texttt{X}]\!])$

# Categorical semantics

Want:

- Compositionality: $[\![\mathtt{F;\ G}]\!] = [\![\mathtt{G}]\!] \circ [\![\mathtt{F}]\!]$
- Concurrency: $[\![\mathtt{F\ par\ G}]\!] = [\![\mathtt{F}]\!] \otimes [\![\mathtt{G}]\!]$
- Recursion: $[\![\mathtt{F(X)}]\!] = [\![\mathtt{F}]\!]([\![\mathtt{X}]\!])$

Where can $[\![\mathtt{F}]\!]$ live?

- $\lambda$-calculus
- partially ordered sets
- categories

# Categorical semantics

Want:

- Compositionality: $[\![\texttt{F; G}]\!] = [\![\texttt{G}]\!] \circ [\![\texttt{F}]\!]$
- Concurrency: $[\![\texttt{F par G}]\!] = [\![\texttt{F}]\!] \otimes [\![\texttt{G}]\!]$
- Recursion: $[\![\texttt{F(X)}]\!] = [\![\texttt{F}]\!]([\![\texttt{X}]\!])$

Where can $[\![\texttt{F}]\!]$ live?

- $\lambda$-calculus
- partially ordered sets
- categories

Instantiate in different categories:

- Isolate differences between quantum and classical behaviour
- Apply quantum thinking to other settings

# Categories

Category theory is a way of thinking more than deep theorems

> *"The essential virtue of category theory is as a discipline for making definitions, the programmer's main task in life."*
>
> *– D. E. Rydeheard*

> *"Good general theory does not search for the maximum generality, but for the right generality."*
>
> *– S. Mac Lane*

# Categories

Categories consist of

- objects $A, B, C, \ldots$
- morphisms $A \xrightarrow{f} B$ going between objects

# Categories

Categories consist of

- objects $A, B, C, \ldots$
- morphisms $A \xrightarrow{f} B$ going between objects

Examples:

- physical systems, physical processes governing them
- data types, algorithms manipulating them
- algebraic/geometric structures, structure-preserving functions
- logical propositions, implications between them

# Categories

Categories consist of

- objects $A, B, C, \ldots$
- morphisms $A \xrightarrow{f} B$ going between objects

Examples:

- physical systems, physical processes governing them
- data types, algorithms manipulating them
- algebraic/geometric structures, structure-preserving functions
- logical propositions, implications between them

Ignore all structure of objects, focus relationships between objects
"Morphisms are more important than objects"

# Categories

A category $\mathbf{C}$ consists of the following data:

- a collection $\mathrm{Ob}(\mathbf{C})$ of objects
- for every pair of objects $A$ and $B$, a collection $\mathbf{C}(A, B)$ of morphisms, with $f \in \mathbf{C}(A, B)$ written $A \xrightarrow{f} B$
- for all morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ a composite $A \xrightarrow{g \circ f} C$
- for every object $A$ an identity morphism $A \xrightarrow{\mathrm{id}_A} A$

such that:

- associativity: $h \circ (g \circ f) = (h \circ g) \circ f$
- identity: $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$

# Sets and functions

The category **Set** of sets and functions:

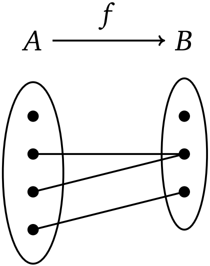
- *objects* are sets $A, B, C, \ldots$
- *morphisms* are functions $f, g, h, \ldots$
- *composition* of $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ is the function $g \circ f : a \mapsto g(f(a))$
- *the identity morphism* on $A$ is the function $\mathrm{id}_A : a \mapsto a$

# Sets and functions

The category **Set** of sets and functions:

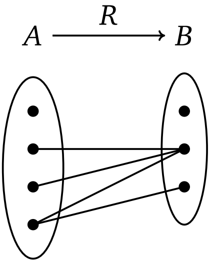
- *objects* are sets $A, B, C, \ldots$
- *morphisms* are functions $f, g, h, \ldots$
- *composition* of $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ is the function $g \circ f : a \mapsto g(f(a))$
- *the identity morphism* on $A$ is the function $\mathrm{id}_A : a \mapsto a$

Think of a function $A \xrightarrow{f} B$ dynamically, as indicating how elements of $A$ can evolve into elements of $B$



# Relations

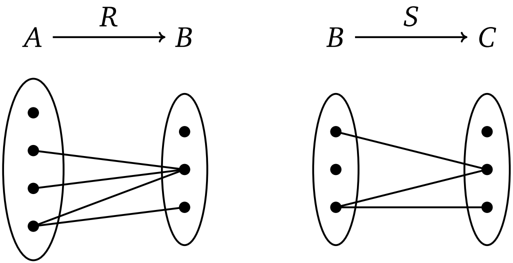
Given sets $A$ and $B$, a relation $A \xrightarrow{R} B$ is a subset $R \subseteq A \times B$.




Nondeterministic: an element of $A$ can relate to more than one element of $B$, or to none.

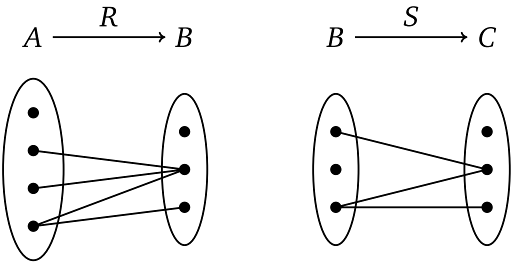
# Composition of relations

Suppose we have a pair of head-to-tail relations:

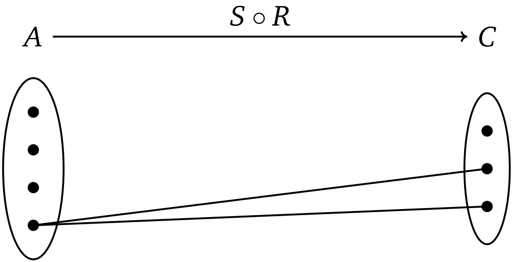


# Composition of relations

Suppose we have a pair of head-to-tail relations:

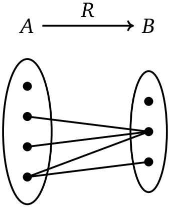



Then our interpretation gives a natural notion of composition:



# Relations as matrices

We can write relations as (0,1)-valued matrices:




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

Composition of relations is then ordinary matrix multiplication, with logical disjunction (OR) and conjunction (AND) for $+$ and $\times$.

# Sets and relations

The category **Rel** of sets and relations:

- *objects* are sets $A, B, C, \ldots$;
- *morphisms* are relations $R \subseteq A \times B$, with $(a, b) \in R$ written $aRb$;
- *composition* $A \xrightarrow{R} B \xrightarrow{S} C$ is $\{(a, c) \in A \times C \mid \exists b \in B \colon aRb, bSc\}$;
- *the identity morphism* on $A$ is $\{(a, a) \in A \times A \mid a \in A\}$.

# Sets and relations

The category **Rel** of sets and relations:

- *objects* are sets $A, B, C, \ldots$;
- *morphisms* are relations $R \subseteq A \times B$, with $(a, b) \in R$ written $aRb$;
- *composition* $A \xrightarrow{R} B \xrightarrow{S} C$ is $\{(a, c) \in A \times C \mid \exists b \in B \colon aRb, bSc\}$;
- *the identity morphism* on $A$ is $\{(a, a) \in A \times A \mid a \in A\}$.

It seems like **Rel** should be a lot like **Set**,
but we will discover it behaves a lot more like **Hilb**.

While **Set** is a setting for classical physics,
and **Hilb** is a setting for quantum physics,
**Rel** is somewhere in the middle.

# Diagrams

Helps to draw diagrams, indicating how morphisms compose

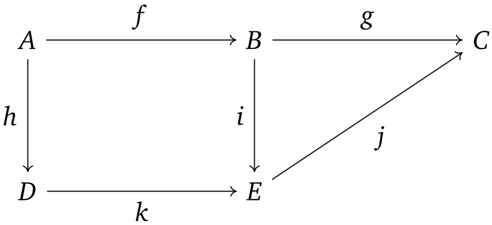



Diagram commutes if every path from object to another is equal

Two ways to speak about equality of composite morphisms:
algebraic equations, and commuting diagrams.

# Terminology

For morphism $A \xrightarrow{f} B$

- $A$ is its domain
- $B$ is its codomain
- $f$ is endomorphism if $A = B$
- $f$ is isomorphism if $f^{-1} \circ f = \mathrm{id}_A, f \circ f^{-1} = \mathrm{id}_B$ for some $B \xrightarrow{f^{-1}} A$
- $A$ and $B$ are isomorphic ($A \simeq B$) if there is isomorphism $A \rightarrow B$

# Terminology

For morphism $A \xrightarrow{f} B$

- $A$ is its domain
- $B$ is its codomain
- $f$ is endomorphism if $A = B$
- $f$ is isomorphism if $f^{-1} \circ f = \mathrm{id}_A, f \circ f^{-1} = \mathrm{id}_B$ for some $B \xrightarrow{f^{-1}} A$
- $A$ and $B$ are isomorphic ($A \simeq B$) if there is isomorphism $A \to B$

If a morphism has an inverse, it is unique:

$$g = g \circ \mathrm{id} = g \circ (f \circ g') = (g \circ f) \circ g' = \mathrm{id} \circ g' = g'$$

# Terminology

For morphism $A \xrightarrow{f} B$

- $A$ is its domain
- $B$ is its codomain
- $f$ is endomorphism if $A = B$
- $f$ is isomorphism if $f^{-1} \circ f = \mathrm{id}_A, f \circ f^{-1} = \mathrm{id}_B$ for some $B \xrightarrow{f^{-1}} A$
- $A$ and $B$ are isomorphic ($A \simeq B$) if there is isomorphism $A \to B$

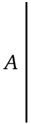
If a morphism has an inverse, it is unique:

$$g = g \circ \mathrm{id} = g \circ (f \circ g') = (g \circ f) \circ g' = \mathrm{id} \circ g' = g'$$

A groupoid is a category where every morphism is an isomorphism

# Graphical notation

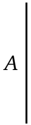
Draw object $A$ as:




It's just a line. Think of it as a picture of the identity morphism $A \xrightarrow{\mathrm{id}_A} A$. Remember: morphisms are more important than objects.

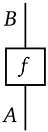
# Graphical notation

Draw object $A$ as:



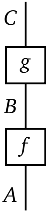

It's just a line. Think of it as a picture of the identity morphism $A \xrightarrow{\mathrm{id}_A} A$. Remember: morphisms are more important than objects.

Draw morphism $A \xrightarrow{f} B$ as:



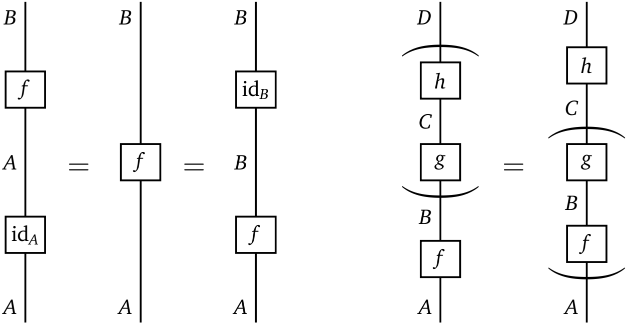
# Graphical notation

Draw composition of $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ as:



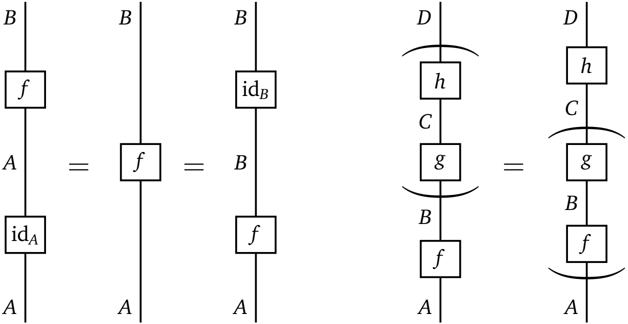
# Graphical notation

Identity law and associativity law become:



# Graphical notation

Identity law and associativity law become:




This *one-dimensional* representation is familiar; we usually draw it horizontally, and call it algebra. The graphical calculus ‘absorbs’ the axioms of a category.

# Functors

Morphisms are more important than objects: what about categories themselves? Given categories $\mathbf{C}$ and $\mathbf{D}$, a functor $F\colon \mathbf{C} \to \mathbf{D}$ is:

- for each object $A \in \mathrm{Ob}(\mathbf{C})$, an object $F(A) \in \mathrm{Ob}(\mathbf{D})$
- for each morphism $A \xrightarrow{f} B$ in $\mathbf{C}$, a morphism $F(A) \xrightarrow{F(f)} F(B)$ in $\mathbf{D}$

such that structure is preserved:

- $F(g \circ f) = F(g) \circ F(f)$ for morphisms $A \xrightarrow{f} B \xrightarrow{g} C$ in $\mathbf{C}$
- $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for objects $A$ in $\mathbf{C}$

# Functors

Morphisms are more important than objects: what about categories themselves? Given categories **C** and **D**, a functor $F\colon \mathbf{C} \to \mathbf{D}$ is:

- for each object $A \in \mathrm{Ob}(\mathbf{C})$, an object $F(A) \in \mathrm{Ob}(\mathbf{D})$
- for each morphism $A \xrightarrow{f} B$ in **C**, a morphism $F(A) \xrightarrow{F(f)} F(B)$ in **D**

such that structure is preserved:

- $F(g \circ f) = F(g) \circ F(f)$ for morphisms $A \xrightarrow{f} B \xrightarrow{g} C$ in **C**
- $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ for objects $A$ in **C**

It is:

- full when $f \mapsto F(f)$ are surjections $\mathbf{C}(A,B) \to \mathbf{D}(F(A),F(B))$
- faithful when $f \mapsto F(f)$ are injections $\mathbf{C}(A,B) \to \mathbf{D}(F(A),F(B))$
- essentially surjective on objects each $B \in \mathrm{Ob}(\mathbf{D})$ is isomorphic to $F(A)$ for some $A \in \mathrm{Ob}(\mathbf{C})$
- equivalence when full, faithful, essentially surjective on objects

# Natural transformations

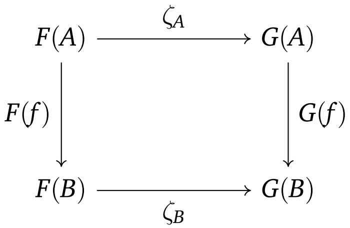
Given functors $F, G\colon \mathbf{C} \to \mathbf{D}$, a natural transformation $\zeta\colon F \Longrightarrow G$ assigns to every object $A$ in $\mathbf{C}$ of a morphism $F(A) \xrightarrow{\zeta_A} G(A)$ in $\mathbf{D}$, such that for every morphism $A \xrightarrow{f} B$ in $\mathbf{C}$:

$$\begin{array}{ccc} F(A) & \xrightarrow{\quad \zeta_A \quad} & G(A) \\ {\scriptstyle F(f)}\big\downarrow & & \big\downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\quad \zeta_B \quad]{} & G(B) \end{array}$$

If every component $\zeta_A$ is an isomorphism then $\zeta$ is called a *natural isomorphism*, and $F$ and $G$ are said to be *naturally isomorphic*.

# Natural transformations

Given functors $F, G\colon \mathbf{C} \to \mathbf{D}$, a natural transformation $\zeta\colon F \Longrightarrow G$ assigns to every object $A$ in $\mathbf{C}$ of a morphism $F(A) \xrightarrow{\zeta_A} G(A)$ in $\mathbf{D}$, such that for every morphism $A \xrightarrow{f} B$ in $\mathbf{C}$:




If every component $\zeta_A$ is an isomorphism then $\zeta$ is called a *natural isomorphism*, and $F$ and $G$ are said to be *naturally isomorphic*.

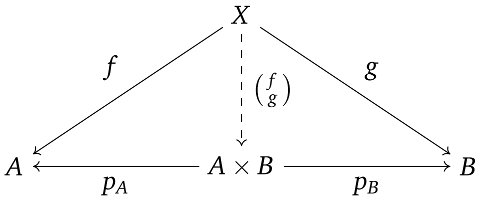
A functor $F\colon \mathbf{C} \to \mathbf{D}$ is an equivalence if and only if there is a functor $G\colon \mathbf{D} \to \mathbf{C}$ and natural isomorphisms $G \circ F \simeq \mathrm{id}_{\mathbf{C}}$ and $F \circ G \simeq \mathrm{id}_{\mathbf{D}}$.

# Products

Given objects $A$ and $B$, a product is:

- an object $A \times B$
- morphisms $A \times B \xrightarrow{p_A} A$ and $A \times B \xrightarrow{p_B} B$

such that any two morphisms $X \xrightarrow{f} A$ and $X \xrightarrow{g} B$ allow a unique morphism $\binom{f}{g} : X \to A \times B$ with $p_A \circ \binom{f}{g} = f$ and $p_B \circ \binom{f}{g} = g$

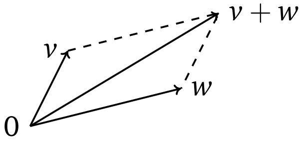



Universal property: $A \times B$ is universal way to put $A$ and $B$ together

# Vector spaces

Set $V$ with element 0, functions $+ \colon V \times V \to V$, and $\cdot \colon \mathbb{C} \times V \to V$

- *additive associativity*: $u + (v + w) = (u + v) + w$;
- *additive commutativity*: $u + v = v + u$;
- *additive unit*: $v + 0 = v$;
- *additive inverses*: there exists a $-v \in V$ such that $v + (-v) = 0$;
- *additive distributivity*: $a \cdot (u + v) = (a \cdot u) + (a \cdot v)$
- *scalar unit*: $1 \cdot v = v$;
- *scalar distributivity*: $(a + b) \cdot v = (a \cdot v) + (b \cdot v)$;
- *scalar compatibility*: $a \cdot (b \cdot v) = (ab) \cdot v$.




Example: $\mathbb{C}^n$

# Linear maps

Function $f \colon V \to W$ is linear when

$$f(v + w) = f(v) + f(w)$$
$$f(a \cdot v) = a \cdot f(v)$$

Vector spaces and linear maps form a category **Vect**

# Bases and matrices

- Vectors $\{e_i\}$ form basis when any vector $v$ takes the form $v = \sum_i v_i e_i$ for $v_i \in \mathbb{C}$ in precisely one way.

- Any vector space has a basis
  any two bases have the same cardinality: dimension

- Finite-dimensional vector spaces and linear maps
  form a category **FVect**

# Bases and matrices

- Vectors $\{e_i\}$ form basis when any vector $v$ takes the form $v = \sum_i v_i e_i$ for $v_i \in \mathbb{C}$ in precisely one way.

- Any vector space has a basis
  any two bases have the same cardinality: dimension

- Finite-dimensional vector spaces and linear maps form a category **FVect**

- Given bases $\{d_i\}$ and $\{e_j\}$, linear map $V \xrightarrow{f} W$ gives matrix $f(d_i)_j$, and vice versa

- There is a category $\mathbf{Mat}_{\mathbb{C}}$ of natural numbers and matrices
  There is an equivalence $\mathbf{Mat}_{\mathbb{C}} \to \mathbf{FVect}$ given by $n \mapsto \mathbb{C}^n$

# Hilbert spaces

Vector space $H$ with inner product $\langle - | - \rangle : H \times H \to \mathbb{C}$ such that

- *conjugate-symmetric*: $\langle v|w \rangle = \langle w|v \rangle^*$
- *linear* in second argument:
  $\langle v|a \cdot w \rangle = a \cdot \langle v|w \rangle$ and $\langle u|v + w \rangle = \langle u|v \rangle + \langle u|w \rangle$
- *positive definite*: $\langle v|v \rangle \geq 0$ with equality iff $v = 0$
- *complete* in the norm $\|v\| = \sqrt{\langle v|v \rangle}$
  (if $\sum_{i=1}^{\infty} \|v_i\| < \infty$ then $\lim_n \|v - \sum_{i=1}^{n} v_i\| = 0$ for some $v$)

# Hilbert spaces

Vector space $H$ with inner product $\langle - | - \rangle \colon H \times H \to \mathbb{C}$ such that

- *conjugate-symmetric*: $\langle v|w \rangle = \langle w|v \rangle^*$
- *linear* in second argument:
  $\langle v|a \cdot w \rangle = a \cdot \langle v|w \rangle$ and $\langle u|v + w \rangle = \langle u|v \rangle + \langle u|w \rangle$
- *positive definite*: $\langle v|v \rangle \geq 0$ with equality iff $v = 0$
- *complete* in the norm $\|v\| = \sqrt{\langle v|v \rangle}$
  (if $\sum_{i=1}^{\infty} \|v_i\| < \infty$ then $\lim_n \|v - \sum_{i=1}^{n} v_i\| = 0$ for some $v$)

Linear $f \colon H \to K$ is bounded when $\|f(v)\| \leq \|f\| \cdot \|v\|$ for some $\|f\| \in \mathbb{R}$

Hilbert spaces and bounded linear maps form category **Hilb**
Finite-dimensional Hilbert spaces form category **FHilb**

# Dual space

- Basis is orthogonal when $\langle e_i | e_j \rangle = 0$ for $i \neq j$;
  orthonormal if $\langle e_i | e_i \rangle = 1$
- Bounded $H \xrightarrow{f} K$ has adjoint $K \xrightarrow{f^\dagger} H$ with $\langle f(v) | w \rangle = \langle v | f^\dagger(w) \rangle$
  (conjugate transpose matrix)
- Given $v \in H$, its ket $\mathbb{C} \xrightarrow{|v\rangle} H$ is $z \mapsto zv$; bra $H \xrightarrow{\langle v|} \mathbb{C}$ is $w \mapsto \langle v | w \rangle$
- Dual Hilbert space $H^*$ is $\mathbf{Hilb}(H, \mathbb{C})$

# Summary

- Categories: objects and (more importantly) morphisms
- Examples: sets and functions, sets and relations, vector spaces and linear functions, Hilbert spaces and bounded linear functions
- Isomorphic objects: behave the same
- Functors: ‘morphisms between categories’
- Equivalent categories: behave the same
- Products: combine objects universally